ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	8
Informational	6

Alert Detail

Medium (Medium)	Proxy Disclosure
Description	1 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://alfatrial.hmsconsulting.it/css/1c61bb34.8b5fefc0.css
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/2d0d4416.e74a64eb.js
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/27ac7332.34cb3cb7.js
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/526e6b0f.4e8676b3.js
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/css/27ac7332.8b5fefc0.css
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/74529264.58c7bb8f.js
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/css/cce381a8.39a71549.css
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/cce381a8.a58789f4.js
Method	GET

Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/2d217329.8776fbda.js
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/css/2aceb3ba.8b5fefc0.css
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/2d21729d.9db92fff.js
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/2d21e021.fe33e005.js
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/css/0afeeed0.57eeba49.css
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/statics/icons/favicon-16x16.png
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/css/4a9ca042.4a2bbf72.css
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/css/3faaeca7.57eeba49.css
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/50fdc712.6379bdc1.js
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/statics/quasar-logo.png
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/2d230f98.4daf0daf.js
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
URL	https://alfatrial.hmsconsulting.it/js/2d0e2700.b791e98e.js
Method	GET
Attack	TRACE, OPTIONS methods with 'Max-Forwards' header. TRACK method.
Instances	99
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.
Other information	Using the TRACE, OPTIONS, and TRACK methods, the following proxy servers have been identified between OWASP ZAP and the application/web server: - Unknown The following web/application server has been identified: - nginx/1.19.0
Reference	https://tools.ietf.org/html/rfc7231#section-5.1.2
CWE Id	200
WASC Id	45
Source ID	1

Medium (Medium) **Apache Range Header DoS (CVE-2011-3192)**

Description	The byterange filter in earlier versions of the Apache HTTP Server allows remote attackers to cause a denial of service (memory and CPU exhaustion) via a Range request header that identifies multiple overlapping ranges. This issue was exploited in the wild in August 2011.
URL	https://alfatrial.hmsconsulting.it/js/2d21f0cb.0d88fcdf.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/2d0e942e.69760301.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/css/4b65d126.c9681678.css
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/2d0a388c.d4ed14ed.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/css/0701133c.74a9f607.css
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/2d2257a5.80d5212f.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/4a9ca042.dc452ecb.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/2d217329.8776fbda.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content

URL	https://alfatrial.hmsconsulting.it/js/0af16d65.ffd2141e.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/2d21a08f.3a4d6c2b.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/2d0e264b.81f946fa.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/2d21e021.fe33e005.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/3faaeca7.e764d254.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/2d2219e2.ccdbe8ca.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/2d0d6586.4564f498.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/e31e1ff8.74d2079f.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/statics/icons/apple-icon-152x152.png
Method	GET
Evidence	HTTP/1.1 206 Partial Content
URL	https://alfatrial.hmsconsulting.it/js/0cfa5d3b.218b08f0.js
Method	GET
Evidence	HTTP/1.1 206 Partial Content
Instances	82
Solution	Upgrade your Apache server to a currently stable version. Alternative solutions or workarounds are outlined in the references.
Reference	https://httpd.apache.org/security/CVE-2011-3192.txt http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2011-3192
CWE Id	400

WASC Id	10
Source ID	1

Medium (Medium)	**X-Frame-Options Header Not Set**
Description	L'intestazione X-Frame-Options non è inclusa nella risposta HTTP per proteggersi da attacchi 'ClickJacking'.
URL	https://alfatrial.hmsconsulting.it/
Method	GET
Parameter	X-Frame-Options
Instances	1
Solution	La stragrande maggioranza dei moderni browser web consente l'intestazione HTTP X-Fram-Options. Assicurati che sia configurato in tutte le pagine web restituite dal tuo sito, se ti aspetti che la pagina venga incorniciata solo dalle pagine del tuo server (ad esempio, fa parte di un FRAMESET), quindi ti consigliamo usa SAMEORIGIN, altrimenti, se non aspetti che la pagina sia in grado di frame, devi usare DENY. ALLOW-FROM consente ai siti web specifici di contrassegnare la pagina web nei browser web compatibili.
Reference	http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx
CWE Id	16
WASC Id	15
Source ID	3

Low (High)	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	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://alfatrial.hmsconsulting.it/js/2d0e2700.b791e98e.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/css/0701133c.74a9f607.css
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/css/3280d326.fcb6c043.css
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/css/526e6b0f.57eeba49.css
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/css/4b65d126.c9681678.css
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/2d0ddddd.7b38b7a4.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/2d2219e2.ccdbe8ca.js
Method	GET

Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/4b65d126.9ff191a3.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/2d0e264b.81f946fa.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/2d0e5af8.f7ae4401.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/06c76a9a.fd949505.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/2aceb3ba.7152616d.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/2d0df1fc.cb83d0e0.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/2d0b9e24.a6479ffd.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/2d21e021.fe33e005.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/vendor.35758b23.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/0af16d65.ffd2141e.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/robots.txt
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/js/2d2257a5.80d5212f.js
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/css/0afeeed0.57eeba49.css
Method	GET
Evidence	nginx/1.19.0
Instances	95

Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens 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
Source ID	3

Low (High) **Strict-Transport-Security Header Not Set**

Description	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://alfatrial.hmsconsulting.it/js/1c61bb34.da4acfc9.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0aa97a.dc2f8c96.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0c8fab.3b879369.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/50fdc712.6379bdc1.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d230f98.4daf0daf.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d21388e.6ea559ae.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d21729d.9db92fff.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/statics/icons/favicon-32x32.png
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0bd1e4.2684e1a7.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/f8e5842c.1fdfbd9e.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/statics/quasar-logo.png
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0f02c9.5d903c4c.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/manifest.json
Method	GET
URL	https://alfatrial.hmsconsulting.it/css/ba44b8a6.39a71549.css
Method	GET

URL	https://alfatrial.hmsconsulting.it/js/cce381a8.a58789f4.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/css/3faaeca7.57eeba49.css
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0deb22.bb1ec74e.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/css/e31e1ff8.fcb6c043.css
Method	GET
URL	https://alfatrial.hmsconsulting.it/css/f8e5842c.fcb6c043.css
Method	GET
URL	https://alfatrial.hmsconsulting.it/css/cce381a8.39a71549.css
Method	GET
Instances	95
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 http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
CWE Id	16
WASC Id	15
Source ID	3

Low (High)	**In Page Banner Information Leak**
Description	The server returned a version banner string in the response content. Such information leaks may allow attackers to further target specific issues impacting the product and version in use.
URL	https://alfatrial.hmsconsulting.it/statics/quasar-logo.png
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/sitemap.xml
Method	GET
Evidence	nginx/1.19.0
URL	https://alfatrial.hmsconsulting.it/robots.txt
Method	GET
Evidence	nginx/1.19.0
Instances	3
Solution	Configure the server to prevent such information leaks. For example: Under Tomcat this is done via the "server" directive and implementation of custom error pages. Under Apache this is done via the "ServerSignature" and "ServerTokens" directives.
Other information	There is a chance that the highlight in the finding is on a value in the headers, versus the actual matched string in the response body.

Reference	https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/
CWE Id	200
WASC Id	13
Source ID	3

Low (Medium) **Feature Policy Header Not Set**

Description	Feature 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. Feature 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://alfatrial.hmsconsulting.it/js/2d21388e.6ea559ae.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0bd1e4.2684e1a7.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0f02c9.5d903c4c.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/f8e5842c.1fdfbd9e.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/cce381a8.a58789f4.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d21729d.9db92fff.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/1c61bb34.da4acfc9.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0aa97a.dc2f8c96.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d230f98.4daf0daf.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/50fdc712.6379bdc1.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0b23f1.7489819d.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/74529264.58c7bb8f.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0b8e56.07c84772.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/526e6b0f.4e8676b3.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/27ac7332.34cb3cb7.js

Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d21da75.701f392a.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d22bdcd.360f4ea7.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0deb22.bb1ec74e.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/4a9ca042.dc452ecb.js
Method	GET
Instances	70
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy https://developers.google.com/web/updates/2018/06/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	16
WASC Id	15
Source ID	3

Low (Medium)	**Intestazione X-Content-Type-Options mancante**
Description	L'intestazione Anti-MIME-Sniffing nell'impostazione X-Content-Type-Options non era impostata su 'nosniff'. Questo permette alle vecchie versioni di Internet Explorer e Chrome di eseguire analisi MIME-sniffing sul corpo della risposta, potenzialmente causando che il corpo della risposta venga interpretato e visualizzato come un tipo di contenuto diverso dal tipo dichiarato. Versioni attuali (inizio 2014) e precedenti di Firefox useranno il tipo di contenuto dichiarato (se uno è impostato), piuttosto che eseguire analisi MIME.
URL	https://alfatrial.hmsconsulting.it/js/4a9ca042.dc452ecb.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d21a08f.3a4d6c2b.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/vendor.35758b23.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d0d4416.e74a64eb.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d0e942e.69760301.js
Method	GET

Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d21f0cb.0d88fcdf.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d21e021.fe33e005.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d217329.8776fbda.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d0e5af8.f7ae4401.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d2219e2.ccdbe8ca.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/06c76a9a.fd949505.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d0bd1e4.2684e1a7.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d0f02c9.5d903c4c.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/0af16d65.ffd2141e.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/f8e5842c.1fdfbd9e.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/css/0cfa5d3b.555e6622.css
Method	GET
Parameter	X-Content-Type-Options

URL	https://alfatrial.hmsconsulting.it/js/0afeeed0.dda0d6bc.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/2d0aa97a.dc2f8c96.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/cce381a8.a58789f4.js
Method	GET
Parameter	X-Content-Type-Options
URL	https://alfatrial.hmsconsulting.it/js/6a606cde.832082f2.js
Method	GET
Parameter	X-Content-Type-Options
Instances	82
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.
Other information	Questo problema è ancora applicato a tutte le pagine che hanno il tipo di errore (401, 403, 500, ecc.), Poichè tutte quelle pagine sono ancora generalmente interessate dai problemi relativi all'iniezione, nel qual caso i browser continuano a funzionare sono ancora preoccupati di rivedere le pagine del loro tipo di contenuto che è reale. Alla soglia "alta", questo scanner non avviserà in merito alle risposte relative all'errore del client o del server.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	**Incomplete or No Cache-control and Pragma HTTP Header Set**
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://alfatrial.hmsconsulting.it/manifest.json
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/css/2b67a116.75c66616.css
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/css/ba44b8a6.39a71549.css
Method	GET
Parameter	Cache-Control

URL	https://alfatrial.hmsconsulting.it/css/4a9ca042.4a2bbf72.css
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/css/22d25230.39a71549.css
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/css/cce381a8.39a71549.css
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/css/810dabda.0eea230b.css
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/css/app.2eb7fe9e.css
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/css/8305a556.8a7909fc.css
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/css/0701133c.74a9f607.css
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/css/4b65d126.c9681678.css
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/css/0cfa5d3b.555e6622.css
Method	GET
Parameter	Cache-Control
URL	https://alfatrial.hmsconsulting.it/
Method	GET
Parameter	Cache-Control
Instances	13
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13

Source ID	3

Low (Medium)	**Content Security Policy (CSP) Header Not Set**
Description	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://alfatrial.hmsconsulting.it/statics/quasar-logo.png
Method	GET
URL	https://alfatrial.hmsconsulting.it/
Method	GET
URL	https://alfatrial.hmsconsulting.it/sitemap.xml
Method	GET
URL	https://alfatrial.hmsconsulting.it/robots.txt
Method	GET
Instances	4
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	16
WASC Id	15
Source ID	3

Low (Low)	**Dangerous JS Functions**
Description	A dangerous JS function seems to be in use that would leave the site vulnerable.
URL	https://alfatrial.hmsconsulting.it/js/vendor.35758b23.js
Method	GET
Evidence	eval
URL	https://alfatrial.hmsconsulting.it/js/6a606cde.832082f2.js
Method	GET
Evidence	eVal
URL	https://alfatrial.hmsconsulting.it/js/50fdc712.6379bdc1.js
Method	GET
Evidence	eVal

URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	eval
Instances	4
Solution	See the references for security advice on the use of these functions.
Reference	https://angular.io/guide/security
CWE Id	749
Source ID	3

Informational (Medium) **Storable and Cacheable Content**

Description	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://alfatrial.hmsconsulting.it/js/06c76a9a.fd949505.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d2219e2.ccdbe8ca.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0ddddd.7b38b7a4.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0df1fc.cb83d0e0.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0b9e24.a6479ffd.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/0af16d65.ffd2141e.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/3faaeca7.e764d254.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/css/3280d326.fcb6c043.css
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0c02d3.33490a48.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0e2700.b791e98e.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/4b65d126.9ff191a3.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d2257a5.80d5212f.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d229481.d3f7ce13.js
Method	GET

