Deloiite

Sites: https://cdn.jsdelivr.net https://academiaderiscos.deloitte.com.br

Generated on qui, 28 set 2023 05:32:05

ZAP Version: 2.13.0

Summary of Alerts

Nível de Risco	Number of Alerts
Alto	2
Médio	6
Baixo	5
Informativo	8

Alertas

Nome	Nível de Risco	Number of Instances
Metadados de nuvem potencialmente expostos	Alto	1
PII Disclosure	Alto	4
Ausência de tokens Anti-CSRF	Médio	35
Configuração Incorreta Entre Domínios	Médio	6
Content Security Policy (CSP) Header Not Set	Médio	16
Hidden File Found	Médio	1
Missing Anti-clickjacking Header	Médio	14
Vulnerable JS Library	Médio	3
Big Redirect Detected (Potential Sensitive Information Leak)	Baixo	10
Cookie with SameSite Attribute None	Baixo	1
Cookie without SameSite Attribute	Baixo	1
Divulgação de Data e Hora - Unix	Baixo	42
X-Content-Type-Options Header Missing	Baixo	107
Authentication Request Identified	Informativo	10
Divulgação de Informações - Comentários Suspeitos	Informativo	107
Modern Web Application	Informativo	10
Re-examine Cache-control Directives	Informativo	17
Retrieved from Cache	Informativo	6
Session Management Response Identified	Informativo	22
User Agent Fuzzer	Informativo	12
User Controllable HTML Element Attribute (Potential XSS)	Informativo	29

Alert Detail

Alto	Metadados de nuvem potencialmente expostos
Descrição	The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure. All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.
URL	https://academiaderiscos.deloitte.com.br/latest/meta-data/
Método	GET
Ataque	169.254.169.254
Evidence	
Other Info	Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned. The meta data returned can include information that would allow an attacker to completely compromise the system.
Instances	1
Solution	Não confie em nenhum dado do usuário nas configurações NGINX. Neste caso, é provavelmente o uso da variável $ host, que é definida no cabeçalho 'Host' e pode ser controlada por um invasor.
Reference	https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/
CWE Id	
WASC Id	
Plugin Id	90034

Alto	PII Disclosure
Descrição	The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-brands-400.eot
Método	GET
Ataque	
Evidence	67327676765651
Other Info	Credit Card Type detected: Maestro Bank Identification Number: 673276 Brand: MAESTRO Category: Emitente: VSB INTERNATIONAL B.V.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-brands-400.ttf
Método	GET
Ataque	
Evidence	67327676765651
Other Info	Credit Card Type detected: Maestro Bank Identification Number: 673276 Brand: MAESTRO Category: Emitente: VSB INTERNATIONAL B.V.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-solid-900.eot
Método	GET
Ataque	
Evidence	672656767676
Other Info	Credit Card Type detected: Maestro Bank Identification Number: 672656 Brand: MAESTRO Category: STANDARD Emitente: WUESTENROT BANK AG PFANDBRIEBANK
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-solid-900.ttf

Método	GET
Ataque	
Evidence	672656767676
Other Info	Credit Card Type detected: Maestro Bank Identification Number: 672656 Brand: MAESTRO Category: STANDARD Emitente: WUESTENROT BANK AG PFANDBRIEBANK
Instances	4
Solution	Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.
Reference	
CWE Id	359
WASC Id	13
Plugin Id	10062

Médio	**Ausência de tokens Anti-CSRF**
Descrição	Não foram localizados tokens Anti-CSRF no formulário de submissão HTML. Uma falsificação de solicitação entre sites (Cross-Site Request Forgery ou simplesmente CSRF) é um ataque que envolve forçar a vítima a enviar uma solicitação HTTP a um destino alvo sem seu conhecimento ou intenção, a fim de realizar uma ação como a vítima. A causa implícita é a funcionalidade do aplicativo usando ações previsíveis em URLs /formulários, de maneira repetível. A natureza do ataque é que o CSRF explora a confiança que um site tem em um usuário. Em contrapartida, um ataque do tipo Cross-Site Scripting (XSS) explora a confiança que um usuário tem em um site. Como o XSS, os ataques CSRF não são necessariamente entre sites, mas também podem ser. A falsificação de solicitação entre sites também é conhecida por "CSRF", "XSRF", "one-click attack", "session riding", "confused deputy", e "sea surf". Os ataques CSRF são efetivos em várias situações, incluindo: * - A vítima tem uma sessão ativa no site de destino; * - A vítima está autenticada por meio de autenticação HTTP no site de destino; * - A vítima está na mesma rede local do site de destino. O CSRF era usado principalmente para executar ações contra um site-alvo usando os privilégios da vítima, mas técnicas recentes foram descobertas para vazamento de informações obtendo acesso às respostas. O risco de vazamento/divulgação não autorizada de informações aumenta drasticamente quando o site de destino é vulnerável a XSS, porque o XSS pode ser usado como uma plataforma para CSRF, permitindo que o ataque opere dentro dos limites da política de mesma origem.
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	<form class="loginform" id="login" method="post" action="https://academiaderiscos.deloitte.com.br/login/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "login_password" "login_username" "logintoken" "rememberusername"].
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	

Evidence	<form class="ccn-mk-fullscreen-searchform" action="https://academiaderiscos.deloitte.com.br/search/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 2: "context" "searchform_button" "searchform_search"].
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	<form class="loginform" id="login" method="post" action="https://academiaderiscos.deloitte.com.br/login/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "login_password" "login_username" "logintoken" "rememberusername"].
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	<form class="ccn-mk-fullscreen-searchform" action="https://academiaderiscos.deloitte.com.br/search/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 2: "context" "searchform_button" "searchform_search"].
URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	<form action="https://academiaderiscos.deloitte.com.br/login/index.php" method="post" id="login">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "anchor" "logintoken" "password" "username"].
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	GET
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/login/forgot_password.php" method="post" accept-charset="utf-8" id="mform1_YLD26zEe1jx9jbz" class="mform">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "_qf__login_forgot_password_form" "id_email" "id_submitbuttonemail" "id_submitbuttonusername" "id_username" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	GET
Ataque	
Evidence	<form action="https://academiaderiscos.deloitte.com.br/login/index.php" method="post" id="login">
Other	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token,

Info	_csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "anchor" "logintoken" "password" "username"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	<form class="loginform" id="login" method="post" action="https://academiaderiscos.deloitte.com.br/login/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "login_password" "login_username" "logintoken" "rememberusername"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	<form class="ccn-mk-fullscreen-searchform" action="https://academiaderiscos.deloitte.com.br/search/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 2: "searchform_button" "searchform_search"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_JG2eUY3hGfevF4Y" class="mform" >
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_SaguyyvET6lbneD" class="mform">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	<form class="loginform" id="login" method="post" action="https://academiaderiscos.deloitte.com.br/login/index.php">
Other	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes

Info	formulários HTML: [Form 1: "login_password" "login_username" "logintoken" "rememberusername"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	<form class="ccn-mk-fullscreen-searchform" action="https://academiaderiscos.deloitte.com.br/search/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 2: "searchform_button" "searchform_search"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_FdBxj7FvqoW1Fe6" class="mform" >
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	<form class="loginform" id="login" method="post" action="https://academiaderiscos.deloitte.com.br/login/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "login_password" "login_username" "logintoken" "rememberusername"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	<form class="ccn-mk-fullscreen-searchform" action="https://academiaderiscos.deloitte.com.br/search/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 2: "searchform_button" "searchform_search"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_tAZogfcW8QYVZhQ" class="mform" >
	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token,

Other Info	_csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	<form class="loginform" id="login" method="post" action="https://academiaderiscos.deloitte.com.br/login/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "login_password" "login_username" "logintoken" "rememberusername"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	<form class="ccn-mk-fullscreen-searchform" action="https://academiaderiscos.deloitte.com.br/search/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 2: "searchform_button" "searchform_search"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_GCEufNFIfqpQj2G" class="mform">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_SlsJYP7LHP2m54X" class="mform" >
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_WmvYdeqj2Rt5oBq" class="mform" >

Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_bAKPA4njFsmJgqp" class="mform" >
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_y47E1ArC7RFSdCr" class="mform" >
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	<form class="loginform" id="login" method="post" action="https://academiaderiscos.deloitte.com.br/login/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "login_password" "login_username" "logintoken" "rememberusername"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	<form class="ccn-mk-fullscreen-searchform" action="https://academiaderiscos.deloitte.com.br/search/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 2: "searchform_button" "searchform_search"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.

