WAS Scan Report

Qualys. Community Edition

Scan Report

12 Jan 2023

Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.

Luis Ricardo Martins
dcspd6lm

Docspider Software
Rua Dr. Placido Gomes de Oliveira, 610
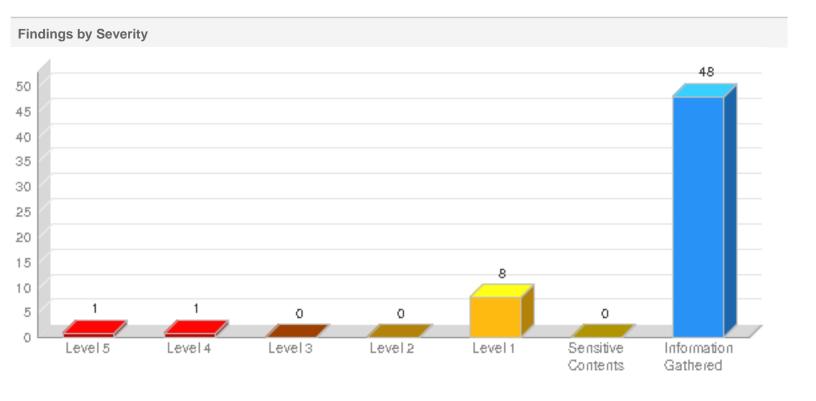Joinville, None 47
Brazil

Target and Filters

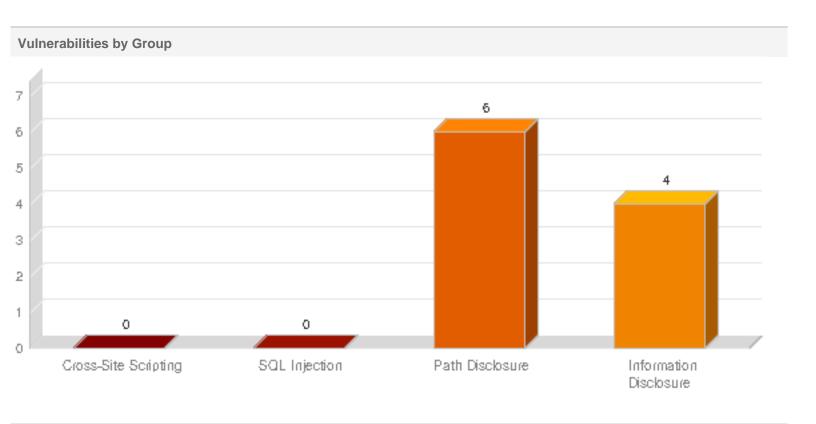|	
Scans (1)	**Web Application Vulnerability Scan - 412-49 - 2023-01-11**
Web Applications (1)	**Docspider 412-49 - PADRÃO SQL**
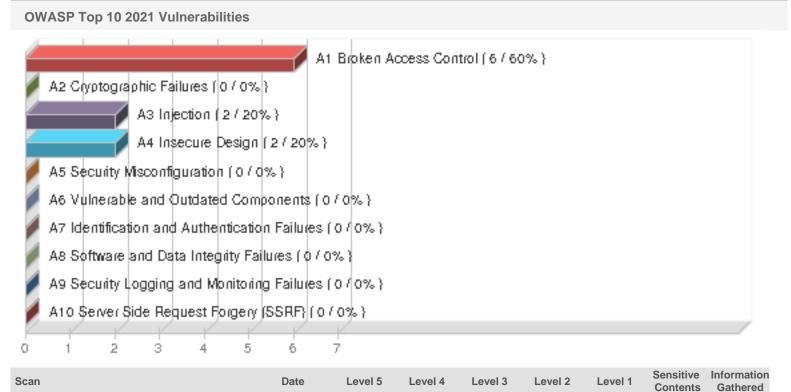
Summary

Security Risk	Vulnerabilities	Sensitive Contents	Information Gathered
HIGH	10	0	48

Findings by Severity

WAS Scan Report

Vulnerabilities by Group

OWASP Top 10 2021 Vulnerabilities

Scan	Date	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
Web Application Vulnerability Scan - 412-49 - 2023-01-11	11 Jan 2023 18:24 GMT-0400	1	1	0	0	8	0	48

Results(58)

Vulnerability (10)

Path Disclosure (6)

   ■ ☐☐☐ **150246 Path-relative stylesheet import (PRSSI) vulnerability** (6)

150246 Path-relative stylesheet import (PRSSI) vulnerability

URL: https://412-49.docspider.com.br/Busca/PalavraIrrelevante

Finding #	**891232**(69622031)	Severity	Confirmed Vulnerability - Level 1
Unique #	**1ecf12aa-6e98-41bb-a522-fcc915e0a02b**		
Group	Path Disclosure	Detection Date	11 Jan 2023 18:24 GMT-0400
CWE	CWE-23		
OWASP	A1 Broken Access Control		
WASC	-		

CVSS V3 Base	3.1	CVSS V3 Temporal	2.9	CVSS V3 Attack Vector	Network

Details

Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to path-relative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, the scan required authentication to be enabled.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://412-49.docspider.com.br/Login
https://412-49.docspider.com.br/Login/Authenticate
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

Payloads

WAS Scan Report

GET https://412-49.docspider.com.br/Busca/PalavraIrrelevante

Referer: https://412-49.docspider.com.br/
Cookie: biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf;
Host: 412-49.docspider.com.br
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Relative Path CSS Links found:
<link href="../../../NAssets/styles/docspider/docspiderPalette.css" rel="stylesheet">
<link href="../../../NAssets/styles/bootstrap/bootstrap.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/kendo.common.min.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-layout.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-grid.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-override.css" rel="stylesheet">

150246 Path-relative stylesheet import (PRSSI) vulnerability

URL: https://412-49.docspider.com.br/Busca/ConfiguracaoGeralBusca

Finding #	**891236**(69622032)
Unique #	**12ba96c7-775c-4f93-91b7-bb26d5a06638**
Group	Path Disclosure
CWE	CWE-23
OWASP	A1 Broken Access Control
WASC	-

Severity	Confirmed Vulnerability - Level 1
Detection Date	11 Jan 2023 18:24 GMT-0400

CVSS V3 Base 3.1   **CVSS V3 Temporal** 2.9   **CVSS V3 Attack Vector** Network

Details

Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to path-relative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, the scan required authentication to be enabled.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://412-49.docspider.com.br/Login
https://412-49.docspider.com.br/Login/Authenticate
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

Payloads

WAS Scan Report

#1 Request

GET https://412-49.docspider.com.br/Busca/ConfiguracaoGeralBusca

Referer: https://412-49.docspider.com.br/
Cookie: biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; _downloadToken=1673472915502,1673472915514;
ASPSESSIONIDAGQQQRDA=CEEHMCOCJAHKFCKNLAIHHGEG; ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf;
Host: 412-49.docspider.com.br
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Relative Path CSS Links found:
<link href="../../../NAssets/styles/docspider/docspiderPalette.css" rel="stylesheet">
<link href="../../../NAssets/styles/bootstrap/bootstrap.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/kendo.common.min.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-layout.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-grid.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-override.css" rel="stylesheet">

WAS Scan Report

150246 Path-relative stylesheet import (PRSSI) vulnerability

URL: https://412-49.docspider.com.br/Busca/RelevanciaOrdenacaoBusca

Finding #	**891242**(69622035)	**Severity**	Confirmed Vulnerability - Level 1
Unique #	**f73eb87e-4d73-47b2-a191-b9814f11ba94**		
Group	Path Disclosure	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-23		
OWASP	A1 Broken Access Control		
WASC	-		
CVSS V3 Base	3.1	**CVSS V3 Temporal** 2.9	**CVSS V3 Attack Vector** Network

---

Details

Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to path-relative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, the scan required authentication to be enabled.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

> https://412-49.docspider.com.br/Login
> https://412-49.docspider.com.br/Login/Authenticate
> https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
> https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

---

Payloads

WAS Scan Report

#1 Request

GET https://412-49.docspider.com.br/Busca/RelevanciaOrdenacaoBusca

Referer: https://412-49.docspider.com.br/
Cookie: biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; _downloadToken=1673472915502,1673472915514;
ASPSESSIONIDAGQQQRDA=CEEHMCOCJAHKFCKNLAIHHGEG; ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf;
Host: 412-49.docspider.com.br
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Relative Path CSS Links found:
<link href="../../../NAssets/styles/docspider/docspiderPalette.css" rel="stylesheet">
<link href="../../../NAssets/styles/bootstrap/bootstrap.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/kendo.common.min.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-layout.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-grid.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-override.css" rel="stylesheet">

WAS Scan Report

150246 Path-relative stylesheet import (PRSSI) vulnerability

URL: https://412-49.docspider.com.br/Busca/PainelExecucaoSentencaBusca

Finding #	**891246**(69622036)	**Severity**	Confirmed Vulnerability - Level 1
Unique #	**d6dad81c-d9c9-4516-bf76-8779304f11ca**		
Group	Path Disclosure	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-23		
OWASP	A1 Broken Access Control		
WASC	-		
CVSS V3 Base	3.1	**CVSS V3 Temporal** 2.9	**CVSS V3 Attack Vector** Network

Details

Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to path-relative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, the scan required authentication to be enabled.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://412-49.docspider.com.br/Login
https://412-49.docspider.com.br/Login/Authenticate
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

Payloads

WAS Scan Report

#1 Request

GET https://412-49.docspider.com.br/Busca/PainelExecucaoSentencaBusca

Referer: https://412-49.docspider.com.br/
Cookie: biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; _downloadToken=1673473251781,1673473251793;
ASPSESSIONIDAGQQQRDA=EEEHMCOCFMCMCEJMABCECDBJ; ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf;
Host: 412-49.docspider.com.br
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this [link](#) to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Relative Path CSS Links found:
<link href="../../../NAssets/styles/docspider/docspiderPalette.css" rel="stylesheet">
<link href="../../../NAssets/styles/bootstrap/bootstrap.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/kendo.common.min.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-layout.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-grid.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-override.css" rel="stylesheet">

WAS Scan Report

■ □ □ 150246 Path-relative stylesheet import (PRSSI) vulnerability

URL: https://412-49.docspider.com.br/Busca/Sinonimo

Finding #	891250(69622037)	**Severity**	Confirmed Vulnerability - Level 1
Unique #	09f23958-0605-4c71-a5d2-82db03a4dd37		
Group	Path Disclosure	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-23		
OWASP	A1 Broken Access Control		
WASC	-		

CVSS V3 Base	3.1	**CVSS V3 Temporal**	2.9	**CVSS V3 Attack Vector**	Network

Details

Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to path-relative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, the scan required authentication to be enabled.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://412-49.docspider.com.br/Login
https://412-49.docspider.com.br/Login/Authenticate
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

Payloads

WAS Scan Report

#1 Request

GET https://412-49.docspider.com.br/Busca/Sinonimo

Referer: https://412-49.docspider.com.br/
Cookie: biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; _downloadToken=1673473653172,1673473653184;
ASPSESSIONIDAGQQQRDA=MEEHMCOCBKHPBIGDCFDKDOAA; ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf;
Host: 412-49.docspider.com.br
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Relative Path CSS Links found:
<link href="../../../NAssets/styles/docspider/docspiderPalette.css" rel="stylesheet">
<link href="../../../NAssets/styles/bootstrap/bootstrap.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/kendo.common.min.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-layout.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-grid.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-override.css" rel="stylesheet">
Please check there may be more pages with relative path CSS links.

WAS Scan Report

■ ☐ ☐ 150246 Path-relative stylesheet import (PRSSI) vulnerability

URL: https://412-49.docspider.com.br/Busca/AgendamentoIndexacao

Finding #	**891254**(69622040)	**Severity**	Confirmed Vulnerability - Level 1
Unique #	**854cd054-0a72-4e6a-ae5c-87a8b1e677ee**		
Group	Path Disclosure	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-23		
OWASP	A1 Broken Access Control		
WASC	-		
CVSS V3 Base	3.1	**CVSS V3 Temporal** 2.9	**CVSS V3 Attack Vector** Network

Details

Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to path-relative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, the scan required authentication to be enabled.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://412-49.docspider.com.br/Login
https://412-49.docspider.com.br/Login/Authenticate
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

Payloads

WAS Scan Report

#1 Request

GET https://412-49.docspider.com.br/Busca/AgendamentoIndexacao

Referer: https://412-49.docspider.com.br/
Cookie: biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; _downloadToken=1673473251781,1673473251793;
ASPSESSIONIDAGQQQRDA=CEEHMCOCJAHKFCKNLAIHHGEG; ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf;
Host: 412-49.docspider.com.br
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Relative Path CSS Links found:
<link href="../../../NAssets/styles/docspider/docspiderPalette.css" rel="stylesheet">
<link href="../../../NAssets/styles/bootstrap/bootstrap.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/kendo.common.min.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-ui/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-layout.css" rel="stylesheet">
<link href="../../../NAssets/styles/docspider/docspider-grid.css" rel="stylesheet">
<link href="../../../NAssets/styles/kendo-override.css" rel="stylesheet">

Information Disclosure (4)

150060 HTTP Response Splitting (1)

WAS Scan Report

██████ 150060 HTTP Response Splitting

URL: https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx

Finding #	**1320698**(69622039)	**Severity**	Confirmed Vulnerability - Level 5
Unique #	**a2beaedd-c1ad-47ec-a0cc-e37e1cbab8d4**		
Group	Information Disclosure	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-113		
OWASP	A3 Injection		
WASC	WASC-24 HTTP REQUEST SPLITTING WASC-25 HTTP RESPONSE SPLITTING		
CVSS V3 Base	5.4	**CVSS V3 Temporal** 5.2	**CVSS V3 Attack Vector** Network

Details

Threat

HTTP Response Splitting attacks occur when the server-side application embeds user-supplied data in HTTP response headers. Examples are an application that embeds user-supplied data in the Location header of a redirection response and an application that embeds user-supplied data in a cookie value.

Impact

As a result of an HTTP Response Splitting attack, user-supplied data becomes part of the HTTP response headers, and can facilitate several attacks including HTML injection, cross-site scripting, web cache poisoning, hijacking pages with user-specific information, and browser cache poisoning.

Solution

Any data from the client side should be URL-encoded before inclusion into HTTP headers such as Location or Set-Cookie. Carriage return and line feed characters should be rejected as well.

Detection Information

Parameter	It has been detected by exploiting the parameter **_downloadToken** of the form located in URL **https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusc BrowseSugestaoBusca.aspx** The payloads section will display a list of tests that show how the param could have been exploited to collect the information
Authentication	In order to detect this vulnerability, the scan required authentication to be enabled.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

> https://412-49.docspider.com.br/Login
> https://412-49.docspider.com.br/Login/Authenticate
> https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
> https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

Payloads

WAS Scan Report

#1 Request

POST https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca. aspx
Referer: https://412-49.docspider.com.br/
Cookie: biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; _downloadToken=1673473653172,1673473653184;
ASPSESSIONIDAGQQQRDA=MEEHMCOCBKHPBIGDCFDKDOAA; ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf;
Host: 412-49.docspider.com.br
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*
Content-Length: 23936
Content-Type: application/x-www-form-urlencoded

RadScriptManager1_TSM=%3B%3BSystem.Web.Extensions%2C%20Version%3D4.0.0.0%2C%20Culture%3Dneutral%2C%20PublicKeyToken
%3D31bf3856ad364e35%3Apt-BR%3Af7ba41a4-e843-4f12-b442-8e407f37c316%3Aea597d4b%3Ab25378d2%3BTelerik.Web.UI%2C%20Version
%3D2021.3.1111.45%2C%20Culture%3Dneutral%2C%20PublicKeyToken%3D121fae78165ba3d4%3Apt-BR%3Ab406acc5-0028-4c73-8915-a9da355d848a
%3A16e4e7cd%3Aed16cbdc%3A4877f69a%3A33715776%3A86526ba7%3A874f8ea2%3Af7645509%3A24ee1bba%3Ac128760b
%3Af46195d3%3A19620875%3Acda80b3%3A383e4ce8%3A88144a7a%3A11a04f7e%3Ae330518b%3A1e771326%3A8e6f0d33%3A1f3a7489%3A6a6d718d%3Ab7778d6c
%3A6d43f6d9%3A2003d0b8%3Aaa288e2d%3A258f1c72%3Ae085fe68%3Ab2e06756%3A92fe8ea0%3Afa31b949%3A490a9d4e%3Abd8f85e4%3B%3BTelerik.Web.UI%2C
%20Version%3D2021.3.1111.45%2C%20Culture%3Dneutral%2C%20PublicKeyToken%3D121fae78165ba3d4%3Apt-BR%3Ab406acc5-0028-4c73-8915-a9da355d848a
%3A58366029&FormDecorator1_ClientState=&RadToolTipManager1_ClientState=&MainSplitter_ClientState=&_downloadToken=q%0d%0aContent-Type
%3Atext%2Fhtml%0d%0aContent-Length%3A20190%0d%0a%0d%0aHTTP%2F1.1%20200%20OK%0d%0aContent-Type%3A%20text%2Fhtml%0d%0aSet-Cookie%3A%20a
%3Dq%0d%0aContent-Length%3A%202%0d%0a%0d%0aAA&ListDialog_ClientState=&RadWindowLogs_ClientState=&TopPane1_ClientState={%22_originalWidth
%22%3A%22%22%2C%22_originalHeight%22%3A%222247px%22%2C%22_collapsedDirection%22%3A1%2C%22_scrollLeft%22%3A0%2C%22_scrollTop%22%3A0%2C
%22_expandedSize%22%3A0%2C%22width%22%3A1022%2C%22height%22%3A47%2C%22collapsed%22%3Afalse%2C%22contentUrl%22%3A%22%2C%22minWidth
%22%3A20%2C%22maxWidth%22%3A10000%2C%22minHeight%22%3A47%2C%22maxHeight%22%3A47%2C%22locked%22%3Afalse}
&RadWindowManager1_ClientState=&__LASTFOCUS=&MainPane_ClientState={%22_originalWidth%22%3A%22%22%2C%22_originalHeight%22%3A%22%22%2C
%22_collapsedDirection%22%3A1%2C%22_scrollLeft%22%3A0%2C%22_scrollTop%22%3A0%2C%22_expandedSize%22%3A0%2C%22width%22%3A1022%2C%22height
%22%3A699%2C%22collapsed%22%3Afalse%2C%22contentUrl%22%3A%22%2C%22minWidth%22%3A20%2C%22maxWidth%22%3A10000%2C%22minHeight%22%3A20%2C
%22maxHeight%22%3A10000%2C%22locked%22%3Afalse}&__EVENTTARGET=&PaneBottomCopyRight_ClientState={%22_originalWidth%22%3A%22%22%2C
%22_originalHeight%22%3A%2218px%22%2C%22_collapsedDirection%22%3A1%2C%22_scrollLeft%22%3A0%2C%22_scrollTop%22%3A0%2C%22_expandedSize
%22%3A0%2C%22width%22%3A1022%2C%22height%22%3A18%2C%22collapsed%22%3Afalse%2C%22contentUrl%22%3A%22%2C%22minWidth%22%3A20%2C
%22maxWidth%22%3A10000%2C%22minHeight%22%3A20%2C%22maxHeight%22%3A10000%2C%22locked%22%3Afalse}
&__EVENTARGUMENT=&__VIEWSTATE=jZNJQ91JR4VTlkpaMSI2lyeTrHX7s9KjxuVcB0q88NyyV9pfSouqvvYOCgftZYff2vRYWXI61GN1Icm5t4fsxGAem7zOpKKgVOBYY91IUcS
%2FcJ7XpQ5bmuTZGs%2Bzj5fom2CQrTtYV542VkAu1i8O%2BjQwJws5o%2BqLEG0IlzPY%2BrVPe1Ay5cO%2Ftx4mW%2BvcM6VVkvXhQsiMxYK%2FP7w2ZSSDc8INrAsB
%2FFNmE8e3PcXFXfm7gKlz98VFp9Dw59PgEJUF4om5aHHMWzd0Fr7xvtKOAIPmRIkPg6iu%2FggX0NE%2BdMP13Rgd5sjJ%2FWfDyMfZQvS1E3tpdD8YpEON8U
%2BYizgyuQ58nlEDmB2s9G%2BAMm7bIodLPwR9m3WmduteeFASIBe6vyAUenbsZVLu7R2hq%2FKtTFVvWoi6YUJ%2FdqxGIJ8ecghyP%2FZXSuu2pla%2Faft8ShcsKQs
%2BqEmUxuRKJ216b37NI9Vovqcjx NJqrf7%2BWtEsbdF%3B2hJ9cbOv3Ym264%2Fx6KCVzq3bQrK%2FvEd7O7RU2HEtT%2BPXTXBvbc432Iw7IDGcPTkJlNNk7GdGWLEc
%2Bpi2aC4RSzlxJ6k%2FWrsIpoDxDP3%2BhQyECWPIc0%2B2nGBuVGQEvW3QKhni7WkLSz335yycZVgMzkwPWLF3DZ%2FgxyOLyI2Dgg6sUkzoj9akHxTOVAL%2FdUuE
%2BK7GNJuX9eCU4aNeS8Y4mBjLcOaOGCUv762MhQxPNf3J4pcfsYrwdj5vHTIekqhM2HHvycMG3mWODKrIJQiqo7X8XY3L6Jm6K8KiYmiqzv9CT4qQ4Gqsz
%2FtVuFOwWZ5ztSQGzCHh8XhtwLEWE9vhnjH%2F98oYFjG7DmYbNh0nkEqF0EiWYxj7ajLAfMV
%2F9st8utIn4OpAPX3FXijs1thkImOccEkBS71bAF7AuRgjewlixjrkfKSHNQsAsPN4Fd5f6%2BapjPpi6bLGyxHUyR1MSmePWvSadlZW7Jin4HX33QbMgPKQHDa99j%2F
%2FvmkytrRsQ77StanuXbikk51wasQBMCQxmPb
%2BTb6eTj6bc9Kv1gylkh53Fz5Jf0wme4cAfRYPaeVByHgBCRMBhhHunXS13HGlDGxgtEn6HFvvUjT8lJtbSlCNbrSxJ01TPICa1RWgvSxs
%2FLQaEMx4iQfLleNvUQ2poD09v5np4vMaZj8AHiHyDJs0Bk9lSPxjDeYVbp73rX8wspVLvwennvL7YCJnKc3osmv3J9ibz60LDfgNgoUIp5eNBXjRQqcSjLOb5uqnWL
%2FKfYoASD5xMHOvCEl0IJX%2FVV%2BonUaD6EwYBrjCf4i47KwSISTVvzLZRYcddr631n5eBPsUJrl8D9CloY
%2FR4DmM2dqCyVzX1y3slQtdnzW5JMBp3XXo4S6%2FDp6UEifEmB1KQFNqgSemR6XZ93RBY0kD6K4%2BNO0%2FsSysa4Cie9KVMoyTgN0AUIbN%2F1FQJXLYHjJE2S0Yx80G
%2FvQYj6W5KOYgr02%2Fl4xM4EIux6u
%2BFQK2oxY2QlHH1Ix5DUDgiuKqK5aRjDdXp2ARXXNQPk2mZMT1WnylAj20sAI8ger9eH6lvcEAhhU9xgKSczrJolAbty0NhsEk2dwl9IXdGD57xay3lWO3ikoIZhKrgMaLPyYuK0
%2BJMsM%2BepSyJuX8YUgbin2Zgios7ZdN95Yd%2BsvzhZT10odx9UCCcod5R7Y54Vd%2FZUpqndxrI%2B0we4p6G1620D76GJ5hmvL7lhfioQ0BCifnp76Xc5Stb
%2BzK6fgaFeZLBksPt9w9WXhTLs9XGc3tgNsISIPU2NiQK8t91vllv1rLzvdPZv1WXK7NxJpYuAILmW286%2FVhBtNUSEhH%2Flhc2dx95579Osy2C6SBTL9pXDVpZef2WR
%2BhAYP2GTDDwCLi83uL2WbzpLg0btyvVLFdKz5CyDEukx0%2F6w9CisPzHZosv7RMk15l3TelVxgFlfx3zxROD9dYOBmd7vhR33dEEPxJbtBGBqysmbvWOsEOj175wRGV5fQIPAM
%2FwoNzNaI4fMMSsvfAjfq7TcRTjWCVvi126tW%2Famx3JbleNNpwL1X6hXvlJ8xWsmyhJ01GIy4Gg6E6bgoLuuEriVD1nqURtLzdfN%2BcHk1DXeOuDiKcxDCd%2FUXRlkWgeiU
%2FFT19qM6M6Q58kbts4GWGvDLS0nz%2F90G3Jfe2juYiVihibmnQcVPocp5Luo3LraD8TvSio%2BU4%2FI5LZFU77rucrUnZzsRlHjFi2WE3CrxR55Wbm
%2BsTeKVHJU1OGfuXOXR63s4j45fgUIQscFbTGZcnPAr4uT8HbaryFWD16o8vWa6nIxwCgSUuu7AZ3bSAdXz8uJaP73NHxMeWcgAy8M92NOZgZOXw
%2BpSs85lRoSirUT4CKkS3jJrOShcyLrkz6wULdMd91S3t0Ig%2FtzA%2BUxKxiRB8wo7tEMfEwOh1TszEcX7Y9nGrZL4izjx6YaNyYMWwYiXX7l2upnyXJUTtKljFl
%2F3EuUpJE1QI7ZAPxA6lUicfjSM8DDRjcREXmyS4fRFLOYjbRE96hHCHsMbZxY2%2F7Q7Citz9UEh%2BQBXC6Lh4QwFf%2Fk0nqnm9LSpJk7St
%2FTUUQgwIqnLbIDq1mKgE6Yu90P6MRgcNfIzRB07FOqn%2B15X9FGmmMHdtrPw3MaXbSdxcPiJPdayChbumOunAmLsYNA%2BI3KtoU6q03FapvL3rmbII9h1xpGiuJBxNwMGCvy
%2BBPAjUPd%2F29TS0784P9kSTmiukeryVTQP%2FO9RCVd5%2BgzI%2BDEwdZ7YhUeDJLbo8EsB%2FneQQQHOK9cYrtJURKB9qN2gnQelL2833ny4JX6w3hBG%2FgxVY%2FIL
%2B9tHHYjFNseB89Vy7L2alxLxoWoYvZoUOQU33GciTKHtAI%2Bg
%2B64GcNcM2%2BrfCBJV9odMDl2WtArFT6Iqo5uwhaR3g4fyxS8zbdyMBWPpTOpyvkGvnBZfUetk8D0YCrhwV1jHkRODDJB0F%2B2D9DLqUjGKcN5801oIWeBuXIUMn
%2FCh3fVHBIyXm5MdmhLdtbCcWqdVcaCf3PPNCMEWNdEZ8TOif53hwFdkU2uk0jSkuW8opq4U8BsYTk%2BINyRd%2FNxa4KF560kteceVEshyElFRToGHXPSOephPaIfRbnyoU7M
%2BaKavhAP75SM6dbw3x6EkV6wz%2FmppBSqsFq%2BLjMzom10mKvpqfkauS5MSqd8%2B3rHilZUN0NnOO7vz33w%2BCgS5Krgi5M2TfK%2BuKyWCX2K
%2B8i6TB7xEFWD1s2imkk47CfOEY9ienFu3Sw%2F2f67wye%2BnYLx1cTl18ZGr%2Fi7k3WiS9M81omJexn48hE2Dd65mIocBP0eU
%2BdEDOPSOWoa3aLyN9EWMAsVw6uGZ8BWwci1p7WTgUpRw3jnT2NMx10f2fVbsn5T1k7%2BHNIVJ%2BW%2FU88DD3%2FQ8cxCKTUrHzEtzv8BPb8yMUIs%2B
%2B6qf5JY5br2v0fzxebGFSvlGij8FNdsidd7XXpTOaPa%2BYGFlrQKYUIJ5IyxAnpK2Xx%2Fieo8%2FN%2BrczzMG3PwEP%2Bxd
%2FUs0xIYKyAOEl2M93Xqzw6qY9SLY7J8I0UlBeaB2eMzXEHlC6PWzcD9nbO71uLRReuKtX8ipx4m
%2B8A4EMIu3yTvgfWtNiZOWDzkaKSJa1FGvjza8TbHjSmHBi9KdA2Qk7EdY3LHS64aKu591etN%2FwIaSd9WkyarV9chsFTVXwDFxPLVXt
%2BnYBonY3Vv9algesBdcalx4d54VZLwO63QfsThSO8ZUylWGMlxof1pnRMZqKSRsCkH2erMW4geJCa%2BNR2DPfc37vezHX6xbaW2s4gCJxKBRNdJ5qew
%2FjoZ8eBqXzt11ZgB6C2cX16IdBRJRvi6LkLWMKsC0Wpp13rcVSs7IOf%2BYOpoud0LMdr95XDQJaqtKDDXRWu2U4DzO57h7Pnjgw
%2FF3q2jvWRmxnLNl1y0ll2ynaAYgWbhWCodOyMHmlUxb%2BgBZ874fsupMkNjBX8WGf2BrKgg0bXAMdnQUR3REohqFVQcM5COrCI8H4tJ4vTUm25mSQE2hW%2Bgu
%2FacXUbrpRvnM1ictSi%2Bn9n62RGto7gvddBtK8fD3xQgxcn9NSiIG9nMWexbJrPj6aP7MHDjHP2O5XNPMzH8od%2BIG87lww
%2BcUMrwbnk8I4dUZkro0KaMiYITSl4TvBYhm5nOpHhYSuOCoGTdLzzEouri5nuBXpHIvE2blRnkXj699Imaqfhm7wLU3OH0f02JSrLjKfQtTCxu
%2FrQHZdjS08RTmaUzT6wJxZJb9XFu4OPtqg1NeKQSe3GCuGm3saS5vD2U7o1xb6p%2Bd%2Bvoc2u6yGDj78DgxVo4%2BNMEi5OghxkX9GztQ00QmZSFl2yvd4Q99G
%2FsmtPLKzv2pyJ67cxoSW0GTZg19%2FixtqtZuZqN4UkRJykv35J9XKcz9SIrf5O3W%2FeNsRomHE58Y%2BIvywqwXGwvj0%2B3ouUA9WtwFBKLkT
%2BYdFMOeuzzoq7TmPmPgVs7%2F7BNpR5hoLzjHjuBUL8x8%2FJts7EAYsQnrFfuiwhiQS3BnOaJ2BtyJntBLPUfnv6lPS7a31jrXIM3GkBAlKBbDXgOX6s3cA0WHCEj5gAsu58qX
%2BtHC%2FWDpGtQm2sIzI1dVW5o8ag%2F%2FV3o2D%2FKVuOU0pPkDiYsqUNZ1NC%2BA0kVsnpij%2FNL%2BVx%2Bv4b%2BszyUDCps65A12R30UBcsGKYj
%2FOr6y5waqvlC5FlglwP9MKbzY3z15AbyGYCssvDwFVWH1oNAY%2F4%2FrrHISL%2FrdGbot%2By4ZNco2dXc7sIe8DH2xPvDadi
%2BABC6d3iFw5%2BUKsPOcvjQ4ATVHGQk8Xgff3XyOXH5wy5V6CSvmpc0oxB7ILXeVPHKzW1vRjjgekZR
%2BxgY9q74yk6a5wZRlqps8WHZGXRqXNjBHuAWIIiv7ZXRYfc2EgZmxZTi6UZ77I0VWczxRO76qizSEEx1%2BBRA8ATsVOGnAb2tzDflQMdfD8o2i4nNydKKXOE5VhZ7SP05WNUS5u
%2BoImTLlAz5%2BFbrivBh3rZMTWwA7OMqrY%2F50gKV75YDctEc56EpFDi3iClxoi%2BCRprW00Nm4x6R6Iu2VKlq%2BmAvF9DVAKjB6QQOBIRxvfYkGdSFCLGHzhw2q90Nemn
%2Bc90D9Lzn%2FpfkYAEmmREYfJGBhwsRZnYIjaBsgesGiohJLoKSqzVnqrUrOL1N5AVzdkj0L959zEWSxPwWuX%2F25ZIT2%2FBR5BG
%2FHFrWa0zEwwsnjY8QeXlFhJYjmcid46aBrzBj29QuviSkvWG%2B2BemncUGuzlFezELDvmWpz4tIJdR%2Fym%2BTm1pYKoAnPdMGtJKnYv4ZwNDKQV26NvHe
%2BEbFrv3kiC8d51VGnM9OQq6FgZ00DEvWjRmgXG8CgdP%2BXqguGwafYrTxVdHFDY4RWnkFQ6ObYqx
%2BPHVazfk6enbCO3cdLFrJnUNwLVAVIX2ch4thLRcWYQDDvvUfA77fLopSXVCNgNnGqaLnAvF4PsU4oNCJiDMPIrHdeuIqdE7W2i8YMwqK
%2F5GPPtCFqFk6eYT7Z0PSjAm5ZRHHPNxZBg3LwY1NvNkwhrneaSnU7wm1inLh13ja%2F%2FaaR
%2Fp3xhVyG43IPDNEAGaKlXRVMnERspHux0jn9ozgUsYO751Ca9LWsrpmluz6jvZznRj3vwtPovG3pW3buJmniGq7c9bKpmmAcRsAst7b5%2FFCMnwFUsk0fQ%2FJQUml

