ZAP Scanning Report

IrisWEB CSI

Site: https://servizi.comune.torino.it

Generated on lun, 7 mar 2022 18:42:26

Summary of Alerts

Livello di Rischio	Number of Alerts
Alto	0
Medio	2
Basso	8
Informativo	4

Avvisi

Nome	Livello di Rischio	Number of Instances
Content Security Policy (CSP) Header Not Set	Medio	6
X-Frame-Options Header Not Set	Medio	4
Cookie No HttpOnly Flag	Basso	1
Cookie Without Secure Flag	Basso	1
Cookie without SameSite Attribute	Basso	1
Incomplete or No Cache-control Header Set	Basso	5
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Basso	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Basso	1
Strict-Transport-Security Disabled	Basso	10
X-Content-Type-Options Header Missing	Basso	8
Cookie Slack Detector	Informativo	1
Information Disclosure - Sensitive Information in URL	Informativo	1
Modern Web Application	Informativo	3
User Agent Fuzzer	Informativo	7

Alert Detail

Medio	Content Security Policy (CSP) Header Not Set
Descrizione	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://servizi.comune.torino.it/
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/cgi-bin/otrs/
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl?Ticket
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/sitemap.xml
Metodo	GET
Attacco	
Evidence	
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medio	X-Frame-Options Header Not Set
Descrizione	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	https://servizi.comune.torino.it/

Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl?Ticket
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	
Evidence	
Instances	4
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Basso	**Cookie No HttpOnly Flag**
Descrizione	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://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	
Evidence	Set-Cookie: IW_IrisWEB
Instances	1
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

Basso	**Cookie Without Secure Flag**
Descrizione	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll

Metodo	GET
Attacco	
Evidence	Set-Cookie: IW_IrisWEB
Instances	1
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

Basso	**Cookie without SameSite Attribute**
Descrizione	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://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	
Evidence	Set-Cookie: IW_IrisWEB
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Basso	**Incomplete or No Cache-control Header Set**
Descrizione	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content.
URL	https://servizi.comune.torino.it/
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl?Ticket
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll

Metodo	GET
Attacco	
Evidence	no-cache
URL	https://servizi.comune.torino.it/robots.txt
Metodo	GET
Attacco	
Evidence	
Instances	5
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
CWE Id	525
WASC Id	13
Plugin Id	10015

Basso	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
Descrizione	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	
Evidence	X-Powered-By: IntraWeb
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

Basso	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Descrizione	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://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	
Evidence	Microsoft-IIS/10.0
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
	http://httpd.apache.org/docs/current/mod/core.html#servertokens

Reference	http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10036

Basso	**Strict-Transport-Security Disabled**
Descrizione	A HTTP Strict Transport Security (HSTS) header was found, but it contains the directive max-age=0 which disables the control and instructs browsers to reset any previous HSTS related settings. See RFC 6797 for further details. 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).
URL	https://servizi.comune.torino.it/
Metodo	GET
Attacco	
Evidence	max-age=0
URL	https://servizi.comune.torino.it/cgi-bin/otrs/
Metodo	GET
Attacco	
Evidence	max-age=0
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl
Metodo	GET
Attacco	
Evidence	max-age=0
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl?Ticket
Metodo	GET
Attacco	
Evidence	max-age=0
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	
Evidence	max-age=0
URL	https://servizi.comune.torino.it/otrs-web/css/Comune/otrs.css
Metodo	GET
Attacco	
Evidence	max-age=0
URL	https://servizi.comune.torino.it/otrs-web/css/Comune/screen.css
Metodo	GET
Attacco	
Evidence	max-age=0
URL	https://servizi.comune.torino.it/otrs-web/images/Comune/product.ico

Metodo	GET
Attacco	
Evidence	max-age=0
URL	https://servizi.comune.torino.it/robots.txt
Metodo	GET
Attacco	
Evidence	max-age=0
URL	https://servizi.comune.torino.it/sitemap.xml
Metodo	GET
Attacco	
Evidence	max-age=0
Instances	10
Solution	Review the configuration of this control. Ensure that your web server, application server, load balancer, etc. is configured to set Strict-Transport-Security with an appropriate max-age value.
Reference	http://tools.ietf.org/html/rfc6797#section-6.2
CWE Id	319
WASC Id	15
Plugin Id	10035