Evidence	php" method="post" accept-charset="utf-8" id="mform1_LjA7EetYiLGkEHu" class="mform">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/login /forgot_password.php" method="post" accept-charset="utf-8" id=" mform1_Fwy57FEwmFclOzf" class="mform">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "_qf__login_forgot_password_form" "id_email" "id_submitbuttonemail" "id_submitbuttonusername" "id_username" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/login /forgot_password.php" method="post" accept-charset="utf-8" id=" mform1_k2g3qC9v0rMZsX3" class="mform">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "_qf__login_forgot_password_form" "id_email" "id_submitbuttonemail" "id_submitbuttonusername" "id_username" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	<form action="https://academiaderiscos.deloitte.com.br/login/index.php" method="post" id=" login">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "anchor" "logintoken" "password" "username"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	<form class="loginform" id="login" method="post" action="https://academiaderiscos.deloitte. com.br/login/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 1: "login_password" "login_username" "logintoken" "rememberusername"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
	<form class="ccn-mk-fullscreen-searchform" action="https://academiaderiscos.deloitte.com.

Evidence	br/search/index.php">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 2: "searchform_button" "searchform_search"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_ZBkpyMpdGMxyGeb" class="mform">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_hmeXuAYN7X9Iwi3" class="mform" >
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	<form autocomplete="off" action="https://academiaderiscos.deloitte.com.br/search/index.php" method="post" accept-charset="utf-8" id="mform1_qaYmu1pFXGUHgS1" class="mform">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] foi encontrado nos seguintes formulários HTML: [Form 3: "_qf__core_search_output_form_search" "areaids" "context" "courseids" "id_q" "id_submitbutton" "id_timeend_enabled" "id_timestart_enabled" "id_title" "mform_isexpanded_id_filtersection" "mform_isexpanded_id_search" "sesskey"].
Instances	35
	Fase: Arquitetura e Design. Use uma biblioteca verificada ou framework que não permita que essa vulnerabilidade ocorra, ou forneça construções/implementações que tornem essa vulnerabilidade mais fácil de evitar. Por exemplo, use pacotes anti-CSRF, como o OWASP CSRFGuard. Fase: Implementação. Certifique-se de que seu aplicativo esteja livre de problemas de cross-site scripting (XSS), porque a maioria das defesas CSRF pode ser contornada usando script controlado por invasor. Fase: Arquitetura e Design.

Solution	Gere um número arbitrário de uso único e exclusivo (ou Nonce = "N" de "number" - número em inglês - e "once" de "uma vez" também em inglês) para cada formulário, coloque o nonce no formulário e verifique-o ao receber o formulário. Certifique-se de que o nonce não seja previsível (CWE-330). Observe que isso pode ser contornado usando XSS. Identifique operações especialmente perigosas. Quando o usuário realizar uma operação perigosa, envie uma solicitação de confirmação separada para garantir que o usuário pretendia realizar aquela operação. Observe que isso pode ser contornado usando XSS. Utilize o controle ESAPI Session Management. Este controle inclui um componente para CSRF. Não use o método GET para qualquer solicitação que acione uma mudança de estado. Fase: Implementação. Verifique o cabeçalho HTTP Referer para ver se a solicitação foi originada de uma página esperada. Isso pode interromper funcionalidades legítimas, porque os usuários ou proxies podem ter desativado o envio do Referer por motivos de privacidade.
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Médio	**Configuração Incorreta Entre Domínios**
Descrição	O carregamento de dados do navegador da web pode ser possível, devido a uma configuração incorreta do Cross Origin Resource Sharing (CORS) no servidor web
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/config/Accessible.js?V=2.7.9
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/config/Safe.js?V=2.7.9
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/extensions/Safe.js?V=2.7.9

Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/localization/pt-br/MathMenu.js?V=2.7.9
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/localization/pt-br/pt-br.js?V=2.7.9
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
Instances	6
Solution	Certifique-se de que dados confidenciais não estejam disponíveis de maneira não autenticada (usando uma lista branca/de permissões de endereços IP, por exemplo). Configure o cabeçalho HTTP "Access-Control-Allow-Origin" para um conjunto mais restritivo de domínios ou remova todos os cabeçalhos CORS inteiramente, para permitir que o navegador web aplique a Same Origin Policy (SOP) de uma maneira mais restritiva.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14

Plugin Id	10098

Médio	Content Security Policy (CSP) Header Not Set
Descrição	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/local/edwiserreports/request_handler.php?action=is_installed_ajax
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	GET
Ataque	
Evidence	
Other Info	

URL	https://academiaderiscos.deloitte.com.br/robots.txt
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/sitemap.xml
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php

Método	POST
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	
Instances	16
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Médio	**Hidden File Found**
Descrição	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	https://academiaderiscos.deloitte.com.br/composer.lock
Método	GET
Ataque	
Evidence	HTTP/1.1 200 OK
Other Info	composer
Instances	1
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html

CWE Id	538
WASC Id	13
Plugin Id	40035

Médio	Missing Anti-clickjacking Header
Descrição	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/local/edwiserreports/request_handler.php?action=is_installed_ajax
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php

Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST

Ataque	
Evidence	
Other Info	
Instances	14
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Médio	**Vulnerable JS Library**
Descrição	A biblioteca identificadabootstrap-select, versão 1.13.2 é vulnerável.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	R.version="1.10.15";R.settings=[];R.models={};R.models.oSearch
Other Info	
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	R.version="1.10.15";R.settings=[];R.models={};R.models.oSearch
Other Info	
URL	https://academiaderiscos.deloitte.com.br/theme/javascript.php/edumy/1685542913/head
Método	GET
Ataque	
Evidence	/*! * Bootstrap-select v1.13.2
Other Info	CVE-2019-20921
Instances	3
Solution	Atualize para a versão mais recente do bootstrap-select.
Reference	https://github.com/snapappointments/bootstrap-select/issues/2199 https://github.com/snapappointments/bootstrap-select/issues/2199#issuecomment-701806876
CWE Id	829
WASC Id	
Plugin Id	10003

