ZAP Scanning Report

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

Generated on dom., 25 jan. 2026 11:12:35

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Nível de Risco	Number of Alerts
Alto	1
Médio	5
Baixo	12
Informativo	4
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	4
Ausência de tokens Anti-CSRF	Médio	1
Content Security Policy (CSP) Header Not Set	Médio	1
Missing Anti-clickjacking Header	Médio	1
Relative Path Confusion	Médio	2
Sub Resource Integrity Attribute Missing	Médio	3
Cookie No HttpOnly Flag	Baixo	2
Cookie Without Secure Flag	Baixo	2
Cookie without SameSite Attribute	Baixo	2
Cross-Domain JavaScript Source File Inclusion	Baixo	2
Detector de Cookie Slack	Baixo	4
Insufficient Site Isolation Against Spectre Vulnerability	Baixo	3
O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"	Baixo	4
Permissions Policy Header Not Set	Baixo	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Baixo	4
Strict-Transport-Security Header Not Set	Baixo	4
X-Content-Type-Options Header Missing	Baixo	1
ZAP is Out of Date	Baixo	2
Non-Storable Content	Informativo	4
Re-examine Cache-control Directives	Informativo	1
Session Management Response Identified	Informativo	2
User Agent Fuzzer	Informativo	47

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://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://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://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://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.
Instances	4
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://datatracker.ietf.org/doc/html/rfc7231#section-5.1.2

CWE Id	204
WASC Id	45
Plugin Id	40025

Médio	Ausência de tokens Anti-CSRF
Descrição	Não foram localizados tokens Anti-CSRF no formulário de submissão HTML. Uma falsificação de solicitação entre sites (Cross-Site Request Forgery ou simplesmente CSRF) é um ataque que envolve forçar a vítima a enviar uma solicitação HTTP a um destino alvo sem seu conhecimento ou intenção, a fim de realizar uma ação como a vítima. A causa implícita é a funcionalidade do aplicativo usando ações previsíveis em URLs/formulários, de maneira repetível. A natureza do ataque é que o CSRF explora a confiança que um site tem em um usuário. Em contrapartida, um ataque do tipo Cross-Site Scripting (XSS) explora a confiança que um usuário tem em um site. Como o XSS, os ataques CSRF não são necessariamente entre sites, mas também podem ser. A falsificação de solicitação entre sites também é conhecida por "CSRF", "XSRF", "one-click attack", "session riding", "confused deputy", e "sea surf". Os ataques CSRF são efetivos em várias situações, incluindo: * - A vítima tem uma sessão ativa no site de destino; * - A vítima está autenticada por meio de autenticação HTTP no site de destino; * - A vítima está na mesma rede local do site de destino. O CSRF era usado principalmente para executar ações contra um site-alvo usando os privilégios da vítima, mas técnicas recentes foram descobertas para vazamento de informações obtendo acesso às respostas. O risco de vazamento/divulgação não autorizada de informações aumenta drasticamente quando o site de destino é vulnerável a XSS, porque o XSS pode ser usado como uma plataforma para CSRF, permitindo que o ataque opere dentro dos limites da política de mesma origem.
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	<form id="fm1" class="form-signin" action="/cas/login;jsessionid=1PViULp6zXdY2kVLYj7iRQwSnRW_vK8iy-9Tlf5.mzmpm01srv046-wildfly?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check" method="post">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] foi encontrado nos seguintes formulários HTML: [Form 1: "_eventId" "execution" "lt" "password" "submit" "username"].
Instances	1

Solution	Fase: Arquitetura e Design. Use uma biblioteca verificada ou framework que não permita que essa vulnerabilidade ocorra, ou forneça construções/implementações que tornem essa vulnerabilidade mais fácil de evitar. Por exemplo, use pacotes anti-CSRF, como o OWASP CSRFGuard. Fase: Implementação. Certifique-se de que seu aplicativo esteja livre de problemas de cross-site scripting (XSS), porque a maioria das defesas CSRF pode ser contornada usando script controlado por invasor. Fase: Arquitetura e Design. Gere um número arbitrário de uso único e exclusivo (ou Nonce = "N" de "number" - número em inglês - e "once" de "uma vez" também em inglês) para cada formulário, coloque o nonce no formulário e verifique-o ao receber o formulário. Certifique-se de que o nonce não seja previsível (CWE-330). Observe que isso pode ser contornado usando XSS. Identifique operações especialmente perigosas. Quando o usuário realizar uma operação perigosa, envie uma solicitação de confirmação separada para garantir que o usuário pretendia realizar aquela operação. Observe que isso pode ser contornado usando XSS. Utilize o controle ESAPI Session Management. Este controle inclui um componente para CSRF. Não use o método GET para qualquer solicitação que acione uma mudança de estado. Fase: Implementação. Verifique o cabeçalho HTTP Referer para ver se a solicitação foi originada de uma página esperada. Isso pode interromper funcionalidades legítimas, porque os usuários ou proxies podem ter desativado o envio do Referer por motivos de privacidade.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