Basso	**X-Content-Type-Options Header Missing**
Descrizione	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://servizi.comune.torino.it/
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl?Ticket
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/otrs-web/css/Comune/otrs.css
Metodo	GET

Attacco	
Evidence	
URL	https://servizi.comune.torino.it/otrs-web/css/Comune/screen.css
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/otrs-web/images/Comune/product.ico
Metodo	GET
Attacco	
Evidence	
URL	https://servizi.comune.torino.it/robots.txt
Metodo	GET
Attacco	
Evidence	
Instances	8
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informativo	**Cookie Slack Detector**
Descrizione	Repeated GET requests: drop a different cookie each time, followed by normal request with all cookies to stabilize session, compare responses against original baseline GET. This can reveal areas where cookie based authentication/attributes are not actually enforced.
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	
Evidence	
Instances	1
Solution	
Reference	http://projects.webappsec.org/Fingerprinting
CWE Id	200
WASC Id	45
Plugin Id	90027

Informativo	**Information Disclosure - Sensitive Information in URL**
Descrizione	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl?Ticket

Metodo	GET
Attacco	
Evidence	Ticket
Instances	1
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10024

Informativo	Modern Web Application
Descrizione	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl
Metodo	GET
Attacco	
Evidence	<a href="" title=""><span>Citt di Torino - Sistema di ticketing</span></a>
URL	https://servizi.comune.torino.it/cgi-bin/otrs/show.pl?Ticket
Metodo	GET
Attacco	
Evidence	<a href="" title=""><span>Citt di Torino - Sistema di ticketing</span></a>
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	
Evidence	<script type="text/javascript"> function getWH(){var a=0,b=0,f=document,e=window,c=e.devicePixelRatio||1;if(e&&e.innerWidth){a=e.innerWidth;b=e.innerHeight}else{if(f.documentElement&&f.documentElement.clientWidth){a=f.documentElement.clientWidth;b=f.documentElement.clientHeight}else{if(f.body&&f.body.clientWidth){a=f.body.clientWidth;b=f.body.clientHeight}}}return[a,b,c]}function consoleError(a){if(window.console&&window.console.error){console.error(a);return true}else{return consoleWrite(a)}}function getNodeText(b){var a="";if(!b){return a}if(b.nodeType===3||b.nodeType===4){return b.data}if(b==b.firstChild){do{a+=getNodeText(b)}while(b==b.nextSibling)}return a}function WriteToDoc(a){var b=document.open("text/html","replace");b.write(a);b.close()}function processAjaxRewrite(c){var a;try{a=getNodeText(c[0]);if(a.slice(0,1)!=="<"){window.location.replace(res)}else{WriteToDoc(a)}}catch(b){consoleError("Error in processAjaxRewrite(): "+a+"\n"+b.message)}}function processAjaxResponse(b){var c=b.getElementsByTagName("response");if(c==null||c.length!=1){return}var a=b.getElementsByTagName("rewrite");if(a.length>0&&a[0].childNodes.length>0){processAjaxRewrite(a[0].childNodes)}}function ajaxGetCallback(b){var a;if(window.ActiveXObject){a=new ActiveXObject("Microsoft.XMLDOM");a.async=false;a.loadXML(b)}else{var c=new DOMParser();a=c.parseFromString(b,"text/xml");c=null}if(a){processAjaxResponse(a);a=null}}function ajaxGet(a,c,d){var b=new XMLHttpRequest();b.open("GET",a+c,true);if(b.responseType){b.responseType="text"}b.onreadystatechange=function(){if(b.readyState===4&&b.status===200&&d){d(b.responseText)}};b.send()}; function get(url) { var s = getWH(); var p = "?IW_AjaxID=" + new Date().getTime(); p += "&IW_width=" + s[0] + "&IW_height=" + s[1] + "&IW_dpr=" + s[2]; ajaxGet(url, p, function(t, s){ajaxGetCallback(t, s);}); } </script>
Instances	3
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	

Plugin Id	10109

Informativo	User Agent Fuzzer
Descrizione	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://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	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	
URL	https://servizi.comune.torino.it/irisweb/W000PIrisWEB_IIS.dll
Metodo	GET
Attacco	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Instances	7
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104