



ZAP by
Checkmarx

ZAP by Checkmarx Scanning Report

Site: <https://alfarate.demo.hmsbox.it>

Generated on Thu, 4 Jun 2026 09:21:07

ZAP Version: 2.17.0

ZAP by [Checkmarx](#)

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	3
Informational	9

Insights

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP errors logged - see the zap. log file for details	10
Low	Warning		ZAP warnings logged - see the zap. log file for details	45
Info	Informational		Percentage of network failures	1 %
Info	Informational	http://alfaplus.demo.hmsbox.it	Percentage of responses with status code 3xx	100 %
Info	Informational	http://alfarate.demo.hmsbox.it	Percentage of responses with status code 3xx	100 %
Info	Informational	http://alfarate.demo.hmsbox.it	Percentage of slow responses	15 %
Info	Informational	http://alfasearch.it	Percentage of responses	100 %

			with status code 3xx	
Info	Informational	https://alfaplus.demo.hmsbox.it	Percentage of responses with status code 2xx	82 %
Info	Informational	https://alfaplus.demo.hmsbox.it	Percentage of responses with status code 3xx	13 %
Info	Informational	https://alfaplus.demo.hmsbox.it	Percentage of responses with status code 4xx	3 %
Info	Informational	https://alfaplus.demo.hmsbox.it	Percentage of endpoints with content type text/css	38 %
Info	Informational	https://alfaplus.demo.hmsbox.it	Percentage of endpoints with content type text/html	46 %
Info	Informational	https://alfaplus.demo.hmsbox.it	Percentage of endpoints with content type text/javascript	15 %
Info	Informational	https://alfaplus.demo.hmsbox.it	Percentage of endpoints with method GET	92 %
Info	Informational	https://alfaplus.demo.hmsbox.it	Percentage of endpoints with method POST	7 %
Info	Informational	https://alfaplus.demo.hmsbox.it	Count of total endpoints	13
Info	Exceeded Low	https://alfaplus.demo.hmsbox.it	Percentage of slow responses	34 %
Info	Informational	https://alfarate.demo.hmsbox.it	Percentage of responses with status code 2xx	53 %

Info	Informational	https://alfarate.demo.hmsbox.it	Percentage of responses with status code 3xx	13 %
Info	Exceeded Low	https://alfarate.demo.hmsbox.it	Percentage of responses with status code 4xx	32 %
Info	Informational	https://alfarate.demo.hmsbox.it	Percentage of endpoints with content type text/css	35 %
Info	Informational	https://alfarate.demo.hmsbox.it	Percentage of endpoints with content type text/html	42 %
Info	Informational	https://alfarate.demo.hmsbox.it	Percentage of endpoints with content type text/javascript	14 %
Info	Informational	https://alfarate.demo.hmsbox.it	Percentage of endpoints with content type text/plain	7 %
Info	Informational	https://alfarate.demo.hmsbox.it	Percentage of endpoints with method GET	92 %
Info	Informational	https://alfarate.demo.hmsbox.it	Percentage of endpoints with method POST	7 %
Info	Informational	https://alfarate.demo.hmsbox.it	Count of total endpoints	14
Info	Informational	https://alfarate.demo.hmsbox.it	Percentage of slow responses	2 %
Info	Informational	https://alfasearch.it	Percentage of responses with status code 2xx	89 %

Info	Informational	https://alfasearch.it	Percentage of responses with status code 4xx	10 %
Info	Informational	https://alfasearch.it	Percentage of endpoints with content type text/html	66 %
Info	Informational	https://alfasearch.it	Percentage of endpoints with content type text/plain	33 %
Info	Informational	https://alfasearch.it	Percentage of endpoints with method GET	100 %
Info	Informational	https://alfasearch.it	Count of total endpoints	3
Info	Informational	https://alfasearch.it	Percentage of slow responses	7 %

Alerts

Name	Risk Level	Number of Instances
CSP: Failure to Define Directive with No Fallback	Medium	Systemic
CSP: script-src unsafe-eval	Medium	Systemic
CSP: script-src unsafe-inline	Medium	Systemic
CSP: style-src unsafe-inline	Medium	Systemic
Cookie No HttpOnly Flag	Low	3
Cookie Without Secure Flag	Low	3
X-Content-Type-Options Header Missing	Low	1
Authentication Request Identified	Informational	1
GET for POST	Informational	1
Re-examine Cache-control Directives	Informational	1
Session Management Response Identified	Informational	4
Tech Detected - Django	Informational	1
Tech Detected - HSTS	Informational	1
Tech Detected - Nginx	Informational	1
User Agent Fuzzer	Informational	Systemic
User Controllable HTML Element Attribute (Potential XSS)	Informational	4