Baixo	**Big Redirect Detected (Potential Sensitive Information Leak)**

Descrição	The server has responded with a redirect that seems to provide a large response. This may indi that although the server sent a redirect it also responded with body content (which may include sensitive details, PII, etc.).
URL	https://academiaderiscos.deloitte.com.br/auth/oidc/
Método	GET
Ataque	
Evidence	
Other Info	Location header URI length: 340 [https://login.microsoftonline.com/deloitte.onmicrosoft.com/oau /authorize?response_type=code&client_id=408d2e62-52a7-46ed-999c-1d9952846738&scope=email&nonce=N651531af2fb71&response_mode=form_post&resource= 3A%2F%2Fgraph.microsoft.com&state=CYKQ3OwCdkTJlGr&redirect_uri=https%3A%2F% 2Facademiaderiscos.deloitte.com.br%2Fauth%2Foidc%2F]. Predicted response size: 640. Resp Body Length: 1.864.
URL	https://academiaderiscos.deloitte.com.br/auth/oidc/
Método	GET
Ataque	
Evidence	
Other Info	Location header URI length: 340 [https://login.microsoftonline.com/deloitte.onmicrosoft.com/oau /authorize?response_type=code&client_id=408d2e62-52a7-46ed-999c-1d9952846738&scope=email&nonce=N651532181c9bc&response_mode=form_post&resource 3A%2F%2Fgraph.microsoft.com&state=0CMALL7ucUTYGqF&redirect_uri=https%3A%2F% 2Facademiaderiscos.deloitte.com.br%2Fauth%2Foidc%2F]. Predicted response size: 640. Resp Body Length: 1.864.
URL	https://academiaderiscos.deloitte.com.br/auth/oidc/
Método	GET
Ataque	
Evidence	
Other Info	Location header URI length: 340 [https://login.microsoftonline.com/deloitte.onmicrosoft.com/oau /authorize?response_type=code&client_id=408d2e62-52a7-46ed-999c-1d9952846738&scope=email&nonce=N6515323d59072&response_mode=form_post&resource 3A%2F%2Fgraph.microsoft.com&state=Ltm9YmEgH74SlKD&redirect_uri=https%3A%2F% 2Facademiaderiscos.deloitte.com.br%2Fauth%2Foidc%2F]. Predicted response size: 640. Resp Body Length: 1.864.
URL	https://academiaderiscos.deloitte.com.br/auth/oidc/
Método	GET
Ataque	
Evidence	
Other Info	Location header URI length: 340 [https://login.microsoftonline.com/deloitte.onmicrosoft.com/oau /authorize?response_type=code&client_id=408d2e62-52a7-46ed-999c-1d9952846738&scope=email&nonce=N651532a08a4a6&response_mode=form_post&resource 3A%2F%2Fgraph.microsoft.com&state=L76gEM900RUXkLa&redirect_uri=https%3A%2F% 2Facademiaderiscos.deloitte.com.br%2Fauth%2Foidc%2F]. Predicted response size: 640. Resp Body Length: 1.864.
URL	https://academiaderiscos.deloitte.com.br/auth/oidc/
Método	GET
Ataque	
Evidence	
Other Info	Location header URI length: 340 [https://login.microsoftonline.com/deloitte.onmicrosoft.com/oau /authorize?response_type=code&client_id=408d2e62-52a7-46ed-999c-1d9952846738&scope=email&nonce=N6515331a39535&response_mode=form_post&resource

	3A%2F%2Fgraph.microsoft.com&state=wnRHwDyekvU9FEs&redirect_uri=https%3A%2F%2Facademiaderiscos.deloitte.com.br%2Fauth%2Foidc%2F]. Predicted response size: 640. Resp Body Length: 1.864.
URL	https://academiaderiscos.deloitte.com.br/auth/oidc/
Método	GET
Ataque	
Evidence	
Other Info	Location header URI length: 340 [https://login.microsoftonline.com/deloitte.onmicrosoft.com/oau /authorize?response_type=code&client_id=408d2e62-52a7-46ed-999c-1d9952846738&scope=email&nonce=N651533690233f&response_mode=form_post&resource= 3A%2F%2Fgraph.microsoft.com&state=oCTX9zx5bedQStA&redirect_uri=https%3A%2F%2Facademiaderiscos.deloitte.com.br%2Fauth%2Foidc%2F]. Predicted response size: 640. Resp Body Length: 1.864.
URL	https://academiaderiscos.deloitte.com.br/auth/oidc/
Método	GET
Ataque	
Evidence	
Other Info	Location header URI length: 340 [https://login.microsoftonline.com/deloitte.onmicrosoft.com/oau /authorize?response_type=code&client_id=408d2e62-52a7-46ed-999c-1d9952846738&scope=email&nonce=N6515340a15ea5&response_mode=form_post&resource 3A%2F%2Fgraph.microsoft.com&state=sD3lvef4DHHRG3x&redirect_uri=https%3A%2F%2Facademiaderiscos.deloitte.com.br%2Fauth%2Foidc%2F]. Predicted response size: 640. Resp Body Length: 1.864.
URL	https://academiaderiscos.deloitte.com.br/auth/oidc/
Método	GET
Ataque	
Evidence	
Other Info	Location header URI length: 340 [https://login.microsoftonline.com/deloitte.onmicrosoft.com/oau /authorize?response_type=code&client_id=408d2e62-52a7-46ed-999c-1d9952846738&scope=email&nonce=N651535245b801&response_mode=form_post&resource 3A%2F%2Fgraph.microsoft.com&state=SeEa6gy2J894T55&redirect_uri=https%3A%2F%2Facademiaderiscos.deloitte.com.br%2Fauth%2Foidc%2F]. Predicted response size: 640. Resp Body Length: 1.864.
URL	https://academiaderiscos.deloitte.com.br/my/
Método	GET
Ataque	
Evidence	
Other Info	Location header URI length: 56 [https://academiaderiscos.deloitte.com.br/login/index.php]. Pred response size: 356. Response Body Length: 1.552.
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	
Other Info	Location header URI length: 56 [https://academiaderiscos.deloitte.com.br/login/index.php]. Pred response size: 356. Response Body Length: 1.552.
Instances	10
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses shoul almost no content.
Reference	

CWE Id	201
WASC Id	13
Plugin Id	10044

Baixo	**Cookie with SameSite Attribute None**
Descrição	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	Set-Cookie: MoodleSession
Other Info	
Instances	1
Solution	Certifique-se de que o atributo SameSite esteja definido como 'lax' ou, de preferência, 'strict' para todos os cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Baixo	**Cookie without SameSite Attribute**
Descrição	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	Set-Cookie: MoodleSession
Other Info	
Instances	1
Solution	Certifique-se de que o atributo SameSite esteja definido como 'lax' ou, de preferência, 'strict' para todos os cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Baixo	**Divulgação de Data e Hora - Unix**
Descrição	Um carimbo de data/hora foi divulgado pela aplicação/servidor web - Unix
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	1683647284

Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	1643828125
Other Info	1643828125, que avalia: 2022-02-02 15:55:25
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	1643828125
Other Info	1643828125, que avalia: 2022-02-02 15:55:25

URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	GET
Ataque	
Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	GET
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	GET
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	GET
Ataque	
Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	GET

Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	GET
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	

Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	

Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/theme/styles.php/edumy/1685542913_1/all
Método	GET
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	1683647284
Other	

Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	1683647284
Other Info	1683647284, que avalia: 2023-05-09 12:48:04
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	1685542913
Other Info	1685542913, que avalia: 2023-05-31 11:21:53
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	1695872167
Other Info	1695872167, que avalia: 2023-09-28 00:36:07
Instances	42
Solution	Confirme manualmente se os dados do carimbo de data/hora não são confidenciais e se os dados não podem ser agregados para divulgar padrões exploráveis.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10096

Baixo	**X-Content-Type-Options Header Missing**
Descrição	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php?info=6-method-calls&cachekey=1695872167&args=%5B%7B%22index%22%3A0%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22cancel%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A1%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22closebuttontitle%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A2%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22loading%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A3%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22savechanges%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A4%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22showless%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core_form%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A5%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22showmore%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core_form%22%2C%22lang%22%3A%22pt_br%22%7D%7D%5D
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php?info=7-method-calls&cachekey=1685542913&args=%5B%7B%22index%22%3A0%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22loading%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A1%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22modal%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A2%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22modal_backdrop%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%