---

%2Bxdjgq1sVEHZf1%2BPSO2Yl5CNdc1%2B5S
%2Bb9AT6oaKJtzToi16IuKChZwYMOSXE2sgdsyvHzMw4gOBP795TEENvc5nbgfHuyu50DPRQbKS3FzDcJ0yIHfWPlFzvqPfJyqqFiYC1si
%2FV4w6TlM3k7ptY5TWRbvn6JLwqq8Tecc%2FTQZJ6ghI7IHGdwvG%2B2N6XMx
%2FkQGwcDAJshydqEFp4%2B9AW0B0hSdvrgOZ0Pnxg5yy1m7juyYHceqo0YJSiyDzQC4P7imjZM%2BzBnlHOWjOAi0el1Te4WeHHldgNFlvwUN7Yx4hl1G
%2B4h2cyLcalyyANjo8gQJcO4tpXPbQgYf9iVWiumyTzGLdLVG8Mg eQDUQoyE8NsPCANFbY%2Bq3%2BLMCq1X9fo9J3zd5OzJchVDG9PeT5%2Bx
%2BoMo98jJZwr64vvv1gPc9V5C00DrIaJxxt1ZrFkE%2FHxBuvZpMQBuOyyRtk3HlplESsITHPgzrKqkxJM4D7QwlPggmc1aP2aVH%2FT0%2FfXF8Jy40BJnEaG5N77h%2Bp
%2BaFAU4Z79IocGha4Ng5StwSJL4%2FFzJO4KOYGnYOhoMDh5%2BJALxw%2BcGbf%2BZo0njTsFDWb82LbZkjOXQoT%2BG8NJVH0RaKEAnpV1tNhGXcgRU2pi
%2F40ngluFArFNkptr0hw1Oevz XTFnAtuYpIRoysfRHOpDH4%2Fld X1tMxiBMBPvAKX75tY%2FXMXH78soTq6RNvSWZRd5kOn0LCCUs%2B8Yz0fRg23kGIrt
%2FsUy9SbMLI3KBBxgHWokyTmLkwPPNyQ
%2FzNxHFShfZRNJLCyHyjcVIpDqg1iW7HixsVLF73bvIMf0ojcZBLo603IakdooX2TAgRRTwfQ7IfvWkc6m85o0RuYlAsvAlytQ3knDkSZATyFjXT
%2BcHq0oqvZwkI8Kxycc9GtBV%2BpVbRJkkXbe%2B1eVI6S%2BrY%2FnpGFxrbs5%2FhTVGey5TuaeoYa5ucBAoigAsmo4hrpLEqQHgGS6mzEQCxA%2FlTdan5bcOEQnSjmYqK
%2F3xPS88npm%2BwuntvdSGEwG2IC756pH6XXjjwffJytIdGEhDbkd%2FjAOj95ci2vgsaTTkvdLEKkOJfBfzLt8zeNEW08Vpww3M6NPEGPzk%2Foxpf1OCRv1dflRLfgaOX
%2F1B6S9r3gEktSid2Yj852oUpRmwTAkPXMlLF5w%2FHEwzptf41fSeNQtPvYHvS7HY3jpELvtS99aA5HllpVcCGnK%2Bxi0leKLvvyqTZzbOUmUonYEQR2Swk
%2BX6fVAyrgt8LtAWkNY7UwpD8Pbig%2BIw5FRXiMz6Gwmb8UEYD%2BKupuKdcemI1405FCtTrR3AcsWXRiFuREqzUEKs3gOB7Bk
%2FTAcrOgyaZANhTaYfUNMbfhhIpAmH0VMxUG%2B%2BsUKMxBK7068Cdswe9jjl3Y3Tc0CgXxJGV5qt46%2Fq53GygLBF0IH9w%2FgdakxOqPv0ZOgKsJDjkv
%2FRntDwgFpw6%2F6vq%2FYN5xXsKK4bxGeDtju7Ye5SKFnVm6RMybE2NXdbuoymduUkoywcsrJwmjY5YIsKh5q6vwsK06kVOv68wUdpVBlvDr7pxCSRdQ
%2B733z17cn4lv8HT3CvZFlwxwZVc5YFWbKpSjp8xDMhv2u36DxdlM1sBW73uxnmzXRJqyA65nyptGjrDy20sB5P%2BY7oSfeVNoZ1OX7HOkKbpWD%2B0ivE
%2Ba6OOSMCi2%2BhYVd%2Ftp61vVninU6e0KrjU3IqZeunaw%2BC%2FE6N02tRX%2FR2nHKinSO4g17waPCMm3ujvI95br0tR2%2BDKE2raMwQb4KrdpDbC1lZMRwNlgh1B
%2FRjyuVSuGH2Fs5qQRouepGdhA4Szj3J%2BbwcjN1Xsssj VYhElAE7bDZmqzlqtoRZIhJ8JX1rUB4xy6TXeZkjs1Tzyw07Le%2F%2FyNFKMb4MZOz5RG0MIC0Qhw66a%2FWGqN
%2FvJpOPrqH%2FGRqqXZnL3sEt17D%2F9DBg2VtmnuJPDmoMcGymUYghvv7oWYI0ij0aEcJqdCUcZ%2BJU6ibkGtit3QQTIHY5nD7ULZEx5sqEAir%2FndYLPh4hd
%2B36cJghdBUQ4xUnwgr
%2BIkzEQOO8w5lp1Ur4nNErdQwX1kkWAWMwJmjYWkmXRrtv4MQVUxVBQ2mhKNV1lC8AZnhpRQ4s5kuufO229Xu891q3vSkPSHbr4mzDel9dxe89TVASgGdOodmngmMF
%2B57uuUKoRGE0sNksCIQf9KYbJtJfZ92qdcyiJpgVDXSejWRStlHOOUxD7o2kFCy
%2FTTtVi7K5clpTvmNe9z62Y4%2BptActlXE0hXnHCh5w4yW0YaDHfENdzmt12ZfB4veCgDHS3SxUB4H7sogeBwTbdm9uBrwuN%2BB%2F2m7PxuF1P3GipBGS9HG
%2Bz6WOmShxIiwY01ov0SIAAjg9zGqYBUP1OmUVy4fmM7yzbayfkZwrl2iqkr03bAbu8%2Fu5AjiOjeEOXaUfbIH%2F%2BpfD0GZlNQ0IqARfSzoHFvCNuRnYIg2kORWl3R
%2B4%2F1CNAOHKi7yqVYoytcPYbphgsKKKvFKFQoGU5fO%2FemRryECVCZndeJwD%2Bm5KDLKrpQinVL7fa9HTXBVNrJMwdeBxlBkp9cdaLg
%2FxqwH9DXub4PEXhJsQv8Tzo9rgwMp13CeHk54BhR5sREhDmHcJ3uBRFmEgVJ9YfWDr8TnTHQECLpaSxkCZB3ZoBttUWEqGSFjMtkSuq8EqrRwO7IE1TSb5NKcoD8SghB2IW
%2FmYvPuvutrvJWSBL0Iv4g3bM8Hj%2FxbVPaI81Ot2fV4UWSZiY5wLfqQ5DO3bopQ%2B
%2FO1ls1pAEKHdk4du23NV5rXetVojlkj6xFYloYv646dO00i5nt9zVYKAO1EMP27NQHVI642z4NjzJRcT0xE5IN8BvWTPn
%2BKsR8XsoFpPMPx3tcaN5ODQ41dgHjIIgxQ3Xz8swZzUaxZz%2BBFl1KK34ukq6lL3ofRryfMnf6hiAdfT
%2BA8z4ty7BfX14Puy203uxv95bh4oJ1L6F6kTg78IZzfxaWQeFADh%2Begv3hl1WqKHChfzBdg8XQmGr%2BMAk0Jllr6vtR%2BMQuCsk
%2BHJ7H9SCIhwFioMFfGQU1N4icqTytb8O4%2BlsOwZ7o4UJsrbS9Ms5sNCvIM3C%2FHU2hH6XkZGy63AMDUq1OeWDlrC5BIINc5ISFkVb%2BbjT2zySWfp%2FmEXDhBwUD%2F
%2Biv1UK7Ob%2F%2F%2F4xQhh8DeXYisDyFjcdJfX29w5nH1Hi57Bvr1D9LcM3dHZeEyW8Ka7aUN6bdaPTP%2FHadyj3e
%2FpbsGySsDhwWVFpTI14R7jJbvTAkTX6G1Cyv5YMq33kJb9Ng4Sd2V6wKn56tCtnwnu%2FcQYQYx92j8RnfgsP3bJck90Q53WQZ57m6uqj8afDc6ZGk
%2Fq91uFYA0OBlyYcOS1oAumn0RH9dyQ5WCyWO1Ys1ORk9WpLzlDv64kE0KPSvzd78Ez7LS81O1xOE1pecElCrATCncx5%2B14peIubfsW4iuZoCKmwyQpHEqSvXx8TEjBiwwbQoR
%2FxzllmfYDE%2BYrIUc8MEVxGUKWlEnijFTYDTRwJP7B8gx7hpeCbjuQebf%2F%2FxlN%2F%2FkUq9%2FwYIo%2BFbhQ2Qg5MBeZ7LkqwrlpMKr0VPUVN
%2FwnwYLDowuE3mPRKR4Za4cJHulNhwGtLkA8h06ny1wgDiYbCVhdP31Zb50JfaOHgmQHmmc6L6O2eVdgxg4ckYsn
%2B2tMe0nQ8Tx0%2B5EItBzrTdnYAwWN0%2FADYjQ8E1uht7KMdkcZkpWyXDfgu3QNE05Ea40Y4GxpOLWfqMV92iN8jN2yZyEtCZK0Y
%2FJoq4ITpZgjqPRMJZidQF5ZWnDxsyHrDhKVzKUY0hhaVdJXOEGnzqNr5pXwKZrCV%2BCcXbCe6Od
%2FJ8XlpnMezmaJzzuB47KevjrY9vVkMLOuYqqHwfJPeSI5Y3Vg0L5sW6hyGrB3KRg9ulHwU6yagrdsy9TgKr4M0zgDIa3nw
%2BYvHVYvjdGQhsCRhmStoQ5nGIvh085n6BVrHhFAfRo1txCtgaSDB86SCxw8k9TR6BpPpItn4mnAItDDv%2BgBnDoGjHEnBy3iT2mSa%2FAFpMTOr9Pi00w5CNoqWcnp7DzP
%2FC9TWypU799wRjtAZvhLkVOClfvxVpAjp%2Fx4dLQJHCSgeMUVDHdE6htrdBF9okud%2F2FW4izq%2FHqbABFKSk%2BQZLrECxE
%2B1KHXJQcRMH3tw714ozjBgnfE8PaozTQqpS1KmFTRuzPKkptCpLFKf9hKrCSrGNQxbqyseD4qgWzgjEeHGr6XhNC3fQJO
%2F6uG9AC6fZjcbE0mMkF69RBWPIOnXvTRODqAWiPk3hSnJ05MRRKuqZ1cXClA8f7OCalm59X2sxB23DQlBjNEGZav52qnlHTTY33DJpFroZoN96%2BGn7%2FNNPUM
%2BdbhH69b9QgqGs5ihOZSNddFgTAzOKYGj2vs86DcVMKE9U0tE5obiWdl1Q%2FpX921YTn7%2BG4YO2eExHLwfJwAka3R%2BZ4Z1RhzmHQzv
%2BSNBP0zWYYC5Q37MIMAfN2PliD8JjBGaywpBNgNevtY2cVpMsXGhtoM0kpf%2F0cf2leS9efFjIh8piLyq2WNcBVu%2BTkb9a2Zg
%2Fo0t4mv5ZuFQCzowdxPEFgjwbhqQ7BvFABKf2ifDo1CpC5o7sHhC9fPrCD1MKsY0jxQUUnQONlxR1ECvmKyGkVd9ekKsVP92wAyPmVP0vvRr1KWTHY7FIzsqpow2pIU%2B
%2Ba9LFrrXV5HdQyyotut75A9iq%2FRNcoHRldaMItPZZHDH6mF3k41jyB7iEViEVZijfc7GCXOP
%2BnZXIub3p2MVo5QY8cXpMj63dli3jisLJ9SW3kBLft2aDdWiI8VNsIwYAMtj0T7Vbw3ek7xKcQ61QHo%2Bj%2FT988%2BebZRp1unwdadxyJv9oEBcWFlbtCL7bcT%2BMm4oI
%2FtQNegcY6pg1OCd2aO%2FGfyESidfXcYYD3IyTB%2F2nLoTT%2BdLekz9PFg6abRaEMI8mj4CbL8jgVIMaDNsUF%2FTHiINR3a1N7lB%2B7Y5wjFjT%2FAoHctbXZul%2F3gk
%2FzPZPupvlltYwN4epobzdFe2%2F2vIOD8iq27R5G0eeBaVhwWwHRVgjpi0WPapXmJd8JVFwSLCHJPwlf3O9L4VpGZ2YegRLLz6RZPqq2X8G9siqFCGDu
%2F1BqcZIqnM7kcLfHedNdiRWCAl0ZkrWsE4Q7NNDz3gDwW4tagP6hSg1fyy8DffPnfvENqLxTFmoSOMkjVRIy8W9se6C%2F%2FCFbNIsXe4w
%2BwMOreBEliA5klYWitUiD3u7VHlW8S8uveK7573eqZANM7s1anwjxzeWwPn9h5RNUxbgxwf5i6Ii1czBNeQcP%2Bp
%2BElH0W1hrwj2YFv4S624%2BxgegCD8%2BNYLrJvAwrADTaCwO12QzEhSikhl2aIVcyYAuhIYjgdDCvHRqQTsDoLE0JzZ8ItCNXSqXh3WM3mwT%2FETauCrWV
%2BVSOkknlPc5tvL2tj4JceY0eLW6cgixDVelAp1NdGqzOesd5I4T%2FTFR3hn3AnsxeAJMKkJJImmSj5%2FBpG
%2BLQsDlAqgVlKuCPAUL3wEbPsD7wakstd2nQlC6JyKI6YPFuncJqgnHvafWvAejsNd8kjhALv7TN8ebK5fFixnVbqM%2Fxh98W7mn
%2FPP7%2Bk9T9ytBn2L7rogoWOz3%2Bmk1SJaYck8DCopZYY9EdX644uSOGJ7UYdsVBWMuyO2okI0u1gDZg91DPJrCLXtK%2FQILxA9Ypu45D6%2FOJ8yiMknuc1G
%2BLj9RBKkEDyT
%2FjCNVUVV7fMtMxwFEWSH6VXytJxFfL4O1wt9ew8mi5Shs0vfpu5oK51FQuLmBzPbUYixMH6M6DoKuewcnvzliPymjaZkFoG4X4Wx8UJt7qYhHDy1958jJjqsmpR2AuHOVojtQIF
%2BFAtjorLdJwd2juGvM5YB0QaKsOHcdn6rRdX4AwmXyT4BvCkixDDu3bR9LhIKdvo9XgTZrKD2z
%2FJbIV0Wyf7jD684iwVQCNd7ksnldgAbBmqPA0%2BmSOVXKiPMv55v4zS8F0R8hFttBjsNNWb
%2BJfCRaRGcXRezGcMfH43sdipXpksQjBXEoE6Uci BTaWWCoHqAnBTEqe22IIgwfPLyM8EioII9PkbJO64xTLvSFbd55jA3ICmvVjOHPJxTFaPFHrLRft2ryhH1YPMujQLjWmnAqC
%2Byz6jgNNXZa%2F4pDEUeeBbniv5xwT%2FK9bK2zbrdFJ5N9hgGMo4HVUxE7J8PIodfHXvZBBUO0PYgGF6CpSh2YlDhmYY7%2FN2%2F
%2BdtWIsilX49FEj2CaFGox9qqqronUrciT%2FBUZoW5jmPwMDw1PNkwEs%2BkYCZcVkYWggUfFY3PyB3cXcmHG2KLBZDQ%2BYxMxp
%2BlX1Zw4H58xAr2rAtZlOKuNShOW0AbyibECixO8IkDpNgh1rMWUR%2BlZKtVq9FZ3gVu0sssx95K4lhRT4kg8CEdNCR5%2FB8OIv6ekHl9t1doq8GA0t3Ff%2B8NLDa5EM
%2FnlFO4DRfatUmXVtq0Z3yiMp3pd9tK%2Bvd4ZDyNJ0PUcQcckP2PG9ZDhcKLOeaPloTAHB4QpXEhdrHqj%2Bl BvZALrF
%2BZ02Bluu6TQro4yoNNulhIu0EkrXjjvACvQLbxATmFGX6X8ldnfVsDtWFdbbKnC0UubtD%2Fu4%2FARxl09n6YNxEKvWMqkiRPf28%2F0fOfhGFz8Oo1Sg2PT7lP5oo0yqk64U
%2FKR8PgHVX91YHzu%2FGplZ
%2BymXefKVMtufOLSgahlxuOlTYF6O4WuEXcX7ZFe5nvVtOftvPMi6QqzkFKnP0UXXI9%2BWfsGjqMIIsmC4wv6VLRrIeLTW7S1g1hXlVcikdYD6b7w50JzXLV9MS5zs
%2BtWjXKygngNvWCw8Ui%2BZXu8To
%2B8X84qliNCUNv7Di1ASUXh4TdKKCB518%2FBjwZvOWdZApRYUj0qjPoTEh8fBJ87EBLay6qRVYSmbKGg6HyzasZV3nkYLTvrurq4NawLEllW2IU12eC98PkXz7HywO71Y9chIVm
%2FRpdFStkd%2Ben5U9yAzimjH%2B2%2B3B3edcspi1QPb0JIUiCnFkO%2BIIrYBUHflTmxrJhF4VigdeqsBNubiWRC9qTCH9PliH%2Fxgi6McgysaesLFDu631lg2QnfuzXmhbfE
%2BIdgATJ7SP44oEx1IntqQdN3IMf4r1neJIv3v7X01FDB36EnddENzz8bND
%2Fn786fmZ258svDbBgqi6p0nFx96fHlaeW1zrxXhZre70imlmWfTuXwevvoIWIzQsSWga1BJWJUHzfvYZ2IchVnZE51mfBMzaVFzXvWjaCpzdQmWg%3D
%3D&__VIEWSTATEGENERATOR=30572B18&__EVENTVALIDATION=W8ZGCW1sdAqs3xbkF5phjTAurUng7MNt7bvt75dPUPFJD7MYN47kJ95qCTRbZ2qrweHV9q8zYm7o6X%2FF
%2F1pZnGQYaxb8PR%2FTgLQJ56O9EvsBrfDOZdM0r1Kjquye%2F4LarfzVnZFB2amNFhLk8FNqUFytriq77esH%2Bfk2Fxjr%2BB8%2Fv4x1KPLkKOvYXxMN3nbxOaZZOQI
%2BnzCYs3IWGR9N2M9wif3PjA55CSoWPEVZOcVQ5y4wHT16H5RdqFhn7BhYPRZXFBAoBuMmgoAIBAWkkos21HuGKdscVvPvWJzQqDFQ6Ins74SPLfyPTBKsgq
%2BLdiwxlcfh4XIJxqaKnm908%2F8%2FS1SfqskrhC4eVpDEwQYw5snsG4pKJ5UGnHlEUDKXXN1yWoXGJUHGaRrCqHhEc3gyObWsioE7NGlptYJRi38HJDQ303osX0v3%2FeVg450
%2F%2FzFzKAmqHdq4Ytj%2F65NvqnSVr0SwxYiCF52dl%2BmT4VrTgnh8sXkGKKbLceKY1XhB0tpmrg32gG7NnHkBdEb%2FA2A6%2BDFuOz6U7KOtYXVUj6KTeye
%2FuByJQPhrdhl1d7IUlZrxaaCxpB44bcSqNiuLkRHUK0hckMu9LWf3lxnkG6%2Buy8rzf91%2FAN8IvdSL0TMMJRPBqIGLooYwY2C
%2Bn8QhNetuV2A69QV3XJNgIursHBAtNIgw%2Balf%2FONDxrN1vkZymi38vuCOGRH2WfAJtMzn3GlqqbQdn
%2Fb31xYHX8xD9XF7Kaq1xAClKTKeGqS99RyyJkUk1mPm2ohvR209MhL2C0prN5NkSseo1q9gDYegO%2FBIZavk0BGKvDKUQWQ1QJdG8d6AnNaNqimMLJjA
%2BajRfR98BsWaVYqpy%2FRrmzlu8awfmF4z1G%2BUj%2BktZOgt9Wr8T0kwY59NtVVOaRjcRyFkxKAwVfydgpmhJ5mLVi%2FMrQiAK%2FLL2I7yiLoeoILtcw
%2BLKn0zNNzU4IXOntdwb1qK3IuPn0MvkDN2YFMgH8GCLXlHWMN9uZ8x%2FeJzdxvo4sL4vnR9%2BPVpCpJLtiCzs31d%2FfNw%2FO%2F5z6I0Wlnkfcq0QojoTsg
%2FqPljHfa64RefSObz7Z8rauNRqwZDsZRkHmt1SOp%2BGribCnFu5VokV5Vl9ynC5wJvwPnpguI1mjYEvWbcOmSAw64pJD15swulSRRJd6I7JPQ3uBpkwogOwM
%2FIG1EQAQVYc7Je8ROcl2hzwQYk%2BMad5NYkqMRlpEOcYOja9TT1XQU5Ee%2Bbb%2FSDIRbXwo%2F7GWyD
%2BXigmBT8jMfysTDS1&RadTabStrip_ClientState={%22selectedIndexes%22%3A[%221%22]%2C%22logEntries%22%3A[]%2C%22scrollState%22%3A{}}
&RadMultiPage1_ClientState={%22selectedIndex%22%3A1%2C%22changeLog%22%3A[]}&hdnNomeUsuario=Luis
%20Martins&hdnIdUsuario=78&hdnIdSortOrder=ASC&searchTermo=discovery&hdnIdSortField=ds_termo_busca&searchTermo_ClientState={%22enabled
%22%3Atrue%2C%22emptyMessage%22%3A%22%22%2C%22validationText%22%3A%22%22%2C%22valueAsString%22%3A%22%22%2C%22lastSetTextBoxValue%22%3A

WAS Scan Report

%22%22}&gridTermos_ClientState=&clearSearch_ClientState={%22text%22%3A%22%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target
%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C
%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled
%22%3Atrue}&rbtExibirStatusTodos_ClientState={%22text%22%3A%22Todas%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target%22%3A
%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C
%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled
%22%3Atrue}&rbtExibirStatusAtivos_ClientState={%22text%22%3A%22Ativas%22%2C%22value%22%3A%22%22%2C%22checked%22%3Atrue%2C%22target%22%3A
%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C
%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled
%22%3Atrue}&sohPortaisSim_ClientState={%22text%22%3A%22Sim%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target%22%3A%22%22%2C
%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C
%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled
%22%3Atrue}&rbtExibirStatusInativos_ClientState={%22text%22%3A%22Inativas%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target
%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C
%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled
%22%3Atrue}&sohPortaisNao_ClientState={%22text%22%3A%22N%C3%A3o%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target%22%3A
%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C
%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled
%22%3Atrue}&&rcbTipoFiltroRlv_ClientState=&gridTermos%24ctl00%24ctl02%24ctl02%24ctl04=%20&sohPortaisTudo_ClientState={%22text%22%3A
%22Nenhum%22%2C%22value%22%3A%22%22%2C%22checked%22%3Atrue%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A
%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull
%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&gridTermos%24ctl00%24ctl02%24ctl02%24ctl07=%20&gridTermos
%24ctl00%24ctl02%24ctl02%24ctl06=%20&radNumRelevancia_ClientState={%22enabled%22%3Afalse%2C%22emptyMessage%22%3A%22%22%2C
%22validationText%22%3A%220%22%2C%22valueAsString%22%3A%220%22%2C%22minValue%22%3A0%2C%22maxValue%22%3A70368744177664%2C
%22lastSetTextBoxValue%22%3A%220%22}&gridTermos%24ctl00%24ctl02%24ctl02%24ctl07=%20&gridTermos
%24ctl00%24ctl02%24ctl02%24ctl08=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl09=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl10=
%20&rcbTipoFiltroRlv=Nenhum&linkConsultar_ClientState={%22text%22%3A%22Consultar%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C
%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack
%22%3Atrue%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C
%22enabled%22%3Atrue}&gridTermos%24ctl00%24ctl02%24ctl02%24ctl11=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl12=%20&gridTermos
%24ctl00%24ctl02%24ctl02%24ctl13=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl15=
%20&rcbFormaRelevancia=Todas&cleanFilters_ClientState={%22text%22%3A%22Filtros%20Padr%C3%B5es%22%2C%22value%22%3A%22%22%2C%22checked
%22%3Afalse%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C
%22autoPostBack%22%3Afalse%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary
%22%3Afalse%2C%22enabled%22%3Atrue}&gridTermos%24ctl00%24ctl02%24ctl02%24ctl16=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl18=
%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl22=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl19=%20&gridTermos
%24ctl00%24ctl02%24ctl02%24ctl23=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl25=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl20=
%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl26=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl27=%20&gridTermos
%24ctl00%24ctl02%24ctl02%24ctl28=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl29=%20&gridTermos%24ctl00%24ctl03%24ctl01%24ctl02=
%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl30=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl31=%20&gridTermos
%24ctl00%24ctl03%24ctl01%24ctl03=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl32=%20&gridTermos%24ctl00%24ctl03%24ctl01%24ctl08=
%20&gridTermos%24ctl00%24ctl03%24ctl01%24ctl09=
%20&gridTermos_ctl00_ctl02_ctl00_toolTipHelpGridTermos_ClientState=&gridTermos_ctl00_ctl03_ctl01_PageSizeComboBox_ClientState=&gridTermo
%24ctl00%24ctl03%24ctl01%24PageSizeComboBox=10&linkConsultar=Consultar

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

HTTP/1.1 200 OK
Content-Type: text/html
Set-Cookie: a=q
Content-Length: 2

AA; path=/; secure; HttpOnly
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length:

* The reflected string on the response webpage indicates that the vulnerability test was successful

150192 HTTP Response Header Injection (1)

WAS Scan Report

150192 HTTP Response Header Injection

URL: https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx

Finding #	**1320696**(69622038)	Severity	Confirmed Vulnerability - Level 4
Unique #	**a5b2fb7b-3367-4fe2-9fb7-e7195f27ceef**		
Group	Information Disclosure	Detection Date	11 Jan 2023 18:24 GMT-0400
CWE	CWE-113		
OWASP	A3 Injection		
WASC	WASC-25 HTTP RESPONSE SPLITTING		
CVSS V3 Base	6.5	CVSS V3 Temporal 6.2	CVSS V3 Attack Vector Network

Details

Threat

HTTP Response Header Injection attacks occur when the server-side application embeds user-supplied data in HTTP response headers without sanitizing. Examples are an application that embeds user-supplied data in the Location header of a redirection response and an application that embeds user-supplied data in a cookie value.

Impact

As a result of an HTTP Response Header Injection attack, user-supplied data becomes part of the HTTP response headers, and can facilitate several attacks including session fixation (by inserting cookies), cookie manipulation (by inserting cookies), HTTP security header bypass (by inserting malicious HTTP response headers like X-Frame-Options, Content Security Policy (CSP) headers). In most cases, HTTP Response Header Injection could lead to HTTP Response Splitting (QID 150060) which can facilitate attacks like HTML injection, cross-site scripting, web cache poisoning, hijacking pages with user-specific information, and browser cache poisoning. HTTP Response Splitting is a special case of HTTP Response Header Injection.

 NOTE: HTTP Response Header Injection could commonly lead to HTTP Response Splitting if CRLF CRLF sequence could be injected in to the response headers. While various web application platforms, programming languages and libraries provide built-in mechanism for protecting against such attacks, in specific cases and combination of server-side technology and browser such protections are found to be inadequate e.g. https://bugs.php.net/bug.php?id=68978. Internet Explorer accepts %0A%20 or %0D%0A%20 as separator in HTTP while other browser treat the new line beginning with space as the continuation of the previous header. Thus the HTTP Header Injection protection provided by PHP header() function might work as expected on other browsers, its inadequate on Internet Explorer browsers.

Solution

Any data from the client side should be URL-encoded before inclusion into HTTP headers such as Location or Set-Cookie. Carriage return and line feed characters should be rejected as well.

Detection Information

Parameter	It has been detected by exploiting the parameter **_downloadToken** of the form located in URL **https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusc BrowseSugestaoBusca.aspx**
	The payloads section will display a list of tests that show how the param could have been exploited to collect the information
Authentication	In order to detect this vulnerability, the scan required authentication to be enabled.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

> https://412-49.docspider.com.br/Login
> https://412-49.docspider.com.br/Login/Authenticate
> https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
> https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

Payloads

WAS Scan Report

POST https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca. aspx

Referer: https://412-49.docspider.com.br/
Cookie: biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; _downloadToken=1673473653172,1673473653184;
ASPSESSIONIDAGQQQRDA=MEEHMCOCBKHPBIGDCFDKDOAA; ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf;
Host: 412-49.docspider.com.br
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*
Content-Length: 23786
Content-Type: application/x-www-form-urlencoded

RadScriptManager1_TSM=%3B%3BSystem.Web.Extensions%2C%20Version%3D4.0.0.0%2C%20Culture%3Dneutral%2C%20PublicKeyToken
%3D31bf3856ad364e35%3Apt-BR%3Af7ba41a4-e843-4f12-b442-8e407f37c316%3Aea597d4b%3Ab25378d2%3BTelerik.Web.UI%2C%20Version
%3D2021.3.1111.45%2C%20Culture%3Dneutral%2C%20PublicKeyToken%3D121fae78165ba3d4%3Apt-BR%3Ab406acc5-0028-4c73-8915-a9da355d848a
%3A16e4e7cd%3Aed16cbdc%3A4877f69a%3A33715776%3A86526ba7%3A874f8ea2%3Af7645509%3A24ee1bba%3Ac128760b
%3Af46195d3%3A19620875%3Acda80b3%3A383e4ce8%3A88144a7a%3A11a04f7e%3Ae330518b%3A1e771326%3A8e6f0d33%3A1f3a7489%3A6a6d718d%3Ab7778d6c
%3A6d43f6d9%3A2003d0b8%3Aaa288e2d%3A258f1c72%3Ae085fe68%3Ab2e06756%3A92fe8ea0%3Afa31b949%3A490a9d4e%3Abd8f85e4%3B%3BTelerik.Web.UI%2C
%20Version%3D2021.3.1111.45%2C%20Culture%3Dneutral%2C%20PublicKeyToken%3D121fae78165ba3d4%3Apt-BR%3Ab406acc5-0028-4c73-8915-a9da355d848a
%3A58366029&FormDecorator1_ClientState=&RadToolTipManager1_ClientState=&MainSplitter_ClientState=&_downloadToken=q%0d
%0aQualys_resp_hdr_injection%3A%20Vulnerable&ListDialog_ClientState=&RadWindowLogs_ClientState=&TopPane1_ClientState={%22_originalWidth
%22%3A%22%22%2C%22_originalHeight%22%3A%2247px%22%2C%22_collapsedDirection%22%3A1%2C%22_scrollLeft%22%3A0%2C%22_scrollTop%22%3A0%2C
%22_expandedSize%22%3A0%2C%22width%22%3A1022%2C%22height%22%3A47%2C%22collapsed%22%3Afalse%2C%22contentUrl%22%3A%22%22%2C%22minWidth
%22%3A20%2C%22maxWidth%22%3A10000%2C%22minHeight%22%3A20%2C%22maxHeight%22%3A47%2C%22locked%22%3Afalse}
&RadWindowManager1_ClientState=&__LASTFOCUS=&MainPane_ClientState={%22_originalWidth%22%3A%22%22%2C%22_originalHeight%22%3A%22%22%2C
%22_collapsedDirection%22%3A1%2C%22_scrollLeft%22%3A0%2C%22_scrollTop%22%3A0%2C%22_expandedSize%22%3A0%2C%22width%22%3A1022%2C%22height
%22%3A699%2C%22collapsed%22%3Afalse%2C%22contentUrl%22%3A%22%22%2C%22minWidth%22%3A20%2C%22maxWidth%22%3A10000%2C%22minHeight%22%3A20%2C
%22maxHeight%22%3A10000%2C%22locked%22%3Afalse}&__EVENTTARGET=&PaneBottomCopyRight_ClientState={%22_originalWidth%22%3A%22%22%2C
%22_originalHeight%22%3A%2218px%22%2C%22_collapsedDirection%22%3A1%2C%22_scrollLeft%22%3A0%2C%22_scrollTop%22%3A0%2C%22_expandedSize
%22%3A0%2C%22width%22%3A1022%2C%22height%22%3A18%2C%22collapsed%22%3Afalse%2C%22contentUrl%22%3A%22%22%2C%22minWidth%22%3A20%2C
%22maxWidth%22%3A10000%2C%22locked%22%3Afalse}
&__EVENTARGUMENT=&__VIEWSTATE=jZNJQ91JR4VTlkpaMSI2lyeTrHX7s9KjxuVcB0q88NyyV9pfSouqvvYOCgftZYff2vRYWXI61GN1Icm5t4fsxGAem7zOpKKgVOBYY91IUcS
%2FcJ7XpQ5bmuTZGs%2BzjSfom2CQrTtYV542VkAu1i8O%2BjQwJws5o%2BqLEG0IlzPY%2BrVPe1Ay5cO%2Ftx4mW%2BvcM6VVkvXhQsiMxYK%2FP7w2ZSSDc8INrAsB
%2FFNmE8e3PcXFXfm7gKlz98VFp9Dw59PgEJUF4om5aHHMWzd0Fr7xvtKOAIPmRIkPg6iu%2FggX0NE%2BdMP13Rgd5sjJ%2FWfDyMfZQvS1E3tpdD8YpEON8U
%2BYizgyuQ58nlEDmB2s9G%2BAMm7bIodLPwR9m3WmduteeFASIBe6vyAUenbsZVLu7R2hq%2FKtTFVvWoi6YUJ%2FdqzGIJ8ecghyP%2FZXSuu2pla%2Faft8ShcsKQs
%2BqEmUxuRKJ216b37NI9Vovqcjx NJqrf7%2BWtEsbdF%2B9cbOv3Ym264%2Fx6KCVzq3bQrK%2FvEd7O7RU2HEtT%2BPXTXBvbc432Iw7IDGcPTkJlNNk7GdGWLEc
%2Bpi2aC4RSz1xJ6k%2FWrsIpoDxDP3%2BhQyECWPIc0%2B2nGBuVGQEvW3QKhni7WkLSz335yycZVgMzkwPWLF3DZ%2FgxyOLyI2Dgg6sUkzoj9akHxTOVAL%2FdUuE
%2BK7GNJuX9eCU4aNeS8Y4mBjLcOaOGCUv762MhQxPNf3J4pcfsYrwdj5vHTIekqhM2HHvycMG3mWODKrIJQiqo7X8XY3L6Jm6K8KiYmiqzv9CT4qQ4Gqsz
%2FtVuFOwWZ5ztSQGzCHh8XhtwLEWE9vhnjH%2F98oYFjG7DmYbNh0nkEqF0EiWYxj7ajLAfMV
%2F9st8utIn4OpAPX3FXijs1thkImOccEkBS71bAF7AuRgjewlixjrkfKSHNQsAsPN4Fd5f6%2BapjPpi6bLGyxHUyR1MSmePWvSadlZW7Jin4HX33QbMgPKQHDa99j%2F
%2FvmkytrRsQ77StanuXbikk51wasQBMCQxmPb
%2BTb6eTj6bc9Kv1gylkh53Fz5Jf0wme4cAfRYPaeVByHgBCRMBhhHunXS13HGlDGxgtEn6HFvvUjT8lJtbSlCNbrSxJ01TPICa1RWgvSxs
%2FLQaEMx4iQfL1eNvUQ2poD09v5np4vMaZj8AHiHyDJs0Bk9lSPxjDeYVbp73rX8wspVLvwennvL7YCJnKc3osmv3J9ibz60LDfgNgoUIp5eNBXjRQqcSjLOb5uqnWL
%2FKfYoASD5xMHOvCEl0IJX%2FVV%2BonUaD6EwYBrjCf4i47KwSISTVvzLZRYcddr631n5eBPsUJrl8D9CloY
%2FR4DmM2dqCyVzX1y3slQtdnzW5JMBp3XXo4S6%2FDp6UEifEmB1KQFNqgSemR6XZ93RBY0kD6K4%2BNO0%2FsSysa4Cie9KVMoyTgN0AUIbN%2F1FQJXLYHjJE2S0Yx80G
%2FvQYj6W5KOYgr02%2Fl4xM4EIux6u
%2BFQK2oxY2Q1HH1Ix5DUDgiuKqK5aRjDdXp2ARXXNQPk2mZMT1WnylAj20sAI8ger9eH6lvcEAhhU9xgKSczrJolAbty0NhsEk2dwl9IXdGD57xay3lWO3ikoIZhKrgMaLPyYuKO
%2BJMsM%2BepSyJuX8YUgbin2Zgios7ZdN95Yd%2BsvzhZT10odx9UCCcod5R7Y54Vd%2FZUpqndxrI%2B0we4p6G1620D76GJ5hmvL7lhfioQ0BCifnp76Xc5Stb
%2BzK6fgaFeZLBksPt9w9WXhTLs9XGc3tgNsISIPU2NiQK8t91vllv1rLzvdPZv1WXK7NxJpYuAILmW286%2FVhBtNUSEhH%2Flhc2dx95579Osy2C6SBTL9pXDVpZef2WR
%2BhAYP2GTDDwCLi83uL2WbzpLg0btyvVLFdKz5CyDEukx0%2F6w9CisPzHZosv7RMk15l3TelVxgFlfx3zxROD9dYOBmd7vhR33dEEPxJbtBGBqysmbvWOsEOjl75wRGV5fQIPAM
%2FwoNzNaI4fMMSsvfAjfq7TcRTjWCVvi126tW%2Famx3JbleNNpwL1X6hXvlJ8xWsmyhJ0lGIy4Gg6E6bgoLuuEriVD1nqURtLzdfN%2BcHk1DXeOuDiKcxDCd%2FUXRlkWgeiU
%2FFT19qM6M6Q58kbts4GWGvDLS0nz%2F90G3Jfe2juYiVihibmnQcVPocp5Luo3LraD8TvSio%2BU4%2FI5LZFU77rucrUnZzsRlHjFi2WE3CrxR55Wbm
%2BsTeKVHJU1OGfuXOXR63s4j45fgUIQscFbTGZcnPAr4uT8HbaryFWD16o8vWa6nIxwCgSUuu7AZ3bSAdXz8uJaP73NHxMeWcgAy8M92NOZgZOXw
%2BpSs851RoSirUT4CKkS3jJrOShcyLrkz6wULdMd91S3t0Ig%2FtzA%2BUxKxiRB8wo7tEMfEwOhlTszEcX7Y9nGrZL4izjx6YaNyYMWwYiXX7l2upnyXJUTtKljFl
%2F3EuUpJE1QI7ZAPxA6lUicfjSM8DDRjcREXmyS4fRFLOYjbRE96hHCHsMbZxY2%2F7Q7Citz9UEh%2BQBXC6Lh4QwFf%2Fk0nqnm9LSpJk7St
%2FTUUQgwIqnLbIDq1mKgE6Yu90P6MRgcNfIzRB07FOqn%2B15X9FGmmMHdtrPw3MaXbSdxcPiJPdayChbumOunAmLsYNA%2BI3KtoU6q03FapvL3rmbII9h1xpGiuJBxNwMGCvy
%2BPAjUPd%2F2P3S0784P9SkTmiukeryVTQP%2FO9RCVd5%2BgzI%2BDEwdZ7YhUeDJLbo8EsB%2FneQQQHOK9cYrtJURKB9qN2gnQelL2833ny4JX6w3hBG%2FgxVY%2FIL
%2F9tHHYjFNseB89Vy7L2alxLxoWoYvZoUOQU33GciTKHtAI%2Bg
%2B64GcNcM2%2BrfCBJV9odMDl2WtArFT6Iqo5uwhaR3g4fyxS8zbdyMBWPpTOpyvkGvnBZfUetk8D0YCrhwVljHkRODDJB0F%2B9DLqUjGKcN5801oIWeBuXIUMn
%2FCh3fVHBIyXm5MdmhLdtbCcWqdVcaCf3PPNCMEWNdEZ8TOif53hwFdkU2uk0jSkuW8opq4U8BsYTk%2BINyRd%2FNxa4KF560kteceVEshyElFRToGHXPSOephPaIfRbnyoU7M
%2BaKavhAP75SM6dbw3x6EkV6wz%2FmppBSqsFq%2BLjMzoml0mKvpqfkauS5MSqd8%2B3rHilZUN0NnOO7vz33w%2BCgS5Krgi5M2TfK%2BuKyWCX2K
%2B8i6TB7xEFWD1s2imkk47CfOEY9ienFu3Sw%2F2f67wye%2BnYLx1cTl18ZGr%2Fi7k3WiS9M81omJexn48hE2Dd65mIocBP0eU
%2BdEDOPSOWoa3aLyN9EWMAsVw6uGZ8BWwci1p7WTgUpRw3jnT2NMx10f2fVbsn5T1k7%2BHNIVJ%2BW%2FU88DD3%2FQ8cxCKTUrHzEtzv8BPb8yMUIs%2B
%2B6qf5JY5br2v0fzxebGFSv lGIj8FNdsidd7XXpTOaPa%2BYGFlrQKYUIJ5IyxAnpK2Xx%2Fieo8%2FN%2BrczzMG3PwEP%2Bxd
%2FUs0xIYKyAOEl2M93Xqzw6qY9SLY7J8I0UlBeaB2eMzXEHlC6PWzcD9nbO71uLRReuKtX8ipx4m
%2B8A4EMIu3yTvgfWtNiZOWDzkaKSJa1FGvjza8TbHjSmHBi9KdA2Qk7d6JXS%2Bmkje3Zi3FoJ3LHS64aKu591etN%2FwIaSd9WkyarV9chsFTVXwDFxPLVXt
%2BnYBonY3Vv9algesBdcalx4d54VZLwO63QfsThSO8ZGVlWGMlxof1npnRMZqKSRsCkH2erMW4gaJCa%2BNR2DPfc37vezHX6xbaW2s4gCJxKBRNdJ5qew
%2Fjo2 eBqXzt1lZgB6C2cXl6IdBRJRvi6LkLWMKsC0Wpp13rcVSs7IOf%2BYOpoud0LMdr95XDQJaqtKDDXRWu2U4DzO57h7Pnjgw
%2FF3q2jvWRmxnLN1ly0ll2ynaAYgWbhWCodOyMHmlUxb%2BgBZ874fsupMkNjBX8WGf2BrKgg0bXAMdnQUR3REohqFVQcM5COrCI8H4tJ4vTUm25mSQE2hW%2Bgu
%2FacXUbrpRvnM1ictSi%2Bn9n62RGto7gvddBtK8fD3xQgxcn9NSiIG9nMWexbJrPj6aP7MSDjHP2O5XNPMzH8od%2BIG87lww
%2BcUMrwbnk8I4dUZkro0KaMiYITS14TvBYhm5nOpHhYSuOCoGTdLzzEouri5nuBXpHIvE2blRnkXj699Imaqfhm7wLU3OH0f02JSrLjKfQtTCxu
%2FrQHZdjS08RTmaUzT6wJxZJb9XFu4OPtqg1NeKQSe3GCuGm3saS5vD2U7o1xb6p%2Bd%2Bvoc2u6yGDj78DgxVo4%2BNMEi5OghxkX9GztQ00QmZSFl2yvd4Q99G
%2FsmtPLKzv2pyJ67cxoSW0GTZg19%2FixtqtZuZqN4UkRJykv35J9XKcz9SIrf5O3W%2FeNsRomHE58Y%2BIvywqwXGwvj0%2B3ouUA9WtwFBKLkT
%2BYdFMOeuzzoq7TmPmPgVs7%2F7BNpR5hoLzjHjuBUL8x8%2FJts7EAYsQnrFfuiwhiQS3BnOaJ2BtyJntBLPUfnv6lPS7a31jrXIM3GkBAlKBbDXgOX6s3cA0WHCEj5gAsu58qX
%2BtHC%2FWDpGtQm2sIzI1dVW5o8ag%2F2FV3o2D%2FKVuOU0pPkDiYsqUNZ1NC%2BA0kVsnpij%2FNL%2BVx%2Bv4b%2BszyUDCps65A12R30UBcsGKYj
%2FOr6y5waqvlC5FlglwP9MKbzY3z15AbyGYCssvDwFVWH1oNAY%2F4%2FrrHISL%2FrdGbot%2By4ZNco2dXc7sIe8DH2xPvDadi
%2BABC6d3iFw5%2BUKsPOcvjQ4ATVHGQk8Xgff3XyOXH5wy5V6CSvmpc0oxB7ILXeVPHKzW1vRjjgekZR
%2BxgY9q74yk6a5wZR1qps8WHZGXRqXNjBHuAWIIiv7ZXRYfc2EgZmxZTi6UZ77I0VWczxRO76qizSEExl%2BRA8ATsVOGnAb2tzDfLQMdfD8o2i4nNydKKXOE5VhZ7SP05WNUS5u
%2BoImTLlAz5%2BFbrivBh3rZMTWwA7OMqrY%2BF50gKV75YDctEc56EpFDi3iClxoi%2BCRprW00Nm4x6R6Iu2VKlq%2BmAvF9DVAKjB6QQOBIRxvfYkGdSFCLGHzhw2q90Nemn
%2Bc9OD9Lzn%2FpfkYAEmmREYfJGBhwsRZnYIjaBsgesGiohJLoKSqzVnqrUrOL1N5AVzdkj0L959zEWSxPwWuX%2F5ZIT2%2FBR5BG
%2FFHFrWa0zEwwsnjY8QeXlFhJYjmcid46aBrzBj29QuviSkvWG%2B2BemncUGuzlFezELDvmWpz4tIJdR%2Fym%2BTm1pYKoAnPdMGtJKnYv4ZwNDKQV26NvHe
%2BEbFrv3kiC8d51VGnM9OQq6FgZ0ODEvWjRmgXG8CgdP%2BXqguGwafYrTxVdHFDY4RWnkFQ6ObYqx
%2BPHVazfk6enbCO3cdLFrJnUNwLVAVIX2ch4thLRcWYQDDvvUfA77fLopSXVCNgNnGqaLnAvF4PsU4oNCJiDMPIrHdeuIqdE7W2i8YMwqK
%2F5GPPtCFqFk6eYT7Z0PSjAm5ZRHHPNxZBg3LwY1NvNkwhrneaSnU7wmlinLh13ja%2F%2FaaR
%2Fp3xhVyG43IPDNEAGaKlXRVMnERspHux0jn9ozgUsYO751Ca9LWsrpmluz6jvZznRj3vwtPovG3pW3buJmniGq7c9bKpmmAcRsAst7b5%2FFCMnwFUsk0fQ%2FJQUml
%2Bxdjgq1sVEHZf1%2BPSO2Yl5CNdc1%2B5S