Alert Detail

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing /excluding them is the same as allowing anything.
URL	https://alfarate.demo.hmsbox.it
Node Name	https://alfarate.demo.hmsbox.it
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://alfarate.demo.hmsbox.it/
Node Name	https://alfarate.demo.hmsbox.it/
Method	GET
Attack	
Evidence	style-src 'self' 'unsafe-inline'; default-src 'none'; connect-src 'self'; frame-src www.canva.com; script-src 'self' 'unsafe-eval' 'unsafe-inline'; img-src 'self'; font-src 'self' data:
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://alfarate.demo.hmsbox.it/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://alfarate.demo.hmsbox.it/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/sitemap.xml
Method	GET
Attack	

Evidence	style-src 'self' 'unsafe-inline'; default-src 'none'; connect-src 'self'; frame-src www.canva.com; script-src 'self' 'unsafe-eval' 'unsafe-inline'; img-src 'self'; font-src 'self' data:
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: script-src unsafe-eval
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://alfarate.demo.hmsbox.it
Node Name	https://alfarate.demo.hmsbox.it
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.demo.hmsbox.it/
Node Name	https://alfarate.demo.hmsbox.it/
Method	GET
Attack	
Evidence	style-src 'self' 'unsafe-inline'; default-src 'none'; connect-src 'self'; frame-src www.canva.com; script-src 'self' 'unsafe-eval' 'unsafe-inline'; img-src 'self'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.demo.hmsbox.it/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	script-src includes unsafe-eval.

URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
Evidence	style-src 'self' 'unsafe-inline'; default-src 'none'; connect-src 'self'; frame-src www.canva.com; script-src 'self' 'unsafe-eval' 'unsafe-inline'; img-src 'self'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.demo.hmsbox.it/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/sitemap.xml
Method	GET
Attack	
Evidence	style-src 'self' 'unsafe-inline'; default-src 'none'; connect-src 'self'; frame-src www.canva.com; script-src 'self' 'unsafe-eval' 'unsafe-inline'; img-src 'self'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: script-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://alfarate.demo.hmsbox.it
Node Name	https://alfarate.demo.hmsbox.it
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.demo.hmsbox.it/
Node Name	https://alfarate.demo.hmsbox.it/
Method	GET

Attack	
Evidence	style-src 'self' 'unsafe-inline'; default-src 'none'; connect-src 'self'; frame-src www.canva.com; script-src 'self' 'unsafe-eval' 'unsafe-inline'; img-src 'self'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.demo.hmsbox.it/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.demo.hmsbox.it/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/sitemap.xml
Method	GET
Attack	
Evidence	style-src 'self' 'unsafe-inline'; default-src 'none'; connect-src 'self'; frame-src www.canva.com; script-src 'self' 'unsafe-eval' 'unsafe-inline'; img-src 'self'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	CSP: style-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://alfarate.demo.hmsbox.it
Node Name	https://alfarate.demo.hmsbox.it
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.demo.hmsbox.it/
Node Name	https://alfarate.demo.hmsbox.it/
Method	GET
Attack	
Evidence	style-src 'self' 'unsafe-inline'; default-src 'none'; connect-src 'self'; frame-src www.canva.com; script-src 'self' 'unsafe-eval' 'unsafe-inline'; img-src 'self'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.demo.hmsbox.it/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-eval' 'unsafe-inline'; connect-src 'self'; img-src 'self'; default-src 'none'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.demo.hmsbox.it/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/sitemap.xml
Method	GET
Attack	
Evidence	style-src 'self' 'unsafe-inline'; default-src 'none'; connect-src 'self'; frame-src www.canva.com; script-src 'self' 'unsafe-eval' 'unsafe-inline'; img-src 'self'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
Instances	Systemic

Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Low	Cookie No HttpOnly Flag
Description	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://alfarate.demo.hmsbox.it
Node Name	https://alfarate.demo.hmsbox.it
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)(csrftoken,next,password,username)
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
Instances	3
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

Low	Cookie Without Secure Flag

Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://alfarate.demo.hmsbox.it
Node Name	https://alfarate.demo.hmsbox.it
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)(csrftoken,next,password,username)
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
Instances	3
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

Low	X-Content-Type-Options Header Missing
Description	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://alfarate.demo.hmsbox.it/robots.txt
Node Name	https://alfarate.demo.hmsbox.it/robots.txt
Method	GET
Attack	