URL	7D%2C%7B%22index%22%3A3%2C%22methodname%22%3A% 22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B% 22component%22%3A%22core%22%2C%22template%22%3A%22modal_save_cancel% 22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22% 7D%7D%2C%7B%22index%22%3A4%2C%22methodname%22%3A% 22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B% 22component%22%3A%22core%22%2C%22template%22%3A%22modal_cancel%22% 2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D% 7D%2C%7B%22index%22%3A5%2C%22methodname%22%3A% 22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B% 22component%22%3A%22core%22%2C%22template%22%3A%22local%2Fmodal% 2Falert%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A% 22pt_br%22%7D%7D%2C%7B%22index%22%3A6%2C%22methodname%22%3A% 22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B% 22component%22%3A%22core%22%2C%22template%22%3A% 22pix_icon_fontawesome%22%2C%22themename%22%3A%22edumy%22%2C%22lang% 22%3A%22pt_br%22%7D%7D%5D
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php? info=core_get_string&cachekey=1695872167&args=%5B%7B%22index%22%3A0%2C% 22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid% 22%3A%22changesmadereallygoaway%22%2C%22stringparams%22%3A%5B%5D%2C% 22component%22%3A%22moodle%22%2C%22lang%22%3A%22pt_br%22%7D%7D%5D
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php? info=core_output_load_fontawesome_icon_system_map&cachekey=1685542913&args=% 5B%7B%22index%22%3A0%2C%22methodname%22%3A% 22core_output_load_fontawesome_icon_system_map%22%2C%22args%22%3A%7B% 22themename%22%3A%22edumy%22%7D%7D%5D
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php? info=core_output_load_template_with_dependencies&cachekey=1685542913&args=%5B% 7B%22index%22%3A0%2C%22methodname%22%3A% 22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B% 22component%22%3A%22core%22%2C%22template%22%3A% 22form_autocomplete_layout%22%2C%22themename%22%3A%22edumy%22%2C% 22lang%22%3A%22pt_br%22%7D%7D%5D
Método	GET
Ataque	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php?info=core_output_load_template_with_dependencies,core_output_load_template_with_dependencies,core_output_load_template_with_dependencies&cachekey=1685542913&args=%5B%7B%22index%22%3A0%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22form_autocomplete_input%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A1%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22form_autocomplete_suggestions%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A2%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22form_autocomplete_selection%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%5D
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/form/form.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/javascript-static.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/jquery/jquery-3.6.1.min.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/polyfills/polyfill.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/requirejs/require.min.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/local/edwiserreports/request_handler.php?action=is_installed_ajax
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/pluginfile.php/1/theme_edumy/favicon/1685542913/DEL_Favicons_IWD_circular.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/pluginfile.php/1/theme_edumy/footerlogo1/1685542913/Logo%20branca.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/pluginfile.php/1/theme_edumy/headerlogo1/1685542913/Logo%20branca.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/pluginfile.php/1/theme_edumy/headerlogo2/1683647284/Logo%20escura.png
Método	GET
Ataque	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/pluginfile.php/1/theme_edumy/headerlogo2/1685542913/Logo%20escura.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/pluginfile.php/1/theme_edumy/headerlogo_mobile/1685542913/Logo%20branca.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/pluginfile.php/1/theme_edumy/login_bg/1685542913/Vendas.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/pluginfile.php/964/block_cocoon_slider_6/slides/1/retinal-biometrics-technology-with-man-s-eye-digital-remix.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET

Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/ccn/visualize/ccn_block/jpeg/thumb/mdl.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/ccn-flaticon/CcnFlaticon.eot
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/ccn-flaticon/CcnFlaticon.svg

Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/ccn-flaticon/CcnFlaticon.ttf
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/ccn-flaticon/CcnFlaticon.woff
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/Flaticon.eot
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/Flaticon.svg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/Flaticon.ttf
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/Flaticon.woff
Método	GET

Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/Flaticon.woff2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/fontawesome-webfont.eot
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/fontawesome-webfont.eot?v=4.7.0
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/fontawesome-webfont.svg?v=4.7.0
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/fontawesome-webfont.ttf?v=4.7.0
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/fontawesome-webfont.woff2?

URL	v=4.7.0
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/fontawesome-webfont.woff?v=4.7.0
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-brands-400.eot
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-brands-400.svg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-brands-400.ttf
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-brands-400.woff
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-brands-400.woff2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-regular-400.eot
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-regular-400.svg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-regular-400.ttf
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-regular-400.woff
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-regular-400.woff2
Método	GET
Ataque	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-solid-900.eot
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-solid-900.svg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-solid-900.ttf
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-solid-900.woff
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/lineawesome/la-solid-900.woff2
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/slick.eot
Método	GET
Ataque	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/slick.svg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/slick.ttf
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/fonts/slick.woff
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/1.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/10.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/11.jpg
Método	GET
Ataque	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/12.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/2.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/2.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/3.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/3.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/4.jpg
Método	GET
Ataque	
Evidence	
Other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/5.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/6.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/7.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/8.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/9.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/background/inner-pagebg.jpg
Método	GET
Ataque	
Evidence	
Other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/ccnPattern.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/header-logo.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/home/wave2.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/home/wave3.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/home/wave4.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/home/wave5.png
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/preloader.gif
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/images/team/upload_photo.jpg
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/style/ajax-loader.gif
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/style/animated-overlay.gif
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/edumy/style/blank.gif
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/image.php/edumy/auth_oidc/1685542913/o365
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/javascript.php/edumy/1685542913/head
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/styles.php/edumy/1685542913_1/all
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/cssgrids/cssgrids-min.css&3.17.2/calendar-base/assets/skins/sam/calendar-base.css&3.17.2/calendarnavigator/assets/skins/sam/calendarnavigator.css&3.17.2/calendar/assets/skins/sam/calendar.css
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/event-mousewheel/event-mousewheel.js&3.17.2/event-resize/event-resize.js&3.17.2/event-hover/event-hover.js&3.17.2/event-touch/event-touch.js&3.17.2/event-move/event-move.js&3.17.2/event-flick/event-flick.js&3.17.2/event-valuechange/event-valuechange.js&3.17.2/event-tap/event-tap.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/intl/intl.js&3.17.2/calendar-base/lang/calendar-base_en.js&3.17.2/datatype-date-parse/datatype-date-parse.js&3.17.2/datatype-date-format/lang/datatype-date-format_en-US.js&3.17.2/datatype-date-

URL	format/datatype-date-format.js&3.17.2/datatype-date-math/datatype-date-math.js&3.17.2/calendar-base/calendar-base.js&3.17.2/plugin/plugin.js&3.17.2/calendarnavigator/calendarnavigator.js&3.17.2/calendar/calendar.js&m/1685542913/form/dateselector/dateselector-debug.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?m/1685542913/core/event/event-debug.js&m/1685542913/filter_mathjaxloader/loader/loader-debug.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?m/1685542913/form/shortforms/shortforms-debug.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.css
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	107
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informativo	**Authentication Request Identified**
Descrição	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	_qf__login_forgot_password_form
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=_qf__login_forgot_password_form referer=https://academiaderiscos.deloitte.com.br/login/forgot_password.php
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	password