WAS Scan Report

%2Bb9AT6oaKJtzToi16IuKChZwYMOSXE2sgdsyvHzMw4gOBP795TEENvc5nbgfHuyu50DPRQbKS3FzDcJ0yIHfWPlFzvqPfJyqqFiYC1si
%2FV4w6TlM3k7ptY5TWRbvn6JLwqq8Tecc%2FTQZJ6ghI7IHGdwvG%2B2N6XMx
%2FkQGwcDAJshydqEFp4%2B9AW0B0hSdvrgOZ0Pnxg5yy1m7juyYHceqo0YJSiyDzQC4P7imjZM%2BzBnlHOWjOAi0el1Te4WeHHldgNFlvwUN7Yx4hl1G
%2B4h2cyLcalyyANjo8gQJcO4tpXPbQgYf9iVWiumyTzGLdLXGV8MegQDUQoyE8NsPCANFbY%2Bq3%2BLMCq1X9fo9J3zd5OzJchVDG9PeT5%2Bx
%2BoMo98jJZwr64vvv1gPc9V5C00DrIaJxxtlZrFkE%2FHxBuvZpMQBuOyyRtk3HlplESsITHPgzrKqkxJM4D7QwlPggmc1aP2aVH%2FT0%2FfXF8Jy40BJnEaG5N77h%2Bp
%2BaFAU4Z79IocGha4Ng5StwSJL4%2FFzJO4KOYGnYOhoMDh5%2BJALxw%2BcGbf%2BZo0njTsFDWb82LbZkjOXQoT%2BG8NJVH0RaKEAnpV1tNhGXcgRU2pi
%2F40ngluFArFNkptr0hwlOevzXTFnAtuYpIRoysfRHOpDH4%2F1dX1tMxiBMBPvAKX75tY%2FXMXH78soTq6RNvSWZRd5kOn0LCCUs%2B8Yz0fRg23kGIrt
%2FsUy9SbMLI3KBBxgHWokyTmLkwPPNyQ
%2FzNxHFShfZRNJLCyHyjcVIpDqg1iW7HixsVLF73bvIMf0ojcZBLo603IakdooX2TAgRRTwfQ7IfvWkc6m85o0RuYlAsvAlytQ3knDkSZATyFjXT
%2BcHq0oqvZwkI8Kxycc9GtBV%2BpVbRJkkXbe%2B1eVI6S%2BrY%2FnpGFxrbs5%2FhTVGey5TuaeoYa5ucBAoigAsmo4hrpLEqQHgGS6mzEQCxA%2FlTdan5bcOEQnSjmYqK
%2F3xPS88npm%2BwuntvdSGEwG2IC756pH6XXjjwffJytIdGEhDbkd%2FjAOj95ci2vgsaTTkvdLEKkOJfBfzLt8zeNEW08Vpww3M6NPEGPzk%2Foxpf1OCRv1dflRLfgaOX
%2F1B6S9r3gEktSid2Yj852oUpRmwTAkPXMlLF5w%2FHEwzptf41fSeNQtPvYHvS7HY3jpELvtS99aA5H11pVcCGnK%2Bxi01eKLvvyqTZzbOUmUonYEQR2Swk
%2BX6fVAyrgt8LtAWkNY7UwpD8Pbig%2BIw5FRXiMz6Gwmb8UEYD%2BKupuKdcemI1405FCtTrR3AcsWXRiFuREqzUEKs3gOB7Bk
%2FTAcrOgyaZANhTaYfUNMbfhhIpAmH0VMxUG%2B%2BsUKMxBK7068Cdswe9jjl3Y3Tc0CgXxJGV5qt46%2Fq53GygLBF0IH9w%2FgdakxOqPv0ZOgKsJDjkv
%2FRntDwgFpw6%2F6vq%2FYN5xXsKK4bxGeDtju7Ye5SKFnVm6RMybE2NXdbuoymduUkoywcsrJwmjY5YIsKh5q6vwsK06kVOv68wUdpVBlvDr7pxCSRdQ
%2B733z17cn4lv8HT3CvZFlwxwZVc5YFWbKpSjp8xDMhv2u36DxdlM1sBW73uxnmzXRJqyA65nyptGjrDy20sB5P%2BY7oSfeVNoZ1OX7HOkKbpWD%2B0ivE
%2B2a6OOSMCi2%2BhYVd%2Ftp6lvVninU6e0KrjU3IqZeunaw%2BC%2FE6N02tRX%2FR2nHKinSO4g17waPCMm3ujvI95br0tR2%2BDKE2raMwQb4KrdpDbC1lZMRwNlgh1B
%2FRjyuVSuGH2Fs5qQRouepGdhA4Szj3J%2BbwcjN1XsssjVYhElAE7bDZmqzlqtoRZIhJ8JX1rUB4xy6TXeZkjs1Tzyw07Le%2F%2FyNFKMb4MZOz5RG0MIC0Qhw66a%2FWGqN
%2FvJpOPrqH%2FGRqqXZnL3sEt17D%2F9DBg2VtmnuJPDmoMcGymUYqhvv7oWYI0ij0aEcJqdCUcZ%2BJU6ibkGtit3QQTIHY5nD7ULZEx5sqEAir%2FndYLPh4hd
%2B36cJghdBUQ4xUnwgr
%2BIkzEQOO8w5lp1Ur4nNErdQwX1kkWAWMwJmjYWkmXRvtv4MQVUxVBQ2mhKNV1lC8AZnhpRQ4s5kuufO229Xu891q3vSkPSHbr4mzDel9dxe89TVASgGdOodmngmMF
%2B57uuUKoRGE0sNksCIQf9KYbJtJfZ92qdcyiJpgVDXSejWRStlHOOUxD7o2kFCy
%2FTTtVi7K5clpTvmNe9z62Y4%2BptAct1XE0hXnHCh5w4yW0YaDHfENdzmt12ZfB4veCgDHS3SxUB4H7sogeBwTbdm9uBrwuN%2BB%2F2m7PxuF1P3GipBGS9HG
%2Bz6WOmShxIiwY0lov0SIAAjg9zGqYBUP1OmUVy4fmM7yzbayfkZwrl2iqkr03bAbu8%2Fu5AjiOjeEOXaUfbIH%2F%2BpfD0GZlNQ0IqARfSzoHFvCNuRnYIg2kORWl3R
%2B4%2F1CNAOHKi7yqVYoytcPYbphgsKKKvFKFQoGU5fO%2FemRryECVCZndeJwD%2Bm5KDLKrpQinVL7fa9HTXBVNrJMwdeBxlBkp9cdaLg
%2FxqwH9DXub4PEXhJsQv8Tzo9rgwMp13CeHk54BhR5sREhDmHcJ3uBRFmEgVJ9YfWDr8TnTHQECLpaSxkCZB3ZoBttUWEqGSFjMtkSuq8EqrRwO7IE1TSb5NKcoD8SghB2IW
%2FmYvPuvutrvJWSBL0Iv4g3bM8Hj%2FxbVPaI81Ot2fV4UWSZiY5wLfqQ5DO3ZbopQ%2B
%2FO1ls1pAEKHdk4du23NV5rXetVojlkj6xFYloYv646dO00i5nt9zVKAO1EMP27NQHVI642z4NjzJRcT0xE5IN8BvWTPn
%2BKsR8XsoFpPMPx3tcaN5ODQ41dgHjIIgxQ3Xz8swZzUaxZz%2BBFl1KK34ukq6lL3ofRryfMnf6hiAdfT
%2BA8z4ty7BfX14Puy203uxv95bh4oJ1L6F6kTg78IZzfxaWQeFADh%2Begv3hl1WqKHChfzBdg8XQmGr%2BMAk0Jllr6vtR%2BMQuCsk
%2BHHJ7H9SCIhwFioMFfGQU1N4icqTytb8O4%2BlsOwZ7o4UJsrbS9Ms5sNCvIM3C%2FHU2hH6XkGy63AMDUq1OeWDlrC5BIINc5ISFkVb%2BbjT2zySWfp%2FmEXDhBwUD%2F
%2Biv1UK7Ob%2F%2F%2F4xQhh8DeXYisDyFjcdJfX29w5nH1Hi57Bvr1D9LcM3dHZeEyW8KKa7aUN6bdaPTP%2FHadyj3e
%2FpbsGySsDhwWVFpTI14R7jJbvTAkTX6G1Cyv5YMq33kJb9Ng4Sd2V6wKn56tCtnwnu%2FcQYQYx92j8RnfgsP3bJck90Q53WQZ57m6uqj8afDc6ZGk
%2Fq9luFYA0OBlyYcOS1oAumn0RH9dyQ5WCyWO1Ys1ORk9WpLzlDv64kE0KPSvzd78Ez7LS8lO1xOE1pecElCrATCncx5%2B14peIubfsW4iuZoCKmwyQpHEqSvXx8TEjBiwwbQoF
%2FxzllmfYDE%2BYrIUc8MEVxGUKWlEmjjFTYDTRwJP7B8gx7hpeCbjuQebf%2F2Fx1N%2F%2FkUq9%2FwYIo%2BFBhQ2Qg5MBeZ7LkqwrlpMKr0VPUVN
%2FwnwYLDowuE3mPRKR4Za4cJHulNhwGtLkA8h06ny1wgDiYbCVhdP31Zb50JfaOHgmQHmmc6L6O2eVdgxg4ckYsn
%2B2tMe0nQ8Tx0%2B5EItBzrTdnYAwwN0%2FaDYiQ8EluhtTKMdkcZkpWyXDfgu3QNE05Ea40Y4GxpOLWfqMV92iN8jN2yZyEtCZK0Y
%2FJoq4ITpZgjqPRMJZidQF5ZWnDxsyHrDhKVzKUY0hhaVdJXOEGnzqNr5pXwKZrCV%2BCcXDcCe6Od
%2FJ8XlpnMezmaJzzuB47KevjrY9vVkMLOuYqqHwfJPeSI5Y3Vg0L5sW6hyGrB3KRg9ulHwU6yagrdsy9TgKr4M0zgDIa3nw
%2BYvHVYvjdGQhsCRhmStoQ5nGIvh085n6BVrHhFAfRo1txCtgaSDB86SCxw8k9TR6BpPpItn4mnAItDDv%2BgBnDoGjHEnBy3iT2mSa%2FAFpMTOr9Pi00w5CNoqWcnp7DzP
%2FC9TWypU799wRjtAZvhLkVOClfvxVpAjp%2Fx4dLQJHCSgeMUVDHdE6htrdBf9okud%2FvE4izq%2FHqbABFKSk%2BQZLrECxE
%2BlKHXJQcRMH3tw714ozjBgnfE8PaozTQqpS1KmFTRuzPKkptCpLfKf9hKrCSrGNQxbqyseD4qgWzgjEeHGr6XhNC3fQJO
%2F6uG9AC6fZjcbE0mMkF69RBWPIOnXvTRODqAWiPk3hSnJ05MRRKuqZ1cXClA8f7OCalm59X2sxB23DQlBjNEGZav52qnlHTTY33DJpFroZoN96%2BGn7%2FNNPUM
%2BdbhH69b9QqgGs5ihOZSNddFgTAzOKYGj2vs86DcVmKFg0tE5obiWdllQ%2FpX921TYn7%2BG4YO2eExHLwfJwAka3R%2BZ4Z1RhzmHQzv
%2BSNBP0zWYYC5Q37MIMAfN2PliD8JjBGaywpBNgNevtY2cVpMsXGhtoM0kpf%2F0cf21eS9efFjIh8piLyq2WNcBVu%2BTkb9a2Zg
%2Fo0t4mv5ZuFQCzowdxPEFgjwbhqQ7BvFABKf2ifDo1CpC5o7sHhC9fPrCD1MKsY0jxQUUnQONlxR1ECvmKyGkVd9ekKsVP92wAyPmVP0vvRr1KWTHY7FIzsqpow2pIU%2B
%2Ba9LFrrXV5HdQyyotut75A9ig%2FNcoHRldaMItPZZHDH6mF3k41jyB7iaEVZijfc7GCXOP
%2BnZXIub3p2MVo5QY8cXpMj63dli3jisLJ9SW3kBLEt2aDdWiI8VNsIwYAMtj0T7Vbw3ek7xKcQ61QHo%2Bj%2FT988%2BebZRp1unwdadxyJv9oEBcWFlbtCL7bcT%2BMm4oI
%2FtQNegcY6pglOCd2aO%2FGFySEidfXcYYD3IyTB%2F2nLoTT%2BdLekz9PFg6abaEMI8mj4CbL8jgVIMaDNsUF%2FTHiINR3a1N7lB%2B7Y5wjFjT%2FAoHctbXZul%2F3gk
%2FzPZPupvlltYwN4epobzdFe2%2F2vIOD8iq27R5G0eeBaVhwWwHRVgjpi0WPapXmJd8JVFwSLCHJPwlf3O9L4VpGZ2YegRLLz6RZPqq2X8G9siqFCGDu
%2F1BqcZIqnM7kcLfHedNdiRWCAl0ZkrWsE4Q7NNDz3gDwW4tagP6hSg1fyy8DffPnfvENqLxTFmoSOMkjVRIy8W9se6C%2F%2FCFbNIsXe4w
%2BwMOreBEliA5klYWitUiD3u7VHlW8S8uveK7573eqZANM7s1anwjxzeWwPn9h5RNUxbgxwf5i6Ii1czBNeQcP%2Bp
%2BElH0W1hrwj2YFv4S624%2BxgegCD8%2BNYLrJvAwrADTaCwO12QzEhSikhl2aIVcyYAuhIYjgdDCvHRqQTsDoLE0JzZ8ItCNXSqXh3WM3mwT%2FETauCrWV
%2BVSOkknlPc5tvL2tj4JceY0eLW6cgixDVe1AplNdGqzOesd5I4T%2FTFR3hn3AnsxeJKMLnJIMmSj5%2FBpG
%2BLQsDlAqgV1KuCPAUL3wEbPsD7wakstd2nQlC6JyKI6YFPFuncJqqnHvafWvAejsNd8kjhALv7TN8ebK5fFixnVbqM%2Fxh98W7mn
%2FFP7%2BBk9T9ytBn2L7rogoWOz3%2Bmk1SJaYck8DCopZYY9EdX644uSOGJ7UYdsVBWMuyO2okI0u1gDZg91DPJrCLXtK%2FQILxA9Ypu45D6%2FOJ8yiMknuc1G
%2BLj9RBKkEDyT
%2FjCNVUVV7fMtMxwFEWSH6VXytJxFfL4O1wt9ew8mi5Shs0vfpu5oK51FQuLmBzPbUYixMH6M6DoKuewcnvzliPymjaZkFoG4X4Wx8UJt7qYhHDy1958jJjqsmpR2AuHOVojtQIF
%2BFAtjorLdJwd2juGvM5YB0QaKsOHcdn6rRdX4AwmXyT4BvCkixDDu3bR9LhIKdvo9XgTZrKD2z
%2FJbIV0Wyf7jD684iwVQCNd7ksnldgAbBmqPA0%2BmSOVXKiPMv55v4zS8F0R8hFttBjsNNWb
%2BJfCRaRGcXRezGcMfH43sdipXpksQjBXEoE6UciBTaWWCoHqAnBTEqe22IIgwfPLyM8EioII9PkbJO64xTLvSFbd55jA3ICmvVjOHPJxTFaPFHrLRft2ryhH1YPMujQLjWmnAQC
%2Byz6jgNNXZa%2F4pDEUeeBbniv5xwf%2FfK9bK2zbrdFJ5N9hgGMo4HVUxE7J8PIodfHXvZBBUO0PYgGF6CpSh2YlDhmYY7%2FN2%2F
%2BdtWIsilX49FEj2CaFGox9qqqronUrciT%2FBUZoW5jmPwMDw1PNkwEs%2BkYCZcVkYWggUfFY3PyB3cXcmHG2KLBZDQ%2BYxMxp
%2BlX1Zw4H58xAr2rAtZlOKuNShOW0AbyibECixO8IkDpNgh1rMWUR%2B1ZKtVq9FZ3gVu0sssx95K4lhRT4kg8CEdNCR5%2FB8OIv6ekHl9t1doq8GA0t3Ff%2B8NLDa5EM
%2FnlFO4DRfatUmXVtq0Z3yiMp3pd9tK%2Bvd4ZDyNJ0PUcQcckP2PG9ZDhcKLOeaPloTAHB4QpXHdrHqj%2BlBvZALrF
%2BZ02Bluu6TQro4yoNNulhIu0EkrXjjvACvQLbxATmFGX6X8ldnfVsDtWFdbbKnC0UubtD%2Fu4%2FARxl09n6YNxEKvWMqkiRPf28%2F0fOfhGFz8Oo1Sg2PT7lP5oo0yqk64U
%2FKR8PgHVX9lYHZu%2FGplZ
%2BymXefKVMtufOLSgahlxuOlTYF6O4WuEXcX7ZFe5nvVtOftvPMi6QqzkFKnP0UXXI9%2BWfsGjqMIIsmC4wv6VLRrIeLTW7S1g1hXlVcikdYD6b7w50JzXLV9MS5zs
%2BtWjXKygngNvWCw8Ui%2BZXu8To
%2B8X84qliNCUNv7Di1ASUXh4TdKKCB518%2FBjwZvOWdZApRYUj0qjPoTEh8fBJ87EBLay6qRVYSmbKGg6HyzasZV3nkYLTvrurq4NawLEllW2IU12eC98PkXz7HywO71Y9chIVn
%2FRpdFStkd%2Ben5U9yAzimjH%2B%2B3edcspi1QPb0JIUiCnFkO%2BIiYBUhflTmxrJhF4VigdeqsBNubiWRC9qTCH9P1iH%2Fxgi6McgysaesLFDu6311g2QnfuzXmhbfE
%2BIdgATJ7SP44oEx1IntqQdN3IMf4r1neJIv3v7X01FDB36EnddENzz8bND
%2Fn786fmZ258svDbBgqi6p0nFx96fHlaeW1zrxXhZre70imlmWfTuXwevvoIWIzQsSWga1BJWJUHzfvYZ2IchVnZE51mfBMzaVFzXvWjaCpzdQmWg%3D
%3D&__VIEWSTATEGENERATOR=30572B18&__EVENTVALIDATION=W8ZGCW1sdAqs3xbkF5pNjTAurUng7MNt7bvt75dPUPFJD7MYN47kJ95qCTRbZ2qrweHV9q8zYm7o6X%2FF
%2F1pZnGQYaxb8PR%2FTgLQJ56O9EvsBrfDOZdM0r1Kjquye%2F4LarfzVnZFB2amNFhL8FNqUFytriq77esH%2B2%2Fxjr%2B2B8%2Fv4x1KPLkKOvYXxMN3nbxOaZZOQI
%2BnzCYs3IWGR9N2M9wif3Pja55CSoWPEVZOcVQ5y4wHT16H5RdqFhn7BhYPRZXFBAoBuMmgoAIBAWkkos21HuGKdscVvPvWJzQqDFQ6Ins74SPLfyPTBKsgq
%2BLdiwxlcfh4XIJxqaKnm908%2F8%2FS1SfqskrhC4eVpDEwQYw5snsG4pKJ5UGnHlEUDKXXN1yWoXGJUHGaRrCqHhEc3gyObWsioE7NGlptYJRi38HJDQ303osX0v3%2FeVg45C
%2F%2FzFzKAmqHdq4Ytj%2F65NvqnSVr0SwxYiCF52dl%2BmT4VrTgnh8sXkGKKbLceKY1XhB0tpmrg32gG7NnHkBdEb%2FA2A6%2BDFuOz6U7KOtYXVUj6KTeye
%2FuByJQPhrdhl1d7IUlZrxaaCxpB44bcSqNiuLkRHUK0hckMu9LWf3lxnkG6%2Buy8rzf9l%2FAN8IvdSL0TMMJRPBqIGLooYwY2C
%2Bn8QhNetuV2A69QV3XJNgIurSHBAtNIgw%2Balf%2FONDxrN1vkZymi38vuCOGRH2WfAJtMzn3GlqqbQdn
%2Fb31xYHX8xD9jKK7aq1xAClKTKeGqS99RyyJkUk1mPm2ohvR209MhL2C0prN5NkSseolq9gDYegO%2FBIZavk0BGKvDKUQWQ1QJdG8d6AnNaNqimMLJjA
%2BajRfR98BsWaVYqpy%2FFrrmzlu8awfmF4z1G%2BUj%2BktZOgt9Wr8TY0kwY59NtVVOaRjcRyFkxKAwVfydgpmhJ5mLVi%2FMrQiAK%2FLL2I7yiLoeoILtcw
%2BLKn0zNNzU4IXOntdwb1qK3IuPn0MvkDN2YFMgH8GCLXlHWMN9uZ8x%2FeJzdxvo4sL4vnR9%2BBPVpCpJLtiCzs31d%2FfNw%2FO%2F5z6I0Wlnkfcq0jojoTsg
%2FqPljHfa64RefSObz7Z8rauNRqwZDsZRkHmt1SOp%2BGribCnFu5VokV5Vl9ynC5wJtwPnpguI1mjYEvWbcOmSAw64pJDl5swulSRRJd6I7JPQ3uBpkwogOwM
%2FIG1EQAQVYc7Je8ROcl2hzwQYk%2BMad5NYkqMR1pEOcYOja9TT1XQU5Ee%2Bb%2FSDIRbXwo%2F7GWyD
%2BXigmBT8jMfysTDS1&RadTabStrip_ClientState={%22selectedIndexes%22%3A[%221%22]%2C%22logEntries%22%3A[]%2C%22scrollState%22%3A{}}
&RadMultiPage1_ClientState={%22selectedIndex%22%3A1%2C%22changeLog%22%3A[]}&hdnNomeUsuario=Luis
%20Martins&hdnIdUsuario=78&hdnIdSortOrder=ASC&searchTermo=discovery&hdnIdSortField=ds_termo_busca&searchTermo_ClientState={%22enabled
%22%3Atrue%2C%22emptyMessage%22%3A%22%22%2C%22validationText%22%3A%22%22%2C%22valueAsString%22%3A%22%22%2C%22lastSetTextBoxValue%22%3A
%22%22}&gridTermos_ClientState=&clearSearch_ClientState={%22text%22%3A%22%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target

WAS Scan Report

%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&rbtExibirStatusTodos_ClientState={%22text%22%3A%22Todas%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&rbtExibirStatusAtivos_ClientState={%22text%22%3A%22Ativas%22%2C%22value%22%3A%22%22%2C%22checked%22%3Atrue%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&sohPortaisSim_ClientState={%22text%22%3A%22Sim%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&rbtExibirStatusInativos_ClientState={%22text%22%3A%22Inativas%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&sohPortaisNao_ClientState={%22text%22%3A%22N%C3%A3o%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&&rcbTipoFiltroRlv_ClientState=&gridTermos%24ctl00%24ctl02%24ctl02%24ctl04=%20&sohPortaisTudo_ClientState={%22text%22%3A%22Nenhum%22%2C%22value%22%3A%22%22%2C%22checked%22%3Atrue%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&gridTermos%24ctl00%24ctl02%24ctl02%24ctl05=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl06=%20&radNumRelevancia_ClientState={%22enabled%22%3Afalse%2C%22emptyMessage%22%3A%22%22%2C%22validationText%22%3A%220%22%2C%22valueAsString%22%3A%220%22%2C%22minValue%22%3A0%2C%22maxValue%22%3A70368744177664%2C%22lastSetTextBoxValue%22%3A%220%22}&rcbFormaRelevancia_ClientState=&gridTermos%24ctl00%24ctl02%24ctl02%24ctl07=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl08=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl09=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl10=%20&rcbTipoFiltroRlv=Nenhum&linkConsultar_ClientState={%22text%22%3A%22Consultar%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Atrue%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&gridTermos%24ctl00%24ctl02%24ctl02%24ctl11=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl12=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl13=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl15=%20&rcbFormaRelevancia=Todas&cleanFilters_ClientState={%22text%22%3A%22Filtros%20Padr%C3%B5es%22%2C%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Afalse%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&gridTermos%24ctl00%24ctl02%24ctl02%24ctl16=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl18=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl22=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl19=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl23=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl25=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl20=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl26=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl27=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl28=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl29=%20&gridTermos%24ctl00%24ctl03%24ctl01%24ctl02=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl30=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl31=%20&gridTermos%24ctl00%24ctl03%24ctl01%24ctl03=%20&gridTermos%24ctl00%24ctl02%24ctl02%24ctl32=%20&gridTermos%24ctl00%24ctl03%24ctl01%24ctl08=%20&gridTermos%24ctl00%24ctl03%24ctl01%24ctl09=%20&gridTermos_ctl00_ctl02_ctl00_toolTipHelpGridTermos_ClientState=&gridTermos_ctl00_ctl03_ctl01_PageSizeComboBox_ClientState=&gridTermo%24ctl00%24ctl03%24ctl01%24PageSizeComboBox=10&linkConsultar=Consultar

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

Date: Thu, 12 Jan 2023 05:42:57 GMT
Cache-Control: private
Content-Type: text/html; charset=utf-8
Qualys_resp_hdr_injection: Vulnerable; path=/; secure; HttpOnly
X-Frame-Options: SAMEORIGIN
x-Content-Type-Options: nosnif
Content-Length: 102044
Set-Cookie: _downloadToken=q; HttpOnly; Secure
Connection: close

150059 Reference to Windows file path is present in HTML (2)

WAS Scan Report

150059 Reference to Windows file path is present in HTML

URL: https://412-49.docspider.com.br/Busca/ConfiguracaoGeralBusca

Finding #	**891238**(69622033)	**Severity**	Potential Vulnerability - Level 1
Unique #	**e509fd9a-cbed-4c39-ba3b-17bd9536bd29**		
Group	Information Disclosure	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-201		
OWASP	A4 Insecure Design		
WASC	WASC-13 INFORMATION LEAKAGE		

CVSS V3 Base	5.3	**CVSS V3 Temporal** 4.7	**CVSS V3 Attack Vector** Network

Details

Threat

Windows specific file path was detected in the response.

Impact

The response may be an error response that disclosed a local file path. This may potentially be a sensitive information.

Solution

The content should be reviewed to determine whether it could be masked or removed.

Detection Information

Parameter No param has been required for detecting the information.

Authentication In order to detect this vulnerability, the scan required authentication to be enabled.

Access Path Here is the path followed by the scanner to reach the exploitable URL:

https://412-49.docspider.com.br/Login
https://412-49.docspider.com.br/Login/Authenticate
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

Payloads

WAS Scan Report

#1 Request

GET https://412-49.docspider.com.br/Busca/ConfiguracaoGeralBusca

Referer: https://412-49.docspider.com.br/
Cookie: biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; _downloadToken=1673472915502,1673472915514;
ASPSESSIONIDAGQQQRDA=CEEHMCOCJAHKFCKNLAIHHGEG; ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf;
Host: 412-49.docspider.com.br
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

```
os_intervalo_indexacao]').val('5');
$('input[name=nm_caminho_log]').val('');
$('#st_ocr_integral_pdf').val(0);
$('input[name=ds_caminho_programa_ocr]').val('C:\\Docspider\\Services\\ServicoIndexacao\\OCR');
$('input[name=ds_caminho_conversor_pdf_img]').val('C:\\Docspider\\Services\\ServicoIndexacao\\PDF');

if ('True' == 'True') {
$('input[name=cd_senha_autenticacao]').val('••••••');
}
}
<
```

*   The reflected string on the response webpage indicates that the vulnerability test was successful

WAS Scan Report

150059 Reference to Windows file path is present in HTML

URL: https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx

Finding #	**891240**(69622034)	**Severity**	Potential Vulnerability - Level 1
Unique #	**68052e4c-8b74-40fa-82d0-a1fd3c8bc8a4**		
Group	Information Disclosure	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-201		
OWASP	A4 Insecure Design		
WASC	WASC-13 INFORMATION LEAKAGE		

CVSS V3 Base	5.3	**CVSS V3 Temporal** 4.7	**CVSS V3 Attack Vector** Network

Details

Threat
Windows specific file path was detected in the response.

Impact
The response may be an error response that disclosed a local file path. This may potentially be a sensitive information.

Solution
The content should be reviewed to determine whether it could be masked or removed.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, the scan required authentication to be enabled.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://412-49.docspider.com.br/Login
https://412-49.docspider.com.br/Login/Authenticate
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx
https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx

Payloads

#1 Request

POST https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx

Referer: https://412-49.docspider.com.br/
Cookie: biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; _downloadToken=1673473653172,1673473653184;
ASPSESSIONIDAGQQQRDA=MEEHMCOCBKHPBIGDCFDKDOAA; ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf;
Host: 412-49.docspider.com.br
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: */*
Content-Length: 18903
Content-Type: application/x-www-form-urlencoded

RadScriptManager1_TSM=%3B%3BSystem.Web.Extensions%2C%20Version%3D4.0.0.0%2C%20Culture%3Dneutral%2C%20PublicKeyToken
%3D31bf3856ad364e35%3Apt-BR%3Af7ba41a4-e843-4f12-b442-8e407f37c316%3Aea597d4b%3Ab25378d2%3BTelerik.Web.UI%2C%20Version
%3D2021.3.1111.45%2C%20Culture%3Dneutral%2C%20PublicKeyToken%3D121fae78165ba3d4%3Apt-BR%3Ab406acc5-0028-4c73-8915-a9da355d848a
%3A16e4e7cd%3Aed16cbdc%3A4877f69a%3A33715776%3A86526ba7%3A874f8ea2%3Af7645509%3A24ee1bba%3Ac128760b
%3Af46195d3%3A19620875%3Acda80b3%3A383e4ce8%3A88144a7a%3A11a04f7e%3Ae330518b%3A1e771326%3A8e6f0d33%3A1f3a7489%3A6a6d718d%3Ab7778d6c
%3A6d43f6d9%3Ab2e06756%3A92fe8ea0%3Afa31b949%3A490a9d4e%3Abd8f85e4%3B%3BTelerik.Web.UI%2C%20Version%3D2021.3.1111.45%2C%20Culture
%3Dneutral%2C%20PublicKeyToken%3D121fae78165ba3d4%3Apt-BR%3Ab406acc5-0028-4c73-8915-a9da355d848a%3A58366029%3A2003d0b8%3Aaa288e2d
%3A258f1c72&hdnNomeUsuario=Luis
%20Martins&hdnIdUsuario=78&FormDecorator1_ClientState=&RadToolTipManager1_ClientState=&MainSplitter_ClientState=&__EVENTTARGET=&__EVENTAR
%2Fbg2APE2vHLEMVyk82ZVW6D%2FODU9csdRjpompciNp5X9ZdkMhGQNkj65WY%2BU%2B%2BpqL
%2BNEFTVfgEuXbmhIYeDuajxJdoIqfSKBO3gLzjGMhZN0%2B8t4vljTQz0UnF0F441k3eo5CYNqPYBf084jDgdvllP6xULRwvBP14ui4ilVZ6yyMsbxictQADCOR
%2FvSp0K4PDtpX0Q8ka6nmyeuN
%2F3RtmLW9knHW25EAPgpdJNHu0MM9BNXtu2KYvgYmp2FNvoqrbehM0TyGJGda3sUGl6HWoRhnX21OPBC8WBq095oOU7t9y3rzfg9B9e6lHInwkPoZQFBrJvRxByxH6%2BSZl0myt
%2B2bsyMks0uM6edQYfQwwkRNUh6MM5QXhpn%2BpQFC%2B2mR09jis7z%2FmqXpj1MbjLVADa1pFdBovMFBRA8Q95LK8jzmWHUZJUry05pdPu%2F1qW3h8KPuPdu
%2BmpcTFd1LhDoJZimBfJBY11dht9lbFitHfIbKf%2Fh6fKmXERIpDZazvi%2BWo2nSPbcge05pn%2FPh5eDGFcHkSJDxc314A2dQy11F23RP2f3yBdbIZMABfN48j
%2B01BKX7%2BR7yZlhQqKWz42Rk7yey5bNidlsTmVkmju0AhpPU5xgYl%2BqJPaBl3pIYMBv2vv
%2FG5EEFGeF96sLVnAcVsLuXfwEc7ljkKTJz1KrUtuNGbwuJPuLq9Q5o7iM3QAeeJrRewcEoZrIoj3lcVsl2JPx2ASUB8zConLlogQ%2B6WH5ZV8vkD
%2FXQUx4YKhVMcA2AyVh2%2F77uQfU1Y10EzQskC0RMKKa2hq8MBp0JeStZ1Z%2FWU%2BgmYzUmGzK%2BaLsqadCh21FDOMjouwGOitOcauJivkqhs2zZF3FwvKKDlw2Up2d
%2FwuiT3PGQwrJziULGhHrI%2Buz6W%2BIJzG%2FgyC5e68R5BJRyAk
%2FWHYPiOHkwxZ55dDR8N1ZaYYINCUI3oUqhUZheMvzpLoFXB5cMsYsBNxIdEyFXARrezU8TRB7aoii8Z7J7HUIgrwz0YyDNrOWcVuQMmAzzxYacTtliOZUYCoJ08elIxpv7uXGX9
%2FSfttuUcSgcj390wWxmVhmU4ukvNV7pqpjA9QyeZl%2BwlkTC4HaEOGbauPCzxOjA3BubsTmbtilYiYUyqql7Ybhe7%2FIIUrENdeu1vdGunHlYT4VxvZwSSN1xoZEc0JQvOaKhC
%2BCXODkYlFzOhrGvlAUgvwEuUlxyZuD3rcMjwiLhJplZ8LLBhnFmrr4nhDJmJATgxSakEcU8qcT3hgzdUyfT2jLe73o1K9sQJCn64WTCkYdMC%2Fo
%2B1YaZI18%2B5FUvMWi5YdGdSF92%2BTvcwM3bcoMVAZn1CLCkmvMl%2F3FM9wuIUHpyl%2BtjerboGsWZH8AK1WlS9TiILmnmAfnP%2Bmdx1kc9WxMfKcfl67tazo%2F8CddO
%2Bmva%2Fq6nc1gNs8s8ftJKK%2BbeBpZ6JFq%2Ftzz3y3oq9u3raAkFl7viTGQIhckDTlYYb7njCy6QZQVHhG4MavvK2eP%2F4sNkjLYqMDTyZ1Mj6G4LJMIjNklvGMWizXv
%2B5UIla0x7QBAxpqi21c7dfLVO9nEFCP3Edg67JtFLRhDX1S5axnec
%2BNi9A20MHCXjHWPOazRbnGoTUuSTQImbE7DLzjkgi9nbrfyiZe76A7uHGAd4bUhsr6MWZfAa93r0Jb4SA4O9qzpuf8oEWwhlPt5waHThHOboIBzmIsuk6f59KGW4ImydfXJTUsX
%2Fy%2F1Mz5lCMMmj7b2ZjZm615%2BX8NbG1yJAMK7E69juRB7UTEt9lbli%2F59uNt%2Bta3PK%2Bb9g8ZKvcQQy3hTkJ8r1OVsZNBviYuvlLSaa9TYhsHf7ytP1S
%2F1NpDY7x4PbkedNCwvJ7fOay3eOModCc1mKOWE8441eN3WKbXUgGpX1CcTzd0T2SJW03iQIfgRID9iRBjj0d3kNH2ETe9EEnpX31WfK17rupOCpbefgNSKCDpwxjJswbb0SxD49
%2BY9KcvZwc2rHUtZ0WKvUTYgJ2eTI38p2clat8GqzkJ4TZrGUE4AXKFeVzeyrwaFLjVlSI4WuleWIj7mIC95py7Wzin
%2Fcf8RfdHRhGuHM1WHqVkvP3v9iZuS3iYrfvHqroXAXsRFRJTdXV0YDwsjHpj7kZrE1Xi2x%2B84ajwHS38jfR%2FU0W%2B
%2Fr7VeMOoUseRUrGZN7b4PlTgunNsc2DsKKEnglJP1QrCJ3meDMlTj0qkCYs4TpT9hNN%2BIwwgyVT%2BQtfiDeo2sOeX%2FEwUUTFMMN2hguN
%2BWg6bRG16jNFKpME5T3r92RwsYGJgN4m77SqwhUuU%2B8U
%2FFz97ZQZ3hlWyTvHnSSNzuulVnTgtIA1BaNBDAvuNR3i0HH9S1RUCh0G3i7bI4HgtZVRB8m784%2Bv63GknG3Og2vNqE%2FCEpzlnTQleqS9c76r
%2FsCFTMOB8dYbj5NuseBSpn6PaFyh%2Flz0HIuXoooPcPMm7OPYPba7tQps%2B7yX0eOW0kZkaiPjs
%2FF0%2FcfZQu1JxkyVCiZkJBHtgTfRHcfFNVgGwe4epoQdkcxetHGr4l5YdtMpqAEd8logfwcWGodVkkekLd5SVktQZMJ3Gv
%2F45%2FUyKGFNG6Mo3ag4i0ZH0fFooJRk5Hyza5iPEqjSMZcrsISPrHQKYcyfSNw%2B11OppqfI6X8zs1Wmdk6hrB%2BDSLJnmQeiwE%2BZZn0txPT
%2BCLTnsw2iOxnulEUcgTfcucA%2BQUaO9UmLH3CLcPwALviPdZ%2B7ulkcytcyBgDFrz%2FNZA4X8gHi05HrUUrVTynvI62XQMg4561lk6d
%2FJMdnE0BIUtmWaVC0sOhHacQOk3MkOV%2BFTOlsSmeSXJexJpOn%2FS8yXbODdFghyGD2T%2F4C1auyBrdTKYKiEVYZ1giYdw0vwveCjbeR
%2BykIpOzwC83hQJq4e8XN2FSn2ow%2FYdSCLKh%2B5b8MR8uqxHfJLXs1K1fyhe7EN3FKrxEjssfIH3YlcWtI7rWH7CJtvSv7GJpjJfHyG0i5vuZdntyBiISwKGrnm%2FVPou
%2BJ90VNbNUHE98UGdUcTkoqljo1EW9t93sVJhH%2Bb9kvXyxYqpXvz8%2Fgf3qCA6xEEhvhkOoC2BrHdXMsYIKAu7MYdumQWbf99SOqoc3kw2e9kF5UWQ0JWjw%2FM
%2FJ8UCW2pbnxra%2FGJP6jMcoVnTvNJrRO0YjpUmRsw06SoYuW3EYu%2FpWGgXD91qwbt8dihLDQ6otnNY3wAvhaCFxnqmI%2BsXTKu8u5C6uVS5g95sFvwO09zCt
%2BQbbAQF5zf3zr3hr0yDUeJUuc5g88FWj5JO3if7YQTPgEO94vNCJnxdQ%2BnGAgK0OQ8mU6xG7RRcY83yc%2BRoMvvvF5SDZ3dSbD
%2Bx1JNi9EHVyTZ9NMaHGn2ci3FU894TiWLAqAAau6lkDWzetvR1wej9vesYJxG%2F2KPlkT6Pk18bZGjUXE5QStkkSuX10hLsAlcN12vaPLG4WQFeiUf32CV1QbPYSQwA
%2B8HDu6PgNO%2BHiX1uspZheHqYpjcrH%2B5jdHAASlGWbzAGZj0QoXVVJRJoGPozwPW8Vgg7ehMwmpxH6nki6iJEOpfDZX1pPiOwP
%2FBzsKgnPWIvwse8DEXXhIVNAdYuQz14PdnjJ1jeyFeAJ6PlrSjzXv6J8xDc7pe6Jw9c%2FCe%2Bb7ATIR7%2B9ngzc1EotJpbDg4QyxNxD84cl
%2FR2aCjJM1YPYB4FK6bCkhdkGp3TaKT3ARJgH5oalMjUeokhLFyjuPrgDOzdEJxp0ANeizY4kgGp7G0H8JNELRKpgn2WnDBhlV1znHNrSDRuBPzoCSHBg1rNZEMYpVNImqpKJnn3
%2FnqxmKc3G3I%2Fu9Vg1HAaPsx88Y%2B2oHpSZXTNdLfSw2YSh53BAmEYGOzxK3WdoSqAw12%2BnPaEziI5nFBsBjr3TsKqb0ZIDWRWJtHfLpWc
%2FHBDQfFHS79n1x5Mhk0oLIZfHhnA%2BcKQBFlHnMCTZ%2FVE7okOo76SsbxAwnqQlbHPevvtLNVIKQ3LLDdJY7wBowiR2pLrvTSN7C%2B5lz4Ti
%2FmKwI0ZfFLrbwqPzFMkhNesWoc1tcDWnzOdRQw9FtfA9qYecgePoHGylPpX8agm5qsjRYY8XCQnBFgCqnqgpDJjsb%2B6FYuZ0k4LVIyzI
%2FV16Dh9sP619%2Fc12LaZvNULLUl1hlhf9%2FV01eqgPtrBqF5P4qYslydSggE0ejt2%2FBJufXzqZr0zwxM631N0ehi%2BuSPz%2B6T3iomhqz
%2BbRsCltpRocmj7mjlb8axM2u%2BgKQrkVEP0RhpR%2FaeUAI1EhGQ0pVjFesC3kPN2cxU5mwQjR%2Fdz8iRVoYeaj
%2FibN9NcnkUYz1BUyGeRoa68DKI77ZMR3la769W1xQvlCh2%2FUfXiVp62FG9LiaRBn4qLP5qO2EEXDwBcA5NVh7LF67V0%2BCcub9%2FZCBaO
%2FSacNDFi0P7KZaLKSf6gC69v4zW7ond8YNkHhmOvS%2F1csgB%2FkokSqjJYtiS5sc
%2B9ccW0p5pdZdYPvb24HinR7pIdL61GY7CBDCp9lfJGiWBi7iQOuVI0JXoNYom2yzADbXL3oHi9t9wOAduJTB76ANi0opcmhPQT
%2Bg1Cjf7SA99OaO57k1KUwbLwcfcIX3si66QkXLOCX7%2Fa8VaI3%2BbNDJsqRECFAcjjmdZa%2FtEstRB%2Ft5QZXHg1wlToSb9Kcd2Ygta9%2FmisUfV6Vf1EGNh
%2F02tAL4ySkkm4WzN9zH7sRcQthHabXrdWjbroF3fMwfaomVViU9gWfcHffNUr0hqvwPz88rRXk0DImOlN5ojq9JOZsfJ32V70pei8WBf02wvp6bvuzcMhq73Y1LIg0fPanBLcsv
%2BoH9IxAMcgR75uzd1LCW6suPuKRPTE7bsndR%2FaGIZYaJOuiQ5Aq2DQ
%2B0tHN0MNLqOy6vD65dl1sU4TDFsYL8iubweAzSnJJl7rZ482W4Fn1Aazk9yyWokP0M07TTbM5ShtXkZOW5ms
%2FNijpjMX1LdOLm851Bvv8qKEz5Hdg3KFFCbVMMWUBVGRUMhQqLcCPN2%2FZjI1PsXoQxAaoSpK1YzHcBhffZssdiFd7%2BjNeMtOoT4n73FXVYpP0b
%2FtqtXhs19EYJ60fpEqOsLQPvQrZ150BVGhKADMyARr7rcm3opy7KKogjPoypoQ6Que4kDnb4%2BimglCDJh7L2jWl77Qn%2FyUYXN%2Bz%2FVFLU147GG8%2FOkJ7u
%2B5SgwZ1vbo89Ulz1d%2B33Q611t4N4XVAu4ACoySFwHynGV%2Bt499eZ8nyos1EPzkl86mAJikkvLsQODrwd7n8sRFvC%2B2H4A
%2BhSpLVbdPAK04BPOQyFSq25j8xRtsrnGAwvFflrFFb%2BZ8Ooocw%2F97apk3CLUF5P
%2FTArvJTZtmWX5NlMHJDzKD6Hndhv3bdfSPtF1dX7HrS5bBetyUjpW5rcOcoHLsbTBkN4z%2BgW83zJrpVnkMIff97%2FW%2F
%2BgchFzS80wWU3F46KISW4aNt23Qv0UOiIZxEt3KhuIaidVVBOrzwpvPgZv55%2F4wreOF5SAnxD7rsyJfN9CuEjadW7wYmss
%2BV72bARf7yggnOL8%2FteqmnuZMBktDlH3AOUxA%2BeydUy0HCNbUfnPM3fsm3FkFQlhAWsg7uFO8qANDAadfVD%2FA4DJMYOJe6jp9jHy0rdNb6AcbD
%2FLOocr0oioGc1BRy5LpnNhcp%2BbRe6LwhFulNLMzvuTJqSWCRRtjfB6hYLxUH0Cgzh9YUmgOFNW8LI1hcyOqCk3SnMOzM8i1lFqh3Wb8tAyumoSCoa
%2BiUPdFu9DcyjW8Zt7GoG23eqQris88HQINkAihycd09ke3Eaj6cUcYhwIaYeA2S4YH0TuvqEb1pA0JRg8ZJ2Pz7qiBsOtSAs8ZGb3xsQ2mikdXpN%2FgAB1m0AsRSbH0%2B
%2BGp67jxR5UGc9tVkAzNzLI6iN7xNQ4N4XnVDznwsTzQPglT1Dby3Nt5KAg4a9tX3WkoTIlE01BZ%2B164nUblpaT6RYe
%2B90xki0YmAAurhoXgAP1NL7BZpup8iLg1LaFigkS3hwAPhCKBC01Z4p2AoCVyj8mJqVA8%2B95OVzQSR5gkhi%2BJnK7YWgzTydA6OaGYK%2FhqFOzGyE7xxyxuM
%2BZentfkfwdoasdC11aegrdnW%2BzZceirtvjWQbdpbHeSCeLc6GcPyWe1%2FPOjJwAzY2HO7t0c%2F%2FqDHQZNIdUhHLMJWKcc7aXmqSJPtgpoVqx6n0v
%2BpJu5OuMmE03dCjJnPjnpwLbwd5hL0NmDc9xNRHUKszguPzCpBP1%2BYRzYbIqg7ivXC3KBAG2GWVAvlXdeohRf2aJdymIPrtmPBW3BbRaWsT6kH%2BlmERCysFam
%2BhkaU5LtATSiapSXS3LL2wGQAEkU6aN5SnHiBE1B1S7BdoN1tlC0xEh6p1zvrZCF%2B%2BznD3VBIxUxR4WEYfRlrcmYj114uT33o7CQypmzFWY9JQb%2FSC
%2BcM7YKy2vzE4%2BXIv648LVQVBuKAns9zFC4cwTRmEXKZz8vR91crwnOY9g4y8ZNUn8FOnig1%2FDm%2ByjUwlm62qHYkJJ9uCMjJ7XMx24pWA
%2FW61ji9wVJTjHe9dAvzs2BRKU%2BIegMtQU14nsvVYEIJxmO%2BT9d759ZEMzvqVAHfmYdiCR%2B%2FCtsovDaGN