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

Informational	Authentication Request Identified
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)(csrfmiddlewaretoken,next,password,username)
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=ZAP passwordParam=password referer=https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/ csrfToken=csrfmiddlewaretoken
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	GET for POST
Description	A request that was originally observed as a POST was also accepted as a GET. This issue does not turn a security weakness unto itself, however, it may facilitate simplification of other attacks. For example, if a POST is subject to Cross-Site Scripting (XSS), then this finding may indicate that a simplified (GET) request may also be possible.
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/

Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (csrfmiddlewaretoken,next,password,username)
Method	GET
Attack	
Evidence	GET https://alfarate.demo.hmsbox.it/admin/login/?csrfmiddlewaretoken=yfkibEdjwAB6u5d9e49HW8pVCLC24XLCxWEroMnBLpAhMcTd6F91U7D/&password=ZAP&username=ZAP HTTP/1.1
Other Info	
Instances	1
Solution	Ensure that only POST is accepted where POST is expected.
Reference	
CWE Id	16
WASC Id	20
Plugin Id	10058

Informational	Re-examine Cache-control Directives
Description	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://alfarate.demo.hmsbox.it/robots.txt
Node Name	https://alfarate.demo.hmsbox.it/robots.txt
Method	GET
Attack	
Evidence	
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

Informational	Session Management Response Identified
Description	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://alfarate.demo.hmsbox.it
Node Name	https://alfarate.demo.hmsbox.it
Method	GET

Attack	
Evidence	csrftoken
Other Info	cookie:csrftoken
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
Evidence	csrftoken
Other Info	cookie:csrftoken
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)(csrftoken,next,password,username)
Method	POST
Attack	
Evidence	csrftoken
Other Info	cookie:csrftoken
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
Evidence	csrftoken
Other Info	cookie:csrftoken
Instances	4
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112

Informational	Tech Detected - Django
Description	The following "Web frameworks" technology was identified: Django. Described as: Django is a Python-based free and open-source web application framework.
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
	<input type="hidden" name="csrftoken" value="

Evidence	CwpfTQ6BqsqXRKrqswKlvEmsn4dP5LtBdJo6YgTFhp89R7uk7l4GuS4LPtATRgc">
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:djangoproject:django:*:*:*:*:* *****
Instances	1
Solution	
Reference	https://djangoproject.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - HSTS
Description	The following "Security" technology was identified: HSTS. Described as: HTTP Strict Transport Security (HSTS) informs browsers that the site should only be accessed using HTTPS.
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
Evidence	Strict-Transport-Security
Other Info	
Instances	1
Solution	
Reference	https://www.rfc-editor.org/rfc/rfc6797#section-6.1
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - Nginx
Description	The following "Web servers, Reverse proxies" technology was identified: Nginx. Described as: Nginx is a web server that can also be used as a reverse proxy, load balancer, mail proxy and HTTP cache.
URL	https://alfarate.demo.hmsbox.it/static/admin/css/login.css
Node Name	https://alfarate.demo.hmsbox.it/static/admin/css/login.css
Method	GET
Attack	
Evidence	nginx
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:f5:nginx:*:*:*:*:* *****
Instances	1
Solution	

Reference	https://nginx.org/en
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	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://alfarate.demo.hmsbox.it
Node Name	https://alfarate.demo.hmsbox.it
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://alfarate.demo.hmsbox.it/
Node Name	https://alfarate.demo.hmsbox.it/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://alfarate.demo.hmsbox.it/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)(csrfmiddlewaretoken,next,password,username)
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Evidence	
Other Info	
Instances	Systemic
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)
Method	GET
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://alfarate.demo.hmsbox.it/admin/login/?next=/sitemap.xml appears to include user input in: a(n) [input] tag [value] attribute The user input found was: next=/sitemap.xml The user-controlled value was: /sitemap.xml
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)(csrfmiddlewaretoken,next,password,username)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/ appears to include user input in: a(n) [a] tag [href] attribute The user input found was: next=/admin/

	The user-controlled value was: /admin/
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)(csrfmiddlewaretoken,next,password,username)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: password=ZAP The user-controlled value was: zap
URL	https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/
Node Name	https://alfarate.demo.hmsbox.it/admin/login/ (next)(csrfmiddlewaretoken,next,password,username)
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://alfarate.demo.hmsbox.it/admin/login/?next=/admin/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: username=ZAP The user-controlled value was: zap
Instances	4
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031