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/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
Instances	1
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/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	x-frame-options
Ataque	
Evidence	
Other Info	
Instances	1
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

Médio	Relative Path Confusion
Descrição	The web server is configured to serve responses to ambiguous URLs in a manner that is likely to lead to confusion about the correct "relative path" for the URL. Resources (CSS, images, etc.) are also specified in the page response using relative, rather than absolute URLs. In an attack, if the web browser parses the "cross-content" response in a permissive manner, or can be tricked into permissively parsing the "cross-content" response, using techniques such as framing, then the web browser may be fooled into interpreting HTML as CSS (or other content types), leading to an XSS vulnerability.
URL	https://portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	https://portaldocontribuinte.at.gov.mz/robots.txt/xrijd/v7kqd
Evidence	<link rel="icon" href="img/favicon.ico">
Other Info	No <base> tag was specified in the HTML <head> tag to define the location for relative URLs. A Content Type of "text/html;charset=UTF-8" was specified. If the web browser is employing strict parsing rules, this will prevent cross-content attacks from succeeding. Quirks Mode in the web browser would disable strict parsing. Quirks Mode is implicitly enabled via the use of an old DOCTYPE with PUBLIC id "-//W3C//DTD XHTML 1.0 Strict//EN", allowing the specified Content Type to be bypassed in some web browsers.
URL	https://portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	https://portaldocontribuinte.at.gov.mz/sitemap.xml/xrijd/v7kqd
Evidence	<link rel="icon" href="img/favicon.ico">
Other Info	No <base> tag was specified in the HTML <head> tag to define the location for relative URLs. A Content Type of "text/html;charset=UTF-8" was specified. If the web browser is employing strict parsing rules, this will prevent cross-content attacks from succeeding. Quirks Mode in the web browser would disable strict parsing. Quirks Mode is implicitly enabled via the use of an old DOCTYPE with PUBLIC id "-//W3C//DTD XHTML 1.0 Strict//EN", allowing the specified Content Type to be bypassed in some web browsers.
Instances	2

Solution	Web servers and frameworks should be updated to be configured to not serve responses to ambiguous URLs in such a way that the relative path of such URLs could be mis-interpreted by components on either the client side, or server side. Within the application, the correct use of the "<base>" HTML tag in the HTTP response will unambiguously specify the base URL for all relative URLs in the document. Use the "Content-Type" HTTP response header to make it harder for the attacker to force the web browser to mis-interpret the content type of the response. Use the "X-Content-Type-Options: nosniff" HTTP response header to prevent the web browser from "sniffing" the content type of the response. Use a modern DOCTYPE such as "<!doctype html>" to prevent the page from being rendered in the web browser using "Quirks Mode", since this results in the content type being ignored by the web browser. Specify the "X-Frame-Options" HTTP response header to prevent Quirks Mode from being enabled in the web browser using framing attacks.
Reference	https://arxiv.org/abs/1811.00917 https://hsivonen.fi/doctype/ https://www.w3schools.com/tags/tag_base.asp
CWE Id	20
WASC Id	20
Plugin Id	10051

Médio	Sub Resource Integrity Attribute Missing
Descrição	The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	<link href='http://fonts.googleapis.com/css?family=Open+Sans:400,600,700' rel='stylesheet' type='text/css'>
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	<script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	<script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
Other Info	
Instances	3
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
CWE Id	345
WASC Id	15
Plugin Id	90003

Baixo	Cookie No HttpOnly Flag
Descrição	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check

Método	GET
Parameter	JSESSIONID
Ataque	
Evidence	Set-Cookie: JSESSIONID
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	JSESSIONID
Ataque	
Evidence	Set-Cookie: JSESSIONID
Other Info	
Instances	2
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Baixo	**Cookie Without Secure Flag**
Descrição	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	JSESSIONID
Ataque	
Evidence	Set-Cookie: JSESSIONID
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	JSESSIONID
Ataque	
Evidence	Set-Cookie: JSESSIONID
Other Info	
Instances	2
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html
CWE Id	614
WASC Id	13
Plugin Id	10011

Baixo	**Cookie without SameSite Attribute**
Descrição	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	JSESSIONID
Ataque	
Evidence	Set-Cookie: JSESSIONID
Other Info	

URL	https://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	JSESSIONID
Ataque	
Evidence	Set-Cookie: JSESSIONID
Other Info	
Instances	2
Solution	Certifique-se de que o atributo SameSite esteja definido como 'lax' ou, de preferência, 'strict' para todos os cookies.
Reference	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Baixo	**Cross-Domain JavaScript Source File Inclusion**
Descrição	The page includes one or more script files from a third-party domain.
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js
Ataque	
Evidence	<script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	https://oss.maxcdn.com/respond/1.4.2/respond.min.js
Ataque	
Evidence	<script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>
Other Info	
Instances	2
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Baixo	**Detector de Cookie Slack**
Descrição	Solicitações GET repetidas: elimine um cookie diferente a cada vez, seguido pela solicitação normal com todos os cookies para estabilizar a sessão, compare as respostas com a linha de base GET original. Isso pode revelar áreas onde a autenticação / atributos baseados em cookies não são realmente aplicados.
URL	https://portaldocontribuinte.at.gov.mz
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [JSESSIONID] Cookies que não tem efeitos esperados podem revelar falhas na aplicação lógica. No pior caso, isso pode revelar aonde a autenticação através de token(s) cookie não é realmente aplicada. These cookies affected the response: These cookies did NOT affect the response: JSESSIONID
URL	https://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	