%2FkaBn83uNv9PDVI9SgwQbyfNGMkAPWjDW9%2BV6cElpYtKbATtDPoz3K4qiOaNZgxSpNw2gY25%2FTTvBjZ9xtcZkV42mTr7bfTa%2FcbYXp3ckLHux8xirqiCxYRjz
%2Bwxe2FsZFh1DYy9ruIjH0%2Fk82eZcWYrg0WO9FwEX8tJw8%2BecguDBPrVIOgp049oX6ZcxCm12oOiO7J9o98c7OsclPuiDNaloMcvsYXA%2F
%2BEYtq9b64uQ3yWJqHn98VWCa5bKEjOJkbMCJny7m08EG7urcenFFgtFRLWMvQWqOAioPlAG7YVJ
%2FYUdbCh7kfaKcVh97DvLWpSdrCwXrzjIFGppag6E2onMKycUBwQP3%2BawN3IuLtqzfxNuPX92Z3nYC%2BgE7uW
%2Fo0vakLMnx7%2FFG9GUcaiApjDNZTEurTbjCPt5eRh6W9KZM%2FAJ5pPx3gJ
%2FjLwSlobduV3MwniyCAgHJAycEH9WMuGUQzdyH8kAQIpd7iSSxV5aD3CZlvG5hlrTX54RjNmwv2lr4DPyj6UVKiGFJczbrU9F%2F
%2BA83hS1DZ58kc2zMvQeeROemn6xrafmqf8O4IuA5Uyc92XecQSQpUd7ZFkcT6Uuixhz9qeQmL9mBsBA6BE4Jl%2BoUuW%2F%2B3juMY%2B
%2FwEUulgBqf5YykWBO88RRJkrtR5id
%2FJfaYyN5RPQPg0jQXYGchZ4e40T4Fv2fwqgNy3uAfERplqTy15WUZqpQ8AEhosFs1poSS2FEaySusHzsBz64uGdIuklWx3SXtlOz3IS06MO3XVC3bJiEsq9k%2BiSz%2B
%2Bcwgd2i2h3j27C0k4laf2F97Y%2FveUGkotpTIiLaWDHrEXIBuMsz43ZyKaQ4kVHKAoEtmH0eGbbXU3hn94ou2E7nE5bm5amzbs8XUl6aSk3GJDgFV0vijIbEeo8SutZQUnRE
%2BVxUIDmet09VD4%2BsAmn8YrWGisQQWe2Jeug%2BL%2B%2FLABgGVsfhoPaFhhGTiUd1D1BKMHRMDds0FpLooA2AQYSEZL42jwPSoxHgR
%2BsCJtrl1vZwGmq6FMgq2trGEseEwG2latM%2Fs1FoZFgKOV3SDFIASA4AYxxFtgLGfsgMV0BHzSmgOgaa0HFydQdQM8oYbS48pjLQLAOMMvYl4gSop8yszYaFAwKp
%2FBGMgdZn6cGHxZiTE7EmNH7tlzvspjop6odR1XcDQlZD6cG
%2BoGCWEqJyr44WIzi24atMC5XXodqlgijmzlZQvJXLQuIo2Hdxq8xPQO6IXaJdBiCeyEkOtOUFCQjarCtbiEDVQtdiEeTee
%2BnP8eO8yK9WsIQhrgQowv9Agw989xICoTQOpIuwJdl6IFJujFkwpiEJwZCn7ISTWERvc2Gjt0k2BN7Q6EMQzu%2BAik%2Bw%2B7RREA0hJ%2B%2BEChQlO8wrhWrSkxB9ADlJ
%2FXAko7pDsGYqrc6znGvcX44OWKEWIi5ZceJerNxHHMZzIebNJtbQM65J2H%2FdGQ1aV7p5LLIGxTtgzi3O5woC96KIkSeqa5nU
%2BP4CYWBNkK88%2FK1psOzK4hnlSufZA8OrSoCcvDLEErxC7v5BFahxoa7KZBy3dDfwWrtfuimYXgAY0mWGjYwl9IwcYP%2B8QnnwZPcngrc3cmhGqn5fP
%2FFxilVH9I6oxWMlvnxEdA3XfDtrmPvdcK9C2nbM5kybcEiQQdFILNV9EAT9LN8LvgEs1R24cXCTsWhoPThvavz%2FMTgMmgmBdgIPx
%2ByO06u16cimRRpcj4fZ1Pj7drWLXfudbeANTwlLUBkifhLSLEz1pokfVLu7BnT6NpDupR%2Bek9sAW9BhcuRpWezzia2oJUwWHR0z9U38fpv
%2FD6iTJ31V0vwRdsFqCCoEWDxCyZ5nL%2BWIpKNhZFUoqY0eGwzjrhUWqBSgFcWoNmxPLn7J1WrjpNM
%2FRRLffotBTnjdnHHrekVGnc15VNLUYcBCfy7KqsxWftFVsnxT4zbgcmSpOn8fv%2BpwgXPHBtqEeb6PoJhar0it4TMBtOeWhdhJKKLWnLZa
%2F4FDN9oZJs621nA6sqIhQKjSjBcP4h0PCXiXMdyefPrZyfd8ywr95pCbIRE2hqk
%2Ba2VaiyJhksIWwlLU0fIJbVYUiJOACjO6DZjY6KQC07IWSfzn7C0ZZRf5is5zR7V6jCY7Oup6sbvJkv%2F8t3UGXjEELrpMxtqCTPrSDjUrcUSlZuzVFUNLtvsbDyPa
%2FEaP4vKVqLe4jR3PLJqQVhkr0N6GSO5KOMp2rrd6FUiSWBWU95z%2FUguRSNpg4tckGiT0FjuWQR4xEQKjlHa5G478A9UNxCGXjG88qRh9WgTmos3VveZni%2Bj4pdt5gdk
%2BUolDFEtwUklgazCsfmdOFrJAeUqm13IB331UNJ18IZbv7VmvXknwhQ0SlqmHU5CUYE9RFZBL28u2c7A2wJS2r%2BuIBz9vrK884MzDa%2FHyiTdD9sHILaWR2uOqi
%2BL9weWuYneXr0lBsF3K6I7ZmvAO%2FgAhHNr2RGbD5OzBzemdndSFAEsCVMnYR%2BEngOUXM0ubjE3EAYPLW9%2B97U%2Ba19YzG3WxezVLi7BbUqogbsKsHIjVa74s1t
%2FFGlK8t7bB45Zvrsa3A5dy1A80KuE3B5SF4lArdCDnTJEIe5Pz3%2FsCyQRK%2BseHgS2sWXLXOtE
%2F0UQlq66Fe7IE0JgItbvjK4snjzlAm0QTFV8FhmE9rVI0w0B9xtmiTxuZ4p5HhO3GpKD8LpDNRrkr8LjZthYT387BQlkA%2BmBhLo1iOBcrUJyskjmRERq9xyX5O5lnQT
%2FjqcneZBzKSCau10AteQ1F3ZpRsE6eWz58Zk6sVn1bTT12RPCrLumrbpQxCXrJ7Ges%2Bn%2Btz2eCBys%2BST%2FvXpO36TVMNtWsbVK7x0pK0AN02dQ4tu7LLsM5LvRppbbh
%2BCZXN8pu3z6mkhc3kHMiHdHS3p8nqryu%2B%2BYm0m%2F5Y3KaCQ
%2BC9TjTlbh6wDXbAAxt8HtanWLHK2E8VuS96d3HSqF0q8s8oiNUyFmmUVNQ3qVajcJ1emC3%2F8Yl4Diy2o5Z9wTUJlyBeaxOQeUQg4KRAXXFgnB94CpP
%2FnlQCr2%2BjAfSJzOXKulCD%2BrDkNVzXW2h9w0xAHR5%2FdOxzFymWLhNxwHSOU4GAIAYsNV%2FI1jl3%2Bi%2F4DoY4sh%2FvJzs5w6pJB9xgy
%2BRwy0ZFa8fKibSSzVtZaNq9xTcYCjW5v6sEAsvt9ywIno9Fj9%2Bj%2FelIR%2BaKguhEk%2FLhrrs67YYGEn7zv96o2v92N%2Fb6PL%2FBeYIiJqiGKX8Ju%2B4kp
%2FdsmAOpPyjo7vtvQifPrwTzCxi4PjL5UZSIXvV0tMEFwUJQqlUQyQIS3ISs1E9ITdFs4C4zvuSdvHMREtMqGJlv37fol3hhDXaWzI6xBGwr6c80wFEPr7EfesEJJTEj8DZ
%2BG1wLfvlDOA3Xa9CXn9KzHFmxfvMJZYReIifdglMZWw42S3C5y9ppjiGOoo0ca0dBp4E8dm5Sim38GUfd%2BVuhekANfuPa5tERbrOAuNAhQzbvtAOSZA6IQv0t5rNiNgOiA
%2BtAxa44jqJrf2kcZTjoJk7oo1VmJWyL%2B3hq3QgdcVXAEcXWM%2BFbAytQcxI%2BFiLYMTTc3M1uKbaCiKRbvuQ
%2BKzckCH6s3q7vl2Ru5uN9ctZM1TVMBpGK3t31BBBa6MWCRApcroPRENUSFJNLCPQCjoXkcRLVraGh8Jlic2sIsT83Hkmb
%2Fmvg3Y9%2FOT9vm2p7x4xOc065vEoUhxbAH0KsATBG29puklwWbNFBI5X0LnK3M2%2Bzr4t%2FVwuYeEvptwQe46hW
%2BdPFQlukRXGhf4RWKueoWZlj0R6g1yjOzvrZAV0JfxMjgSo%2Ff%2B%2BcpO28NCrnOrqghUsXOXxAR9iVNEGYQPK3AX1bM7fdcGma8%2FoI
%2FHeooW9BFg6onilEUMAkXaYcjWmNumVyIdHARiZ3r9zq71H3mdlEHn7Z58s6VF4ZGlEtZrhCmgdnl0wZq9QcJcpLcP7nsvbvpD%2BRCurSQTIY
%2Bm3LVp68%2Fc7RkUlqJ6x66adsw882GcNpRHWfMjuflHwMQ09ZjwY49luhhv6thi2Y%2F5nMDRFox8seKm9shzQwjwZltsjGYF%2FTFpTSyD2YSs7V%2Fob6nanWiH04AFs
%2FZ4zg6foNInKjac6wAV8GEN07guCRwJfTSYTMC5eml9ZVjXE%2Fcv3n%2F7kjslzJtGAL56jqSlTcg80gOJhkn21o5doFAut
%2FCb0%2BOQwTDWz2I1WVaiKe3X4Xw5Y4il1S6WGiaGh8ZEN5%2BphXOVjKUueLs7kS4MHohC8q27B%2FJ3Jw%2BV88LHP3ky4dIjwmzdISJIIFP%2FbLkngadIbNuWl
%2FhFP47quuR%2FgGYbrnanPYyrPyLNdAbbubBdgsyuupS8pBLG3n1rc%2F5GUyddhZeWqtDVz0OPGQaiKUL8M8hJdfzZVO1XjEMn46TyE87Qcgw5ySUBNBce%2FKUxo%2BWS1P
%2Bi3gMrS3d3goCRhOV2z08VQ4m3cmS%2BQaoO7zeCVCYrn3qldhvnIniLV8DLG%2BzBrIH0MDh9SWk
%2B0arJ7FPEUXyDxDj1NxrTM8fUs0BIiiuKP2v6p3rseNt9ZffU96esCek6xVHN1QTakUqSn%2FK9Qg42AeHok3u2%2F14VdZ0g8KDLN
%2F4FoHo2XIOr4JMBvaDbg7QStY6HwSFRwLp4mBrvPpj8pLDrVg4Cj4bsCFpFjlHTzeyBGwjqramRwaQyPqBEZpfAnG81cwiL604Pt5ElxUW9UO2WtrXpsVyZpyvdFtOrQbKy3tU
%2B6kXFKoXfUbYDpQHpZNtZGdV3DPb6QQnmOMpxsD5uZa8t6Eh8Mt%2BK1WvGtUYYa%2BG3D8EWxdzXR2myFF5VyXD
%2B0Sjmf46IfT4pIxcCAWlKwWxkapOuB7TUGgpni2iqIfPg%3D
%3D&RadToolTipCuringa_ClientState=&__VIEWSTATEGENERATOR=A8003BBD&__EVENTVALIDATION=AQKHiMGPI7oS0FQGq5JWeMr9528dkJSUVDlSguuh%2FWszQS
%2B7dmuzHkWnz06kzi5ZU5H8rvWCZik9sxvhBezfY5mNyHmEMsFogViWdY%2Bi2OEH4UWmQuIkZp5fzAW5k2Fll0tI0Rsrmbe9w5twVFVB%2BF8ljzU7hBNQO31RbYOu
%2FLy92Ur1rPhi3XOPC635As3WQOXPmMnukXzy6y
%2BAbPfj5o1oVZqmTZwTxj5os8Gp5gLxS81YukcLFlK1Nv6IkkOnK3FMfo1aGuDxK6WbGBbTuN7%2F6aCqvt1s8KyMkIk8XNV3d4DmTvPI5zgOFU
%2Fsp9t0y7%2F2FyopPoi6gt4xH%2BHAXCgyFbZHd9jnmuIbMFM67N
%2F3AnpYzOSY9Gag3IqjLxGKLdyokPmdT3HvFrg1AhhPi8YR3CMrR4SEzZyj8u2NO9cEvrUfBIbqJ8ZIgVF5bn3K66ZR0Ra41zghfWE
%2B2%2BWonElG8swxO02f192c7bxlYWRZtvD%2Bi47s3Y0%2BjnwKznbiEp7ymCU8Nzae2rTd%2FqB44Om8JcUhk9Vli0w%2FpGzJKXru2rdq1s22jicj75qn
%2FVeUbqloEpdrvw9HRtW2AyAVH%2BlqpHPl0Eox7Yx2mgZz2f%2ByGLarZmukHyOyApdLgrUtkWrym1HOZ0%2Fl
%2FqdeVlzzlVbYddOBS6ZqNQrGeKLFJt8OfE2HpPw4OlWFUnSMWBEeubV6dPOyQYHIcPhAlOXT3GBbwDXYNqNmjjlcAzWjCuHLriXjcr0EsZCu3SMuukzjkBvNwdRQhbqy
%2BENbBRtZW72EOnGMsH78b4HdLAcx5tc5%2BJ9H%2BXizfJxNGW025Ro%2Bv39bkfWAHhZwTEmsSqAgoYq%2BOILVnqqYvUuz8xRqAlHDk9clNCyR%2FSmdhkA1hMrbZ2hCxkDzg
%2FxjZG2OSqzQ9NOYz%2FOylh0SVSWBNuHDHEJi6FofVLFKi%2FffpfGgRA5h7xdwzNaP1ownHJG%2BR2Gjca1VGasE3BO4I
%2BGhWPoxKUXujSu8CqogveKisgGRzngKh6F0qGw4De68qCsWIBdmfN1vUZo5L9cDZl45mJ%2FN1Rw8Jlq%2BcCrMUTrvG5FdE3sj8%2Fp%2FXncY0r9xmGQmemWm2VEaW7kkj
%2BG00LTsxLZXDY3YAWqt1krodBVnXyrNEz%2FGqxGBcIb0a1cllNAHPsBtgOGwccwAJF%2BJqapdmYhzbF4Lm0%3D&TopPane1_ClientState={%22_originalWidth%22%3A
%22%22%2C%22_originalHeight%22%3A%2247px%22%2C%22_collapsedDirection%22%3A1%2C%22_scrollLeft%22%3A0%2C%22_scrollTop%22%3A0%2C
%22_expandedSize%22%3A0%2C%22width%22%3A1022%2C%22height%22%3A47%2C%22collapsed%22%3Afalse%2C%22contentUrl%22%3A%22%22%2C%22minWidth
%22%3A20%2C%22maxWidth%22%3A10000%2C%22minHeight%22%3A47%2C%22maxHeight%22%3A47%2C%22locked%22%3Afalse}
&MainPane_ClientState={%22_originalWidth%22%3A%22%22%2C%22_originalHeight%22%3A%22%22%2C%22_collapsedDirection%22%3A1%2C%22_scrollLeft
%22%3A0%2C%22_scrollTop%22%3A0%2C%22_expandedSize%22%3A0%2C%22width%22%3A1022%2C%22height%22%3A699%2C%22collapsed%22%3Afalse%2C
%22contentUrl%22%3A%22%22%2C%22minWidth%22%3A20%2C%22maxWidth%22%3A10000%2C%22minHeight%22%3A20%2C%22maxHeight%22%3A10000%2C%22locked
%22%3Afalse}&ListDialog_ClientState=&PaneBottomCopyRight_ClientState={%22_originalWidth%22%3A%22%22%2C%22_originalHeight%22%3A%2218px
%22%2C%22_collapsedDirection%22%3A1%2C%22_scrollLeft%22%3A0%2C%22_scrollTop%22%3A0%2C%22_expandedSize%22%3A0%2C%22width%22%3A1022%2C
%22height%22%3A18%2C%22collapsed%22%3Afalse%2C%22contentUrl%22%3A%22%22%2C%22minWidth%22%3A20%2C%22maxWidth%22%3A10000%2C%22minHeight
%22%3A20%2C%22maxHeight%22%3A10000%2C%22locked%22%3Afalse}
&RadWindowLogs_ClientState=&RadWindowManager1_ClientState=&RadMultiPage1_ClientState=&RadTabStrip_ClientState={%22selectedIndexes
%22%3A[%221%22]%2C%22logEntries%22%3A[]%2C%22scrollState%22%3A{}}
&hdnIdSortField=id_leiaute_html&hdnIdSortOrder=ASC&RadGridLeiaute_ClientState=&searchLeiaute=discovery&searchLeiaute_ClientState={%22enab
%22%3Atrue%2C%22emptyMessage%22%3A%22%22%2C%22validationText%22%3A%22discovery%22%2C%22valueAsString%22%3A%22discovery%22%2C
%22lastSetTextBoxValue%22%3A%22discovery%22}&RadToolTipHelp_ClientState=&linkConsultar_ClientState={%22text%22%3A%22Consultar%22%2C
%22value%22%3A%22%22%2C%22checked%22%3Afalse%2C%22target%22%3A%22%22%2C%22navigateUrl%22%3A%22%22%2C%22commandName%22%3A%22%22%2C
%22commandArgument%22%3A%22%22%2C%22autoPostBack%22%3Atrue%2C%22selectedToggleStateIndex%22%3A0%2C%22validationGroup%22%3Anull%2C
%22readOnly%22%3Afalse%2C%22primary%22%3Afalse%2C%22enabled%22%3Atrue}&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl04=%20&RadGridLeiaute
%24ctl00%24ctl02%24ctl02%24ctl05=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl06=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl07=
%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl08=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl09=%20&RadGridLeiaute
%24ctl00%24ctl02%24ctl02%24ctl10=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl11=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl12=
%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl13=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl14=%20&RadGridLeiaute
%24ctl00%24ctl02%24ctl02%24ctl15=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl16=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl17=
%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl19=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl23=%20&RadGridLeiaute
%24ctl00%24ctl02%24ctl02%24ctl20=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl24=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl26=
%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl21=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl27=%20&RadGridLeiaute
%24ctl00%24ctl02%24ctl02%24ctl29=%20&RadGridLeiaute%24ctl00%24ctl03%24ctl01%24ctl02=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl30=

%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl31=%20&RadGridLeiaute%24ctl00%24ctl03%24ctl01%24ctl03=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl32=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl34=%20&RadGridLeiaute%24ctl00%24ctl03%24ctl01%24ctl08=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl35=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl37=%20&RadGridLeiaute%24ctl00%24ctl03%24ctl01%24ctl09=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl38=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl40=%20&RadGridLeiaute%24ctl00%24ctl02%24ctl02%24ctl41=%20&RadGridLeiaute_ctl00_ctl03_ctl01_PageSizeComboBox_ClientState=&RadGridLeiaute%24ctl00%24ctl03%24ctl01%24PageSizeComboBox=10&linkConsultar=Consultar

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

><td align="center" valign="middle" style="width:80px;white-space:nowrap;">Sim</td><td align="center" valign="middle" style="width:80px;white-space:nowrap;">Sim</td><td align="left" valign="middle" style="width:180px;">C:\Docspider\Repositorio_Arquivos\Docspider_SQLServer\LEIAUTE\</td><td align="center" valign="middle" style="width:65px;white-space:nowrap;">Ativo</td><td align="center" valign="middle" style="width:70px;white-space:nowrap;">Liberado</td><td align="cente

* The reflected string on the response webpage indicates that the vulnerability test was successful

Information Gathered (48)

Scan Diagnostics (37)

150042 Server Returns HTTP 5XX Error Code During Scanning (1)

150042 Server Returns HTTP 5XX Error Code During Scanning

Finding #	415448 (69622000)	Severity	Information Gathered - Level 3
Unique #	b5fdf1ab-2857-4778-96d5-36bbeb6a104a		
Group	Scan Diagnostics	Detection Date	11 Jan 2023 18:24 GMT-0400
CWE	CWE-209, CWE-550		
OWASP	A5 Security Misconfiguration		
WASC	WASC-14 SERVER MISCONFIGURATION		

Details

Threat

During the WAS scan, links with HTTP 5xx response code were observed and these are listed in the Results section. The HTTP 5xx message indicates a server error. The list of supported 5xx response code are as below:

500 - Internal Server Error
501 - Not Implemented
502 - Bad Gateway
503 - Service Unavailable
504 - Gateway Timeout
505 - HTTP Version Not Supported

Impact

The presence of a HTTP 5xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depends on responses to detect many vulnerabilities if the link does not respond with an expected response then vulnerabilities present on such links may not be detected.

Solution

Review each link to determine why the server encountered an error when responding to the link. Review and investigate the results of QID 150528 which lists 4xx errors and QID 150019 which lists unexpected response codes.

Results

https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError

150125 File Upload Form Found (1)

WAS Scan Report

150125 File Upload Form Found

Finding #	**439745**(69622011)	**Severity**	Information Gathered - Level 3
Unique #	**1b2c55ca-9189-4f74-b438-86cc928f0214**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

A file upload form found while crawling the web application.

Impact

Without proper safeguards, a file upload form can introduce significant risk to an application.

Solution

Ensure the file upload functionality was implemented securely. See 8 Basic Rules to Implement Secure File Uploads for more information.

Results

https://412-49.docspider.com.br/Generic/Transacao/UploadArquivos/BrowseUploadArquivos.aspx

150018 Connection Error Occurred During Web Application Scan (1)

WAS Scan Report

150018 Connection Error Occurred During Web Application Scan

Finding #	**415435**(69621983)	**Severity**	Information Gathered - Level 2
Unique #	**2463be31-161f-4409-add1-213d71edb052**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following are some of the possible reasons for the timeouts or connection errors:
1. A disturbance in network connectivity between the scanner and the web application occurred.
2. The web server or application server hosting the application was taken down in the midst of a scan.
3. The web application experienced an overload, possibly due to load generated by the scan.
4. An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
5. A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
6. Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

Impact

Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

Solution

First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

Results

Total number of unique links that encountered connection errors: 1
Links with highest number of connection errors:
 1 https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx -FORMDATA- RadScriptManager1_TSM=%3B%3BSystem.Web.Extensions%2C%20Version%3D4.0.0.0%2C%20Culture%3Dneutral%2C%20PublicKeyToken%3D31bf3856ad364e35%3Apt-BR%3Af7ba41a4-e843-4f12-b442-8e407f37c316%3Aea597d4b%3Ab25378d2%3BTelerik.Web.UI%2C%20Version%3D2021.3.1111.45%2C%20Culture%3Dneutral%2C%20PublicKeyToken%3D121fae78165ba3d4%3Apt-BR%3Ab406acc5-0028-4c73-8915-a9da355d848a%3A16e4e7cd%3Aed16cbdc%3A4877f69a%3A33715776%3A8652

Phase wise summary of timeout and connection errors encountered:
ePhaseFormParameterTestsAuth : 0 1

150065 Large Amount of .NET ViewState Data (1)

WAS Scan Report

150065 Large Amount of .NET ViewState Data

Finding #	**438208**(69622013)	**Severity**	Information Gathered - Level 2
Unique #	**f2607c53-fb07-49c4-af55-72e2d7e5ef76**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-16		
OWASP	-		
WASC	-		

Details

Threat

The .NET __VIEWSTATE form field takes up an exceptionally large amount of space in the HTML document.

Impact

Saving large amounts of data in the ViewState field increases the size of a web page and affects the bandwidth used by the Web server and browser.

In some cases, the ViewState field may be tracking data that isn't necessary to tracking state information between requests. In these cases the extra data merely increase the Web page's size without proving any benefit to the application's performance or usability. Consequently, the use of ViewState may be detrimental to the site's performance.

Solution

Review the application's use of the ViewState property in each of its forms to ensure unnecessary data is not being serialized.

Results

Size of encoded VIEWSTATE: 93592 bytes
Exceeds threshold of 65535 bytes
URI: https://412-49.docspider.com.br/workflow/cadastros/calendarios/FrmCadastroDiasNaoUteis.aspx?idcalendario=1

Size of encoded VIEWSTATE: 121408 bytes
Exceeds threshold of 65535 bytes
URI: https://412-49.docspider.com.br/Workflow/Transacao/ExportacaoImportacaoTipoProcesso.aspx

Size of encoded VIEWSTATE: 96704 bytes
Exceeds threshold of 65535 bytes
URI: https://412-49.docspider.com.br/workflow/cadastros/calendarios/FrmCadastroDiasNaoUteis.aspx?idcalendario=1

Size of encoded VIEWSTATE: 96704 bytes
Exceeds threshold of 65535 bytes
URI: https://412-49.docspider.com.br/workflow/cadastros/calendarios/FrmCadastroDiasNaoUteis.aspx?idcalendario=1

150375 PII Fields Found (1)

150375 PII Fields Found

Finding #	**415453**(69622007)
Unique #	**add1040a-097b-4547-b4a5-ae4a3c4af031**

Severity	Information Gathered - Level 2

Group	Scan Diagnostics
CWE	CWE-359
OWASP	A2 Cryptographic Failures
WASC	WASC-13 INFORMATION LEAKAGE

Detection Date	11 Jan 2023 18:24 GMT-0400

Details

Threat

Personally Identifiable Information(PII) is found on the form(s) on the Web Application.

Impact

Improper handling of the PII can lead to loss of reputation for the organization and the individuals whose personal information is stored. Attackers can use this information for more focused attacks in the future.

Solution

Please review all the PII fields below in the report and if required, PII should be obtained by lawful and fair means.

Results

Parent URI: https://412-49.docspider.com.br/Login

PII fields Found:
Login Name
Password

Parent URI: https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx

PII fields Found:
Email

Parent URI: https://412-49.docspider.com.br/Workflow/Consultas/MonitorGrafico/Web/ProcessMonitor.aspx

PII fields Found:
Login Name

Parent URI: https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx

PII fields Found:
Email

Parent URI: https://412-49.docspider.com.br/GED/Cadastros/TiposDeOpiniaoDeDocumento/BrowseCadastroTiposDeOpiniao.aspx

PII fields Found:
Password

Parent URI: https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx

PII fields Found:
Email

Parent URI: https://412-49.docspider.com.br/GED/Cadastros/TiposDeOpiniaoDeDocumento/BrowseCadastroTiposDeOpiniao.aspx

PII fields Found:
Password

6 DNS Host Name (1)

WAS Scan Report

6 DNS Host Name

Finding #	415467(69621988)
Unique #	e2480d98-24ad-48c5-bf8f-c9b64f3eb07b

Severity	Information Gathered - Level 1
Detection Date	11 Jan 2023 18:24 GMT-0400

Group	Scan Diagnostics
CWE	-
OWASP	-
WASC	-

Details

Threat

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	-
IP	131.161.43.118
Port	-
Result	#table IP_address Host_name 131.161.43.118 No_registered_hostname

38116 SSL Server Information Retrieval (1)

WAS Scan Report

38116 SSL Server Information Retrieval

Finding #	**415474**(69622028)	**Severity**	Information Gathered - Level 1
Unique #	**b7c3a2f8-da82-4306-85c7-a75bc3043c59**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	412-49.docspider.com.br
IP	131.161.43.118
Port	443
Result	#table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ TLSv1_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1 COMPRESSION_METHOD None _ _ _ RC4-MD5 RSA R MD5 RC4(128) MEDIUM RC4-SHA RSA RSA SHA1 RC4(128) MEDIUM IDEA-CBC-SHA RSA RSA SHA1 IDEA(128) MEDIUM DES-CBC3-SHA RSA RSA S 3DES(168) MEDIUM EDH-RSA-DES-CBC3-SHA DH RSA SHA1 3DES(168) MEDIUM AES128-SHA RSA RSA SHA1 AES(128) MEDIUM DHE-RSA-AES12& SHA DH RSA SHA1 AES(128) MEDIUM AES256-SHA RSA RSA SHA1 AES(256) HIGH DHE-RSA-AES256-SHA DH RSA SHA1 AES(256) HIGH CAMELLI/ SHA RSA RSA SHA1 Camellia(128) MEDIUM DHE-RSA-CAMELLIA128-SHA DH RSA SHA1 Camellia(128) MEDIUM CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH DHE-RSA-CAMELLIA256-SHA DH RSA SHA1 Camellia(256) HIGH SEED-SHA RSA RSA SHA1 SEED(128) MEDIUM DHE-RSA-SEEC SHA DH RSA SHA1 SEED(128) MEDIUM ECDHE-RSA-RC4-SHA ECDH RSA SHA1 RC4(128) MEDIUM ECDHE-RSA-DES-CBC3-SHA ECDH RSA SHA1 3DES(168) MEDIUM ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH AEC RC4-SHA ECDH None SHA1 RC4(128) MEDIUM AECDH-DES-CBC3-SHA ECDH None SHA1 3DES(168) MEDIUM AECDH-AES128-SHA ECDH None SH/ AES(128) MEDIUM AECDH-AES256-SHA ECDH None SHA1 AES(256) HIGH TLSv1.1_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1.1 COMPRESSION_METHOD None _ _ _ RC4-MD5 RSA RSA MD5 RC4(128) MEDIUM RC4-SHA RSA RSA SHA1 RC4(128) MEDIUM IDEA-CBC-SHA RSA SHA1 IDEA(128) MEDIUM DES-CBC3-SHA RSA RSA SHA1 3DES(168) MEDIUM EDH-RSA-DES-CBC3-SHA DH RSA SHA1 3DES(168) MEDIUM AES12& SHA RSA RSA SHA1 AES(128) MEDIUM DHE-RSA-AES128-SHA DH RSA SHA1 AES(128) MEDIUM AES256-SHA RSA RSA SHA1 AES(256) HIGH DHE- AES256-SHA DH RSA SHA1 AES(256) HIGH CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM DHE-RSA-CAMELLIA128-SHA DH RSA SHA1 Camellia(128) MEDIUM CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH DHE-RSA-CAMELLIA256-SHA DH RSA SHA1 Camellia(256) HIGH SEEL SHA RSA RSA SHA1 SEED(128) MEDIUM DHE-RSA-SEED-SHA DH RSA SHA1 SEED(128) MEDIUM ECDHE-RSA-RC4-SHA ECDH RSA SHA1 RC4(128 MEDIUM ECDHE-RSA-DES-CBC3-SHA ECDH RSA SHA1 3DES(168) MEDIUM ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM ECDHE RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH AECDH-RC4-SHA ECDH None SHA1 RC4(128) MEDIUM AECDH-DES-CBC3-SHA ECDH None SH/ 3DES(168) MEDIUM AECDH-AES128-SHA ECDH None SHA1 AES(128) MEDIUM AECDH-AES256-SHA ECDH None SHA1 AES(256) HIGH TLSv1.2_PROTOCOL_IS_ENABLED _ _ _ _ _ TLSv1.2 COMPRESSION_METHOD None _ _ _ RC4-MD5 RSA RSA MD5 RC4(128) MEDIUM RC4-SHA RS RSA SHA1 RC4(128) MEDIUM IDEA-CBC-SHA RSA RSA SHA1 IDEA(128) MEDIUM DES-CBC3-SHA RSA RSA SHA1 3DES(168) MEDIUM EDH-RSA-DE CBC3-SHA DH RSA SHA1 3DES(168) MEDIUM AES128-SHA RSA RSA SHA1 AES(128) MEDIUM DHE-RSA-AES128-SHA DH RSA SHA1 AES(128) MED AES256-SHA RSA RSA SHA1 AES(256) HIGH DHE-RSA-AES256-SHA DH RSA SHA1 AES(256) HIGH CAMELLIA128-SHA RSA RSA SHA1 Camellia(128 MEDIUM DHE-RSA-CAMELLIA128-SHA DH RSA SHA1 Camellia(128) MEDIUM DHE-RSA-AES128-SHA256 DH RSA SHA256 AES(128) MEDIUM DHE-R§ AES256-SHA256 DH RSA SHA256 AES(256) HIGH CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH DHE-RSA-CAMELLIA256-SHA DH RSA SH/ Camellia(256) HIGH SEED-SHA RSA RSA SHA1 SEED(128) MEDIUM DHE-RSA-SEED-SHA DH RSA SHA1 SEED(128) MEDIUM AES128-GCM-SHA256 I RSA AEAD AESGCM(128) MEDIUM AES256-GCM-SHA384 RSA RSA AEAD AESGCM(256) HIGH DHE-RSA-AES128-GCM-SHA256 DH RSA AEAD AESGCM(128) MEDIUM DHE-RSA-AES256-GCM-SHA384 DH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-RC4-SHA ECDH RSA SHA1 RC4(128) MED

