ZAP Scanning Report

Site: https://cas-portaldocontribuinte.at.gov.mz

Generated on seg., 3 nov. 2025 22:44:29

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Nível de Risco	Number of Alerts
Alto	1
Médio	2
Baixo	6
Informativo	5
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alertas

Nome	Nível de Risco	Number of Instances
Proxy Disclosure	Alto	11
Content Security Policy (CSP) Header Not Set	Médio	5
Missing Anti-clickjacking Header	Médio	3
Insufficient Site Isolation Against Spectre Vulnerability	Baixo	10
O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"	Baixo	10
Permissions Policy Header Not Set	Baixo	5
Server Leaks Version Information via "Server" HTTP Response Header Field	Baixo	10
Strict-Transport-Security Header Not Set	Baixo	9
X-Content-Type-Options Header Missing	Baixo	7
Divulgação de Informações - Comentários Suspeitos	Informativo	3
Non-Storable Content	Informativo	1
Re-examine Cache-control Directives	Informativo	3
Storable and Cacheable Content	Informativo	9
User Agent Fuzzer	Informativo	12

Alert Detail

Alto	Proxy Disclosure
Descrição	3 proxy server(s) were detected or fingerprinted. This information helps a potential attacker to determine - A list of targets for an attack against the application. - Potential vulnerabilities on the proxy servers that service the application. - The presence or absence of any proxy-based components that might cause attacks against the application to be detected, prevented, or mitigated.
URL	https://cas-portaldocontribuinte.at.gov.mz

Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	
Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	
Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	
Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	
Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/favicon.ico
Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	
Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/jbosscommunity_logo_hori_white.png
Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	

Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	
Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	
Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	
Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly.css
Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	
Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly_logo.png
Método	GET
Parameter	
Ataque	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Evidence	
Other Info	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between ZAP and the application/web server: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The following web/application server has been identified: - Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 The 'TRACE' method is enabled on one or more of the proxy servers, or on the origin server. This method leaks all information submitted from the web browser and proxies back to the user agent. This may facilitate 'Cross Site Tracing' attacks.

Instances	11
Solution	Disable the 'TRACE' method on the proxy servers, as well as the origin web/application server. Disable the 'OPTIONS' method on the proxy servers, as well as the origin web/application server, if it is not required for other purposes, such as 'CORS' (Cross Origin Resource Sharing). Configure the web and application servers with custom error pages, to prevent 'fingerprintable' product-specific error pages being leaked to the user in the event of HTTP errors, such as 'TRACK' requests for non-existent pages. Configure all proxies, application servers, and web servers to prevent disclosure of the technology and version information in the 'Server' and 'X-Powered-By' HTTP response headers.
Reference	https://tools.ietf.org/html/rfc7231#section-5.1.2
CWE Id	204
WASC Id	45
Plugin Id	40025

Médio	**Content Security Policy (CSP) Header Not Set**
Descrição	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Médio	**Missing Anti-clickjacking Header**
Descrição	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	x-frame-options
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	x-frame-options
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET
Parameter	x-frame-options
Ataque	
Evidence	
Other Info	
Instances	3
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Baixo	**Insufficient Site Isolation Against Spectre Vulnerability**
Descrição	Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	Cross-Origin-Resource-Policy
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	Cross-Origin-Resource-Policy

Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/favicon.ico
Método	GET
Parameter	Cross-Origin-Resource-Policy
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/jbosscommunity_logo_hori_white.png
Método	GET
Parameter	Cross-Origin-Resource-Policy
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly.css
Método	GET
Parameter	Cross-Origin-Resource-Policy
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly_logo.png
Método	GET
Parameter	Cross-Origin-Resource-Policy
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	Cross-Origin-Embedder-Policy
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	Cross-Origin-Embedder-Policy
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	Cross-Origin-Opener-Policy
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	Cross-Origin-Opener-Policy
Ataque	

Evidence	
Other Info	
Instances	10
Solution	Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages. 'same-site' is considered as less secured and should be avoided. If resources must be shared, set the header to 'cross-origin'. If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy
CWE Id	693
WASC Id	14
Plugin Id	90004

Baixo	**O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"**
Descrição	O servidor da web/aplicativo está vazando informações por meio de um ou mais cabeçalhos de resposta HTTP "X-Powered-By". O acesso a essas informações pode facilitar que os invasores identifiquem outras estruturas/componentes dos quais seu aplicativo da web depende e as vulnerabilidades às quais esses componentes podem estar sujeitos.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/favicon.ico
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/jbosscommunity_logo_hori_white.png
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET
Parameter	

Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly.css
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly_logo.png
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
Instances	10
Solution	Certifique-se de que seu servidor web, servidor de aplicativos, balanceador de carga, etc. esteja configurado para suprimir cabeçalhos "X-Powered-By".
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10037

Baixo	**Permissions Policy Header Not Set**
Descrição	Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	
Ataque	

Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy https://developer.chrome.com/blog/feature-policy/ https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	693
WASC Id	15
Plugin Id	10063

Baixo	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Descrição	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/favicon.ico

Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/jbosscommunity_logo_hori_white.png
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly.css
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly_logo.png
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
Instances	10
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Baixo	Strict-Transport-Security Header Not Set
Descrição	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/favicon.ico
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/jbosscommunity_logo_hori_white.png
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly.css
Método	GET
Parameter	
Ataque	

Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly_logo.png
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Baixo	**X-Content-Type-Options Header Missing**
Descrição	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	x-content-type-options
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	x-content-type-options
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://cas-portaldocontribuinte.at.gov.mz/favicon.ico
Método	GET
Parameter	x-content-type-options
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://cas-portaldocontribuinte.at.gov.mz/jbosscommunity_logo_hori_white.png
Método	GET
Parameter	x-content-type-options
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET
Parameter	x-content-type-options
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly.css
Método	GET
Parameter	x-content-type-options
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly_logo.png
Método	GET
Parameter	x-content-type-options
Ataque	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	7
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informativo	**Divulgação de Informações - Comentários Suspeitos**
Descrição	The response appears to contain suspicious comments which may help an attacker.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in likely comment: "<!-- ~ JBoss, Home of Professional Open Source. ~ Copyright (c) 2014, Red Hat, Inc., and individual contributors ~ as indi", see evidence field for the suspicious comment/snippet.
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in likely comment: "<!-- ~ JBoss, Home of Professional Open Source. ~ Copyright (c) 2014, Red Hat, Inc., and individual contributors ~ as indi", see evidence field for the suspicious comment/snippet.
URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET

Parameter	
Ataque	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in likely comment: "<!-- ~ JBoss, Home of Professional Open Source. ~ Copyright (c) 2011, Red Hat, Inc., and individual contributors ~ as indi", see evidence field for the suspicious comment/snippet.
Instances	3
Solution	Remova todos os comentários que retornam informações que podem ajudar um invasor e corrigir quaisquer problemas subjacentes aos quais eles se referem.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informativo	**Non-Storable Content**
Descrição	The response contents are not storable by caching components such as proxy servers. If the response does not contain sensitive, personal or user-specific information, it may benefit from being stored and cached, to improve performance.
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	
Ataque	
Evidence	302
Other Info	
Instances	1
Solution	The content may be marked as storable by ensuring that the following conditions are satisfied: The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable) The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood) The "no-store" cache directive must not appear in the request or response header fields For caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the response For caching by "shared" caches such as "proxy" caches, the "Authorization" header field must not appear in the request, unless the response explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control response directives) In addition to the conditions above, at least one of the following conditions must also be satisfied by the response: It must contain an "Expires" header field It must contain a "max-age" response directive For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive It must contain a "Cache Control Extension" that allows it to be cached It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Informativo	**Re-examine Cache-control Directives**
Descrição	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://cas-portaldocontribuinte.at.gov.mz/

Método	GET
Parameter	cache-control
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	cache-control
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET
Parameter	cache-control
Ataque	
Evidence	
Other Info	
Instances	3
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informativo	**Storable and Cacheable Content**
Descrição	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://cas-portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://cas-portaldocontribuinte.at.gov.mz/documentation.html
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://cas-portaldocontribuinte.at.gov.mz/favicon.ico
Método	GET
Parameter	
Ataque	
Evidence	

Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://cas-portaldocontribuinte.at.gov.mz/jbosscommunity_logo_hori_white.png
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://cas-portaldocontribuinte.at.gov.mz/noredirect.html
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://cas-portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://cas-portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly.css
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://cas-portaldocontribuinte.at.gov.mz/wildfly_logo.png
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
Instances	9
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.

Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Informativo	**User Agent Fuzzer**
Descrição	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/console
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	12
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Sequence Details

With the associated active scan results.