Other Info	userParam=logintoken userValue=0CXH7F5Mr0ovxcz1ThCOACjxvdmE0HEA passwordParam=password referer=https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	password
Other Info	userParam=logintoken userValue=44u2lot1ASLQaIkSl93uov4fXfTQIZjm passwordParam=password referer=https://academiaderiscos.deloitte.com.br/login/index.php
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	password
Other Info	userParam=logintoken userValue=c8h34HToE8FFaOGbwQPf9nIwuAlzCs1Q passwordParam=password referer=https://academiaderiscos.deloitte.com.br/login/index.php
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	password
Other Info	userParam=logintoken userValue=Gcnl8L8gUI5Aga4mT9jRHumZeCYCyZkn passwordParam=password referer=https://academiaderiscos.deloitte.com.br/
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	password
Other Info	userParam=logintoken userValue=Gcnl8L8gUI5Aga4mT9jRHumZeCYCyZkn passwordParam=password referer=https://academiaderiscos.deloitte.com.br/login/index.php
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	password
Other Info	userParam=logintoken userValue=LoyzNYTusQYUJC8sTTxUlSoDhnaCuY3e passwordParam=password referer=https://academiaderiscos.deloitte.com.br/login/index.php
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	password
Other Info	userParam=logintoken userValue=LoyzNYTusQYUJC8sTTxUlSoDhnaCuY3e passwordParam=password referer=https://academiaderiscos.deloitte.com.br/search/index.php
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	password
	userParam=logintoken userValue=mYGBUrcZzAc9UYwXvI0kobdbd0uFxmUv

Other Info	passwordParam=password referer=https://academiaderiscos.deloitte.com.br/search/index.php
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	password
Other Info	userParam=logintoken userValue=wtrmqb6nAzor3HAEEqo1qnrnr6jCyF61 passwordParam=password referer=https://academiaderiscos.deloitte.com.br/login/
Instances	10
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informativo	**Divulgação de Informações - Comentários Suspeitos**
Descrição	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/', '', see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	bug
Other	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib

Info	/requirejs.php/1685542913/', '', see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/form/form.js
Método	GET
Ataque	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected 4 times, the first in the element starting with: "node.on('change',this.updateEventDependencies,this)}else if (nodeName=='SELECT'){node.on('change',this.updateEventDependencies,th", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/javascript-static.js
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "require(['core_form/changechecker'],function(FormChangeChecker){YUI().use('moodle-core-notification-confirm',function(Y){var con", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/javascript-static.js
Método	GET
Ataque	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "return M.util.pending_js.length};M.util.get_string=function(identifier,component,a){var stringvalue;if(M.cfg.developerdebug){if(", see evidence field for the suspicious comment /snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/javascript-static.js
Método	GET
Ataque	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 3 times, the first in the element starting with: "a.append(this.icon);var animation=new Y.Anim({node:this.div, duration:0.3,easing:Y.Easing.easeBoth,to:{height:caption.get('offset", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/javascript-static.js
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "animation.run()},this,animation)};M.util.CollapsibleRegion.prototype.userpref=null;M.util.CollapsibleRegion.prototype.div=null;M", see evidence field for the suspicious comment /snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/jquery/jquery-3.6.1.min.js
Método	GET
Ataque	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports? module.exports=e.document?t(e,!0):function(", see evidence field for the suspicious

	comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/polyfills/polyfill.js
Método	GET
Ataque	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 2 times, the first in the element starting with: "!function(t){"use strict";var r,n,e;r=[function(t,r,n){n(1),n(64),n(65),n(66),n(67),n(68),n(69),n(70),n(71),n(72),n(73),n(74),n(", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/javascript.php/1685542913/lib/polyfills/polyfill.js
Método	GET
Ataque	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "!function(){function t(t,e){e=e||{bubbles:!1,cancelable:!1,detail:void 0};var n=document.createEvent("CustomEvent");return n.ini", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 14 times, the first in the element starting with: "define("core/url",["jquery","core/config"],(function($,config){return {fileUrl:function(relativeScript,slashArg){var url=config.w", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 2 times, the first in the element starting with: "define("core/emoji/data",["exports"],(function(_exports){Object.defineProperty(_exports,"__esModule",{value:!0}),_exports.byShor", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "define("mod_assign/grading_panel",["jquery","core/yui","core/notification","core/templates","core/fragment","core/ajax","core/st", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 26 times, the first in the element starting with: "var root,definition;root=window,definition=function(){var noop=function(){},isIE="undefined"!=typeof window&&void 0!==window.nav", see evidence field for the suspicious comment/snippet.

URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 51 times, the first in the element starting with: " * mouse position to prevent the mouse from covering it. If this attribute", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 493 times, the first in the element starting with: " * @license http://www.gnu.org/copyleft/gpl.html GNU GPL v3 or later", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 33 times, the first in the element starting with: "define("core/tag",["jquery","core/ajax","core/templates","core /notification","core/str","core/modal_factory","core/modal_events"", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 66 times, the first in the element starting with: " * A module to help with toggle select/deselect all.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	todo
Other Info	The following pattern was used: \bTODO\b and was detected 4 times, the first in the element starting with: " * @todo MDL-73117 This will be deleted in Moodle 4.4.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 97 times, the first in the element starting with: " * Initializes and handles events in the user menu.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	username

Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: ""use strict";define('local_edwiserreports/completion', ["jquery","./variables",". /common","./select2"],function(e,t,a){return{in", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core/first.js
Método	GET
Ataque	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 3 times, the first in the element starting with: " * Create a list (for example `<ul>` or `<tbody>`) where each draggable element has a drag handle.", see evidence field for the suspicious comment /snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 14 times, the first in the element starting with: "define("core/url",["jquery","core/config"],(function($,config){return {fileUrl:function(relativeScript,slashArg){var url=config.w", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 2 times, the first in the element starting with: "define("core/emoji/data",["exports"],(function(_exports){Object.defineProperty (_exports,"__esModule",{value:!0}),_exports.byShor", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "define("mod_assign/grading_panel",["jquery","core/yui","core/notification","core/templates","core/fragment","core/ajax","core/st", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 26 times, the first in the element starting with: "var root,definition;root=window,definition=function(){var noop=function(){},isIE="undefined"!=typeof window&&void 0!==window.nav", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	from
Other	The following pattern was used: \bFROM\b and was detected 51 times, the first in the

Info	element starting with: " * mouse position to prevent the mouse from covering it. If this attribute", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 493 times, the first in the element starting with: " * @license http://www.gnu.org/copyleft/gpl.html GNU GPL v3 or later", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 33 times, the first in the element starting with: "define("core/tag",["jquery","core/ajax","core/templates","core /notification","core/str","core/modal_factory","core/modal_events"", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 66 times, the first in the element starting with: " * A module to help with toggle select/deselect all.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	todo
Other Info	The following pattern was used: \bTODO\b and was detected 4 times, the first in the element starting with: " * @todo MDL-73117 This will be deleted in Moodle 4.4.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 97 times, the first in the element starting with: " * Initializes and handles events in the user menu.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js
Método	GET
Ataque	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: ""use strict";define('local_edwiserreports/completion', ["jquery","./variables",". /common","./select2"],function(e,t,a){return{in", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/core_form/events.js

Método	GET
Ataque	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 3 times, the first in the element starting with: " * Create a list (for example `<ul>` or `<tbody>`) where each draggable element has a drag handle.", see evidence field for the suspicious comment /snippet.
URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib /requirejs.php/1685542913/', ", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib /requirejs.php/1685542913/', ", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	GET
Ataque	

Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/', ", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/', ", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/', ", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	bug

Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib /requirejs.php/1685542913/', ", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib /requirejs.php/1685542913/', ", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib /requirejs.php/1685542913/', ", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/javascript.php/edumy/1685542913/head
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "if($(".path-admin-report-overviewstats").length){$(".chartslist").each (function(){$(this).addClass("row");$(this).find(">li").ea", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/javascript.php/edumy/1685542913/head
Método	GET
Ataque	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "if (elem.attr('data-ccnheight')!=currentHeight){scrollMsgContainer();scrollMsg()}});if($("#quiz-time-left").length){if(!$('#quiz", see evidence field for the suspicious comment/snippet.