URL	https://alfatrial.hmsconsulting.it/js/2d0e264b.81f946fa.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0e5af8.f7ae4401.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2aceb3ba.7152616d.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/css/22d25230.39a71549.css
Method	GET
URL	https://alfatrial.hmsconsulting.it/robots.txt
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/0cfa5d3b.218b08f0.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/app.230a2341.js
Method	GET
Instances	95
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.
Other information	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. https://tools.ietf.org/html/rfc7234
Reference	https://tools.ietf.org/html/rfc7231 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	524
WASC Id	13
Source ID	3

Informational (Medium) **Modern Web Application**

Description	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://alfatrial.hmsconsulting.it/js/vendor.35758b23.js
Method	GET
Evidence	<a>
URL	https://alfatrial.hmsconsulting.it/
Method	GET
Evidence	<script type=text/javascript src=js/app.230a2341.js></script>
Instances	2

Solution	This is an informational alert and so no changes are required.
Other information	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Reference	
Source ID	3

Informational (Medium)	**User Agent Fuzzer**
Description	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://alfatrial.hmsconsulting.it/statics
Method	GET
Parameter	Header User-Agent
Attack	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
URL	https://alfatrial.hmsconsulting.it/css
Method	GET
Parameter	Header User-Agent
Attack	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
URL	https://alfatrial.hmsconsulting.it/js
Method	GET
Parameter	Header User-Agent
Attack	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
URL	https://alfatrial.hmsconsulting.it/statics/icons
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
URL	https://alfatrial.hmsconsulting.it/statics/icons
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
URL	https://alfatrial.hmsconsulting.it/js
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
URL	https://alfatrial.hmsconsulting.it/statics/icons
Method	GET
Parameter	Header User-Agent

Attack	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
URL	https://alfatrial.hmsconsulting.it/css
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
URL	https://alfatrial.hmsconsulting.it/statics
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
URL	https://alfatrial.hmsconsulting.it/css
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
URL	https://alfatrial.hmsconsulting.it/statics/icons
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
URL	https://alfatrial.hmsconsulting.it/statics
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
URL	https://alfatrial.hmsconsulting.it/statics/icons
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
URL	https://alfatrial.hmsconsulting.it/css
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
URL	https://alfatrial.hmsconsulting.it/statics/icons
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
URL	https://alfatrial.hmsconsulting.it/js
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
URL	https://alfatrial.hmsconsulting.it/statics
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
URL	https://alfatrial.hmsconsulting.it/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
URL	https://alfatrial.hmsconsulting.it/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
URL	https://alfatrial.hmsconsulting.it/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Instances	37
Solution	
Reference	https://owasp.org/wstg
Source ID	1

Informational (Medium)	**Base64 Disclosure**
Description	Base64 encoded data was disclosed by the application/web server
URL	https://alfatrial.hmsconsulting.it/js/vendor.35758b23.js
Method	GET
Evidence	sha512-NHLbDQxz25CfpFJQWJMnE8t2wM5H1YOWh6a5jYyiinDLZ0FlZWrCNrblT0sVOrTuunGp20trexDez5O9BcB2hw==
URL	https://alfatrial.hmsconsulting.it/css/app.2eb7fe9e.css
Method	GET
Evidence	/fonts/KFOkCnqEu92Fr1MmgVxIIzQ
URL	https://alfatrial.hmsconsulting.it/js/2d0e264b.81f946fa.js
Method	GET
Evidence	Th1_Th2_Th3_Th4_Th5_Th6_Th7_Th8_Th9_Th10_Th11_Th12
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=
Instances	4
Solution	Manually confirm that the Base64 data does not leak sensitive information, and that the data cannot be aggregated/used to exploit other vulnerabilities.

Other information	²\x0016¹×o\x001c¶ÃC\x001cöä'é\x0014”\x0016$ÉÄòÝ°3‘õ`å¡é®cc(¢œ2ÙÐYYZ°-¹SÒÅN;®œjvÒÚÞÄ7³äïAp\x001d¡
Reference	https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Source ID	3

Informational (Low) **Information Disclosure - Suspicious Comments**

Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://alfatrial.hmsconsulting.it/js/2d0e942e.69760301.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0c0a08.07f45907.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/06c76a9a.fd949505.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0aa97a.dc2f8c96.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0c8fab.3b879369.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0c02d3.33490a48.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0df1fc.cb83d0e0.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0deb22.bb1ec74e.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d21e021.fe33e005.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/50fdc712.6379bdc1.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0b9e24.a6479ffd.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/3280d326.4c33bbe8.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0c7eef.3e4def19.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d22bdcd.360f4ea7.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/0cfa5d3b.218b08f0.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d2257a5.80d5212f.js

Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0ddddd.7b38b7a4.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d0e2700.b791e98e.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/4a9ca042.dc452ecb.js
Method	GET
URL	https://alfatrial.hmsconsulting.it/js/2d21da75.701f392a.js
Method	GET
Instances	57
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Other information	The following comment/snippet was identified via the pattern: \bSELECT\b (window["webpackJsonp"]=window["webpackJsonp"]||[]).push([["2d0e942e"], {"8d7c":function(e,a,r){"use strict";Object.defineProperty(a,"__esModule", {value:!0}),a.default=void 0,r("28a5");var i={lang:"tr",label: {clear:"Temizle",ok:"Tamam",cancel:"İptal",close:"Kapat",set:"Ayarla",select:"Seç",reset:"Sıfırla", remove:"Kaldır",update:"Güncelle",create:"Oluştur",search:"Ara",filter:"Süz",refresh:"Yenile"},dat e: {days:"Pazar_Pazartesi_Salı_Çarşamba_Perşembe_Cuma_Cumartesi".split("_"),daysShort:"P az_Pzt_Sal_Çar_Per_Cum_Cmt".split("_"),months:"Ocak_Şubat_Mart_Nisan_Mayıs_Haziran_ Temmuz_Ağustos_Eylül_Ekim_Kasım_Aralık".split("_"),monthsShort:"Oca_Şub_Mar_Nis_May _Haz_Tem_Ağu_Eyl_Eki_Kas_Ara".split("_"),firstDayOfWeek:1,format24h:!0},pullToRefresh: {pull:"Yenilemek için aşağı çekin",release:"Yenilemek için bırakın",refresh:"Yenileniyor..."},table: {noData:"Veri yok",noResults:"Uyuşan kayıt bulunamadı",loading:"Yükleniyor...",selectedRecords:function(e){return e+" seçili kayıt."},recordsPerPage:"Sayfa başına kayıt:",allRows:"Tümü",pagination:function(e,a,r){return e+"-"+a+" toplam "+r},columns:"Sütunlar"},editor: {url:"URL",bold:"Kalın",italic:"Eğik",strikethrough:"Üstü çizili",underline:"Altı çizili",unorderedList:"Sırasız Liste",orderedList:"Sıralı Liste",subscript:"Alt betik",superscript:"Üst betik",hyperlink:"Köprü",toggleFullscreen:"Tam ekranı Aç-Kapa",quote:"Alıntı",left:"Sola hizala",center:"Ortala",right:"Sağa hizala",justify:"Sığdır",print:"Yazdır",outdent:"Girintiyi azalt",indent:"Girintiyi artır",removeFormat:"Biçimlendirmeyi kaldır",formatting:"Biçimliyor",fontSize:"Yazı Tipi Boyutu",align:"Hizala",hr:"Yatay Çizgi Ekle",undo:"Geri Al",redo:"Yinele",header1:"Başlık 1",header2:"Başlık 2",header3:"Başlık 3",header4:"Başlık 4",header5:"Başlık 5",header6:"Başlık 6",paragraph:"Paragraf",code:"Kod",size1:"Çok küçük",size2:"Küçük",size3:"Normal",size4:"Orta-geniş",size5:"Büyük",size6:"Çok büyük",size7:"En büyük",defaultFont:"Varsayılan Yazı Tipi"},tree:{noNodes:"Düğüm yok",noResults:"Uyuşan düğüm bulunamadı"}};a.default=i}}]);
Reference	
CWE Id	200
WASC Id	13
Source ID	3

Informational (Low) **Timestamp Disclosure - Unix**

Description	A timestamp was disclosed by the application/web server - Unix
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	1802195444
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	10079487

URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	829329135
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	112637215
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	1711684554
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	1762050814
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	1504918807
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	314042704
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	1303535960
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	13434879
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	1943803523
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	198958881
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	40735498
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	1913087877
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	366619977
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	1994146192

URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	853044451
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	20971520
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	16711680
URL	https://alfatrial.hmsconsulting.it/js/7a29f2d5.074cd961.js
Method	GET
Evidence	1068828381
Instances	176
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Other information	1802195444, which evaluates to: 2027-02-09 18:50:44
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Source ID	3