ECDHE-RSA-DES-CBC3-SHA ECDH RSA SHA1 3DES(168) MEDIUM ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES(128) MEDIUM ECDHE-RSA-AE SHA ECDH RSA SHA1 AES(256) HIGH AECDH-RC4-SHA ECDH None SHA1 RC4(128) MEDIUM AECDH-DES-CBC3-SHA ECDH None SHA1 3DES(168 MEDIUM AECDH-AES128-SHA ECDH None SHA1 AES(128) MEDIUM AECDH-AES256-SHA ECDH None SHA1 AES(256) HIGH ECDHE-RSA-AES128- SHA256 ECDH RSA SHA256 AES(128) MEDIUM ECDHE-RSA-AES256-SHA384 ECDH RSA SHA384 AES(256) HIGH ECDHE-RSA-AES128-GCM-SHA2 ECDH RSA AEAD AESGCM(128) MEDIUM ECDHE-RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH AES128-SHA256 RSA RSA SH, AES(128) MEDIUM AES256-SHA256 RSA RSA SHA256 AES(256) HIGH TLSv1.3_PROTOCOL_IS_DISABLED _ _ _ _ _

WAS Scan Report

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
RC4-MD5	RSA	RC4(128)	MEDIUM	RSA	MD5	TLSv1
RC4-SHA	RSA	RC4(128)	MEDIUM	RSA	SHA1	TLSv1
IDEA-CBC-SHA	RSA	IDEA(128)	MEDIUM	RSA	SHA1	TLSv1
DES-CBC3-SHA	RSA	3DES(168)	MEDIUM	RSA	SHA1	TLSv1
EDH-RSA-DES-CBC3-SHA	RSA	3DES(168)	MEDIUM	DH	SHA1	TLSv1
AES128-SHA	RSA	AES(128)	MEDIUM	RSA	SHA1	TLSv1
DHE-RSA-AES128-SHA	RSA	AES(128)	MEDIUM	DH	SHA1	TLSv1
AES256-SHA	RSA	AES(256)	HIGH	RSA	SHA1	TLSv1
DHE-RSA-AES256-SHA	RSA	AES(256)	HIGH	DH	SHA1	TLSv1
CAMELLIA128-SHA	RSA	Camellia(128)	MEDIUM	RSA	SHA1	TLSv1
DHE-RSA-CAMELLIA128-SHA	RSA	Camellia(128)	MEDIUM	DH	SHA1	TLSv1
CAMELLIA256-SHA	RSA	Camellia(256)	HIGH	RSA	SHA1	TLSv1
DHE-RSA-CAMELLIA256-SHA	RSA	Camellia(256)	HIGH	DH	SHA1	TLSv1
SEED-SHA	RSA	SEED(128)	MEDIUM	RSA	SHA1	TLSv1
DHE-RSA-SEED-SHA	RSA	SEED(128)	MEDIUM	DH	SHA1	TLSv1
ECDHE-RSA-RC4-SHA	RSA	RC4(128)	MEDIUM	ECDH	SHA1	TLSv1
ECDHE-RSA-DES-CBC3-SHA	RSA	3DES(168)	MEDIUM	ECDH	SHA1	TLSv1
ECDHE-RSA-AES128-SHA	RSA	AES(128)	MEDIUM	ECDH	SHA1	TLSv1
ECDHE-RSA-AES256-SHA	RSA	AES(256)	HIGH	ECDH	SHA1	TLSv1
AECDH-RC4-SHA	None	RC4(128)	MEDIUM	ECDH	SHA1	TLSv1

WAS Scan Report

Info List

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
AECDH-DES-CBC3-SHA	None	3DES(168)	MEDIUM	ECDH	SHA1	TLSv1
AECDH-AES128-SHA	None	AES(128)	MEDIUM	ECDH	SHA1	TLSv1
AECDH-AES256-SHA	None	AES(256)	HIGH	ECDH	SHA1	TLSv1

WAS Scan Report

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
RC4-MD5	RSA	RC4(128)	MEDIUM	RSA	MD5	TLSv1.1
RC4-SHA	RSA	RC4(128)	MEDIUM	RSA	SHA1	TLSv1.1
IDEA-CBC-SHA	RSA	IDEA(128)	MEDIUM	RSA	SHA1	TLSv1.1
DES-CBC3-SHA	RSA	3DES(168)	MEDIUM	RSA	SHA1	TLSv1.1
EDH-RSA-DES-CBC3-SHA	RSA	3DES(168)	MEDIUM	DH	SHA1	TLSv1.1
AES128-SHA	RSA	AES(128)	MEDIUM	RSA	SHA1	TLSv1.1
DHE-RSA-AES128-SHA	RSA	AES(128)	MEDIUM	DH	SHA1	TLSv1.1
AES256-SHA	RSA	AES(256)	HIGH	RSA	SHA1	TLSv1.1
DHE-RSA-AES256-SHA	RSA	AES(256)	HIGH	DH	SHA1	TLSv1.1
CAMELLIA128-SHA	RSA	Camellia(128)	MEDIUM	RSA	SHA1	TLSv1.1
DHE-RSA-CAMELLIA128-SHA	RSA	Camellia(128)	MEDIUM	DH	SHA1	TLSv1.1
CAMELLIA256-SHA	RSA	Camellia(256)	HIGH	RSA	SHA1	TLSv1.1
DHE-RSA-CAMELLIA256-SHA	RSA	Camellia(256)	HIGH	DH	SHA1	TLSv1.1
SEED-SHA	RSA	SEED(128)	MEDIUM	RSA	SHA1	TLSv1.1
DHE-RSA-SEED-SHA	RSA	SEED(128)	MEDIUM	DH	SHA1	TLSv1.1
ECDHE-RSA-RC4-SHA	RSA	RC4(128)	MEDIUM	ECDH	SHA1	TLSv1.1
ECDHE-RSA-DES-CBC3-SHA	RSA	3DES(168)	MEDIUM	ECDH	SHA1	TLSv1.1
ECDHE-RSA-AES128-SHA	RSA	AES(128)	MEDIUM	ECDH	SHA1	TLSv1.1
ECDHE-RSA-AES256-SHA	RSA	AES(256)	HIGH	ECDH	SHA1	TLSv1.1
AECDH-RC4-SHA	None	RC4(128)	MEDIUM	ECDH	SHA1	TLSv1.1

WAS Scan Report

Info List

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
AECDH-DES-CBC3-SHA	None	3DES(168)	MEDIUM	ECDH	SHA1	TLSv1.1
AECDH-AES128-SHA	None	AES(128)	MEDIUM	ECDH	SHA1	TLSv1.1
AECDH-AES256-SHA	None	AES(256)	HIGH	ECDH	SHA1	TLSv1.1

WAS Scan Report

Info List

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
RC4-MD5	RSA	RC4(128)	MEDIUM	RSA	MD5	TLSv1.2
RC4-SHA	RSA	RC4(128)	MEDIUM	RSA	SHA1	TLSv1.2
IDEA-CBC-SHA	RSA	IDEA(128)	MEDIUM	RSA	SHA1	TLSv1.2
DES-CBC3-SHA	RSA	3DES(168)	MEDIUM	RSA	SHA1	TLSv1.2
EDH-RSA-DES-CBC3-SHA	RSA	3DES(168)	MEDIUM	DH	SHA1	TLSv1.2
AES128-SHA	RSA	AES(128)	MEDIUM	RSA	SHA1	TLSv1.2
DHE-RSA-AES128-SHA	RSA	AES(128)	MEDIUM	DH	SHA1	TLSv1.2
AES256-SHA	RSA	AES(256)	HIGH	RSA	SHA1	TLSv1.2
DHE-RSA-AES256-SHA	RSA	AES(256)	HIGH	DH	SHA1	TLSv1.2
CAMELLIA128-SHA	RSA	Camellia(128)	MEDIUM	RSA	SHA1	TLSv1.2
DHE-RSA-CAMELLIA128-SHA	RSA	Camellia(128)	MEDIUM	DH	SHA1	TLSv1.2
DHE-RSA-AES128-SHA256	RSA	AES(128)	MEDIUM	DH	SHA256	TLSv1.2
DHE-RSA-AES256-SHA256	RSA	AES(256)	HIGH	DH	SHA256	TLSv1.2
CAMELLIA256-SHA	RSA	Camellia(256)	HIGH	RSA	SHA1	TLSv1.2
DHE-RSA-CAMELLIA256-SHA	RSA	Camellia(256)	HIGH	DH	SHA1	TLSv1.2
SEED-SHA	RSA	SEED(128)	MEDIUM	RSA	SHA1	TLSv1.2
DHE-RSA-SEED-SHA	RSA	SEED(128)	MEDIUM	DH	SHA1	TLSv1.2
AES128-GCM-SHA256	RSA	AESGCM(128)	MEDIUM	RSA	AEAD	TLSv1.2
AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	RSA	AEAD	TLSv1.2

WAS Scan Report

Info List

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
DHE-RSA-AES128-GCM-SHA256	RSA	AESGCM(128)	MEDIUM	DH	AEAD	TLSv1.2
DHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	DH	AEAD	TLSv1.2
ECDHE-RSA-RC4-SHA	RSA	RC4(128)	MEDIUM	ECDH	SHA1	TLSv1.2
ECDHE-RSA-DES-CBC3-SHA	RSA	3DES(168)	MEDIUM	ECDH	SHA1	TLSv1.2
ECDHE-RSA-AES128-SHA	RSA	AES(128)	MEDIUM	ECDH	SHA1	TLSv1.2
ECDHE-RSA-AES256-SHA	RSA	AES(256)	HIGH	ECDH	SHA1	TLSv1.2
AECDH-RC4-SHA	None	RC4(128)	MEDIUM	ECDH	SHA1	TLSv1.2
AECDH-DES-CBC3-SHA	None	3DES(168)	MEDIUM	ECDH	SHA1	TLSv1.2
AECDH-AES128-SHA	None	AES(128)	MEDIUM	ECDH	SHA1	TLSv1.2
AECDH-AES256-SHA	None	AES(256)	HIGH	ECDH	SHA1	TLSv1.2
ECDHE-RSA-AES128-SHA256	RSA	AES(128)	MEDIUM	ECDH	SHA256	TLSv1.2
ECDHE-RSA-AES256-SHA384	RSA	AES(256)	HIGH	ECDH	SHA384	TLSv1.2
ECDHE-RSA-AES128-GCM-SHA256	RSA	AESGCM(128)	MEDIUM	ECDH	AEAD	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	ECDH	AEAD	TLSv1.2
AES128-SHA256	RSA	AES(128)	MEDIUM	RSA	SHA256	TLSv1.2
AES256-SHA256	RSA	AES(256)	HIGH	RSA	SHA256	TLSv1.2

38291 SSL Session Caching Information (1)

38291 SSL Session Caching Information

Finding #	**415470**(69622024)
Unique #	**205114da-cb69-4360-9d84-4e9ed21323c0**

Severity	Information Gathered - Level 1

Group	Scan Diagnostics
CWE	-
OWASP	-
WASC	-

Detection Date	11 Jan 2023 18:24 GMT-0400

Details

Threat

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

Impact

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	412-49.docspider.com.br
IP	131.161.43.118
Port	443
Result	TLSv1 session caching is enabled on the target. TLSv1.1 session caching is enabled on the target. TLSv1.2 session caching is enabled on the target.

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (1)

WAS Scan Report

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

Finding #	415472(69622026)	**Severity**	Information Gathered - Level 1
Unique #	95cbe900-29a0-4f73-a542-487cbfd0c073		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	412-49.docspider.com.br
IP	131.161.43.118
Port	443
Result	#table cols=2 my_version target_version 0304 0303 0399 0303 0400 0303 0499 0303

38609 SSL Server default Diffie-Hellman prime information (1)

WAS Scan Report

38609 SSL Server default Diffie-Hellman prime information

Finding #	**415473**(69622027)	**Severity**	Information Gathered - Level 1
Unique #	**5506fe87-3c48-414e-a455-d6ccbbe5d587**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Diffie-Hellman is a popular cryptographic algorithm used by SSL/TLS. - For fixed primes: 1024 and below are considered unsafe. - For variable primes: 512 is unsafe. 768 is probably mostly safe, but might not be for long. 1024 and above are considered safe.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	412-49.docspider.com.br
IP	131.161.43.118
Port	443
Result	SSL server default to use Diffie-Hellman key exchange method with variable 2048(bits) prime

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (1)

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

Finding #	**415475**(69622029)	**Severity**	Information Gathered - Level 1
Unique #	**103be54b-616f-43c5-97ac-11416d915497**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes and strengths.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	412-49.docspider.com.br
IP	131.161.43.118
Port	443
Result	#table cols="6" NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1 _ _ _ _ _ RSA _ 2048 no 110 lov _ 2048 yes 110 low ECDHE secp256r1 256 yes 128 low ECDHA secp256r1 256 yes 128 low TLSv1.1 _ _ _ _ _ RSA _ 2048 no 110 low DHE _ 2048 yes 11 ECDHE secp256r1 256 yes 128 low ECDHA secp256r1 256 yes 128 low TLSv1.2 _ _ _ _ _ RSA _ 2048 no 110 low DHE _ 2048 yes 110 low ECDHE secp2 256 yes 128 low ECDHA secp256r1 256 yes 128 low

WAS Scan Report

Info List

Info #1

Kexs

Kex	Group	Protocol	Key Size	Fwd Sec	Classical	Quantam
RSA		TLSv1	2048	no	110	low
DHE		TLSv1	2048	yes	110	low
ECDHE		TLSv1	256	yes	128	low
ECDHA		TLSv1	256	yes	128	low
RSA		TLSv1.1	2048	no	110	low
DHE		TLSv1.1	2048	yes	110	low
ECDHE		TLSv1.1	256	yes	128	low
ECDHA		TLSv1.1	256	yes	128	low
RSA		TLSv1.2	2048	no	110	low
DHE		TLSv1.2	2048	yes	110	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHA		TLSv1.2	256	yes	128	low

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (1)

WAS Scan Report

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties

Finding #	415476(69622030)	**Severity**	Information Gathered - Level 1
Unique #	435616a7-d75c-4a0d-aca6-c8956643277c		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following is a list of detected SSL/TLS protocol properties.

Impact

Items include:
- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	412-49.docspider.com.br
IP	131.161.43.118
Port	443
Result	#table cols="2" NAME STATUS TLSv1 _ Extended_Master_Secret no Encrypt_Then_MAC no Heartbeat yes Truncated_HMAC no Cipher_priority_controlle server OCSP_stapling no SCT_extension no TLSv1.1 _ Extended_Master_Secret no Encrypt_Then_MAC no Heartbeat yes Truncated_HMAC no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no TLSv1.2 _ Extended_Master_Secret no Encrypt_Then_MAC no Heartbeat yes Truncated_HMAC no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no

WAS Scan Report

Info List

Info #1

Props

Name	Value	Protocol
Extended Master Secret	no	TLSv1
Encrypt Then MAC	no	TLSv1
Heartbeat	yes	TLSv1
Truncated HMAC	no	TLSv1
Cipher priority controlled by	server	TLSv1
OCSP stapling	no	TLSv1
SCT extension	no	TLSv1
Extended Master Secret	no	TLSv1.1
Encrypt Then MAC	no	TLSv1.1
Heartbeat	yes	TLSv1.1
Truncated HMAC	no	TLSv1.1
Cipher priority controlled by	server	TLSv1.1
OCSP stapling	no	TLSv1.1
SCT extension	no	TLSv1.1
Extended Master Secret	no	TLSv1.2
Encrypt Then MAC	no	TLSv1.2
Heartbeat	yes	TLSv1.2
Truncated HMAC	no	TLSv1.2
Cipher priority controlled by	server	TLSv1.2
OCSP stapling	no	TLSv1.2
SCT extension	no	TLSv1.2

42350 TLS Secure Renegotiation Extension Support Information (1)

42350 TLS Secure Renegotiation Extension Support Information

Finding #	**415471**(69622025)	**Severity**	Information Gathered - Level 1
Unique #	**f2d44b91-10a2-4c03-b94d-2bc08376d79f**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	412-49.docspider.com.br
IP	131.161.43.118
Port	443
Result	TLS Secure Renegotiation Extension Status: supported.

45038 Host Scan Time - Scanner (1)

WAS Scan Report

45038 Host Scan Time - Scanner

Finding #	**415455**(69622010)	**Severity**	Information Gathered - Level 1
Unique #	**f5c05972-3d5e-4193-8342-c3413acc2f2a**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

Impact

N/A

Solution

N/A

Results

Scan duration: 42914 seconds

Start time: Wed, Jan 11 2023, 21:23:58 GMT

End time: Thu, Jan 12 2023, 09:19:12 GMT

86002 SSL Certificate - Information (1)

WAS Scan Report

86002 SSL Certificate - Information

Finding #	415468(69622023)	**Severity**	Information Gathered - Level 1
Unique #	86f95c32-dc1c-4674-a6db-5e5c9d74cac3		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

SSL certificate information is provided in the Results section.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	412-49.docspider.com.br
IP	131.161.43.118
Port	443
Result	#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _03:13:a1:88:65:cb:df:c4:fe:39:cf:8d:38:32:d1:d1_ (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName US _organizationName DigiCert_Inc _organizationalUnitName www.digicert.com _commonName GeoTrust_RSA_CA_2018 (0)SUBJECT_NAME _ countryName BR _stateOrProvinceName Santa_Catarina _localityNam JOINVILLE _organizationName DOCSPIDER_SOFTWARE_S.A. _commonName *.docspider.com.br (0)Valid_From Jul_11_00:00:00_2022_GMT (0)Valid_ Aug_11_23:59:59_2023_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0) _00:b4:0b:48:eb:18:f2:b6:b2:3c:ed:ef:79:58:f8: (0) _1e:7c:d7:e9:dc:bd:1d:66:3e:a6:57:c5:a2:0e:a6: (0) _af:ee:a5:5c:56:38:96:38:7b:0b:ea:48:4a:da:e3: (0) _4 64:4b:a6:54:8f:62:16:c6:c7:ea:26:d4:78:1e: (0) _2d:cd:1e:8f:ad:f0:f0:2f:e7:ca:09:c8:b9:a2:24: (0) _02:75:ec:f8:ae:77:90:f9:a8:f8:05:93:02:76:9d: (0) _7e:ca: 3f:ec:d8:a3:6e:8d:df:ae:57:d4:bf:0f:71: (0) _0a:a1:57:2a:6a:a9:d5:51:3d:ba:d9:69:79:bb:2f: (0) _60:ea:75:d6:b0:23:b8:1e:fe:93:e9:62:7e:b4:05: (0) _28:ac:7d 98:5f:fd:f8:97:64:89:f7:8e:c8: (0) _c4:b4:e5:28:a8:58:b6:6f:2b:ff:28:ce:24:43:6f: (0) _68:ef:84:6e:8a:a1:a1:ec:14:c9:18:d3:ed:06:2f: (0) _e5:e9:c0:7b:c2:7f:b0:3b:d6:7e:cb:ff:2a:05:26: (0) _99:74:ec:6f:12:b1:a1:3a:22:10:f8:d7:20:f9:2e: (0) _44:f0:60:e8:08:14:34:72:07:ac:c5:58:21:15:bb: (0) _93:1d:bf:ec:cb:a1:cc:af:82:05:90:41:c2:bd:3b: (0) _26:4c:1f:7c:aa:22:0a:78:f3:98:9e:40:6a:bc:6a: (0) _f3:33 (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _ (0)X509v3_Authority_Key_Identifier _keyid:90:58:FF:B0:9C:75:A8:51:54:77:B1:ED:F2:A3:43:16:38:9E:6C:C5 (0)X509v3_Subject_Key_Identifier _AF:1E:35:1B:47:47:96:56:DA:2F:A7:E2:46:D5:7E:1C:ED:0E:7C:0D (0)X509v3_Subject_Alternative_Name _DNS:*.docspider.com.br,_DNS:docspider.com.br (0)X509v3_Key_Usage critical (0) _Digital_Signature,_Key_Encipherment (0)X509v3_Extended_Key_Us _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://cdp.geotrust.com GeoTrustRSACA2018.crl (0)X509v3_Certificate_Policies _Policy:_2.23.140.1.2.2 (0) _CPS:_http://www.digicert.com/CPS (0)Authority_Information_Access _OCSP_-_URI:http://status.geotrust.com (0) _CA_Issuers_-_URI:http://cacerts.geotrust.com/GeoTrustRSACA2018.crt (0)X509v3_Basic_Constraints _CA:F (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_AD:F7:BE:FA:7C:FF:10:C8:8B:9D:3D:9C:1E:3E:18:6A _B4:67:29:5D:CF:B1:0C:24:CA:85:86:34:EB:DC:82:8A (0) _Timestamp_:_Jul_11_16:12:54.223_2022_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa- SHA256 (0) _30:45:02:21:00:B6:2C:32:A1:2B:5B:6F:3C:3D:EF:17: (0) _0B:B5:C5:EC:FF:8F:E5:4E:3F:EB:A3:FD:CE:EB:03:46: (0) _3A:89:1E: 97:05:02:20:51:93:D3:78:6B:F1:5C:42:55: (0) _65:AB:B1:96:3E:C8:A0:B1:8B:66:58:21:C2:C1:65:5C: (0) _22:02:E6:0F:6D:ED:8A (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_35:CF:19:1B:BF:B1:6C:57:BF:0F:AD:4C:6D:42:CB:BB: (0) _B6:27:20:26:51:EA: 3F:E1:2A:EF:A8:03:C3:3B:D6:4C (0) _Timestamp_:_Jul_11_16:12:54.215_2022_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:44:02:20:03:20:FE:60:71:24:92:4E:E3:BC:04:54: (0) _2B:21:32:F1:85:FF:D2:27:34:C3:19:EA:8E:53:8C:83: (0) _AA:D1:12:A6:02:20:00:A2:E8:18:B4:72:1B:AF:CA:F3: (0) _04:54:3E:3C:15:AD:68:3E:49:3A:38:7C:61:ED:BA:5C: (0) _58:81:B3:D4:E1:04 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_B3:73:77:07:E1:84:50:F8:63:86:D6:05:A9:DC:11:09: (0) _4A:79:2D:B1:67:0C:0B: 87:DC:F0:03:0E:79:36:A5:9A (0) _Timestamp_:_Jul_11_16:12:54.259_2022_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:44:02:20:4C:FC:CE:0C:11:CD:25:61:F7:78:E5:AD: (0) _D4:BE:7C:EE:80:3E:B9:0C:C6:23:57:26:68:FE:E7:35: (0) _48:C3:8D:86:02:20:6C:96:46:87:6A: 4F:B9:87:CF:D8: (0) _FF:F9:E4:40:24:D1:B3:22:B3:3B:BA:3A:99:8F:95:E7: (0) _B4:AA:C9:D6:DA:FF (0)Signature (256_octets) (0) 08:ed:78:a0:59:99:f5:d9: 91:89:27:0b:12:ec (0) c5:b9:70:02:db:0a:53:3b:aa:66:2c:fd:25:b4:44:42 (0) 5e:e4:c4:52:25:99:95:bf:24:35:ed:5f:24:22:6a:a0 (0) ce:aa:aa: 2d:b0:90:f1:48:45:96:a2:f4:30:86:29:45 (0) a1:8e:de:ad:77:12:f6:71:cd:01:ad:6a:bc:ca:7c:a3 (0) 86:29:66:9e:f3:35:11:c3:8c:2b:b2:15:f0:4c:32:36 (0) 90:af:c2:78:0c:c5:10:04:78:e8:34:3e:64:1a:4e:30 (0) 39:d2:6b:50:35:e4:66:14:c5:49:29:fb:9f:48:8c:fc (0) 20:a7:bb:75:b0:7d:9e:25:74:46:39:6f:c6:27:45:08 (0 e0:8f:c2:3d:c2:f1:54:ef:1b:e1:7f:6d:f3:63:34:de (0) 5b:fb:5c:11:a1:f2:b5:d4:57:89:72:6e:66:c9:ee:70 (0) 2a:2c:e9:64:51:d9:7a:f2:7e:28:76:12:ee:a3:4a:9d (0) b0:a6:be:7f:60:f6:6c:d4:a5:90:d9:84:49:e8:c5:b0 (0) ab:cb:17:bb:0a:73:ae:7e:c7:cd:9f:31:96:f7:79:45 (0) e5:04:22:15:2a:41:ad:9c:0d:ea:de:0b:b0:29:2c:36 (0 8d:d2:62:ef:6a:d4:f0:0f:9d:81:30:0a:89:fb:33

WAS Scan Report

Info List

Info #1

Certificate Fingerprint:B0E5168FBABE0776E1CCA450548947A104BF33650A7AE8906EFC5CF55688B765

150007 Web Application Authentication Method (1)

150007 Web Application Authentication Method

Finding #	**415459**(69622015)	Severity	Information Gathered - Level 1
Unique #	**9123330d-7c98-44e6-b5d5-e868f3a80c87**		
Group	Scan Diagnostics	Detection Date	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Web application authentication was performed for the scan. The Results section includes a list of authentication credentials used.

Impact

N/A

Solution

N/A

Results

Auth successful against form: https://412-49.docspider.com.br/Login
Web Application Authentication Record: Form Auth Record form, #56163
User Name: luis

150009 Links Crawled (1)

WAS Scan Report

▪	**150009 Links Crawled**		

Finding #	**415464**(69622019)	**Severity**	Information Gathered - Level 1
Unique #	**6da8a297-dd42-463c-9032-57647c8b0b6c**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
 - All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

Impact

N/A

Solution

N/A

Results

Duration of crawl phase (seconds): 2925.00
Number of links: 180
(This number excludes form requests and links re-requested during authentication.)

https://41-9.docspider.com.br/PortalDocumentos/UltimasAtualizacoes
https://412-49.docspider.com.br/
https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=13
https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=154
https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=19
https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=33
https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=53
https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=55
https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=56
https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=64
https://412-49.docspider.com.br/Assets/Images/16x16/application_form_magnify.png
https://412-49.docspider.com.br/Assets/Images/16x16/arrow_refresh_small.png
https://412-49.docspider.com.br/Assets/Images/16x16/cancel_disable.png
https://412-49.docspider.com.br/Assets/Images/16x16/draw_eraser.png
https://412-49.docspider.com.br/Assets/Images/16x16/export_excel.png
https://412-49.docspider.com.br/Assets/Images/16x16/file_extension_log.png
https://412-49.docspider.com.br/Assets/Images/16x16/help.png
https://412-49.docspider.com.br/Assets/Images/16x16/menu.png
https://412-49.docspider.com.br/Assets/Images/seta-para-direita.png
https://412-49.docspider.com.br/Assets/Images/seta-para-esquerda.png
https://412-49.docspider.com.br/Ativar
https://412-49.docspider.com.br/Busca/AgendamentoIndexacao
https://412-49.docspider.com.br/Busca/ConfiguracaoGeralBusca
https://412-49.docspider.com.br/Busca/PainelControleIndexacao
https://412-49.docspider.com.br/Busca/PainelExecucaoSentencaBusca
https://412-49.docspider.com.br/Busca/PalavraIrrelevante
https://412-49.docspider.com.br/Busca/PalavraIrrelevante/Buscar
https://412-49.docspider.com.br/Busca/RelevanciaOrdenacaoBusca
https://412-49.docspider.com.br/Busca/Sinonimo
https://412-49.docspider.com.br/Buscar
https://412-49.docspider.com.br/Clientes/DocspiderSQL/Default.htm
https://412-49.docspider.com.br/Default.htm
https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx
https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx
https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx
https://412-49.docspider.com.br/GED/Cadastros/PontosDeControle/BrowseCadastroClassPontosControle.aspx
https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx

https://412-49.docspider.com.br/GED/Cadastros/TiposDeDocumento/BrowseCadastroTiposDeDocumento.aspx
https://412-49.docspider.com.br/GED/Cadastros/TiposDeIndexador/BrowseCadastroTiposIndexador.aspx
https://412-49.docspider.com.br/GED/Cadastros/TiposDeOpiniaoDeDocumento/BrowseCadastroTiposDeOpiniao.aspx
https://412-49.docspider.com.br/GED/Cadastros/TiposDeReferenciaParaPerguntasDeDocumento/BrowseCadastroTiposDeReferenciaParaPerguntas.aspx
https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx
https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx
https://412-49.docspider.com.br/GED/Consultas/DocumentsStatistics/DocumentsStatistics.aspx
https://412-49.docspider.com.br/GED/Consultas/Indicadores/DocumentStatisticPanel/DocumentStatisticPanel.aspx
https://412-49.docspider.com.br/GED/Consultas/Indicadores/QuestionStatisticPanel/QuestionStatisticPanel.aspx
https://412-49.docspider.com.br/GED/Consultas/Indicadores/SearchStatisticPanel/SearchStatisticPanel.aspx
https://412-49.docspider.com.br/GED/Transacao/CargaDocumentos/PainelCargaDocumentos.aspx
https://412-49.docspider.com.br/GED/Transacao/PainelPerguntas/BrowsePainelPerguntas.aspx
https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx
https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx?RadUrid=0e278a3a-71c3-4ca6-90ec-7aa1514e1dd9
https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx?RadUrid=f466c819-a2a5-4f33-a513-3512689d1fda
https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaSuporte/TransferenciaAreaSuporte.aspx
https://412-49.docspider.com.br/GED/Transacao/TransferenciaPasta/BrowseTransferDocumentsToAnotherFolder.aspx
https://412-49.docspider.com.br/GED/WebResource.axd?d=TRgOLop0UyoHAlAOOH7wlfg16VC12byHTu7xJk7GMfJ12xRoO8TsUeOTta89BGwU6NXSEhsLtYl4bMpSQVdMTMA4yxrPj_gZ1YC7ZB7k9lvTOQCXHeZpJfxtMuEBax50wJ1vei8XmVJf7K1JKn7aG7IxOjMNmi6cSiX01&t=638089669480620669
https://412-49.docspider.com.br/GED/WebResource.axd?d=s2U5mT2X08GzLVMLP1sBkI1tI6AGDtJMkTN-1EPIlM8_i1p4-noXI4qMoIEWU1pSsEFZiQJheRw8EpttQ8RRSoajjd-lp9H-jA_wrmA7DFs9Oht8yl9Z6zM5biTOGHktXo4w8TeEZNi9vj9y9my_aMC8rMVSOhgFNQz8btdlKXXtvE4g6tx9U6sPFWDgXjOlAbAliYn-K3ywg7rnfb0BnQ2&t=638089669490933368
https://412-49.docspider.com.br/GED/WebResource.axd?d=xdaW2rHWkELFGrbWB5VtkwgyELyOkeaxvtduOUhheuGVSNYSYzCB47aHCTp-HwOKjBPRLD_aDPRPqfSWwLEl82X8UT8X5D8lGrweteSgcqObYl_Wtiw_427fxvX0Lj-7CB1aoEDS1FCA-_jQZnCoVrySM36cH2X-5Qt7HeyaVcsXiseTJuUSZ8_38HNeOdWR0&t=638089669480620669
https://412-49.docspider.com.br/Generic/Cadastros/Parametros/BrowseCadastroParametros.aspx
https://412-49.docspider.com.br/Generic/Transacao/AlterarParametros/BrowseAlterarParametros.aspx?grupo=12
https://412-49.docspider.com.br/Generic/Transacao/DownloadArquivos/BrowseDownloadArquivos.aspx
https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/Execucao.aspx?q=11
https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/PainelSentencaSQL.aspx
https://412-49.docspider.com.br/Generic/Transacao/UploadArquivos/BrowseUploadArquivos.aspx
https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx
https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx
https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx
https://412-49.docspider.com.br/Global/Cadastros/Diretorias/BrowseCadastroDiretoria.aspx
https://412-49.docspider.com.br/Global/Cadastros/Diretorios/BrowseCadastroDiretorio.aspx
https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx
https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx
https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx
https://412-49.docspider.com.br/Global/Cadastros/Idiomas/BrowseCadastroIdioma.aspx
https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx
https://412-49.docspider.com.br/Global/Cadastros/PerfisVisualizacao/BrowseCadastroPerfilVisualizacao.aspx
https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx
https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx
https://412-49.docspider.com.br/Global/Cadastros/Usuarios/BrowseCadastroUsuario.aspx
https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx
https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
https://412-49.docspider.com.br/Global/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=RadScriptManager1_TSM&compress=1&_TSM_CombinedScripts_=%3b%3bSystem.Web.Extensions%2c+Version%3d4.0.0.0%2c+Culture%3dneutral%2c+PublicKeyToken%3d31bf3856ad364e35%3apt-BR%3af7ba41a4-e843-4f12-b442-8e407f37c316%3aea597d4b%3ab25378d2%3bTelerik.Web.UI%2c+Version%3d2021.3.1111.45%2c+Culture%3dneutral%2c+PublicKeyToken%3d121fae78165ba3d4%3apt-BR%3ab406acc5-0028-4c73-8915-a9da355d848a%3a16e4e7cd%3aed16cbdc%3af7645509%3a24ee1bba%3ac128760b%3a874f8ea2%3af46195d3%3a33715776%3a19620875%3acda80b3%3a383e4ce8%3a4877f69a%3a86526ba7%3a11a04f7e%3ae330518b%3a1e771326%3a88144a7a%3a8e6f0d33%3a1f3a7489%3a6a6d718d%3ab2e06756%3a92fe8ea0%3afa31b949%3a490a9d4e%3abd8f85e4
https://412-49.docspider.com.br/Global/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=scriptManager_TSM&compress=1&_TSM_CombinedScripts_=%3b%3bSystem.Web.Extensions%2c+Version%3d4.0.0.0%2c+Culture%3dneutral%2c+PublicKeyToken%3d31bf3856ad364e35%3apt-BR%3af7ba41a4-e843-4f12-b442-8e407f37c316%3aea597d4b%3ab25378d2%3bTelerik.Web.UI%2c+Version%3d2021.3.1111.45%2c+Culture%3dneutral%2c+PublicKeyToken%3d121fae78165ba3d4%3apt-BR%3ab406acc5-0028-4c73-8915-a9da355d848a%3a16e4e7cd%3aed16cbdc%3a4877f69a%3a33715776%3a86526ba7%3a874f8ea2%3af7645509%3a24ee1bba%3ac128760b%3af46195d3%3a19620875%3acda80b3%3a383e4ce8%3a88144a7a%3a11a04f7e%3ae330518b%3a1e771326%3a8e6f0d33%3a1f3a7489%3a6a6d718d%3ab7778d6c%3a6d43f6d9%3ab2e06756%3a92fe8ea0%3afa31b949%3a490a9d4e%3abd8f85e4
https://412-49.docspider.com.br/Global/Transacao/Sincronismo/BrowseLogGeral.aspx
https://412-49.docspider.com.br/Global/Transacao/Sincronismo/BrowseSincAplicado.aspx?skin=Web20
https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx
https://412-49.docspider.com.br/Global/Transacao/UsuarioSubstituto/DefinirUsuarioSubstituto.aspx
https://412-49.docspider.com.br/Global/WebResource.axd?d=2AszK6veUVMmmAigugstESZhDxV7wLlH2iF4Z1M0viiMVAUf07m2DczzjerhrScJlj-KKIzugVyEyG4OApKKdN6-1SNYHa00MgkwQMrfJDvPE36Zds5tF2nlIAGe4Ie5J1QFIODgxZRFAT5kYm7btHZv09azgeWVaGNDummAwH8fFnXcyP5kkk8C-MD9B7Cf4xl4HC3j3Ekjf9FOxL5X0g2&t=638089669490933368
https://412-49.docspider.com.br/Global/WebResource.axd?d=BJbMyFFUsMNCyC7iCxSFyU_6tseJecUeeUVbDS0V5-QmHeA9NgsDUewb46b-LpMjs7pL93627BrRkrsPw8XWTEexT4OTCigxcWZCovXBjuawFol_m0VH2RVVUONmipj9c4kycQp-yBiDVFZyUtpi92cJ-rkhXYyJqaq2G-YpIO9OogxI3TyWUsPSc5eabeSy0&t=638089669480620669
https://412-49.docspider.com.br/Global/WebResource.axd?d=MXgY26JaQwbFUvrpZL9oMeiq0ZHceGzaQB7yD2mOBynF4zf-WmaQ6Z5DSw6ZKTu9netJWtJXQezuT1O1zabju8NYCGx0xHLrlE-zh5SIYZVKVGfvB6jgdXI-TpK_Po7-p_jRessx2DzqXRM7INcDSPkUyVmWK35z6ms5OwGMHaFGHKdjQFPsAZvcRPF-CWS5yCPuRrQEx8rnC5DWL703XA2&t=638089669490933368
https://412-49.docspider.com.br/Global/WebResource.axd?d=Sy0b6rN6aDu9HWPir-p1zOrelM0X0o18ZCg08KhUc7kN6fP6PHuf0rRRlMIC3kz06FDlurTaSSBCGgCBEQObI6lTtn8K0qCm0hxVhkaL87n-ssMwgWDrWnXIJ6p_rarMpVw1aZVOe4wgQpe1iHgvtdmx8dYpiF9OJ7rn_enQKyNFUP-EUnivoQ6yF1gtuAWx0&t=638089669480620669
https://412-49.docspider.com.br/Global/WebResource.axd?d=s2U5mT2X08GzLVMLP1sBkC8jFBuAVA-nl8NVJDLvdHlshC0uu0oO6UmNJ-o_t8P6wePMsz4TwyPSNSYiu7QwzR2Ghsnp74OQh4_olpltFaPKWEIFV4SPHk7ofSf8rH3-5-fnw5QUbF_vRDxOg2FGkODy6sJS4BRHif8KkJDnF3iYOyi9FvekiMUPAU7bATjituhDXLjsFJMAIqBD5GAabA2&t=638089669490933368
https://412-49.docspider.com.br/Global/Zoom/ZoomArea.aspx?tipoSelecao=1
https://412-49.docspider.com.br/Global/Zoom/ZoomDiretoria.aspx
https://412-49.docspider.com.br/Global/Zoom/ZoomDiretoria.aspx?chamador=diretoria&idempresa=
https://412-49.docspider.com.br/Global/Zoom/ZoomEmpresa.aspx?chamador=empresa
https://412-49.docspider.com.br/Inativar
https://412-49.docspider.com.br/Login
https://412-49.docspider.com.br/Login/Authenticate
https://412-49.docspider.com.br/NAssets/images/favicon.png
https://412-49.docspider.com.br/NAssets/images/logo.png
https://412-49.docspider.com.br/NAssets/scripts/docspider/jquery-extensions.js
https://412-49.docspider.com.br/NAssets/scripts/docspider/plugins/form.js