URL	https://academiaderiscos.deloitte.com.br/theme/javascript.php/edumy/1685542913/head
Método	GET
Ataque	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 2 times, the first in the element starting with: "!function(e,t){function n(t){e.fn.cycle.debug&&i(t)}function i(){window.console&&console.log&&console.log("[cycle] "+Array.proto", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/javascript.php/edumy/1685542913/head
Método	GET
Ataque	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 3 times, the first in the element starting with: "!function(t,e){"function"==typeof define&&define.amd?define("jquery-bridget/jquery-bridget",["jquery"],function(i){return e(t,i)", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/javascript.php/edumy/1685542913/head
Método	GET
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: " * Requires: jQuery v1.3.2 or later", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/javascript.php/edumy/1685542913/head
Método	GET
Ataque	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "!function(t,e,n,o){"use strict";function i(t,e){var o,i,a,s=[],r=0;t&&t.isDefaultPrevented()||(t.preventDefault(),e=e||{},t&&t.d", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/javascript.php/edumy/1685542913/head
Método	GET
Ataque	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 11 times, the first in the element starting with: "void 0===jQuery.migrateMute&&(jQuery.migrateMute=!0),function(e){"function"==typeof define&&define.amd?define(["jquery"],window,", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/javascript.php/edumy/1685542913/head
Método	GET
Ataque	
Evidence	todo
Other Info	The following pattern was used: \bTODO\b and was detected 5 times, the first in the element starting with: " * @todo Lazy Load Icon", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET
Ataque	

Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 7 times, the first in the element starting with: " // We allow this because of a bug in IE8/9 that throws an error", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET
Ataque	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected 9 times, the first in the element starting with: " // https://bugs.jquery.com/ticket/4833", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET
Ataque	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 54 times, the first in the element starting with: " // Return just the one element from the set", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 8 times, the first in the element starting with: " // IE8 throws error here and will not see later tests", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET
Ataque	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 3 times, the first in the element starting with: " // IE 11/Edge don't find elements on a `[name='']` query in some cases.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET
Ataque	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 19 times, the first in the element starting with: " select,", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET
Ataque	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 4 times, the first in the element starting with: " // TODO: identify versions", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET

Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 9 times, the first in the element starting with: " // Can be adjusted by the user", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET
Ataque	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 2 times, the first in the element starting with: " username: null,", see evidence field for the suspicious comment /snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/jquery.php/core/jquery-3.6.1.js
Método	GET
Ataque	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 10 times, the first in the element starting with: " // For CommonJS and CommonJS-like environments where a proper `window`", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/event-mousewheel/event-mousewheel.js&3.17.2/event-resize/event-resize.js&3.17.2/event-hover/event-hover.js&3.17.2/event-touch/event-touch.js&3.17.2/event-move/event-move.js&3.17.2/event-flick/event-flick.js&3.17.2/event-valuechange/event-valuechange.js&3.17.2/event-tap/event-tap.js
Método	GET
Ataque	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 9 times, the first in the element starting with: " // interval bumped from 40 to 100ms as of 3.4.1", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/event-mousewheel/event-mousewheel.js&3.17.2/event-resize/event-resize.js&3.17.2/event-hover/event-hover.js&3.17.2/event-touch/event-touch.js&3.17.2/event-move/event-move.js&3.17.2/event-flick/event-flick.js&3.17.2/event-valuechange/event-valuechange.js&3.17.2/event-tap/event-tap.js
Método	GET
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 3 times, the first in the element starting with: " sub._timer = Y.later(delay, Y, function () {", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/event-mousewheel/event-mousewheel.js&3.17.2/event-resize/event-resize.js&3.17.2/event-hover/event-hover.js&3.17.2/event-touch/event-touch.js&3.17.2/event-move/event-move.js&3.17.2/event-flick/event-flick.js&3.17.2/event-valuechange/event-valuechange.js&3.17.2/event-tap/event-tap.js
Método	GET
Ataque	
Evidence	select
Other	The following pattern was used: \bSELECT\b and was detected 7 times, the first in the

Info	element starting with: "`<input>`, `<textarea>`, `<select>`, or `[contenteditable="true"]` node changes", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/event-mousewheel/event-mousewheel.js&3.17.2/event-resize/event-resize.js&3.17.2/event-hover/event-hover.js&3.17.2/event-touch/event-touch.js&3.17.2/event-move/event-move.js&3.17.2/event-flick/event-flick.js&3.17.2/event-valuechange/event-valuechange.js&3.17.2/event-tap/event-tap.js
Método	GET
Ataque	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in the element starting with: " TODO: Add additional checks to get it to work for child nodes", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/event-mousewheel/event-mousewheel.js&3.17.2/event-resize/event-resize.js&3.17.2/event-hover/event-hover.js&3.17.2/event-touch/event-touch.js&3.17.2/event-move/event-move.js&3.17.2/event-flick/event-flick.js&3.17.2/event-valuechange/event-valuechange.js&3.17.2/event-tap/event-tap.js
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 6 times, the first in the element starting with: " The user can over-ride this by setting a more lenient -ms-touch-action property on a node (such as pan-x, pan-y, etc.) via C", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/event-mousewheel/event-mousewheel.js&3.17.2/event-resize/event-resize.js&3.17.2/event-hover/event-hover.js&3.17.2/event-touch/event-touch.js&3.17.2/event-move/event-move.js&3.17.2/event-flick/event-flick.js&3.17.2/event-valuechange/event-valuechange.js&3.17.2/event-tap/event-tap.js
Método	GET
Ataque	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: " * where the listener is attached. The subscriber can specify a minimum distance or velocity for", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/intl/intl.js&3.17.2/calendar-base/lang/calendar-base_en.js&3.17.2/datatype-date-parse/datatype-date-parse.js&3.17.2/datatype-date-format/lang/datatype-date-format_en-US.js&3.17.2/datatype-date-format/datatype-date-format.js&3.17.2/datatype-date-math/datatype-date-math.js&3.17.2/calendar-base/calendar-base.js&3.17.2/plugin/plugin.js&3.17.2/calendarnavigator/calendarnavigator.js&3.17.2/calendar/calendar.js&m/1685542913/form/dateselector/dateselector-debug.js
Método	GET
Ataque	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 24 times, the first in the element starting with: " * @return {Array} An `Array` of `Date`s from a given month.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/intl/intl.js&3.17.2/calendar-base/lang/calendar-base_en.js&3.17.2/datatype-date-parse/datatype-date-parse.js&3.17.2/datatype-date-format/lang/datatype-date-format_en-US.js&3.17.2/datatype-date-format/datatype-date-format.js&3.17.2/datatype-date-math/datatype-date-math.js&3.17.2