Other Info	NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [JSESSIONID] Cookies que não tem efeitos esperados podem revelar falhas na aplicação lógica. No pior caso, isso pode revelar aonde a autenticação através de token(s) cookie não é realmente aplicada. These cookies affected the response: These cookies did NOT affect the response: JSESSIONID
URL	https://portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [JSESSIONID] Cookies que não tem efeitos esperados podem revelar falhas na aplicação lógica. No pior caso, isso pode revelar aonde a autenticação através de token(s) cookie não é realmente aplicada. These cookies affected the response: These cookies did NOT affect the response: JSESSIONID
URL	https://portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	NOTE: Because of its name this cookie may be important, but dropping it appears to have no effect: [JSESSIONID] Cookies que não tem efeitos esperados podem revelar falhas na aplicação lógica. No pior caso, isso pode revelar aonde a autenticação através de token(s) cookie não é realmente aplicada. These cookies affected the response: These cookies did NOT affect the response: JSESSIONID
Instances	4
Solution	
Reference	https://cwe.mitre.org/data/definitions/205.html
CWE Id	205
WASC Id	45
Plugin Id	90027

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/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	Cross-Origin-Resource-Policy
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	Cross-Origin-Embedder-Policy
Ataque	
Evidence	
Other Info	
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	Cross-Origin-Opener-Policy
Ataque	
Evidence	
Other Info	
Instances	3

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/Reference/Headers/Cross-Origin-Embedder-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/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	Os seguintes cabeçalhos X-Powered-By também foram encontrados:X-Powered-By: JSP/2.3
URL	https://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	X-Powered-By: Undertow/1
Other Info	
Instances	4
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/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
Instances	1
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/Reference/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/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	WildFly/10
Other Info	
Instances	4
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/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	
Instances	4
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/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
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	1
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

Baixo	**ZAP is Out of Date**
Descrição	The version of ZAP you are using to test your app is out of date and is no longer being updated. The risk level is set based on how out of date your ZAP version is.
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	The latest version of ZAP is 2.17.0
URL	https://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	
Evidence	
Other Info	The latest version of ZAP is 2.17.0
Instances	2
Solution	Download the latest version of ZAP from https://www.zaproxy.org/download/ and install it.
Reference	https://www.zaproxy.org/download/
CWE Id	1104
WASC Id	45
Plugin Id	10116

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/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	
Ataque	
Evidence	no-store
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	
Ataque	

Evidence	no-store
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	
Ataque	
Evidence	no-store
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	
Ataque	
Evidence	no-store
Other Info	
Instances	4
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/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	cache-control
Ataque	
Evidence	no-cache, no-store
Other Info	
Instances	1

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	Session Management Response Identified
Descrição	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://cas-portaldocontribuinte.at.gov.mz/cas/login?service=https%3A%2F%2Fportaldocontribuinte.at.gov.mz%2Fj_spring_cas_security_check
Método	GET
Parameter	JSESSIONID
Ataque	
Evidence	JSESSIONID
Other Info	cookie:JSESSIONID
URL	https://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	JSESSIONID
Ataque	
Evidence	JSESSIONID
Other Info	cookie:JSESSIONID
Instances	2
Solution	Este é um alerta informativo e não uma vulnerabilidade, portanto não há nada a ser corrigido.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112

Informativo	User Agent Fuzzer
Descrição	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	https://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
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://portaldocontribuinte.at.gov.mz
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
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://portaldocontribuinte.at.gov.mz/
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	https://portaldocontribuinte.at.gov.mz/robots.txt
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://portaldocontribuinte.at.gov.mz/robots.txt
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://portaldocontribuinte.at.gov.mz/robots.txt
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://portaldocontribuinte.at.gov.mz/robots.txt
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://portaldocontribuinte.at.gov.mz/robots.txt
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://portaldocontribuinte.at.gov.mz/robots.txt
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://portaldocontribuinte.at.gov.mz/robots.txt
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://portaldocontribuinte.at.gov.mz/robots.txt
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://portaldocontribuinte.at.gov.mz/robots.txt
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://portaldocontribuinte.at.gov.mz/robots.txt
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://portaldocontribuinte.at.gov.mz/robots.txt
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	

Other Info	
URL	https://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
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://portaldocontribuinte.at.gov.mz/sitemap.xml
Método	GET
Parameter	Cabeçalho do Agente de Usuário
Ataque	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	47
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Sequence Details

With the associated active scan results.