https://412-49.docspider.com.br/NAssets/scripts/kendo-ui/cultures/kendo.culture.pt-BR.min.js
https://412-49.docspider.com.br/NAssets/scripts/kendo-ui/jszip.min.js
https://412-49.docspider.com.br/NAssets/styles/docspider/docspider-layout.css
https://412-49.docspider.com.br/NAssets/styles/docspider/docspiderPalette.css
https://412-49.docspider.com.br/NAssets/styles/kendo-override.css
https://412-49.docspider.com.br/Portal/Cadastros/Menu/BrowseCadastroMenu.aspx
https://412-49.docspider.com.br/Portal/Cadastros/Pastas/BrowseCadastroPasta.aspx
https://412-49.docspider.com.br/Portal/Cadastros/Portal/BrowseCadastroPortal.aspx
https://412-49.docspider.com.br/Portal/Consultas/Logs/FrmLogExecMenu.aspx
https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?PortalID=1
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?PortalID=17
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?PortalID=2
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?PortalID=22
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?PortalID=4
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?PortalID=5
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
https://412-49.docspider.com.br/PortalDocumentos
https://412-49.docspider.com.br/PortalDocumentos/
https://412-49.docspider.com.br/PortalDocumentos/?PortalID=1
https://412-49.docspider.com.br/PortalDocumentos/?PortalID=17
https://412-49.docspider.com.br/PortalDocumentos/?PortalID=2
https://412-49.docspider.com.br/PortalDocumentos/?PortalID=3
https://412-49.docspider.com.br/PortalDocumentos/?PortalID=4
https://412-49.docspider.com.br/PortalDocumentos/?PortalID=9
https://412-49.docspider.com.br/PortalDocumentos/Atividades
https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos
https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos/Buscar
https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?PageNumber=1&PageSize=50&HasNextPage=False&TotalItemCount=3
https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoBuscaFiltro=1&modoBusca=1&tipoBusca=2&semAsPalavras=1&comValidadeIndefinida=1
https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoDeBusca=1
https://412-49.docspider.com.br/PortalDocumentos/Content/view-resources/Views/_Bundles/LayoutPortalDocumentos.min.css
https://412-49.docspider.com.br/PortalDocumentos/Content/view-resources/Views/_Bundles/common-styles.min.css
https://412-49.docspider.com.br/PortalDocumentos/ControleCodigoDocumento
https://412-49.docspider.com.br/PortalDocumentos/DocumentosPorAreas
https://412-49.docspider.com.br/PortalDocumentos/DocumentosPorIndexadores
https://412-49.docspider.com.br/PortalDocumentos/DocumentosPorPasta
https://412-49.docspider.com.br/PortalDocumentos/DocumentosPorTipo
https://412-49.docspider.com.br/PortalDocumentos/Error/
https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError
https://412-49.docspider.com.br/PortalDocumentos/GerenciarDocumentos
https://412-49.docspider.com.br/PortalDocumentos/Home
https://412-49.docspider.com.br/PortalDocumentos/MaisAcessados
https://412-49.docspider.com.br/PortalDocumentos/MeusFavoritos
https://412-49.docspider.com.br/PortalDocumentos/PortalDocumentos/RegistrarLogBuscaUtilizada
https://412-49.docspider.com.br/PortalDocumentos/Scripts/GetScripts
https://412-49.docspider.com.br/PortalDocumentos/TutoriaisDicas
https://412-49.docspider.com.br/PortalDocumentos/UltimasAtualizacoes
https://412-49.docspider.com.br/PortalDocumentos/UltimosAcessados
https://412-49.docspider.com.br/PortalDocumentos?PortalID=9
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYwN+5uS7pfhkp/iLsKtTAzCaR2iv08waBtavfJq9j
+aTSQqRvSyHxM7SKs9PdlsiskZFbjIlIiskCTDbAyjUozZWSXhmqZOY86ams2L4ajTu5qi0eF67BPPs/GvBmBTN5vxyWto/CWXxZw==
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYwN+5uS7pfhkp/iLsKtTAzCaR2iv08waBtavfJq9j
+aTSQqRvSyHxM7SKs9PdlsiskZFbjIlIiskCTDbAyjUozZWSXhmqZOY86ams2L4ajTu5s8zWEj7Xc9764GrwnRXwXL2zEgUt2LAdQ==
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYwyEmMqp3cPv+w8+650FvBB2k0fS0bLBpNx8VAfU1ZIA
+nbXmbBoxYWkIEaea54TtxK6ucSmFU57NbN/6/uFQzqX28DR2R8AUrGrJMX9YYw3Jow4iVUJ8WG7KPzAkaOZ3XYvjg8vq5Aug==
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYxoVTrMpTD
+llnitJq6mSMkvR79sUQ5GHx41dnNd946AJX4e4LAVz0cfheIQtX1YVBvuQXFsUTAWyy62IkXAW60voa8oeOMkVllbDjnxmCBuhChEjZASKrwipRPvUhFX/Or5xgUb/
zTd7HFSE3bWde0RshklWxKbZQ=
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYxoVTrMpTD
+llnitJq6mSMkvR79sUQ5GHx41dnNd946AJX4e4LAVz0cfheIQtX1YVBvuQXFsUTAWyy62IkXAW60voa8oeOMkVllbDjnxmCBuk+rLUp0kAYW9355LoZ2Wy+oqn0KZGobEQ==
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYy/j+pgWnKLxuttbqR5OYWJvZKqe36MsqWQn3/
aMs5mlVgUTx4S08FeLss0qboEapVPjD4ZvIMys4DkoTkfWIMa5eRZr0ioHJ5CxPopv3CpJ7CunaL9ZiceG1fsKUjvALHsI3lx0r1GB65UbSvIDuZbvvgcebNO5cw=
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYzEmnmzgvPVBpNggiUfd483y5ywYRjwnj1GcAj7/Xh+7wjIL
+T70E2gxwZ6Vm5ZUd0axjMKhPglBGejSR16c54ikNVHG0XjXoIrjKjFMMN2r8dZ4cvbSPEeQ6zqOI6XS7ui9lzmSl+VTw==
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYzR3une9eMfxfzQThoCrc7gcKxIaqwLaveprr/jO3CXtCBlrSr9S1RKI8dF3FxYO
+n0Nzm2ZLrD0Qo0mDL2SHMq+NtEofyhy9mglGQxJvhLVBwIhH6zXpG9ikQCwmpYYboi7LmH0k5tahSEzj0BNEVexZL/EGiT6hw=
https://412-49.docspider.com.br/Workflow/Cadastros/HorarioDeTurno/BrowseCadastroHorarioTurno.aspx
https://412-49.docspider.com.br/Workflow/Cadastros/Papeis/BrowseCadastroPapeis.aspx
https://412-49.docspider.com.br/Workflow/Cadastros/TipoDeAnexo/BrowseCadastroTipoDeAnexo.aspx
https://412-49.docspider.com.br/Workflow/Consultas/FrmConsultaProcesso.aspx
https://412-49.docspider.com.br/Workflow/Consultas/MonitorGrafico/Web/ProcessMonitor.aspx
https://412-49.docspider.com.br/Workflow/Transacao/ExportacaoImportacaoTipoProcesso.aspx
https://412-49.docspider.com.br/asp/Solucao_Normativos/Cadastros/IDSWK.PNCTREST.FRAME.MAIN.asp
https://412-49.docspider.com.br/asp/Usuario/adm_transfere_tarefa_usuario_wf.asp
https://412-49.docspider.com.br/asp/Usuario/frm_transfere_tarefa_usuario_wf.asp
https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_programa_wf.asp
https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_programa_wf.asp?pagina=1&order=1&linkAtual=1&tipoOrdem=DESC&linhas=15&palavra=1
https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_tipo_formulario.asp
https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_tipo_formulario.asp?pagina=1&order=1&linkAtual=1&tipoOrdem=DESC&linhas=15&tipoform=&palavra=1
https://412-49.docspider.com.br/asp/wf_002/browse_delete_fluxo.asp?botaovoltar=sim
https://412-49.docspider.com.br/asp/wf_002/frm_deleta_fluxo.asp
https://412-49.docspider.com.br/asp/wf_002/wf.asp
https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCadastroTipoFeriado.aspx
https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCalendarios.aspx

https://412-49.docspider.com.br/workflow/cadastros/calendarios/FrmCadastroDiasNaoUteis.aspx?idcalendario=1
http://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError

150010 External Links Discovered (1)

150010 External Links Discovered

Finding #	**415462**(69622017)	**Severity**	Information Gathered - Level 1
Unique #	**c2fed8aa-5f4e-4d5b-8eda-cd9a0699ef27**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

Impact

N/A

Solution

N/A

Results

Number of links: 29
https://github.com/elastic/elasticsearch/blob/7.10/licenses/ELASTIC-LICENSE.txt
https://41-9.docspider.com.br/Custom/Images/Docspider_Logo_Natal.png
https://41-9.docspider.com.br/Custom/Images/corp_sub.png
https://41-9.docspider.com.br/Custom/theme/docspider.css
https://41-9.docspider.com.br/Global/Transacao/UsuarioSubstituto/DefinirUsuarioSubstituto.aspx
https://41-9.docspider.com.br/Login/Login?prg=https://41-9.docspider.com.br/PortalDocumentos/UltimasAtualizacoes&anonimo=True
https://41-9.docspider.com.br/NAssets/images/favicon.png
https://41-9.docspider.com.br/NAssets/images/logo.png
https://41-9.docspider.com.br/PortalDocumentos/
https://41-9.docspider.com.br/PortalDocumentos/?PortalID=2
https://41-9.docspider.com.br/PortalDocumentos/Content/lib/kendo-ui/scripts/cultures/kendo.culture.pt-BR.min.js
https://41-9.docspider.com.br/PortalDocumentos/Content/lib/kendo-ui/scripts/messages/kendo.messages.pt-BR.min.js
https://41-9.docspider.com.br/PortalDocumentos/Content/view-resources/Views/_Bundles/LayoutPortalDocumentos.min.css
https://41-9.docspider.com.br/PortalDocumentos/Content/view-resources/Views/_Bundles/LayoutPortalDocumentos.min.js
https://41-9.docspider.com.br/PortalDocumentos/Content/view-resources/Views/_Bundles/app-layout-libs.min.js
https://41-9.docspider.com.br/PortalDocumentos/Content/view-resources/Views/_Bundles/common-scripts.min.js
https://41-9.docspider.com.br/PortalDocumentos/Content/view-resources/Views/_Bundles/common-styles.min.css
https://41-9.docspider.com.br/PortalDocumentos/Content/view-resources/Views/_Bundles/vendors.bundle.min.css
https://41-9.docspider.com.br/PortalDocumentos/DocumentosPorAreas
https://41-9.docspider.com.br/PortalDocumentos/DocumentosPorIndexadores
https://41-9.docspider.com.br/PortalDocumentos/DocumentosPorTipo
https://41-9.docspider.com.br/PortalDocumentos/Home
https://41-9.docspider.com.br/PortalDocumentos/MaisAcessados
https://41-9.docspider.com.br/PortalDocumentos/Scripts/GetScripts
https://41-9.docspider.com.br/PortalDocumentos/UltimasAtualizacoes
https://41-9.docspider.com.br/PortalDocumentos/UltimosAcessados
https://localhost/jF0uQ6fYD
https://localhost/jzP2md08A
https://go.microsoft.com/fwlink/?LinkID=82731

150014 External Form Actions Discovered (1)

150014 External Form Actions Discovered

Finding #	**769348**(69622020)
Unique #	**3c00c63a-37f6-45b8-a762-ee89d013bd8c**
Group	Scan Diagnostics
CWE	-
OWASP	-
WASC	-

Severity	Information Gathered - Level 1
Detection Date	11 Jan 2023 18:24 GMT-0400

Details

Threat

The external form actions discovered by the Web application scanning engine are provided in the Results section. These links were present within HTML forms on the target Web application, but were not crawled.

Impact

N/A

Solution

N/A

Results

Number of forms: 1
Form on page https://41-9.docspider.com.br/PortalDocumentos/UltimasAtualizacoes submits to https://41-9.docspider.com.br/PortalDocumentos/UltimasAtualizacoes

150020 Links Rejected By Crawl Scope or Exclusion List (1)

WAS Scan Report

150020 Links Rejected By Crawl Scope or Exclusion List

Finding #	**415440**(69621989)	**Severity**	Information Gathered - Level 1
Unique #	**80cb76db-aff3-42af-8423-e041774a2ea3**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

Impact

Links listed here were neither crawled or tested by the Web application scanning engine.

Solution

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

Results

Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)
https://41-9.docspider.com.br/PortalDocumentos/e1aRiAKPbLnV.html
https://41-9.docspider.com.br/PortalDocumentos/.
https://41-9.docspider.com.br/PortalDocumentos/../
https://41-9.docspider.com.br/PortalDocumentos/icons/small/

External links discovered:
https://github.com/elastic/elasticsearch/blob/7.10/licenses/ELASTIC-LICENSE.txt
https://41-9.docspider.com.br/Custom/Images/Docspider_Logo_Natal.png
https://41-9.docspider.com.br/Custom/Images/corp_sub.png
https://41-9.docspider.com.br/Custom/theme/docspider.css
https://41-9.docspider.com.br/Global/Transacao/UsuarioSubstituto/DefinirUsuarioSubstituto.aspx
https://41-9.docspider.com.br/Login/Login?prg=https://41-9.docspider.com.br/PortalDocumentos/UltimasAtualizacoes&anonimo=True
https://41-9.docspider.com.br/NAssets/images/favicon.png
https://41-9.docspider.com.br/NAssets/images/logo.png
https://41-9.docspider.com.br/PortalDocumentos/
https://41-9.docspider.com.br/PortalDocumentos/?PortalID=2

IP based excluded links:

Logout links detected:
https://41-9.docspider.com.br/Login/Logout
https://412-49.docspider.com.br/Global/WebResource.axd?
d=-5d2ExITdtgvTPW2fvOYY-6WXIB3ImAHm7pShTxz4d4cKlum5Nbz19QB6zJc1ZaE8XmK2oGCNoW4fM9GXxUjesyQK_OSw971K4R2VtNHJsAABY9g_uL3UzMcHVgUolyW-TED-
CWdI9ct0QG0CbVr_PiQKh_T3GrkrKw1CBQCwV4kd1TZPNBHxyqtQ-Tq7CaPKxdwaoDEbUOr_emFXaWFng2&t=638089669490933368
https://412-49.docspider.com.br/Login/Logout
https://412-49.docspider.com.br/login/logout.aspx
https://412-49.docspider.com.br/login/logout.aspx?prg=/portaladmin/frmstart.aspx&url=url=portal=
javascript:logoutUser();
Links rejected during the test phase not reported due to volume of links.

WAS Scan Report

▭ **150021 Scan Diagnostics** (1)

WAS Scan Report

150021 Scan Diagnostics

Finding #	415441(69621990)	**Severity**	Information Gathered - Level 1
Unique #	23026f26-989a-41fd-9ac0-6d5aeb092bfc		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Impact

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

Solution

No action is required.

Results

Loaded 0 exclude list entries.
Loaded 0 allow list entries.
Target web application page https://412-49.docspider.com.br/ fetched. Status code:200, Content-Type:text/html, load time:1 milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 10 minutes (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 70 requests, 55 seconds. Completed 70 requests of 70 estimated requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 10 minutes (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 56 requests, 32 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
Maximum request count reached: 300
Collected 999 links overall in 0 hours 48 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests (0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 125) + files:(0 x 163) + directories:(9 x 153) + paths:(0 x 316) = total (1377)
Batch #0 WS Directory Path manipulation: estimated time < 10 minutes
WS Directory Path manipulation: 9 vulnsigs tests, completed 1143 requests, 176 seconds. Completed 1143 requests of 1377 estimated requests (83.0065%). All tests completed.
Batch #0 WS enumeration: estimated time < 30 minutes (11 tests, 307 inputs)
WS enumeration: 11 vulnsigs tests, completed 1427 requests, 224 seconds. Completed 1427 requests of 3377 estimated requests (42.2564%). All tests completed.
The following form(s) found with more than 50 fields. These form(s) will take large time for testing.
field count: 245 action uri:https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx
field count: 243 action uri:https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx
field count: 216 action uri:https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx
field count: 213 action uri:https://412-49.docspider.com.br/Workflow/Consultas/MonitorGrafico/Web/ProcessMonitor.aspx
field count: 159 action uri:https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaSuporte/TransferenciaAreaSuporte.aspx
field count: 147 action uri:https://412-49.docspider.com.br/GED/Transacao/TransferenciaPasta/BrowseTransferDocumentsToAnotherFolder.aspx
field count: 136 action uri:https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx
field count: 132 action uri:https://412-49.docspider.com.br/GED/Transacao/PainelPerguntas/BrowsePainelPerguntas.aspx
field count: 126 action uri:https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx
field count: 115 action uri:https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/PainelSentencaSQL.aspx
field count: 113 action uri:https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx
field count: 112 action uri:https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx
field count: 111 action uri:https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/PainelSentencaSQL.aspx
field count: 110 action uri:https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx?RadUrid=f466c819-a2a5-4f33-a513-3512689d1fda
field count: 109 action uri:https://412-49.docspider.com.br/Workflow/Consultas/FrmConsultaProcesso.aspx
field count: 109 action uri:https://412-49.docspider.com.br/Workflow/Consultas/FrmConsultaProcesso.aspx
field count: 109 action uri:https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx?RadUrid=0e278a3a-71c3-4ca6-90ec-7aa1514e1dd9
field count: 107 action uri:https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx
field count: 101 action uri:https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx
field count: 96 action uri:https://412-49.docspider.com.br/Workflow/Cadastros/HorarioDeTurno/BrowseCadastroHorarioTurno.aspx
field count: 95 action uri:https://412-49.docspider.com.br/Global/Cadastros/Usuarios/BrowseCadastroUsuario.aspx
field count: 89 action uri:https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx
field count: 84 action uri:https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
field count: 82 action uri:https://412-49.docspider.com.br/GED/Transacao/PainelPerguntas/BrowsePainelPerguntas.aspx
field count: 81 action uri:https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCadastroTipoFeriado.aspx
field count: 81 action uri:https://412-49.docspider.com.br/Workflow/Transacao/ExportacaoImportacaoTipoProcesso.aspx
field count: 80 action uri:https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx
field count: 76 action uri:https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx
field count: 74 action uri:https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx

field count: 68 action uri:https://412-49.docspider.com.br/GED/Cadastros/TiposDeReferenciaParaPerguntasDeDocumento/BrowseCadastroTiposDeReferenciaParaPerguntas.aspx
field count: 68 action uri:https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCalendarios.aspx
field count: 66 action uri:https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx
field count: 65 action uri:https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx
field count: 61 action uri:https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx
field count: 59 action uri:https://412-49.docspider.com.br/GED/Cadastros/TiposDeOpiniaoDeDocumento/BrowseCadastroTiposDeOpiniao.aspx
field count: 59 action uri:https://412-49.docspider.com.br/workflow/cadastros/calendarios/FrmCadastroDiasNaoUteis.aspx?idcalendario=1
field count: 59 action uri:https://412-49.docspider.com.br/Portal/Consultas/Logs/FrmLogExecMenu.aspx
field count: 59 action uri:https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx
field count: 59 action uri:https://412-49.docspider.com.br/GED/Cadastros/PontosDeControle/BrowseCadastroClassPontosControle.aspx
field count: 59 action uri:https://412-49.docspider.com.br/Generic/Transacao/AlterarParametros/BrowseAlterarParametros.aspx?grupo=12
field count: 58 action uri:https://412-49.docspider.com.br/Portal/Consultas/Logs/FrmLogExecMenu.aspx
field count: 58 action uri:https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx
field count: 58 action uri:https://412-49.docspider.com.br/GED/Cadastros/TiposDeReferenciaParaPerguntasDeDocumento/BrowseCadastroTiposDeReferenciaParaPerguntas.aspx
field count: 58 action uri:https://412-49.docspider.com.br/Global/Transacao/UsuarioSubstituto/DefinirUsuarioSubstituto.aspx
field count: 58 action uri:https://412-49.docspider.com.br/workflow/cadastros/calendarios/FrmCadastroDiasNaoUteis.aspx?idcalendario=1
field count: 57 action uri:https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx
field count: 57 action uri:https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx
field count: 57 action uri:https://412-49.docspider.com.br/Global/Transacao/UsuarioSubstituto/DefinirUsuarioSubstituto.aspx
field count: 57 action uri:https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx
field count: 54 action uri:https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx
field count: 54 action uri:https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx
field count: 53 action uri:https://412-49.docspider.com.br/Global/Cadastros/Usuarios/BrowseCadastroUsuario.aspx
field count: 53 action uri:https://412-49.docspider.com.br/Generic/Cadastros/Parametros/BrowseCadastroParametros.aspx
field count: 53 action uri:https://412-49.docspider.com.br/Workflow/Cadastros/TipoDeAnexo/BrowseCadastroTipoDeAnexo.aspx
field count: 52 action uri:https://412-49.docspider.com.br/Global/Zoom/ZoomEmpresa.aspx?chamador=empresa
field count: 51 action uri:https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCadastroTipoFeriado.aspx
field count: 51 action uri:https://412-49.docspider.com.br/Portal/Cadastros/Portal/BrowseCadastroPortal.aspx
field count: 51 action uri:https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
field count: 51 action uri:https://412-49.docspider.com.br/Global/Cadastros/PerfisVisualizacao/BrowseCadastroPerfilVisualizacao.aspx
Batch #1 URI parameter manipulation (no auth): estimated time < 1 minute (112 tests, 0 inputs)
Batch #1 URI parameter manipulation (no auth): 112 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 URI blind SQL manipulation (no auth): estimated time < 1 minute (8 tests, 0 inputs)
Batch #1 URI blind SQL manipulation (no auth): 8 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 URI parameter time-based tests (no auth): estimated time < 1 minute (14 tests, 0 inputs)
Batch #1 URI parameter time-based tests (no auth): 14 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): estimated time < 1 minute (1 tests, 0 inputs)
Batch #1 URI parameter time-based tests for Apache Struts Vulnerabilities (no auth): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #1 URI parameter manipulation (auth): estimated time < 30 minutes (112 tests, 22 inputs)
Batch #1 URI parameter manipulation (auth): 112 vulnsigs tests, completed 2658 requests, 1379 seconds. Completed 2658 requests of 2464 estimated requests (107.873%). All tests completed.
Batch #1 Form parameter manipulation (auth): estimated time < 24 hours (112 tests, 2094 inputs)
Batch #1 Form parameter manipulation (auth): 112 vulnsigs tests, completed 112706 requests, 38082 seconds. Completed 112706 requests of 234528 estimated requests (48.0565%). Module did not finish.
Scan stopped at established time limit in order to report results.
Duration of Crawl Time: 2925.00 (seconds)
Duration of Test Phase: 39986.00 (seconds)
Total Scan Time: 42911.00 (seconds)

Total requests made: 118698
Average server response time: 1.01 seconds

Average browser load time: 1.02 seconds
Scan stopped at established time limit in order to report results.

150024 Scan Time Limit Reached (1)

WAS Scan Report

150024 Scan Time Limit Reached

Finding #	**438202**(69621993)	Severity	Information Gathered - Level 1
Unique #	**ab913baf-d6ab-4a20-ab52-f48d64bd2f8a**		
Group	Scan Diagnostics	Detection Date	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The scan engine reached its internal time limit for this scan. The scan was stopped in order to collect and report the results so far.

Impact

Not all tests have been completed. Therefore, some vulnerabilities may exist in the target application on links that the scanner has not yet tested. The scanner uses an iterative approach to determine the order in which links are tested. Links are selected in a breadth-first manner that takes into account how many connections each link has to other pages. This helps the scanner identify and test popular links first in order to have a useful coverage of the web application.

Solution

Application responsiveness is the most important factor in overall scan time. Review the average server response time reported by the scanner. Anything over 2 seconds is quite slow.

Scan time can potentially be reduced by one or more of the following methods:

- Make changes to improve the application's responsiveness.
- Increase the scan intensity setting.
- Reduce the SmartScan depth setting.
- Add redundant links configuration to reduce the number of unnecessary tests being performed.
- For applications with a large number of cookies, exclude the cookie/header tests (QIDs 150002, 150046, 150047, 150048).
- Exclude particular QIDs such as those related to XSS or SQL injection (and consequently running multiple scans with different QIDs enabled).

Results

Scan stopped at established time limit in order to report results.

150026 Maximum Number of Links Reached During Crawl (1)

WAS Scan Report

150026 Maximum Number of Links Reached During Crawl

Finding #	415443(69621992)	**Severity**	Information Gathered - Level 1
Unique #	f1e70e5a-e20b-486e-ac2b-5879dae485e8		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The maximum number of links specified for this scan has been reached. The links crawled to reach this threshold can include requests made via HTML form submissions and links requested in anonymous and authenticated states. Consequently, the list of links crawled (QID 150009) may reflect a lower number than the combination of links and forms requested during the crawl.

Impact

Some links that lead to different areas of the site's functionality may have been missed.

Solution

Increase the maximum number of links in order to ensure broader coverage of the Web application. It is important to note that increasing the number of links crawled can dramatically increase the time required to test the Web application.

Results

Maximum request count reached: 300

150028 Cookies Collected (1)

150028 Cookies Collected

Finding #	**415445**(69621996)
Unique #	**79d0a043-732a-446f-bf42-549ffbeb763b**
Group	Scan Diagnostics
CWE	-
OWASP	-
WASC	-

Severity	Information Gathered - Level 1
Detection Date	11 Jan 2023 18:24 GMT-0400

Details

Threat

The cookies listed in the Results section were set by the web application during the crawl phase.

Impact

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

Solution

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

Results

Total cookies: 4
biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; secure; HttpOnly; SameSite=Lax; path=/ First set at URL: https://412-49.docspider.com.br/Login/Authenticate
ASP.NET_SessionId=jfrezx1bhono4vnfk3qbnenf; secure; HttpOnly; SameSite=Lax; path=/ First set at URL: https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
_downloadToken=1673472915502,1673472915514; secure; HttpOnly; path=/ First set at URL: https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx
ASPSESSIONIDAGQQQRDA=DDEHMCOCNFJLOKOCGGMDNFBG; secure; HttpOnly; path=/ First set at URL: https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_tipo_formulario.asp

150029 Session Cookies (1)

WAS Scan Report

150029 Session Cookies

Finding #	**439744**(69621997)	**Severity**	Information Gathered - Level 1
Unique #	**ad3fbbde-ef7c-440c-8412-d41092cac2d5**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were identified as affecting the user's authenticated session to the Web application.

Impact

Session cookies are used to uniquely identify a user to a Web application. A compromised session cookie can lead to user impersonation.

Solution

Review the session cookies and verify that they do not contain sensitive values. Randomly generated session cookies should not exhibit a predictable pattern.

Results

Total cookies: 2
biblioteca=12345; path=/; domain=41-9.docspider.com.br; secure; httponly
biblioteca={731dfe1e-e4dd-496a-8dc3-c4468afbc8ee}; secure; HttpOnly; SameSite=Lax; path=/ First set at URL: https://412-49.docspider.com.br/Login/Authenticate

150054 Email Addresses Collected (1)

150054 Email Addresses Collected

Finding #	**438205**(69622005)
Unique #	**e347b862-4a3c-4808-912a-3c69bf2620c1**
Severity	Information Gathered - Level 1
Group	Scan Diagnostics
CWE	CWE-359
Detection Date	11 Jan 2023 18:24 GMT-0400
OWASP	-
WASC	-

Details

Threat

The email addresses listed in the Results section were collected from the returned HTML content during the crawl phase.

Impact

Email addresses may help a malicious user with brute force and phishing attacks.

Solution

Review the email list to see if they are all email addresses you want to expose.

Results

Number of emails: 7
alana.silva@docspider.com.br first seen at https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
albert@docspider.com.br first seen at https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
ale@ale.com.br first seen at https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
andre.santos@docspider.com.br first seen at https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
bismark.oliveira@docspider.com.br first seen at https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
d@d.com first seen at https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
was@qualys.com first seen at https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx

150066 Summary of .NET ViewState Fields (1)

WAS Scan Report

150066 Summary of .NET ViewState Fields

Finding #	**415456**(69622012)	Severity	Information Gathered - Level 1
Unique #	**1f162e1d-b6b2-4f21-b4e4-0be53ed4bac2**		
Group	Scan Diagnostics	Detection Date	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

One or more forms were detected that include a .NET ViewState field. Descriptive information about these fields is included in the Results section.

Impact

No specific security concerns are raised by this information. In general, the use of ViewState fields should be reviewed to ensure that they are implemented correctly within server-side code. ViewState objects should be encrypted or include an HMAC to prevent tampering. ViewState objects should not contain unnecessary static content that would make the field size large and therefore negatively impact performance.

Solution

This is merely informational data about the Web application. No further action is required.

Results

__VIEWSTATE statistics:
Fields analyzed: 151
Average size (bytes): 15803.79
Median size (bytes): 11025.94
Maximum size (bytes): 121408.00
Approximate percentage of bytes used by __VIEWSTATE values within all pages inspected by the crawler: 14.72 (2386372.00 out of 16214672.00)

150082 Protection against Clickjacking (1)

WAS Scan Report

150082 Protection against Clickjacking

Finding #	**415436**(69621984)
Unique #	**84c72abb-5b22-4ed3-a28d-b8416c760375**
Group	Scan Diagnostics
CWE	-
OWASP	-
WASC	-

Severity	Information Gathered - Level 1
Detection Date	11 Jan 2023 18:24 GMT-0400

Details

Threat

The URLs listed have protection against Clickjacking. The protection is implemented via the X-Frame-Options response header.

Impact

X-Frame-Options header is used to prevent framing of the page.

Solution

N/A

Results

https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx
https://412-49.docspider.com.br/PortalDocumentos/Home
https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx
https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx
https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx
https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYwyEmMqp3cPv+w8+650FvBB2k0fS0bLBpNx8VAfU1ZIA
+nbXmbBoxYWkIEaea54TtxK6ucSmFU57NbN/6/uFQzqX28DR2R8AUrGrJMX9YYw3Jow4iVUJ8WG7KPzAkaOZ3XYvjg8vq5Aug==
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYxoVTrMpTD
+llnitJq6mSMkvR79sUQ5GHx41dnNd946AJX4e4LAVz0cfheIQtX1YVBvuQXFsUTAWyy62IkXAW60voa8oeOMkVllbDjnxmCBuhChEjZASKrwipRPvUhFX/Or5xgUb/
zTd7HFSE3bWde0RshklWxKbZQ=
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYxoVTrMpTD
+llnitJq6mSMkvR79sUQ5GHx41dnNd946AJX4e4LAVz0cfheIQtX1YVBvuQXFsUTAWyy62IkXAW60voa8oeOMkVllbDjnxmCBuk+rLUp0kAYW9355LoZ2Wy+oqn0KZGobEQ==
https://412-49.docspider.com.br/PublishViewer/VisualizadorDocumentos/?query=X3viIDWAxYzEmnmzgvPVBpNggiUfd483y5ywYRjwnj1GcAj7/Xh+7wjIL
+T70E2gxwZ6Vm5ZUd0axjMKhPglBGejSR16c54ikNVHG0XjXoIrjKjFMMN2r8dZ4cvbSPEeQ6zqOI6XS7ui9lzmSl+VTw==

150100 Selenium Diagnostics (1)

150100 Selenium Diagnostics

Finding #	**415446**(69621999)	**Severity**	Information Gathered - Level 1
Unique #	**0c254ea2-1544-4a09-9380-ce2f3973030b**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Messages from Selenium log are provided

Impact

This information does not necessarily imply problems with the Web application.

Solution

This information may useful in changing/tuning the Selenium script.

Results

Log for Selenium script: portalcorporativo
Executing: |open | https://41-9.docspider.com.br/PortalDocumentos/UltimasAtualizacoes | |
Executing: |click | id=portalIcon | |
Executing: |click | link=Gestão e Processos | |
currentTest.recordFailure: Element link=Gestão e Processos not found
The execution of the script did not complete due to an internal time limit.

150104 Form Contains Email Address Field (1)

150104 Form Contains Email Address Field

Finding #	**438204**(69622002)	**Severity**	Information Gathered - Level 1
Unique #	**6050c549-b19a-45bb-b093-6d14ca9e7d6b**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The HTML form contains a field that collects an email address.

Impact

In some web apps, forms that collect email addresses also generate messages to back-end systems whenever the form is submitted. If no rate limiting or CAPTCHA is applied to form submissions, then vulnerability tests against this form may produce a significant amount of messages. If too many messages are generated, then it may produce a Denial of Service situation.

Solution

Review the form to determine if it produces an email message each time it is submitted. If so, consider excluding this form from being tested or disable the messaging during the web application scan. Forms that generate messages can be abused by malicious users to create Denial of Service attacks. Apply rate limiting to the form in order to throttle the number of times it may be submitted by a user or by an IP address; or apply a CAPTCHA to it to reduce the chance of automated tools being used against the form.

Results

https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx
https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx

150115 Authentication Form found (1)

WAS Scan Report

150115 Authentication Form found

Finding #	415450(69622003)	**Severity**	Information Gathered - Level 1
Unique #	79801b60-51f3-46a6-b9d2-b13aaf89de95		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Authentication Form was found during the web application crawling.

Impact

N/A

Solution

N/A

Results

Authentication form found at: https://412-49.docspider.com.br/Login
Action uri: https://412-49.docspider.com.br/Login/Authenticate
Fields: username, password

150152 Forms Crawled (1)

WAS Scan Report

	150152 Forms Crawled		

Finding #	**415444**(69621994)	**Severity**	Information Gathered - Level 1
Unique #	**70f27688-eca3-46c8-ba4d-063ab3f285fe**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Results section lists the unique forms that were identified and submitted by the scanner. The forms listed in this QID do not include authentication forms (i.e. login forms), which are reported separately under QID 150115.

The scanner does a redundancy check on forms by inspecting the form fields. Forms determined to be the redundant based on identical form fields will not be tested. If desired, you can enable 'Include form action URI in form uniqueness calculation' in the WAS option profile to have the scanner also consider the form's action attribute in the redundancy check.

NOTE: Any regular expression specified under 'Redundant Links' are not applied to forms. Forms (unique or redundant) are not reported under QID 150140.

Impact

N/A

Solution

N/A

Results

Total internal forms seen (this count includes duplicate forms): 135

Crawled forms (Total: 123)
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115
Form #:1 Action URI:https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx (found at: https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, idusuario, RadToolTipManager1_ClientState and 23 more field(s).

Form #:2 Action URI:https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx (found at: https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, RadToolTipManager1_ClientState, FormDecorator1_ClientState and 15 more field(s).

Form #:3 Action URI:https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos (found at: https://412-49.docspider.com.br/PortalDocumentos/Home)
Form Fields: termoDeBusca

Form #:4 Action URI:https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx)
Form Fields: scriptManager_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 19 more field(s).

Form #:5 Action URI:https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos (found at: https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoDeBusca=1)
Form Fields: termoBuscaFiltro, modoBusca, tipoBusca, semAsPalavras, comValidadeIndefinida and 10 field(s) without name.

Form #:6 Action URI:https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos (found at: https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoDeBusca=1)
Form Fields: PageNumber, PageSize, HasNextPage, TotalItemCount

Form #:7 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, hdnNomeUsuario, __EVENTVALIDATION, hdnIdUsuario, FormDecorator1_ClientState and 24 more field(s).

Form #:8 Action URI:https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 19 more field(s).

Form #:9 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnIdUsuario, hdnNomeUsuario, hdnidArea, FormDecorator1_ClientState and 44 more field(s).

Form #:10 Action URI:https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx)
Form Fields: scriptManager_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState and 41 more field(s).

Form #:11 Action URI:https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 27 more field(s).

Form #:12 Action URI:https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 25 more field(s).

Form #:13 Action URI:https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos (found at: https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoBuscaFiltro=1&modoBusca=1&tipoBusca=2&semAsPalavras=1&comValidadeIndefinida=1)
Form Fields: termoBuscaFiltro, modoBusca, tipoBusca, semAsPalavras, comValidadeIndefinida and 8 field(s) without name.

Form #:14 Action URI:https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos (found at: https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?PageNumber=1&PageSize=50&HasNextPage=False&TotalItemCount=3)
Form Fields: termoBuscaFiltro, modoBusca, tipoBusca, semAsPalavras, comValidadeIndefinida and 12 field(s) without name.

Form #:15 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState and 50 more field(s).

Form #:16 Action URI:https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, hdnTipoUsuario and 20 more field(s).

Form #:17 Action URI:https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState and 41 more field(s).

Form #:18 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx)
Form Fields: RadScriptManager1_TSM, hdnIdUsuario, hdnNomeUsuario, hdnidArea, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState and 46 more field(s).

Form #:19 Action URI:https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 24 more field(s).

Form #:20 Action URI:https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx (found at: https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, RadWindowZoomUser_ClientState, RadWindowFilter_ClientState and 93 more field(s).

Form #:21 Action URI:https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 19 more field(s).

Form #:22 Action URI:https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState and 51 more field(s).

Form #:23 Action URI:https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState, __EVENTTARGET, ListMult_ClientState and 50 more field(s).

Form #:24 Action URI:https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx)
Form Fields: __LASTFOCUS, RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 28 more field(s).

Form #:25 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 24 more field(s).

Form #:26 Action URI:https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, hdnTipoUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState and 42 more field(s).

Form #:27 Action URI:https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState,

RadToolTipManager1_ClientState and 25 more field(s).

Form #:28 Action URI:https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState and 54 more field(s).

Form #:29 Action URI:https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx?RadUrid=0e278a3a-71c3-4ca6-90ec-7aa1514e1dd9 (found at: https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, RadFormDecorator1_ClientState, hdnIdPortal and 101 more field(s).

Form #:30 Action URI:https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx)
Form Fields: __LASTFOCUS, RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 33 more field(s).

Form #:31 Action URI:https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx (found at: https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx)
Form Fields: RadScriptManager1_TSM, RadWindowZoomUser_ClientState, RadWindowFilter_ClientState, RadWindowManager1_ClientState, FormDecorator1_ClientState, RadWindowFilter_C_wndFiltroSplitter_ClientState and 107 more field(s).

Form #:32 Action URI:https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState and 39 more field(s).

Form #:33 Action URI:https://412-49.docspider.com.br/Generic/Transacao/DownloadArquivos/BrowseDownloadArquivos.aspx (found at: https://412-49.docspider.com.br/Generic/Transacao/DownloadArquivos/BrowseDownloadArquivos.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 27 more field(s).

Form #:34 Action URI:https://412-49.docspider.com.br/GED/Consultas/Indicadores/QuestionStatisticPanel/QuestionStatisticPanel.aspx (found at: https://412-49.docspider.com.br/GED/Consultas/Indicadores/QuestionStatisticPanel/QuestionStatisticPanel.aspx)
Form Fields: RadScriptManager2_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, FormDecorator1_ClientState, MainSplitter_ClientState, RadPane1_ClientState and 3 more field(s).

Form #:35 Action URI:https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState, __EVENTTARGET, ListMult_ClientState and 100 more field(s).

Form #:36 Action URI:https://412-49.docspider.com.br/Workflow/Consultas/FrmConsultaProcesso.aspx (found at: https://412-49.docspider.com.br/Workflow/Consultas/FrmConsultaProcesso.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState and 101 more field(s).

Form #:37 Action URI:https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState, __LASTFOCUS, RadWindowLogs_ClientState and 58 more field(s).

Form #:38 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState and 50 more field(s).

Form #:39 Action URI:https://412-49.docspider.com.br/GED/Transacao/PainelPerguntas/BrowsePainelPerguntas.aspx (found at: https://412-49.docspider.com.br/GED/Transacao/PainelPerguntas/BrowsePainelPerguntas.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 74 more field(s).

Form #:40 Action URI:https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState, __EVENTTARGET, RadWindowLogs_ClientState and 52 more field(s).

Form #:41 Action URI:https://412-49.docspider.com.br/GED/Transacao/CargaDocumentos/PainelCargaDocumentos.aspx (found at: https://412-49.docspider.com.br/GED/Transacao/CargaDocumentos/PainelCargaDocumentos.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, RadToolTipManager1_ClientState, FormDecorator1_ClientState and 14 more field(s).

Form #:42 Action URI:https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/PainelSentencaSQL.aspx (found at: https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/PainelSentencaSQL.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 103 more field(s).

Form #:43 Action URI:https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx (found at: https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 208 more field(s).

Form #:44 Action URI:https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx?RadUrid=f466c819-a2a5-4f33-a513-3512689d1fda (found at: https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, caixaDeProgresso_C_RadProgressManager1_ClientState, __VIEWSTATE, caixaDeProgresso_C_RadProgressArea1_ClientState and 104 more field(s).

Form #:45 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Diretorias/BrowseCadastroDiretoria.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Diretorias/BrowseCadastroDiretoria.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 28 more field(s).

Form #:46 Action URI:https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, _downloadToken, ListDialog_ClientState, RadWindowLogs_ClientState and 69 more field(s).

Form #:47 Action URI:https://412-49.docspider.com.br/Portal/Cadastros/Menu/BrowseCadastroMenu.aspx (found at: https://412-49.docspider.com.br/Portal/Cadastros/Menu/BrowseCadastroMenu.aspx)
Form Fields: scriptManager_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 18 more field(s).

Form #:48 Action URI:https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx (found at: https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, RadWindowZoomUser_ClientState, RadWindowFilter_ClientState and 104 more field(s).

Form #:49 Action URI:https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 19 more field(s).

Form #:50 Action URI:https://412-49.docspider.com.br/Workflow/Cadastros/Papeis/BrowseCadastroPapeis.aspx (found at: https://412-49.docspider.com.br/Workflow/Cadastros/Papeis/BrowseCadastroPapeis.aspx)
Form Fields: __LASTFOCUS, RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 27 more field(s).

Form #:51 Action URI:https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx (found at: https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 43 more field(s).

Form #:52 Action URI:https://412-49.docspider.com.br/Generic/Transacao/DownloadArquivos/BrowseDownloadArquivos.aspx (found at: https://412-49.docspider.com.br/Generic/Transacao/DownloadArquivos/BrowseDownloadArquivos.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 27 more field(s).

Form #:53 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Usuarios/BrowseCadastroUsuario.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Usuarios/BrowseCadastroUsuario.aspx)
Form Fields: __LASTFOCUS, scriptManager_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, hdnTipoUsuario and 43 more field(s).