	/calendar-base/calendar-base.js&3.17.2/plugin/plugin.js&3.17.2/calendarnavigator /calendarnavigator.js&3.17.2/calendar/calendar.js&m/1685542913/form/dateselector /dateselector-debug.js
Método	GET
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 6 times, the first in the element starting with: " * Checks whether the first date comes later than the second.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/intl/intl.js&3.17.2 /calendar-base/lang/calendar-base_en.js&3.17.2/datatype-date-parse/datatype-date-parse. js&3.17.2/datatype-date-format/lang/datatype-date-format_en-US.js&3.17.2/datatype-date-format/datatype-date-format.js&3.17.2/datatype-date-math/datatype-date-math.js&3.17.2 /calendar-base/calendar-base.js&3.17.2/plugin/plugin.js&3.17.2/calendarnavigator /calendarnavigator.js&3.17.2/calendar/calendar.js&m/1685542913/form/dateselector /dateselector-debug.js
Método	GET
Ataque	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 13 times, the first in the element starting with: " * to select one or more dates, or ranges of dates. Calendar", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/intl/intl.js&3.17.2 /calendar-base/lang/calendar-base_en.js&3.17.2/datatype-date-parse/datatype-date-parse. js&3.17.2/datatype-date-format/lang/datatype-date-format_en-US.js&3.17.2/datatype-date-format/datatype-date-format.js&3.17.2/datatype-date-math/datatype-date-math.js&3.17.2 /calendar-base/calendar-base.js&3.17.2/plugin/plugin.js&3.17.2/calendarnavigator /calendarnavigator.js&3.17.2/calendar/calendar.js&m/1685542913/form/dateselector /dateselector-debug.js
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 4 times, the first in the element starting with: " * Takes a native JavaScript Date and formats it as a string for display to user.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?3.17.2/intl/intl.js&3.17.2 /calendar-base/lang/calendar-base_en.js&3.17.2/datatype-date-parse/datatype-date-parse. js&3.17.2/datatype-date-format/lang/datatype-date-format_en-US.js&3.17.2/datatype-date-format/datatype-date-format.js&3.17.2/datatype-date-math/datatype-date-math.js&3.17.2 /calendar-base/calendar-base.js&3.17.2/plugin/plugin.js&3.17.2/calendarnavigator /calendarnavigator.js&3.17.2/calendar/calendar.js&m/1685542913/form/dateselector /dateselector-debug.js
Método	GET
Ataque	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 2 times, the first in the element starting with: " * range 01 to 53, where week 1 is the first week that has at least 4 days", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?m/1685542913/core/event /event-debug.js&m/1685542913/filter_mathjaxloader/loader/loader-debug.js
Método	GET
Ataque	
Evidence	debug

Other Info	The following pattern was used: \bDEBUG\b and was detected 4 times, the first in the element starting with: " Y.log('Event fired: ' + e.type, 'debug', LOGNAME);", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?m/1685542913/core/event/event-debug.js&m/1685542913/filter_mathjaxloader/loader/loader-debug.js
Método	GET
Ataque	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: " * of global events that can be subscribed to, or fired from any plugin.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?m/1685542913/core/event/event-debug.js&m/1685542913/filter_mathjaxloader/loader/loader-debug.js
Método	GET
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 4 times, the first in the element starting with: "// (at your option) any later version.", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?m/1685542913/core/event/event-debug.js&m/1685542913/filter_mathjaxloader/loader/loader-debug.js
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: " * user text that could have equations in it. MathJax can typeset the equations", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?m/1685542913/form/shortforms/shortforms-debug.js
Método	GET
Ataque	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: " fieldset.get('id') + """, 'debug', 'moodle-form-shortforms');", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 12 times, the first in the element starting with: " // HTMLElementCollection bug).", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	bugs
Other	The following pattern was used: \bBUGS\b and was detected 2 times, the first in the

Info	element starting with: " // (https://bugs.webkit.org/show_bug.cgi?id=16020)", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 31 times, the first in the element starting with: " debug: true,", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	FIXME
Other Info	The following pattern was used: \bFIXME\b and was detected 4 times, the first in the element starting with: " // FIXME: need to support '65,esc' => keypress, keydown", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 373 times, the first in the element starting with: " so it may not reflect the correct version number when YUI is run from", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 24 times, the first in the element starting with: " core: ['get', 'features', 'intl-base', 'yui-log', 'yui-later', 'loader-base', 'loader-rollup', 'loader-yui3'],", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 40 times, the first in the element starting with: " or `.js`, with or without a following query string). If the file type can't", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 22 times, the first in the element starting with: "Note: elements that are also collections, such as `<form>` and `<select>`", see evidence field for the suspicious comment/snippet.

URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 64 times, the first in the element starting with: " //TODO I hate this entire method, it needs to be fixed ASAP (3.5.0) ^davglass", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 43 times, the first in the element starting with: " * section in the JSON user guide for caveats. The default value is true", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 3 times, the first in the element starting with: " * <dt>username</dt>", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/theme/yui_combo.php?rollup/3.17.2/yui-moodlesimple.js
Método	GET
Ataque	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 64 times, the first in the element starting with: " The main use case for this method is in "mashups" where several third-party", see evidence field for the suspicious comment/snippet.
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/config/Accessible.js?V=2.7.9
Método	GET
Ataque	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected 4 times, the first in the element starting with: "(function(d,h,l,g,m,b,j){var p="2.7.9";var i=MathJax.Extension;var c=i.MathEvents={version:p};var k=d.config.menuSettings;var o=", see evidence field for the suspicious comment/snippet.
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/config/Accessible.js?V=2.7.9
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "(function(a,e,b,f){var c=b.config.menuSettings;var d=MathJax.Extension.AssistiveMML={version:"2.7.9",config:b.CombineConfig("Ass", see evidence field for the suspicious comment/snippet.
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured

Método	GET
Ataque	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "if(document.getElementById&&document.childNodes&&document.createElement){if(!(window.MathJax&&MathJax.Hub)){if(window.MathJax){w", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/', ", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib/requirejs.php/1685542913/', ", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 3 times, the first in the element starting with: "<script> //<![CDATA[var M = {}; M.yui = {}; M.pageloadstarttime = new Date(); M.cfg = {"wwwroot":"https:\/\/academiaderiscos.de", see evidence field for the suspicious comment/snippet.
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	

Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in the element starting with: "<script> //<![CDATA[var require = { baseUrl : 'https://academiaderiscos.deloitte.com.br/lib /requirejs.php/1685542913/', '', see evidence field for the suspicious comment/snippet.
Instances	107
Solution	Remova todos os comentários que retornam informações que podem ajudar um invasor e corrigir quaisquer problemas subjacentes aos quais eles se referem.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informativo	**Modern Web Application**
Descrição	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://academiaderiscos.deloitte.com.br/index.php?redirect=0
Método	GET
Ataque	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	Nome de usuário ou senha errados. Por favor tente outra vez.
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
	

Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	Nome de usuário ou senha errados. Por favor tente outra vez.
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	10
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informativo	**Re-examine Cache-control Directives**

Descrição	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php?info=6-method-calls&cachekey=1695872167&args=%5B%7B%22index%22%3A0%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22cancel%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A1%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22closebuttontitle%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A2%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22loading%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A3%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22savechanges%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A4%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22showless%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core_form%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A5%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22showmore%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22core_form%22%2C%22lang%22%3A%22pt_br%22%7D%7D%5D
Método	GET
Ataque	
Evidence	public, max-age=7776000, immutable
Other Info	
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php?info=7-method-calls&cachekey=1685542913&args=%5B%7B%22index%22%3A0%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22loading%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A1%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22modal%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A2%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22modal_backdrop%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A3%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22modal_save_cancel%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A4%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22modal_cancel%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A5%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22local%2Fmodal%2Falert%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A6%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22pix_icon_fontawesome%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%5D
Método	GET
Ataque	