Form #:54 Action URI:https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_tipo_formulario.asp?pagina=1&order=1&linkAtual=1&tipoOrdem=DESC&linhas=15&tipoform=&palavra=1 (found at: https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_tipo_formulario.asp)
Form Fields: btn1, btn2, palavra, btn3, link, linhas, paginadestino

Form #:55 Action URI:https://412-49.docspider.com.br/Workflow/Consultas/FrmConsultaProcesso.aspx (found at: https://412-49.docspider.com.br/Workflow/Consultas/FrmConsultaProcesso.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState and 101 more field(s).

Form #:56 Action URI:https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/Execucao.aspx?q=11 (found at: https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/Execucao.aspx?q=11)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 29 more field(s).

Form #:57 Action URI:https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState, __LASTFOCUS, RadWindowLogs_ClientState and 73 more field(s).

Form #:58 Action URI:https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_programa_wf.asp?pagina=1&order=1&linkAtual=1&tipoOrdem=DESC&linhas=15&palavra=1 (found at: https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_programa_wf.asp)
Form Fields: btn1, btn2, palavra, btn3, linhas, paginadestino

Form #:59 Action URI:https://412-49.docspider.com.br/GED/Transacao/PainelPerguntas/BrowsePainelPerguntas.aspx (found at: https://412-49.docspider.com.br/GED/Transacao/PainelPerguntas/BrowsePainelPerguntas.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter1_ClientState, ListDialog_ClientState, __EVENTTARGET, RadWindowZoom_ClientState and 125 more field(s).

Form #:60 Action URI:https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCadastroTipoFeriado.aspx (found at: https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCadastroTipoFeriado.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, hdnSortField and 72 more field(s).

Form #:61 Action URI:https://412-49.docspider.com.br/Global/Cadastros/PerfisVisualizacao/BrowseCadastroPerfilVisualizacao.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/PerfisVisualizacao/BrowseCadastroPerfilVisualizacao.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, hdnTipoUsuario and 22 more field(s).

Form #:62 Action URI:https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState, __EVENTTARGET, RadWindowLogs_ClientState and 82 more field(s).

Form #:63 Action URI:https://412-49.docspider.com.br/Workflow/Cadastros/HorarioDeTurno/BrowseCadastroHorarioTurno.aspx (found at: https://412-49.docspider.com.br/Workflow/Cadastros/HorarioDeTurno/BrowseCadastroHorarioTurno.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 40 more field(s).

Form #:64 Action URI:https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/PainelSentencaSQL.aspx (found at: https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/PainelSentencaSQL.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, tooltipLogs_ClientState, ListDialog_ClientState and 109 more field(s).

Form #:65 Action URI:https://412-49.docspider.com.br/Global/Transacao/UsuarioSubstituto/DefinirUsuarioSubstituto.aspx (found at: https://412-49.docspider.com.br/Global/Transacao/UsuarioSubstituto/DefinirUsuarioSubstituto.aspx)
Form Fields: ScriptManager_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, MainSplitter_ClientState, RadToolTipHelp_ClientState and 49 more field(s).

Form #:66 Action URI:https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx (found at: https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, RadWindowZoom_ClientState, __EVENTTARGET and 237 more field(s).

Form #:67 Action URI:https://412-49.docspider.com.br/workflow/cadastros/calendarios/FrmCadastroDiasNaoUteis.aspx?idcalendario=1 (found at: https://412-49.docspider.com.br/workflow/cadastros/calendarios/FrmCadastroDiasNaoUteis.aspx?idcalendario=1)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 50 more field(s).

Form #:68 Action URI:https://412-49.docspider.com.br/Workflow/Transacao/ExportacaoImportacaoTipoProcesso.aspx (found at: https://412-49.docspider.com.br/Workflow/Transacao/ExportacaoImportacaoTipoProcesso.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 73 more field(s).

Form #:69 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Diretorias/BrowseCadastroDiretoria.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Diretorias/BrowseCadastroDiretoria.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, RadWindowZoom_ClientState and 31 more field(s).

Form #:70 Action URI:https://412-49.docspider.com.br/Workflow/Cadastros/TipoDeAnexo/BrowseCadastroTipoDeAnexo.aspx (found at: https://412-49.docspider.com.br/Workflow/Cadastros/TipoDeAnexo/BrowseCadastroTipoDeAnexo.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 18 more field(s).

Form #:71 Action URI:https://412-49.docspider.com.br/asp/Usuario/adm_transfere_tarefa_usuario_wf.asp (found at: https://412-49.docspider.com.br/asp/Usuario/frm_transfere_tarefa_usuario_wf.asp)
Form Fields: btn1, btn2, metodo, btn3, idretorno, dsretorno, hidden_idcriador, btnnovopapel, id_centro_adm, todos1, id_cd_colaborador, todos2, nm_cd_colaborador, cd_centro_adm and 8 more field(s).

Form #:72 Action URI:https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, _downloadToken, ListDialog_ClientState, RadWindowLogs_ClientState and 119 more field(s).

Form #:73 Action URI:https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, __EVENTTARGET and 59 more field(s).

Form #:74 Action URI:https://412-49.docspider.com.br/Workflow/Consultas/MonitorGrafico/Web/ProcessMonitor.aspx (found at: https://412-49.docspider.com.br/Workflow/Consultas/MonitorGrafico/Web/ProcessMonitor.aspx)
Form Fields: RadScriptManager_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnIsAllAreasChecked, hdnIdUsuario, hdnParamUrlFilter and 204 more field(s).

Form #:75 Action URI:https://412-49.docspider.com.br/Workflow/Cadastros/Papeis/BrowseCadastroPapeis.aspx (found at: https://412-49.docspider.com.br/Workflow/Cadastros/Papeis/BrowseCadastroPapeis.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, hdnExpandCollapse, hdnExpanded, TopPane_ClientState and 31 more field(s).

Form #:76 Action URI:https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx (found at: https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, RadWindowZoom_ClientState, __EVENTTARGET and 68 more field(s).

Form #:77 Action URI:https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCalendarios.aspx (found at: https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCalendarios.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 59 more field(s).

Form #:78 Action URI:https://412-49.docspider.com.br/asp/wf_002/browse_delete_fluxo.asp?botaovoltar=sim (found at: https://412-49.docspider.com.br/asp/wf_002/frm_deleta_fluxo.asp)
Form Fields: frm, btn1, tipoform, isPostBack, id_de, tipo_formulario, statusFiltro, id_ate, descricao, solicitacao_de, solicitacao_ate

Form #:79 Action URI:https://412-49.docspider.com.br/GED/Cadastros/TiposDeOpiniaoDeDocumento/BrowseCadastroTiposDeOpiniao.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/TiposDeOpiniaoDeDocumento/BrowseCadastroTiposDeOpiniao.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 25 more field(s).

Form #:80 Action URI:https://412-49.docspider.com.br/Generic/Cadastros/Parametros/BrowseCadastroParametros.aspx (found at: https://412-49.docspider.com.br/Generic/Cadastros/Parametros/BrowseCadastroParametros.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 23 more field(s).

Form #:81 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Usuarios/BrowseCadastroUsuario.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Usuarios/BrowseCadastroUsuario.aspx)
Form Fields: scriptManager_TSM, hdnNomeUsuario, hdnIdUsuario, hdnTipoUsuario, FormDecorator1_ClientState, hdnIdCentroAdmPrincipal, RadToolTipManager1_ClientState, hdnIdSortField and 87 more field(s).

Form #:82 Action URI:https://412-49.docspider.com.br/GED/Cadastros/TiposDeReferenciaParaPerguntasDeDocumento/BrowseCadastroTiposDeReferenciaParaPerguntas.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/TiposDeReferenciaParaPerguntasDeDocumento/BrowseCadastroTiposDeReferenciaParaPerguntas.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 25 more field(s).

Form #:83 Action URI:https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/Execucao.aspx?q=11 (found at: https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/Execucao.aspx?q=11)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialogZoom_ClientState, RadWindowManager1_ClientState and 36 more field(s).

Form #:84 Action URI:https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCadastroTipoFeriado.aspx (found at: https://412-49.docspider.com.br/workflow/cadastros/calendarios/BrowseCadastroTipoFeriado.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, hdnSortField, hdnSortOrder, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState and 43 more field(s).

Form #:85 Action URI:https://412-49.docspider.com.br/Portal/Cadastros/Portal/BrowseCadastroPortal.aspx (found at: https://412-49.docspider.com.br/Portal/Cadastros/Portal/BrowseCadastroPortal.aspx)
Form Fields: scriptManager_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 20 more field(s).

Form #:86 Action URI:https://412-49.docspider.com.br/Global/Cadastros/PerfisVisualizacao/BrowseCadastroPerfilVisualizacao.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/PerfisVisualizacao/BrowseCadastroPerfilVisualizacao.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, hdnTipoUsuario, FormDecorator1_ClientState, hdnSortField, RadToolTipManager1_ClientState, hdnSortOrder and 43 more field(s).

Form #:87 Action URI:https://412-49.docspider.com.br/GED/Cadastros/PontosDeControle/BrowseCadastroClassPontosControle.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/PontosDeControle/BrowseCadastroClassPontosControle.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 25 more field(s).

Form #:88 Action URI:https://412-49.docspider.com.br/Workflow/Cadastros/HorarioDeTurno/BrowseCadastroHorarioTurno.aspx (found at: https://412-49.docspider.com.br/Workflow/Cadastros/HorarioDeTurno/BrowseCadastroHorarioTurno.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter1_ClientState, wnd1_ClientState, RadWindowManager1_ClientState and 90 more field(s).

Form #:89 Action URI:https://412-49.docspider.com.br/Portal/Cadastros/Pastas/BrowseCadastroPasta.aspx (found at: https://412-49.docspider.com.br/Portal/Cadastros/Pastas/BrowseCadastroPasta.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager2_ClientState and 18 more field(s).

Form #:90 Action URI:https://412-49.docspider.com.br/Global/Transacao/UsuarioSubstituto/DefinirUsuarioSubstituto.aspx (found at: https://412-49.docspider.com.br/Global/Transacao/UsuarioSubstituto/DefinirUsuarioSubstituto.aspx)
Form Fields: ScriptManager_TSM, MainSplitter_ClientState, RadToolTipHelp_ClientState, RadWindowManager_ClientState, __EVENTTARGET, __EVENTARGUMENT, TopPane1_ClientState and 51 more field(s).

Form #:91 Action URI:https://412-49.docspider.com.br/Portal/Consultas/Logs/FrmLogExecMenu.aspx (found at: https://412-49.docspider.com.br/Portal/Consultas/Logs/FrmLogExecMenu.aspx)
Form Fields: ScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 40 more field(s).

Form #:92 Action URI:https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaSuporte/TransferenciaAreaSuporte.aspx (found at: https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaSuporte/TransferenciaAreaSuporte.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, RadFormDecorator1_ClientState, hdnIdPortal and 151 more field(s).

Form #:93 Action URI:https://412-49.docspider.com.br/workflow/cadastros/calendarios/FrmCadastroDiasNaoUteis.aspx?idcalendario=1 (found at: https://412-49.docspider.com.br/workflow/cadastros/calendarios/FrmCadastroDiasNaoUteis.aspx?idcalendario=1)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, hdnRangeMinMaxDate, MainSplitter_ClientState, RadToolTipCuringa_ClientState and 53 more field(s).

Form #:94 Action URI:https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx (found at: https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, RadWindowZoom_ClientState, __EVENTTARGET and 239 more field(s).

Form #:95 Action URI:https://412-49.docspider.com.br/Generic/Transacao/AlterarParametros/BrowseAlterarParametros.aspx?grupo=12 (found at: https://412-49.docspider.com.br/Generic/Transacao/AlterarParametros/BrowseAlterarParametros.aspx?grupo=12)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 51 more field(s).

Form #:96 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Diretorios/BrowseCadastroDiretorio.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Diretorios/BrowseCadastroDiretorio.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, hdnIdSortField and 19 more field(s).

Form #:97 Action URI:https://412-49.docspider.com.br/Workflow/Cadastros/TipoDeAnexo/BrowseCadastroTipoDeAnexo.aspx (found at: https://412-49.docspider.com.br/Workflow/Cadastros/TipoDeAnexo/BrowseCadastroTipoDeAnexo.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState and 46 more field(s).

Form #:98 Action URI:https://412-49.docspider.com.br/asp/Usuario/frm_transfere_tarefa_usuario_wf.asp (found at: https://412-49.docspider.com.br/asp/Usuario/frm_transfere_tarefa_usuario_wf.asp)
Form Fields: btn2, btn1

Form #:99 Action URI:https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/LeiauteHtml/BrowseLeiauteHtml.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, __EVENTTARGET and 129 more field(s).

Form #:100 Action URI:https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx (found at: https://412-49.docspider.com.br/Global/Consultas/SearchUsers/BrowseSearchUsers.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, RadWindowZoom_ClientState, __EVENTTARGET and 78 more field(s).

Form #:101 Action URI:https://412-49.docspider.com.br/asp/wf_002/frm_deleta_fluxo.asp (found at: https://412-49.docspider.com.br/asp/wf_002/frm_deleta_fluxo.asp)
Form Fields: btnhabilita, btndesabilita, button2, btnapagar, btnlog, tipofiltro, tipoform, palavra, dstipoform, botao, linhas, paginadestino

Form #:102 Action URI:https://412-49.docspider.com.br/GED/Cadastros/TiposDeOpiniaoDeDocumento/BrowseCadastroTiposDeOpiniao.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/TiposDeOpiniaoDeDocumento/BrowseCadastroTiposDeOpiniao.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState, __EVENTTARGET, RadWindowLogs_ClientState and 52 more field(s).

Form #:103 Action URI:https://412-49.docspider.com.br/Generic/Cadastros/Parametros/BrowseCadastroParametros.aspx (found at: https://412-49.docspider.com.br/Generic/Cadastros/Parametros/BrowseCadastroParametros.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState, __EVENTTARGET, RadWindowLogs_ClientState and 46 more field(s).

Form #:104 Action URI:https://412-49.docspider.com.br/GED/Cadastros/TiposDeReferenciaParaPerguntasDeDocumento/BrowseCadastroTiposDeReferenciaParaPerguntas.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/TiposDeReferenciaParaPerguntasDeDocumento/BrowseCadastroTiposDeReferenciaParaPerguntas.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, TopPane1_ClientState, ListDialog_ClientState and 52 more field(s).

Form #:105 Action URI:https://412-49.docspider.com.br/GED/Transacao/TransferenciaPasta/BrowseTransferDocumentsToAnotherFolder.aspx (found at: https://412-49.docspider.com.br/GED/Transacao/TransferenciaPasta/BrowseTransferDocumentsToAnotherFolder.aspx)
Form Fields: RadScriptManager_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnFolderID, hdnTrue, hdnIdSortField, hdnIdSortOrder and 137 more field(s).

Form #:106 Action URI:https://412-49.docspider.com.br/Generic/Transacao/UploadArquivos/BrowseUploadArquivos.aspx (found at: https://412-49.docspider.com.br/Generic/Transacao/UploadArquivos/BrowseUploadArquivos.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, FormDecorator1_ClientState and 30 more field(s).

Form #:107 Action URI:https://412-49.docspider.com.br/Portal/Cadastros/Portal/BrowseCadastroPortal.aspx (found at: https://412-49.docspider.com.br/Portal/Cadastros/Portal/BrowseCadastroPortal.aspx)
Form Fields: scriptManager_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState, __EVENTTARGET, RadWindowLogs_ClientState and 44 more field(s).

Form #:108 Action URI:https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/Execucao.aspx?q=11 (found at: https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/Execucao.aspx?q=11)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 33 more field(s).

Form #:109 Action URI:https://412-49.docspider.com.br/GED/Cadastros/TiposDeDocumento/BrowseCadastroTiposDeDocumento.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/TiposDeDocumento/BrowseCadastroTiposDeDocumento.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 29 more field(s).

Form #:110 Action URI:https://412-49.docspider.com.br/GED/Cadastros/TiposDeIndexador/BrowseCadastroTiposIndexador.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/TiposDeIndexador/BrowseCadastroTiposIndexador.aspx)
Form Fields: RadStyleSheetManager1_TSSM, RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState and 35 more field(s).

Form #:111 Action URI:https://412-49.docspider.com.br/GED/Cadastros/PontosDeControle/BrowseCadastroClassPontosControle.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/PontosDeControle/BrowseCadastroClassPontosControle.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, ListDialog_ClientState, __EVENTTARGET, ListMult_ClientState and 52 more field(s).

Form #:112 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Idiomas/BrowseCadastroIdioma.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Idiomas/BrowseCadastroIdioma.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario, hdnIdSortField and 19 more field(s).

Form #:113 Action URI:https://412-49.docspider.com.br/Portal/Consultas/Logs/FrmLogExecMenu.aspx (found at: https://412-49.docspider.com.br/Portal/Consultas/Logs/FrmLogExecMenu.aspx)
Form Fields: ScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, __EVENTTARGET, __EVENTARGUMENT, RadWindowZoomMenu_ClientState and 52 more field(s).

Form #:114 Action URI:https://412-49.docspider.com.br/Global/Cadastros/Diretorios/BrowseCadastroDiretorio.aspx (found at: https://412-49.docspider.com.br/Global/Cadastros/Diretorios/BrowseCadastroDiretorio.aspx)
Form Fields: RadScriptManager1_TSM, hdnNomeUsuario, hdnIdUsuario, hdnIdSortField, hdnIdSortOrder, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState and 42 more field(s).

Form #:115 Action URI:https://412-49.docspider.com.br/asp/Usuario/adm_transfere_tarefa_usuario_wf.asp (found at: https://412-49.docspider.com.br/asp/Usuario/frm_transfere_tarefa_usuario_wf.asp)
Form Fields: btn1, btn2, metodo, btn3, idretorno, dsretorno, hidden_idcriador, btnnovopapel, todos1, id_centro_adm, todos2, id_cd_colaborador, btnexcluipapel, nm_cd_colaborador and 8 more field(s).

Form #:116 Action URI:https://412-49.docspider.com.br/GED/Cadastros/TiposDeReferenciaParaPerguntasDeDocumento/BrowseCadastroTiposDeReferenciaParaPerguntas.aspx (found at: https://412-49.docspider.com.br/GED/Cadastros/TiposDeReferenciaParaPerguntasDeDocumento/BrowseCadastroTiposDeReferenciaParaPerguntas.aspx)
Form Fields: RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, TopPane1_ClientState, ListDialog_ClientState and 62 more field(s).

Form #:117 Action URI:https://412-49.docspider.com.br/Generic/Transacao/UploadArquivos/BrowseUploadArquivos.aspx (found at: https://412-49.docspider.com.br/Generic/Transacao/UploadArquivos/BrowseUploadArquivos.aspx)
Form Fields: RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, hdnNomeUsuario, hdnIdUsuario,

FormDecorator1_ClientState and 28 more field(s).

Form #:118 Action URI:https://412-49.docspider.com.br/Portal/Consultas/Logs/FrmLogExecMenu.aspx (found at: https://412-49.docspider.com.br/Portal/Consultas/Logs/FrmLogExecMenu.aspx)
Form Fields: ScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, __EVENTTARGET, __EVENTARGUMENT, RadWindowZoomMenu_ClientState and 51 more field(s).

Form #:119 Action URI:https://412-49.docspider.com.br/PortalDocumentos/DocumentosPorTipo (found at: https://412-49.docspider.com.br/PortalDocumentos/DocumentosPorTipo)
Form Fields: tipoDocumento_input, tipoDocumento

Form #:120 Action URI:https://412-49.docspider.com.br/PortalDocumentos/DocumentosPorAreas (found at: https://412-49.docspider.com.br/PortalDocumentos/DocumentosPorAreas)
Form Fields: empresas_input, empresas, diretorias_input, diretorias, areas_input, areas

Form #:121 Action URI:https://412-49.docspider.com.br/Global/Zoom/ZoomEmpresa.aspx?chamador=empresa (found at: https://412-49.docspider.com.br/Global/Zoom/ZoomEmpresa.aspx?chamador=empresa)
Form Fields: __LASTFOCUS, RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 29 more field(s).

Form #:122 Action URI:https://412-49.docspider.com.br/Global/Zoom/ZoomDiretoria.aspx?chamador=diretoria&idempresa= (found at: https://412-49.docspider.com.br/Global/Zoom/ZoomDiretoria.aspx?chamador=diretoria&idempresa=)
Form Fields: __LASTFOCUS, RadScriptManager1_TSM, __EVENTTARGET, __EVENTARGUMENT, __VIEWSTATE, __VIEWSTATEGENERATOR, __EVENTVALIDATION, FormDecorator1_ClientState, RadToolTipManager1_ClientState and 36 more field(s).

Form #:123 Action URI:https://412-49.docspider.com.br/Global/Zoom/ZoomEmpresa.aspx?chamador=empresa (found at: https://412-49.docspider.com.br/Global/Zoom/ZoomEmpresa.aspx?chamador=empresa)
Form Fields: __LASTFOCUS, RadScriptManager1_TSM, FormDecorator1_ClientState, RadToolTipManager1_ClientState, MainSplitter_ClientState, RadToolTipHelp_ClientState, RadWindowManager1_ClientState and 45 more field(s).

NOTE: Forms with exactly the same form fields were considered identical even if they had different action URI. Only one such form is crawled, the other forms with exactly the same form fields are considered duplicate and are not crawled. If they are different forms and each of them should be crawled then change the scan settings accordingly.

The following forms were not crawled as their fields matched Form #6 above:
Form Action URI: https://412-49.docspider.com.br/PortalDocumentos/MeusFavoritos
Form Action URI: https://412-49.docspider.com.br/PortalDocumentos/DocumentosPorTipo
Form Action URI: https://412-49.docspider.com.br/PortalDocumentos/MaisAcessados
Form Action URI: https://412-49.docspider.com.br/PortalDocumentos/DocumentosPorAreas

The following forms were not crawled as their fields matched Form #29 above:
Form Action URI: https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx?RadUrid=56ad99a4-1d83-46f7-96c4-7414b506223b
Form Action URI: https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx?RadUrid=f466c819-a2a5-4f33-a513-3512689d1fda

The following forms were not crawled as their fields matched Form #34 above:
Form Action URI: https://412-49.docspider.com.br/GED/Consultas/Indicadores/SearchStatisticPanel/SearchStatisticPanel.aspx
Form Action URI: https://412-49.docspider.com.br/GED/Consultas/Indicadores/DocumentStatisticPanel/DocumentStatisticPanel.aspx

The following forms were not crawled as their fields matched Form #122 above:
Form Action URI: https://412-49.docspider.com.br/Global/Zoom/ZoomDiretoria.aspx

150170 Logout Links Discovered (1)

150170 Logout Links Discovered

Finding #	**415449**(69622001)
Unique #	**dca6359c-108c-4b0a-9292-adee9aaaefa7**
Group	Scan Diagnostics
CWE	-
OWASP	-
WASC	-

Severity	Information Gathered - Level 1
Detection Date	11 Jan 2023 18:24 GMT-0400

Details

Threat

The logout links discovered by the scanner are provided in the Results section. These links were present on the web application, but were not crawled since crawling these links would terminate the active authenticated session and negatively impact the crawling.

Logout links are identified automatically based on common logout regex patterns used by web applications. If the automatic identification technique does not work for your web application, you can configure a custom Logout Regular Expression for the web app under 'Exclusions' in the WAS UI.

Impact

N/A

Solution

N/A

Results

Number of logout links detected: 6
https://41-9.docspider.com.br/Login/Logout
https://412-49.docspider.com.br/Global/WebResource.axd?
d=-5d2ExITdtgvTPW2fvOYY-6WXlB3ImAHm7pShTxz4d4cKlum5Nbz19QB6zJc1ZaE8XmK2oGCNoW4fM9GXxUjesyQK_OSw971K4R2VtNHJsAABY9g_uL3UzMcHVgUolyW-TED-
CWdI9ct0QG0CbVr_PiQKh_T3GrkrKw1CBQCwV4kd1TZPNBHxyqtQ-Tq7CaPKxdwaoDEbUOr_emFXaWFng2&t=638089669490933368
https://412-49.docspider.com.br/Login/Logout
https://412-49.docspider.com.br/login/logout.aspx
https://412-49.docspider.com.br/login/logout.aspx?prg=/portaladmin/frmstart.aspx&url=url=portal=
javascript:logoutUser();

150176 In-scope JavaScript Libraries Detected (1)

WAS Scan Report

150176 In-scope JavaScript Libraries Detected

Finding #	**415451** (69622004)	**Severity**	Information Gathered - Level 1
Unique #	**3fcec98a-8881-4392-9b3c-29994c748ab8**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-200		
OWASP	-		
WASC	-		

Details

Threat

WAS will report "in-scope" JavaScript libraries discovered by the scanner during crawling and are provided in the Results section. In-scope means, links that are considered to be "in-scope" per the configuration set up for the Web Application. The discovered libraries are reported only once, based on the page on which they were first detected.

Each library is reported along with other information such as the URL of page on which it was first found, the version, and the URL of the .js file.

Impact

When including third-party JavaScript libraries, the application must effectively trust those libraries added. Without sufficient protection mechanisms, the functionality may be malicious in nature (i.e. either by coming from an untrusted source, being spoofed, or being modified in transit from a trusted source).

Solution

Use digital signatures or similar mechanisms to verify the software or data is from the expected source and has not been altered. Ensure libraries and dependencies, are consuming trusted repositories. If you have a higher risk profile, consider hosting an internal known-good repository that's vetted.

Results

Number of unique JS libraries: 8
Javascript library : Bootstrap
Version : 4.3.1
Script uri : https://412-49.docspider.com.br/NAssets/scripts/bootstrap/bootstrap.js
Found on the following page(only first page is reported):
 https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError

===

Javascript library : METAGeneratorReports
Version : Microsoft Visual InterDev 1.0
Found on the following page(only first page is reported):
 https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_programa_wf.asp

===

Javascript library : METAGeneratorReports
Version : Microsoft Visual Studio .NET 7.1
Found on the following page(only first page is reported):
 https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=53

===

Javascript library : PopperJS
Found on the following page(only first page is reported):
 https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError

===

Javascript library : jQuery
Version : 3.6.0
Script uri : https://412-49.docspider.com.br/NAssets/scripts/jquery/jquery-3.6.0.js
Found on the following page(only first page is reported):
 https://412-49.docspider.com.br/Login

===

Javascript library : jQuery.ui.autocomplete
Version : 1.13.2
Script uri : https://412-49.docspider.com.br/assets/scripts/jquery-ui-1.13.2.min.js
Found on the following page(only first page is reported):

https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

===

Javascript library : jQuery.ui.dialog
Version : 1.13.2
Script uri : https://412-49.docspider.com.br/assets/scripts/jquery-ui-1.13.2.min.js
Found on the following page(only first page is reported):
https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

===

Javascript library : jQuery.ui.tooltip
Version : 1.13.2
Script uri : https://412-49.docspider.com.br/assets/scripts/jquery-ui-1.13.2.min.js
Found on the following page(only first page is reported):
https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx

===

150247 Web Server and Technologies Detected (1)

WAS Scan Report

150247 Web Server and Technologies Detected

Finding #	415452(69622006)	**Severity**	Information Gathered - Level 1
Unique #	57eae5eb-431e-4f20-b5d0-bd50357fd391		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-200		
OWASP	-		
WASC	-		

Details

Threat

Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

Impact

An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

Solution

Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:

Results

Number of technologies detected: 4
Technology name: Apache
Technology version: Apache 2.2.3
Matched Components:
header match:
 Server:Apache/2.2.3 (Red Hat)
Matched links: reporting only first 3 links
http://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError

Technology name: Bootstrap
Matched Components:
html response match:
 spider não funciona corretamente sem o JavaScript ativado. Ative-o para continuar.
 </noscript>
 <link rel="shortcut icon" href="https://412-49.docspider.com.br/NAssets/images/favicon.png">
 <link href="https://412-49.docspider.com.br/NAssets/styles/bootstrap/bootstrap.css" rel="stylesheet">
 <link href="https://412-49.docspider.com.br/NAssets/styles/docspider/docspider.css" rel="stylesheet">
 <link href="https://412-49.docspider.com.br/NAssets/styles/theme/docspider.css"
script tag match:
 <script src="https://412-49.docspider.com.br/NAssets/scripts/bootstrap/bootstrap.js"></script>
 <script src="https://412-49.docspider.com.br/NAssets/scripts/bootstrap/popper.js"></script>
Matched links: reporting only first 3 links
https://412-49.docspider.com.br/
https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError

Technology name: Microsoft ASP.NET
Matched Components:
html response match:
 9:e330518b:1e771326:8e6f0d33:1f3a7489:b2e06756:92fe8ea0:fa31b949:490a9d4e:bd8f85e4">
 <input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="">
 <input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="">
 <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="LU+kLkDScVllCjrcBwKwUkbt74pqJVYFNWaW/sZuWhixJ59cRMXIghNUk/
Y2zQmLTXj0PdrZYacDXJyuW20CBSKRih+XtES5qtgm1gCW2oXBsXJ1L6h8HNfFYrkfiFLNpo7VOLRCvzqzYU9n9T50JzN6KeWNNXOOHVY1kl2zqGF
+NCLUQ8IrGFJSbaxTtCNmVyO8EbzghNUrc
cookie match:
 ASP.NET_SessionId:jfrezx1bhono4vnfk3qbnenf
 ASPSESSIONIDAGQQQRDA:CEEHMCOCJAHKFCKNLAIHHGEG
Matched links: reporting only first 3 links
https://412-49.docspider.com.br/PortalAdmin/frmStart.aspx?portal=1
https://412-49.docspider.com.br/PortalDocumentos
https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError

WAS Scan Report

150528 Server Returns HTTP 4XX Error Code During Scanning (1)

150528 Server Returns HTTP 4XX Error Code During Scanning

Finding #	**586763**(69621987)	Severity	Information Gathered - Level 1
Unique #	**89869df9-4742-460e-9ea5-b7fa8f570894**		
Group	Scan Diagnostics	Detection Date	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

During the WAS scan, links with HTTP 4xx response code were observed and these are listed in the Results section. The HTTP 4xx message indicates a client error. The list of supported 4xx response code are as below:

400 - Bad Request
401 - Unauthorized
403 - Forbidden
404 - Not Found
405 - Method Not Allowed
407 - Proxy Authentication Required
408 - Request Timeout
413 - Payload Too Large
414 - URI Too Long

Impact

The presence of a HTTP 4xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depends on responses to detect many vulnerabilities if the link does not respond with an expected response then any vulnerabilities present on such links may not be detected.

Solution

Review each link to determine why the client encountered an error while requesting the link. Additionally review and investigate the results of QID 150042 which lists 5xx errors, QID 150019 which lists unexpected response codes and QID 150097 which lists a potential blocked request.

Results

Number of links with 4xx response code: 6
(Only first 50 such links are listed)

404 https://412-49.docspider.com.br/Ativar
404 https://412-49.docspider.com.br/Buscar
404 https://412-49.docspider.com.br/Clientes/DocspiderSQL/Default.htm
404 https://412-49.docspider.com.br/Default.htm
404 https://412-49.docspider.com.br/Inativar
401 https://412-49.docspider.com.br/Login/Authenticate

150546 First Link Crawled Response Code Information (1)

WAS Scan Report

150546 First Link Crawled Response Code Information

Finding #	**586764**(69621998)	**Severity**	Information Gathered - Level 1
Unique #	**1dfcbc52-1545-4c4f-b02e-a63270a4826c**		
Group	Scan Diagnostics	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Web server returned the following information from where the Web application scanning engine initiated. Information reported includes First Link Crawled, response Code, response Header, and response Body (first 500 characters). The first link crawled is the "Web Application URL (or Swagger file URL)" set in the Web Application profile.

Impact

An erroneous response might be indicative of a problem in the Web server, or the scan configuration.

Solution

Review the information to check if this is in line with the expected scan configuration. Refer to the output of QIDs 150009, 150019, 150021, 150042 and 150528 (if present) for additional details.

Results

Base URI: https://412-49.docspider.com.br/
Response Code: 200
Response Header:
 Date: Wed, 11 Jan 2023 21:24:08 GMT
 Content-Type: text/html; charset=ISO-8859-1
 Content-Encoding: gzip
 Last-Modified: Mon, 05 Jul 2021 22:43:41 GMT
 Accept-Ranges: bytes
 ETag: "9d444f34ef71d71:0"
 Vary: Accept-Encoding
 X-Frame-Options: SAMEORIGIN
 x-Content-Type-Options: nosnif

Response Body:
<!DOCTYPE html><html lang="pt-BR"><head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
<meta name="description" content="Docspider Login">
<title>Docspider | Login</title>
<noscript>
Lamentamos, mas o Docspider não funciona corretamente sem o JavaScript ativado. Ative-o para continuar.
</noscript>
<link rel="shortcut icon" href="ht
...

Security Weaknesses (11)

150089 Links to non-routable resources discovered in externally facing content (1)

150089 Links to non-routable resources discovered in externally facing content

Finding #	474590(69621995)
Unique #	a982636b-e08f-40eb-ac90-00c7599857b1
Group	Security Weaknesses
CWE	-
OWASP	-
WASC	-

Severity	Information Gathered - Level 3
Detection Date	11 Jan 2023 18:24 GMT-0400

Details

Threat

Links pointing to non-routable IPs (see RFC 1918 - Address Allocation for Private Internets) were discovered on the externally-facing content. These links were present on the target Web application, but were not crawled.

Impact

Such links could be either result of bad link resolution during porting QA web application to production, or due to injected malicious content to access for example customer's network equipment.

Solution

Review the links and ensure only valid links are served by the web application.

Results

total links pointing to internal resources: 2
https://localhost/jF0uQ6fYD discovered on external page: https://412-49.docspider.com.br/asp/wf_002/frm_deleta_fluxo.asp
https://localhost/jzP2md08A discovered on external page: https://412-49.docspider.com.br/asp/wf_002/frm_deleta_fluxo.asp

150210 Information Disclosure via Response Header (1)

WAS Scan Report

150210 Information Disclosure via Response Header

Finding #	**415437**(69621985)
Unique #	**5225e00f-e3c2-4105-a3a0-2bcc61a0f278**

Severity	Information Gathered - Level 3

Group	Security Weaknesses
CWE	CWE-16, CWE-201
OWASP	A5 Security Misconfiguration
WASC	WASC-15 APPLICATION MISCONFIGURATION

Detection Date	11 Jan 2023 18:24 GMT-0400

Details

Threat

HTTP response headers like 'Server', 'X-Powered-By', 'X-AspNetVersion', 'X-AspNetMvcVersion' could disclose information about the platform and technologies used by the website. The HTTP response include one or more such headers.

Impact

The headers can potentially be used by attackers for fingerprinting and launching attacks specific to the technologies and versions used by the web application. These response headers are not necessary for production sites and should be disabled.

Solution

Disable such response headers, remove them from the response, or make sure that the header value does not contain information which could be used to fingerprint the server-side components of the web application.

Results

One or more response headers disclosing information about the application platform were present on the following pages:
(Only first 50 such pages are reported)

GET http://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError response code: 301
Server: Apache/2.2.3 (Red Hat)

150203 Misconfigured header: X-Content-Type-Options (1)

WAS Scan Report

150203 Misconfigured header: X-Content-Type-Options

Finding # 415463(69622018)	**Severity** Information Gathered - Level 2
Unique # e69e01fb-5d01-45ac-9b8d-3fac635e644b	
Group Security Weaknesses	**Detection Date** 11 Jan 2023 18:24 GMT-0400
CWE CWE-16, CWE-1032	
OWASP A5 Security Misconfiguration	
WASC WASC-15 APPLICATION MISCONFIGURATION	

Details

Threat

X-Content-Type-Options response header is configured incorrectly. The scanner reports misconfigured X-Content-Type-Options header on all types of static and dynamic responses. The checks are performed on 4xx and 5xx responses too. It is possible to see a directory reported under this QID as well.

Impact

All Web browsers employ a content-sniffing algorithm that inspects the contents of HTTP responses and also occasionally overrides the MIME type provided by the server. These algorithms let browsers render 1% of HTTP responses where Content-Type header is missing. When these content sniffing algorithms are not designed with proper security considerations, an attacker can leverage the functionality to perform cross-site scripting (XSS) attack. This specific case is known as a Content-Sniffing XSS (CS-XSS) attack. If X-Content-Type-Options header value is not set correctly, an attacker can potentially trick the browser into treating a non-HTML response as HTML.

Solution

It is recommended to set the value of the X-Content-Type-Options header to 'nosniff'. Also ensure that the Content-Type header is set correctly on responses.

Results

X-Content-Type-Options: Header misconfigured
Expected value: nosniff.
Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/ response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/Login/Authenticate response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/NAssets/images/favicon.png response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/NAssets/styles/bootstrap/bootstrap.css response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/NAssets/styles/docspider/docspider.css response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Login/Views/Shared/Common.css response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/NAssets/styles/theme/docspider.css response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/NAssets/scripts/jquery/jquery-3.6.0.js response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError response code: 500

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/NAssets/images/logo.png response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/NAssets/styles/docspider/docspider-font-icon.css response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/NAssets/scripts/bootstrap/popper.js response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/NAssets/scripts/bootstrap/bootstrap.js response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/NAssets/styles/docspider/error-style.css response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/PortalDocumentos/Home response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=WU6bd74ziZ3ixaEoFn-7VTYpFuBsV29bPcmQWwoV7SMPUaR3FLIiFA-ogJeyedaandpqbubDc8FTsBasWWQRiIxU4JlOYbaS2i032jxGj9jZ4dwL9L7VXUGn9laj7eKxiLu-n2dBagfCOcNnOiXPv6gY3lvuhKgTF_0O9Qw90QWe3ordZtO6y7HQIWDJWoeTWfyctukCehrAw0ETzt12Bw2&t=638089669490933368 response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoDeBusca=1 response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?
termoBuscaFiltro=1&modoBusca=1&tipoBusca=2&semAsPalavras=1&comValidadeIndefinida=1 response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Busca/PalavraIrrelevante response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?PageNumber=1&PageSize=50&HasNextPage=False&TotalItemCount=3 response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/Busca/Sinonimo response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:

X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=53 response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=GBn3eDvns8PQD2wVQLVg8stGbq2PkYGYf16n6Cu-CFFpa6OTrR94X5ngrfd548MeQLkFK_z89b-SQ5xJTVFsAE9moGhT_NW2zxsy-ndKDzwuuIvDcpB1sroE4h6JJfnQdcumiL7BXCGCfKvcWd9voUBDgA7bawx7mPNX1vAz0W6tbEGu4MBYvCdiqMe6en6s78YtMBlDkEQ6mZ3ZjF0gyQ2&t=638089669490933368 response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: GET https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx response code: 200

X-Content-Type-Options: Header misconfigured. Misconfigured response header:
X-Content-Type-Options:nosnif on the link: POST https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200

150206 Content-Security-Policy Not Implemented (1)

150206 Content-Security-Policy Not Implemented

Finding #	**415465**(69622021)
Unique #	**d6de9b1c-27cd-4150-aa7b-87143576d83f**

Severity	Information Gathered - Level 2

Group	Security Weaknesses
CWE	CWE-16, CWE-1032
OWASP	A5 Security Misconfiguration
WASC	WASC-15 APPLICATION MISCONFIGURATION

Detection Date	11 Jan 2023 18:24 GMT-0400

Details

Threat

No Content-Security-Policy (CSP) is specified for the page. WAS checks for the missing CSP on all static and dynamic pages. It checks for CSP in the response headers (Content-Security-Policy, X-Content-Security-Policy or X-Webkit-CSP) and in response body (http-equiv="Content-Security-Policy" meta tag).

HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security it's important to set appropriate CSP policies on 4xx and 5xx responses as well.

Impact

Content-Security Policy is a defense mechanism that can significantly reduce the risk and impact of XSS attacks in modern browsers. The CSP specification provides a set of content restrictions for web resources and a mechanism for transmitting the policy from a server to a client where the policy is enforced. When a Content Security Policy is specified, a number of default behaviors in user agents are changed; specifically inline content and JavaScript eval constructs are not interpreted without additional directives. In short, CSP allows you to create a whitelist of sources of the trusted content. The CSP policy instructs the browser to only render resources from those whitelisted sources. Even though an attacker can find a security vulnerability in the application through which to inject script, the script won't match the whitelisted sources defined in the CSP policy, and therefore will not be executed.