Evidence	public, max-age=7776000, immutable
Other Info	
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php?info=core_get_string&cachekey=1695872167&args=%5B%7B%22index%22%3A0%2C%22methodname%22%3A%22core_get_string%22%2C%22args%22%3A%7B%22stringid%22%3A%22changesmadereallygoaway%22%2C%22stringparams%22%3A%5B%5D%2C%22component%22%3A%22moodle%22%2C%22lang%22%3A%22pt_br%22%7D%7D%5D
Método	GET
Ataque	
Evidence	public, max-age=7776000, immutable
Other Info	
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php?info=core_output_load_fontawesome_icon_system_map&cachekey=1685542913&args=%5B%7B%22index%22%3A0%2C%22methodname%22%3A%22core_output_load_fontawesome_icon_system_map%22%2C%22args%22%3A%7B%22themename%22%3A%22edumy%22%7D%7D%5D
Método	GET
Ataque	
Evidence	public, max-age=7776000, immutable
Other Info	
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php?info=core_output_load_template_with_dependencies&cachekey=1685542913&args=%5B%7B%22index%22%3A0%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22form_autocomplete_layout%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%5D
Método	GET
Ataque	
Evidence	public, max-age=7776000, immutable
Other Info	
URL	https://academiaderiscos.deloitte.com.br/lib/ajax/service-nologin.php?info=core_output_load_template_with_dependencies.core_output_load_template_with_dependencies.core_output_load_template_with_dependencies&cachekey=1685542913&args=%5B%7B%22index%22%3A0%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22form_autocomplete_input%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A1%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22form_autocomplete_suggestions%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%2C%7B%22index%22%3A2%2C%22methodname%22%3A%22core_output_load_template_with_dependencies%22%2C%22args%22%3A%7B%22component%22%3A%22core%22%2C%22template%22%3A%22form_autocomplete_selection%22%2C%22themename%22%3A%22edumy%22%2C%22lang%22%3A%22pt_br%22%7D%7D%5D
Método	GET
Ataque	

Evidence	public, max-age=7776000, immutable
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/
Método	GET
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	GET
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	GET
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	GET
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform

Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP
Método	GET
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Other Info	
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Other Info	
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	private, pre-check=0, post-check=0, max-age=0, no-transform
Other Info	
Instances	17
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informativo	**Retrieved from Cache**
Descrição	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/config/Accessible.js?V=2.7.9
Método	GET

Ataque	
Evidence	HIT
Other Info	
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/config/Safe.js?V=2.7.9
Método	GET
Ataque	
Evidence	HIT
Other Info	
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/extensions/Safe.js?V=2.7.9
Método	GET
Ataque	
Evidence	HIT
Other Info	
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/localization/pt-br/MathMenu.js?V=2.7.9
Método	GET
Ataque	
Evidence	HIT
Other Info	
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/localization/pt-br/pt-br.js?V=2.7.9
Método	GET
Ataque	
Evidence	HIT
Other Info	
URL	https://cdn.jsdelivr.net/npm/mathjax@2.7.9/MathJax.js?delayStartupUntil=configured
Método	GET
Ataque	
Evidence	HIT
Other Info	
Instances	6
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	
WASC Id	
Plugin Id	10050

Informativo	**Session Management Response Identified**
Descrição	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	07r5sdq2jbdhdv63a7e9pgmmf1
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	509bre2v1aap0k464f30j8i90o
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	55hqkbv1ot1lpf1tk9fpcp2nbr
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	6satoe81pr2m30b598bto47dlt
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	7jen2n7nahlm0cam1nhv5u55h4
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	

Evidence	8s3v1qngoui1gahdullrp53bj7
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	9dsqqgt9ii2gqv4c8kbvgi2rl3
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	b6v2krd08h33ae2g3peoeviv9r
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	b8fs1lhgrlo8orv312hdef4vro
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	dvihr0t59s8rrqsagjdsg38tdb
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	evi34rblglsk17inr0qgp8526s
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	gc9dk4s7hvefhj6jml0e2pmslf
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	hla8mdj53pdvnhpfqb73tvbbjs
Other	

Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	i14lrhv1vemq8hsoie007dhkdr
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	japsvubkt69k8bdlvfnlo07d14
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	jhjh9b8qbrdcucisptl3158jij
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	lfmb6qnqn6qptbb3gua0hohvmg
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	tpe54ldcbtpervs495jcm4qul9
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	7jen2n7nahlm0cam1nhv5u55h4
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	9dsqqgt9ii2gqv4c8kbvgi2rl3
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/

Método	GET
Ataque	
Evidence	b6v2krd08h33ae2g3peoeviv9r
Other Info	cookie:MoodleSession
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	
Evidence	dvihr0t59s8rrqsagjdsg38tdb
Other Info	cookie:MoodleSession
Instances	22
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112

Informativo	**User Agent Fuzzer**
Descrição	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other	

Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	

Other Info	
URL	https://academiaderiscos.deloitte.com.br/
Método	GET
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	12
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Informativo	**User Controllable HTML Element Attribute (Potential XSS)**
Descrição	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP
Método	GET
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php?context=2&q=ZAP appears to include user input in: a(n) [input] tag [value] attribute The user input found was: q=ZAP The user-controlled value was: zap
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2
Método	GET
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php?q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx&context=2 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: q=CdHoiJUWppEVBptEeEjlmFdwWhnDaCOXKzzQIpIGCZyVqmcx The user-controlled value was: cdhoijuwppevbpteeejlmfdwwhndacoxkzzqipigczyvqmcx
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2
Método	GET
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php?q=CZyVqmcx&context=2 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: q=CZyVqmcx The user-controlled value was: czyvqmcx
URL	https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP

Método	GET
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php?q=ZAP appears to include user input in: a(n) [input] tag [value] attribute The user input found was: q=ZAP The user-controlled value was: zap
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/login/forgot_password.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: email=zaproxy@example.com The user-controlled value was: zaproxy@example.com
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/login/forgot_password.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: sesskey=yyJ5JOHu8B The user-controlled value was: yyj5johu8b
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/login/forgot_password.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submitbuttonemail=Buscar The user-controlled value was: buscar
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/login/forgot_password.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submitbuttonusername=Buscar The user-controlled value was: buscar
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/login/forgot_password.php appears to include user input in: a(n) [input] tag [value]

	attribute The user input found was: username=ZAP The user-controlled value was: zap
URL	https://academiaderiscos.deloitte.com.br/login/forgot_password.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/login/forgot_password.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: username=ZAP The user-controlled value was: zaproxy@example.com
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/login/index.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: password=ZAP The user-controlled value was: zap
URL	https://academiaderiscos.deloitte.com.br/login/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/login/index.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: username=ZAP The user-controlled value was: zap
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: areaids=_qf__force_multiselect_submission The user-controlled value was: _qf__force_multiselect_submission
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [option] tag [value] attribute The user input found was: areaids[]=mod_data-activity The user-controlled value was: mod_data-activity
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: courseids=_qf__force_multiselect_submission The user-controlled value was: _qf__force_multiselect_submission
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: q=ZAP The user-controlled value was: zap
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [input] tag [name] attribute The user input found was: searchwithin=course The user-controlled value was: courseids
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [option] tag [value] attribute The user input found was: searchwithin=course The user-controlled value was: course
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [select] tag [name] attribute The user input found was: searchwithin=course The user-controlled value was: courseids[]
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: sesskey=yyJ5JOHu8B The user-controlled value was: yyj5johu8b
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [input] tag [placeholder] attribute The user input found was: submitbutton=Pesquisar The user-controlled value was: pesquisar cursos ...
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submitbutton=Pesquisar The user-controlled value was: pesquisar
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [option] tag [value] attribute The user input found was: timeend[day]=28 The user-controlled value was: 28
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [option] tag [value] attribute The user input found was: timeend[minute]=56 The user-controlled value was: 56
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [option] tag [value] attribute The user input found was: timeend[year]=2023 The user-controlled value was: 2023
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [option] tag [value] attribute The user input found was: timestart[day]=28 The user-controlled value was: 28
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [option] tag [value] attribute The user input found was: timestart[minute]=56 The user-controlled value was: 56
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [option] tag [value] attribute The user input found was: timestart[year]=2023 The user-controlled value was: 2023
URL	https://academiaderiscos.deloitte.com.br/search/index.php
Método	POST
Ataque	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://academiaderiscos.deloitte.com.br/search/index.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: title=ZAP The user-controlled value was: zap
Instances	29
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute
CWE Id	20
WASC Id	20
Plugin Id	10031