The absence of Content Security Policy in the response will allow the attacker to exploit vulnerabilities as the protection provided by the browser is not at all leveraged by the Web application. If secure CSP configuration is not implemented, browsers will not be able to block content-injection attacks such as Cross-Site Scripting and Clickjacking.

Solution

Appropriate CSP policies help prevent content-injection attacks such as cross-site scripting (XSS) and clickjacking. It's recommended to add secure CSP policies as a part of a defense-in-depth approach for securing web applications.

References:
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://developers.google.com/web/fundamentals/security/csp/

Results

Content-Security-Policy: Header missing
Response headers on link: GET https://412-49.docspider.com.br/ response code: 200
Date: Wed, 11 Jan 2023 21:24:08 GMT
Content-Type: text/html; charset=ISO-8859-1
Content-Encoding: gzip
Last-Modified: Mon, 05 Jul 2021 22:43:41 GMT
Accept-Ranges: bytes
ETag: "9d444f34ef71d71:0"
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
x-Content-Type-Options: nosnif

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://412-49.docspider.com.br/ response code: 200
POST https://412-49.docspider.com.br/Login/Authenticate response code: 200
GET https://412-49.docspider.com.br/NAssets/images/favicon.png response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/bootstrap/bootstrap.css response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/docspider.css response code: 200
GET https://412-49.docspider.com.br/Login/Views/Shared/Common.css response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/theme/docspider.css response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/jquery/jquery-3.6.0.js response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError response code: 500

GET https://412-49.docspider.com.br/NAssets/images/logo.png response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/docspider-font-icon.css response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/bootstrap/popper.js response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/bootstrap/bootstrap.js response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/error-style.css response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/Home response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=WU6bd74ziZ3ixaEoFn-7VTYpFuBsV29bPcmQWwoV7SMPUaR3FLIiFA-
ogJeyedaandpqbubDc8FTsBasWWQRiIxU4JlOYbaS2i032jxGj9jZ4dwL9L7VXUGn9laj7eKxiLu-
n2dBagfCOcNnOiXPv6gY3lvuhKgTF_0O9Qw90QWe3ordZtO6y7HQIWDJWoeTWfyctukCehrAw0ETzt12Bw2&t=638089669490933368 response code: 200
GET https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoDeBusca=1 response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoBuscaFiltro=1&modoBusca=1&tipoBusca=2&semAsPalavras=1&comValidadeIndefinida=1 response code: 200
GET https://412-49.docspider.com.br/Busca/PalavraIrrelevante response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?PageNumber=1&PageSize=50&HasNextPage=False&TotalItemCount=3 response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200
POST https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx response code: 200
GET https://412-49.docspider.com.br/Busca/Sinonimo response code: 200
GET https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=53 response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=GBn3eDvns8PQD2wVQLVg8stGbq2PkYGYf16n6Cu-CFFpa6OTrR94X5ngrfd548MeQLkFK_z89b-
SQ5xJTVFsAE9moGhT_NW2zxsy-
ndKDzwuuIvDcpB1sroE4h6JJfnQdcumiL7BXCGCfKvcWd9voUBDgA7bawx7mPNX1vAz0W6tbEGu4MBYvCdiqMe6en6s78YtMBlDkEQ6mZ3ZjF0gyQ2&t=638089669490933368 response code:
200
POST https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200

150208 Missing header: Referrer-Policy (1)

150208 Missing header: Referrer-Policy

Finding #	**415438**(69621986)
Unique #	**d71ca155-09d1-4227-9257-b2c1723aa55e**

Severity	Information Gathered - Level 2

Group	Security Weaknesses
CWE	CWE-16, CWE-1032
OWASP	A5 Security Misconfiguration
WASC	WASC-15 APPLICATION MISCONFIGURATION

Detection Date	11 Jan 2023 18:24 GMT-0400

Details

Threat

No Referrer Policy is specified for the link. WAS checks for the missing Referrer Policy on all static and dynamic pages. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

If the Referrer Policy header is not found , WAS checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

Impact

The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

Solution

Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Results

Referrer-Policy: Header missing
Response headers on link: GET https://412-49.docspider.com.br/ response code: 200
Date: Wed, 11 Jan 2023 21:24:08 GMT
Content-Type: text/html; charset=ISO-8859-1
Content-Encoding: gzip
Last-Modified: Mon, 05 Jul 2021 22:43:41 GMT
Accept-Ranges: bytes
ETag: "9d444f34ef71d71:0"
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
x-Content-Type-Options: nosnif

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://412-49.docspider.com.br/ response code: 200
POST https://412-49.docspider.com.br/Login/Authenticate response code: 200
GET https://412-49.docspider.com.br/NAssets/images/favicon.png response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/bootstrap/bootstrap.css response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/docspider.css response code: 200
GET https://412-49.docspider.com.br/Login/Views/Shared/Common.css response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/theme/docspider.css response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/jquery/jquery-3.6.0.js response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError response code: 500
GET https://412-49.docspider.com.br/NAssets/images/logo.png response code: 200

GET https://412-49.docspider.com.br/NAssets/styles/docspider/docspider-font-icon.css response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/bootstrap/popper.js response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/bootstrap/bootstrap.js response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/error-style.css response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/Home response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=WU6bd74ziZ3ixaEoFn-7VTYpFuBsV29bPcmQWwoV7SMPUaR3FLIiFA-ogJeyedaandpqbubDc8FTsBasWWQRiIxU4JlOYbaS2i032jxGj9jZ4dwL9L7VXUGn9laj7eKxiLu-n2dBagfCOcNnOiXPv6gY3lvuhKgTF_0O9Qw90QWe3ordZtO6y7HQIWDJWoeTWfyctukCehrAw0ETzt12Bw2&t=638089669490933368 response code: 200
GET https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoDeBusca=1 response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoBuscaFiltro=1&modoBusca=1&tipoBusca=2&semAsPalavras=1&comValidadeIndefinida=1 response code: 200
GET https://412-49.docspider.com.br/Busca/PalavraIrrelevante response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?PageNumber=1&PageSize=50&HasNextPage=False&TotalItemCount=3 response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200
POST https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx response code: 200
GET https://412-49.docspider.com.br/Busca/Sinonimo response code: 200
GET https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=53 response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=GBn3eDvns8PQD2wVQLVg8stGbq2PkYGYf16n6Cu-CFFpa6OTrR94X5ngrfd548MeQLkFK_z89b-SQ5xJTVFsAE9moGhT_NW2zxsy-ndKDzwuuIvDcpB1sroE4h6JJfnQdcumiL7BXCGCfKvcWd9voUBDgA7bawx7mPNX1vAz0W6tbEGu4MBYvCdiqMe6en6s78YtMBlDkEQ6mZ3ZjF0gyQ2&t=638089669490933368 response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200

150248 Missing header: Permissions-Policy (1)

WAS Scan Report

150248 Missing header: Permissions-Policy

Finding #	**438206**(69622008)	**Severity**	Information Gathered - Level 2
Unique #	81b0385d-2eab-49b3-a3a5-324bf4b04297		
Group	Security Weaknesses	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-284		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

The Permissions-Policy response header is not present.

Impact

Permissions-Policy allows web developers to selectively enable, disable, or modify the behavior of some of the browser features and APIs within their application.

A user agent has a set of supported features(Policy Controlled Features), which is the set of features which it allows to be controlled through policies.

Not defining policy for unused and risky policy controlled features may leave application vulnerable.

Solution

It is recommended to define policy for policy controlled features to make application more secure.

References:
Permissions-Policy W3C Working Draft
Policy Controlled Features

Results

Permissions-Policy: Header missing
Response headers on link: GET https://412-49.docspider.com.br/ response code: 200
Date: Wed, 11 Jan 2023 21:24:08 GMT
Content-Type: text/html; charset=ISO-8859-1
Content-Encoding: gzip
Last-Modified: Mon, 05 Jul 2021 22:43:41 GMT
Accept-Ranges: bytes
ETag: "9d444f34ef71d71:0"
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
x-Content-Type-Options: nosnif

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://412-49.docspider.com.br/ response code: 200
POST https://412-49.docspider.com.br/Login/Authenticate response code: 200
GET https://412-49.docspider.com.br/NAssets/images/favicon.png response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/bootstrap/bootstrap.css response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/docspider.css response code: 200
GET https://412-49.docspider.com.br/Login/Views/Shared/Common.css response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/theme/docspider.css response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/jquery/jquery-3.6.0.js response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError response code: 500
GET https://412-49.docspider.com.br/NAssets/images/logo.png response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/docspider-font-icon.css response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/bootstrap/popper.js response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/bootstrap/bootstrap.js response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/error-style.css response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/Home response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=WU6bd74ziZ3ixaEoFn-7VTYpFuBsV29bPcmQWwoV7SMPUaR3FLIiFA-
ogJeyedaandpqbubDc8FTsBasWWQRiIxU4JlOYbaS2i032jxGj9jZ4dwL9L7VXUGn9laj7eKxiLu-
n2dBagfCOcNnOiXPv6gY3lvuhKgTF_0O9Qw90QWe3ordZtO6y7HQIWDJWoeTWfyctukCehrAw0ETzt12Bw2&t=638089669490933368 response code: 200
GET https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200

POST https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoDeBusca=1 response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoBuscaFiltro=1&modoBusca=1&tipoBusca=2&semAsPalavras=1&comValidadeIndefinida=1 response code: 200
GET https://412-49.docspider.com.br/Busca/PalavraIrrelevante response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?PageNumber=1&PageSize=50&HasNextPage=False&TotalItemCount=3 response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200
POST https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx response code: 200
GET https://412-49.docspider.com.br/Busca/Sinonimo response code: 200
GET https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=53 response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=GBn3eDvns8PQD2wVQLVg8stGbq2PkYGYf16n6Cu-CFFpa6OTrR94X5ngrfd548MeQLkFK_z89b-
SQ5xJTVFsAE9moGhT_NW2zxsy-
ndKDzwuuIvDcpB1sroE4h6JJfnQdcumiL7BXCGCfKvcWd9voUBDgA7bawx7mPNX1vAz0W6tbEGu4MBYvCdiqMe6en6s78YtMBlDkEQ6mZ3ZjF0gyQ2&t=638089669490933368 response code:
200
POST https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200

150249 Misconfigured Header: Cache-Control (1)

WAS Scan Report

150249 Misconfigured Header: Cache-Control

Finding #	**438207**(69622009)	**Severity**	Information Gathered - Level 2
Unique #	**f5046513-34e6-4465-acc9-cb906ec2b711**		
Group	Security Weaknesses	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-525		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

Cache-Control header present but directives may not configured to adequately safeguard sensitive information.

For Example:
Cache-Control directive set to public.

max-age value is greater than 86400.

Impact

If directive is set to public, the resource can be stored by any cache.

If max-age value is greater than 86400 for sensitive information may lead to information leakage.

Solution

Please check that resources with sensitive information are not configured with Cache-Control public directive.

Also please make sure that max-age directive value set properly to not cache sensitive information for longer period than needed.

References:
Mozilla Documentation Cache-Control

Results

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/Login/Views/Shared/Common.css response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=WU6bd74ziZ3ixaEoFn-7VTYpFuBsV29bPcmQWwoV7SMPUaR3FLIiFA-ogJeyedaandpqbubDc8FTsBasWWQRiIxU4JlOYbaS2i032jxGj9jZ4dwL9L7VXUGn9laj7eKxiLu-n2dBagfCOcNnOiXPv6gY3lvuhKgTF_0O9Qw90QWe3ordZtO6y7HQIWDJWoeTWfyctukCehrAw0ETzt12Bw2&t=638089669490933368 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=GBn3eDvns8PQD2wVQLVg8stGbq2PkYGYf16n6Cu-CFFpa6OTrR94X5ngrfd548MeQLkFK_z89b-SQ5xJTVFsAE9moGhT_NW2zxsy-ndKDzwuuIvDcpB1sroE4h6JJfnQdcumiL7BXCGCfKvcWd9voUBDgA7bawx7mPNX1vAz0W6tbEGu4MBYvCdiqMe6en6s78YtMBlDkEQ6mZ3ZjF0gyQ2&t=638089669490933368 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:public, max-age=31536000 on the link: GET https://412-49.docspider.com.br/PortalAdmin/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=RadScriptManager1_TSM&compress=1&_TSM_CombinedScripts_=%3b%3bSystem.Web.Extensions%2c+Version%3d4.0.0.0%2c+Culture%3dneutral%2c+PublicKeyToken%3d31bf3856ad364e35%3apt-BR%3af7ba41a4-e843-4f12-b442-8e407f37c316%3aea597d4b%3ab25378d2%3bTelerik.Web.UI%2c+Version%3d2021.3.1111.45%2c+Culture%3dneutral%2c+PublicKeyToken%3d121fae78165ba3d4%3apt-BR%3ab406acc5-0028-4c73-8915-a9da355d848a%3a16e4e7cd%3aed16cbdc%3af7645509%3a88144a7a%3a4877f69a%3a33715776%3a86526ba7%3a874f8ea2%3a24ee1bba%3ac128760b%3af46195d3%3a19620875%3acda80b3%3a383e4ce8%3a11a04f7e%3aa1a4383a%3a6d43f6d9%3ae330518b%3a1e771326%3a8e6f0d33%3a1f3a7489%3ab2e06756%3a92fe8ea0%3afa31b949%3a490a9d4e%3abd8f85e4 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=dLtIFocIUn_6CH4geLlN-p3aD-LdGyzGrdMUJw6OZWl5ZxCgqv3__izHjQo1HD_94qxlhj9Jyg31RGFihhCfDfenSfrPHIfhVv800w4SozHUoHDxmTCW-dSm-CgE3gTwHba6Rmcsxz0pZCEpbRrPXT4t0mQpqNi6fJB0z72gTgBGfoadiNEWdry-3c16h1_O0&t=638089669480620669 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.

Cache-Control:public on the link: GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=MY6Dg9PtzUVZ78bK4R8qvNyjr6sR_IBMAiwezJpT-yRuJXo35H6WqE3IKL_tMWk_4XlDsqOwjuxKREWmy5j0aLhYWUDiWbGRZlp-AaaSE2z20P7yOzb2LjFtEUOW_7Ei-ZuKfqhK3UR6fn0Ochgx9LVp5X2cJTS12bUpMt6gnfuPTondq5M8qRhpuoCtBVoa0&t=638089669480620669 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=Sy0b6rN6aDu9HWPir-p1zBJRnRKCChCjmorYB5tKQc7SUPqMntUGAMx4v8iMg5MJSNwdwfMS1GTROrg5GM7x4RNPl_teZnHT2k4OIz8MKpZ19sEulxM7C5Enh_noVcbkHwMqe49oog6dUtTZWeY-dGeOjZMxBbg9sGjMy4m4uPG94VrLY2wPPq3dk9IZz8Lg0&t=638089669480620669 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=2AszK6veUVMmmAigugstETaNLIDaAoHf5dZyVgvCQT7xFCaxlUrN81pBa-CuZhKG9CygcLWdnmQZGoGUVsllKbwgJOJG4m9dEu39pZ7rtueRu0zvO3lya3PDVmOdgJUAPEB8bg3OYAzHw8hhBEbj_H_Y9QM2agFzMlCOn2UTI7Q16kiLjMaMLfslB6mthp516m7O_YlG9g4s
response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=oHeFs-vFgpFaFPDLm0Y4YeZpOLhZl0hzrvVKkOGXckfx-iOJRacsDtypLG4Jqzb2neAhifUx79ImBYEK7aBQgsrVia_Xkl8Xpsy20XTRy4V40CabN5FT2ldWOVedue8s5-i37AziNaDRwpaz6RD1AOjUuOcCAzC7CqtEVI6mXlRxWIfjvgzxTlJqc_-AZvT80&t=638089669480620669 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=xGMtP4F6JAwD6n6BMSVyxUvszhLTAemCWNmcmb1M0x6fjxxzawlCkW1kx_5pyAURuhTHec9eXBLfMF8rsybdPYYNn5iOTlLPHBBAGvp2A-zeIqyE7AHW3RgJe8jDL-iMvYxmnPKl0BDZc4OK7coXCYMiCRUKr6268QBpW31UMleu3suiKvNM-s-bBQEm92QSk_VTHEwdfR-H6yn_Tm9Z_w2&t=638089669490933368 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/Global/WebResource.axd?d=xdaW2rHWkELFGrbWB5Vtk0nwkQDU13z-i1Xo3SIUfQk5SFACfHK-5QEDSUnWokqosNC9NbReyujAxKV6aLeG9UDS8nmualHoGJYtVDefLBUzMBksgqH6PC6CjJu8znN9dmnhuK-DidRSoF-JybPIxqZz-En3G_JtngxoOUfGhdttg0UOBT8BNJDwsbOvMSlT0&t=638089669480620669 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/Global/WebResource.axd?d=pynGkmcFUV13He1Qd6_TZJBNgYPfeenQk08ChD7hGjchvlLLYruMNacFwTkhu4DU1e3RBiMAPo9xaXaCfPK1UA2&t=637453961640000000 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/Global/WebResource.axd?d=s-JKKg1ZQXNcRCC0VH8qILSikZ2RMwCcexb-2_yGl73fJik9wnC78O3DyuTGi4tRvhzWXaDWUgwmOyRPfqV3gdFNAY3NvBLUsjm6Ledtg8CO-embihnM0Yvqzi_xlpW2_XZY6KS1b59po7HAp_GLS8EJUd-8HSDExSgNBY3bx7VN9LpfWfdLnfhl0n2dcWp056VT96fCcSSVl5lSRl-mgQ2&t=638089669490933368 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:public, max-age=31536000 on the link: GET https://412-49.docspider.com.br/Global/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=RadScriptManager1_TSM&compress=1&_TSM_CombinedScripts_=%3b%3bSystem.Web.Extensions%2c+Version%3d4.0.0.0%2c+Culture%3dneutral%2c+PublicKeyToken%3d31bf3856ad364e35%3apt-BR%3af7ba41a4-e843-4f12-b442-8e407f37c316%3aea597d4b%3ab25378d2%3bTelerik.Web.UI%2c+Version%3d2021.3.1111.45%2c+Culture%3dneutral%2c+PublicKeyToken%3d121fae78165ba3d4%3apt-BR%3ab406acc5-0028-4c73-8915-a9da355d848a%3a16e4e7cd%3aed16cbdc%3a4877f69a%3a33715776%3a86526ba7%3a874f8ea2%3af7645509%3a24ee1bba%3ac128760b%3af46195d3%3a19620875%3acda80b3%3a383e4ce8%3a88144a7a%3a11a04f7e%3ae330518b%3a1e771326%3a8e6f0d33%3a1f3a7489%3a6a6d718d%3ab7778d6c%3a6d43f6d9%3ab2e06756%3a92fe8ea0%3afa31b949%3a490a9d4e%3abd8f85e4 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/Global/ScriptResource.axd?d=nv7asgRUU0tRmHNR2D6t1D5lKGQiPsRHxe3e4nls-ssJ8FJmZj8NI-Wcbn68XxdMHROhvcsr_UygAotofU0M6OXWZCbD9j-0q2DMsndXQ2dNqMXvs77cO_0RjwaW8nWJyhUjIFW8cXEvfbal6BJ_eg2&t=79e27d6 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:public, max-age=31536000 on the link: GET https://412-49.docspider.com.br/Global/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=RadScriptManager1_TSM&compress=1&_TSM_CombinedScripts_=%3b%3bSystem.Web.Extensions%2c+Version%3d4.0.0.0%2c+Culture%3dneutral%2c+PublicKeyToken%3d31bf3856ad364e35%3apt-BR%3af7ba41a4-e843-4f12-b442-8e407f37c316%3aea597d4b%3ab25378d2%3bTelerik.Web.UI%2c+Version%3d2021.3.1111.45%2c+Culture%3dneutral%2c+PublicKeyToken%3d121fae78165ba3d4%3apt-BR%3ab406acc5-0028-4c73-8915-a9da355d848a%3a16e4e7cd%3aed16cbdc%3a4877f69a%3a33715776%3a86526ba7%3a874f8ea2%3af7645509%3a24ee1bba%3ac128760b%3af46195d3%3a19620875%3acda80b3%3a383e4ce8%3a88144a7a%3a11a04f7e%3ae330518b%3a1e771326%3a8e6f0d33%3a1f3a7489%3a6a6d718d%3ab7778d6c%3a6d43f6d9%3ae085fe68%3ab2e06756%3a92fe8ea0%3afa31b949%3a490a9d4e%3abd8f85e4 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/GED/WebResource.axd?d=GDbtDjWQpDx4io7GeCJyIWgGNYqwjmEtv58P1VfGelGa0GIgHybXjAnb4Q4DyumRs4msA5As27adaGUD6SyZQYm11TiwPj09IFyn7J6lpODN7s-7vrBaCqlx8f0g9K9uofpmjwSTtwVTSbPufY5JFBVIz3D-o9Ur4kESs5vbEh5ZeL0&t=638089669480620669 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/GED/WebResource.axd?d=MXgY26JaQwbFUvrpZL9oMS9OGDQaICUqSb9tD6fjme4rinTroYeyt3ZY11litJVcHDaYGMjFhmYoNMx70XQXcWu9wYmGIRot75XlEUNcShrHm_Ya1zkorIoO26f8-GGsvx3fUzvUMruvX2Stz4xXh5vTEp5Txvr5tiBMopi8Z3wq4dw8ezZhURioQYbs7UQ3yRoQ8uk8VomCpKzqMCTmBg2&t=638089669490933368 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/GED/WebResource.axd?d=MtJ0pTJ0U6V9nyEI-32pl3rdgIUeCJgTrAo0tRdmQ6bDKvt6ojutxIcLNEhfpJVX6MqSN2pFB9LSdtY1i445FFqPwiuLllEgq0mGqbwaCtnzgw5A6DYZYwrjpCpkQ79oubS5KTfiugZ9jyM7wVlgwSdh(
response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/GED/WebResource.axd?d=dLtIFocIUn_6CH4geLlN-l5WFWxgOfai84NXJE0KI4-JDCYJ2qgmRVepyGTzmbwzjjt_rrvUDaGpBTFu88_fgniESKog2kW5WQj7EtcKH7Fdj9jMhnvkcaSWoPA9izVaLO26LpuViHhmZQXsChQ_5JLcol0KLLZ7jleFzF6guASAZYOeJU_3EQ74TQmv26kY
response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.
Cache-Control:public on the link: GET https://412-49.docspider.com.br/GED/WebResource.axd?d=xGMtP4F6JAwD6n6BMSVyxS6JXfZO4uu-eKDD4vXyy2kcOoc8KfsqEQZs53r1qwN5Z7m-gKlPWNTjRBleMSXPqIJNL0SQQrmkdOK9NaLR7UvSNJC9us-QoLNXxXLM0ilShl9R5uhT62G6tHogyC2tO644NcNEe6nsfn8Rwz3Febl-GBYWBbS19PBJ6ChgojQxCoAjvYqepzziq6iJbx4hhg2&t=638089669490933368 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found. Cache-Control max-age directive's value is greater than 86400.
Cache-Control:public, max-age=31536000 on the link: GET https://412-49.docspider.com.br/GED/Telerik.Web.UI.WebResource.axd?_TSM_HiddenField_=RadScriptManager1_TSM&compress=1&_TSM_CombinedScripts_=%3b%3bSystem.Web.Extensions%2c+Version%3d4.0.0.0%2c+Culture%3dneutral%2c+PublicKeyToken

%3d31bf3856ad364e35%3apt-BR%3af7ba41a4-e843-4f12-b442-8e407f37c316%3aea597d4b%3ab25378d2%3bTelerik.Web.UI%2c+Version%3d2021.3.1111.45%2c+Culture%3dneutral%2c +PublicKeyToken%3d121fae78165ba3d4%3apt-BR%3ab406acc5-0028-4c73-8915-a9da355d848a%3a16e4e7cd%3aed16cbdc%3a4877f69a %3a33715776%3a86526ba7%3a874f8ea2%3af7645509%3a24ee1bba%3ac128760b%3af46195d3%3a19620875%3acda80b3%3a383e4ce8%3a88144a7a%3a11a04f7e%3ae330518b %3a1e771326%3a8e6f0d33%3a1f3a7489%3a6a6d718d%3ab7778d6c%3a6d43f6d9%3ab2e06756%3a92fe8ea0%3afa31b949%3a490a9d4e%3abd8f85e4 response code: 200

150262 Missing header: Feature-Policy (1)

WAS Scan Report

150262 Missing header: Feature-Policy

Finding #	**415457** (69622014)	**Severity**	Information Gathered - Level 2
Unique #	**b67fc96f-06eb-4f43-a4fa-bd84ed493251**		
Group	Security Weaknesses	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The Feature-Policy response header is not present.

Impact

Feature Policy allows web developers to selectively enable, disable, and modify the behavior of certain APIs and web features such as "geolocation","camera", "usb", "fullscreen", "animations" etc in the browser.

These policies restrict what APIs the site can access or modify the browser's default behavior for certain features.

Solution

It is recommended to set the Feature-Policy header to selectively enable, disable, and modify the behavior of certain APIs and web features.

References:
- https://www.w3.org/TR/feature-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Results

Feature-Policy: Header missing
Response headers on link: GET https://412-49.docspider.com.br/ response code: 200
Date: Wed, 11 Jan 2023 21:24:08 GMT
Content-Type: text/html; charset=ISO-8859-1
Content-Encoding: gzip
Last-Modified: Mon, 05 Jul 2021 22:43:41 GMT
Accept-Ranges: bytes
ETag: "9d444f34ef71d71:0"
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
x-Content-Type-Options: nosnif

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://412-49.docspider.com.br/ response code: 200
POST https://412-49.docspider.com.br/Login/Authenticate response code: 200
GET https://412-49.docspider.com.br/NAssets/images/favicon.png response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/bootstrap/bootstrap.css response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/docspider.css response code: 200
GET https://412-49.docspider.com.br/Login/Views/Shared/Common.css response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/theme/docspider.css response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/jquery/jquery-3.6.0.js response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError response code: 500
GET https://412-49.docspider.com.br/NAssets/images/logo.png response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/docspider-font-icon.css response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/bootstrap/popper.js response code: 200
GET https://412-49.docspider.com.br/NAssets/scripts/bootstrap/bootstrap.js response code: 200
GET https://412-49.docspider.com.br/NAssets/styles/docspider/error-style.css response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/Home response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=WU6bd74ziZ3ixaEoFn-7VTYpFuBsV29bPcmQWwoV7SMPUaR3FLIiFA-ogJeyedaandpqbubDc8FTsBasWWQRiIxU4JlOYbaS2i032jxGj9jZ4dwL9L7VXUGn9laj7eKxiLu-n2dBagfCOcNnOiXPv6gY3lvuhKgTF_0O9Qw90QWe3ordZtO6y7HQIWDJWoeTWfyctukCehrAw0ETzt12Bw2&t=638089669490933368 response code: 200
GET https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoDeBusca=1 response code: 200

GET https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoBuscaFiltro=1&modoBusca=1&tipoBusca=2&semAsPalavras=1&comValidadeIndefinida=1 response code: 200
GET https://412-49.docspider.com.br/Busca/PalavraIrrelevante response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?PageNumber=1&PageSize=50&HasNextPage=False&TotalItemCount=3 response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200
POST https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx response code: 200
GET https://412-49.docspider.com.br/Busca/Sinonimo response code: 200
GET https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=53 response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx response code: 200
GET https://412-49.docspider.com.br/PortalAdmin/WebResource.axd?d=GBn3eDvns8PQD2wVQLVg8stGbq2PkYGYf16n6Cu-CFFpa6OTrR94X5ngrfd548MeQLkFK_z89b-SQ5xJTVFsAE9moGhT_NW2zxsy-ndKDzwuuIvDcpB1sroE4h6JJfnQdcumiL7BXCGCfKvcWd9voUBDgA7bawx7mPNX1vAz0W6tbEGu4MBYvCdiqMe6en6s78YtMBlDkEQ6mZ3ZjF0gyQ2&t=638089669490933368 response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200

150135 HTTP Strict Transport Security (HSTS) header missing or misconfigured (1)

150135 HTTP Strict Transport Security (HSTS) header missing or misconfigured

Finding #	**415460**(69622016)	**Severity**	Information Gathered - Level 1
Unique #	**548a5045-9119-4577-b821-e97a02c49cb2**		
Group	Security Weaknesses	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-523		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

HTTP Strict Transport Security (HSTS) header was found to be missing or misconfigured. The HSTS header instructs browsers that all subsequent connections to the website, for a configurable amount of time, should be performed over a secure (HTTPS) connection only. Additionally, it instructs browsers that users should not be permitted to bypass SSL/TLS certificate errors, in the event of an expired or otherwise untrusted certificate for example.

Impact

If HSTS header is not set, users are potentially vulnerable to man-in-the-middle (MITM) attacks, SSL stripping, and passive eavesdropper attacks.

Solution

For information about how to implement the HSTS header properly, refer to the OWASP HTTP Strict Transport Security Cheat Sheet.

Results

Strict Transport Security header missing for
https://412-49.docspider.com.br/Generic/Transacao/DownloadArquivos/BrowseDownloadArquivos.aspx

150204 Missing header: X-XSS-Protection (1)

WAS Scan Report

150204 Missing header: X-XSS-Protection

Finding #	**415466**(69622022)	Severity	Information Gathered - Level 1
Unique #	**48ffc8ad-9152-4993-b964-4e9444812c34**		
Group	Security Weaknesses	Detection Date	11 Jan 2023 18:24 GMT-0400
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-XSS-Protection response header is not present.

Impact

The X-XSS-Protection response header provides a layer of protection against reflected cross-site scripting (XSS) attacks by instructing browsers to abort rendering a page in which a reflected XSS attack has been detected. This is a best-effort second line of defense measure which helps prevent an attacker from using evasion techniques to avoid the neutralization mechanisms that the filters use by default. When configured appropriately, browser-level XSS filters can provide additional layers of defense against web application attacks.

Note that HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security the X-XSS-Protection header should be set on 4xx and 5xx responses as well.

Solution

It is recommend to set X-XSS-Protection header with value set to '1; mode=block' on all the relevant responses to activate browser's XSS filter.

NOTE: The X-XSS-Protection header is not supported by all browsers. Google Chrome and Safari are some of the browsers which support it, Firefox on the other hand does not support the header. X-XSS-Protection header does not guarantee a complete protection against XSS. For better protection against XSS attacks, the web application should use secure coding principles. Also, consider leveraging the Content-Security-Policy (CSP) header, which is supported by all browsers.

Using X-XSS-Protection could have unintended side effects, please understand the implications carefully before using it.

References:
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection
- https://blog.innerht.ml/the-misunderstood-x-xss-protection/
- https://www.mbsd.jp/blog/20160407.html
- https://www.chromium.org/developers/design-documents/xss-auditor

Results

X-Xss-Protection: Header missing
Response headers on link: GET https://412-49.docspider.com.br/ response code: 200
Date: Wed, 11 Jan 2023 21:24:08 GMT
Content-Type: text/html; charset=ISO-8859-1
Content-Encoding: gzip
Last-Modified: Mon, 05 Jul 2021 22:43:41 GMT
Accept-Ranges: bytes
ETag: "9d444f34ef71d71:0"
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
x-Content-Type-Options: nosnif

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://412-49.docspider.com.br/ response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/Error/InternalServerError response code: 500
GET https://412-49.docspider.com.br/PortalAdmin/form/frmMain.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/Home response code: 200
GET https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Transacao/Sincronismo/PainelSincronismo.aspx response code: 200

GET https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoDeBusca=1 response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/TiposUsuario/BrowseCadastroTiposUsuario.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?termoBuscaFiltro=1&modoBusca=1&tipoBusca=2&semAsPalavras=1&comValidadeIndefinida=1 response code: 200
GET https://412-49.docspider.com.br/Busca/PalavraIrrelevante response code: 200
GET https://412-49.docspider.com.br/PortalDocumentos/BuscaDocumentos?PageNumber=1&PageSize=50&HasNextPage=False&TotalItemCount=3 response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Especialidades/BrowseCadastroEspecialidade.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/CentroAdministracao/BrowseCadastroCentroAdministracao.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Areas/BrowseCadastroArea.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/NiveisAcesso/BrowseCadastroNivelAcesso.aspx response code: 200
POST https://412-49.docspider.com.br/GED/Cadastros/Categorias/BrowseCadastroTiposCategoria.aspx response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx response code: 200
GET https://412-49.docspider.com.br/Busca/Sinonimo response code: 200
GET https://412-49.docspider.com.br/ASP/wf_002/adm_030_create_decisao.asp?tipoform=53 response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/ClassPerfisVisualizacao/BrowseCadastroClassPerfilVisualizacao.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/TipoAcesso/BrowseCadastroTipoAcesso.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Consultas/SearchAccessUsers/BrowseSearchAccessUsers.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/GrupoUsuarios/BrowseCadastroGrupoUsuario.aspx response code: 200
GET https://412-49.docspider.com.br/Generic/Transacao/DownloadArquivos/BrowseDownloadArquivos.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Consultas/Indicadores/QuestionStatisticPanel/QuestionStatisticPanel.aspx response code: 200
GET https://412-49.docspider.com.br/Workflow/Consultas/FrmConsultaProcesso.aspx response code: 200
POST https://412-49.docspider.com.br/GED/Cadastros/MotivosCriacaoRevisao/BrowseCadastroDeMotivos.aspx response code: 200
POST https://412-49.docspider.com.br/Global/Cadastros/Empresas/BrowseCadastroEmpresa.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Transacao/PainelPerguntas/BrowsePainelPerguntas.aspx response code: 200
POST https://412-49.docspider.com.br/GED/Cadastros/TiposDeRisco/BrowseCadastroTiposDeRisco.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Transacao/CargaDocumentos/PainelCargaDocumentos.aspx response code: 200
GET https://412-49.docspider.com.br/Generic/Transacao/ExecucaoSQL/PainelSentencaSQL.aspx response code: 200
GET https://412-49.docspider.com.br/GED/Consultas/DocPorPrevRev/BrowseDocPorPrevRev.aspx response code: 200
POST https://412-49.docspider.com.br/GED/Transacao/TransferenciaDocumentoAreaProprietaria/TransferenciaAreaProprietaria.aspx?RadUrid=56ad99a4-1d83-46f7-96c4-7414b506223b response code: 200
GET https://412-49.docspider.com.br/Global/Cadastros/Diretorias/BrowseCadastroDiretoria.aspx response code: 200
POST https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx response code: 200

150277 Cookie without SameSite attribute (1)

WAS Scan Report

150277 Cookie without SameSite attribute

Finding #	**415442**(69621991)	**Severity**	Information Gathered - Level 1
Unique #	**d26ed41f-0b07-4ebb-9280-068294a4f11e**		
Group	Security Weaknesses	**Detection Date**	11 Jan 2023 18:24 GMT-0400
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

The cookies listed in the Results section are missing the SameSite attribute.

Impact

The SameSite cookie attribute is an effective countermeasure against cross-site request forgery (CSRF) attacks. Note that a missing SameSite attribute does not mean the web application is automatically vulnerable to CSRF. The scanner will report QID 150071 if a CSRF vulnerability is detected.

Solution

Consider adding the SameSite attribute to the cookie(s) listed.

More information:
DZone article
OWASP CSRF Prevention Cheat Sheet

Results

Total cookies: 2
ASPSESSIONIDAGQQQRDA=DDEHMCOCNFJLOKOCGGMDNFBG; path=/; domain=412-49.docspider.com.br; secure; httponly | First set at URL: https://412-49.docspider.com.br/asp/wf_002/browse_cadastro_tipo_formulario.asp
_downloadToken=1673472915502,1673472915514; path=/; domain=412-49.docspider.com.br; secure; httponly | First set at URL: https://412-49.docspider.com.br/GED/Cadastros/SugestaoBusca/BrowseSugestaoBusca.aspx

Appendix

Scan Details

Web Application Vulnerability Scan - 412-49 - 2023-01-11

Reference	was/1673472167572.493891
Date	11 Jan 2023 18:24 GMT-0400
Mode	On-Demand
Type	Vulnerability
Authentication	form
Scanner Appliance	External (IP: 64.39.98.42, Scanner: 12.12.38-1, WAS: 8.22.60-1, Signatures: 2.5.674-2)
Profile	Initial WAS Options
DNS Override	-
Duration	11:55:14
Status	Time Limit Reached
Authentication Status	Successful

Option Profile Details

Form Submission	BOTH
Form Crawl Scope	Do not include form action URI in uniqueness calculation
Maximum links to test in scope	300
User Agent	-
Request Parameter Set	Initial Parameters
Document Type	Ignore common binary files
Enhanced Crawling	Disabled
SmartScan	Disabled
Timeout Error Threshold	100
Unexpected Error Threshold	300
Performance Settings	Pre-defined
Scan Intensity	Low
Bruteforce Option	Minimal
Detection Scope	Core
Include additional XSS payloads	No
Credit Card Numbers Search	Off
Social Security Numbers (US) Search	Off

Web Application Details: Docspider 412-49 - PADRÃO SQL

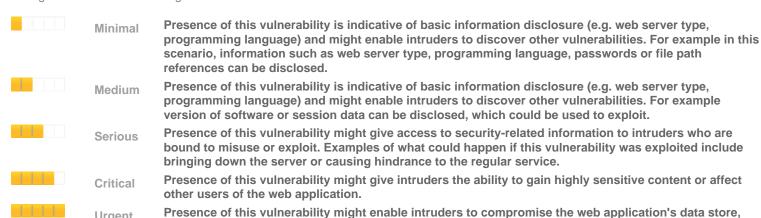|	
Name	Docspider 412-49 - PADRÃO SQL
ID	2181947
URL	https://412-49.docspider.com.br
Owner	Luis Ricardo Martins (dcspd6lm)
Scope	Limit to URL hostname
Tags	-
Custom Attributes	-

Severity Levels
Confirmed Vulnerabilities

Vulnerabilities (QIDs) are design flaws, programming errors, or mis-configurations that make your web application and web application platform susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information to a complete compromise of the web application and/or the web application platform. Even if the web application isn't fully compromised, an exploited vulnerability could still lead to the web application being used to launch attacks against users of the site.

|		
	Minimal	**Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.**
	Medium	**Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.**
	Serious	**Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels.**
	Critical	**Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks.**
	Urgent	**Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture.**

Potential Vulnerabilities
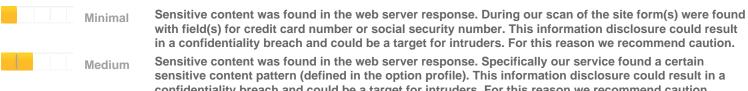
Potential Vulnerabilities indicate that the scanner observed a weakness or error that is commonly used to attack a web application, and the scanner was unable to confirm if the weakness or error could be exploited. Where possible, the QID's description and results section include information and hints for following-up with manual analysis. For example, the exploitability of a QID may be influenced by characteristics that the scanner cannot confirm, such as the web application's network architecture, or the test to confirm exploitability requires more intrusive testing than the scanner is designed to conduct.

	Minimal	**Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.**
	Medium	**Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.**
	Serious	**Presence of this vulnerability might give access to security-related information to intruders who are bound to misuse or exploit. Examples of what could happen if this vulnerability was exploited include bringing down the server or causing hindrance to the regular service.**
	Critical	**Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the web application.**
	Urgent	**Presence of this vulnerability might enable intruders to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture. For example in this scenario, the web application users can potentially be targeted if the application is exploited.**

Sensitive Content

Sensitive content may be detected based on known patterns (credit card numbers, social security numbers) or custom patterns (strings, regular expressions), depending on the option profile used. Intruders may gain access to sensitive content that could result in misuse or other exploits.

	Minimal	**Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.**
	Medium	**Sensitive content was found in the web server response. Specifically our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.**
	Serious	**Sensitive content was found in the web server response - a valid social security number or credit card information. This infomation disclosure could result in a confidentiality breach, and it gives intruders access to valid sensitive content that could be misused.**

Information Gathered

Information Gathered issues (QIDs) include visible information about the web application's platform, code, or architecture. It may also include information about users of the web application.

	Minimal	**Intruders may be able to retrieve sensitive information related to the web application platform.**
	Medium	**Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.**
	Serious	**Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.**