ZAP by Checkmarx Scanning Report

Site: https://alfarate.aslfoggia.hmsbox.it

Generated on Wed, 29 Jan 2025 00:00:40

ZAP Version: 2.16.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	5
Low	3
Informational	8

Alerts

Name	Risk Level	Number of Instances
CSP: Wildcard Directive	Medium	12
CSP: script-src unsafe-eval	Medium	12
CSP: script-src unsafe-inline	Medium	12
CSP: style-src unsafe-inline	Medium	12
Content Security Policy (CSP) Header Not Set	Medium	1
Cookie No HttpOnly Flag	Low	8
Cookie Without Secure Flag	Low	8
Strict-Transport-Security Header Not Set	Low	18
Authentication Request Identified	Informational	3
Information Disclosure - Suspicious Comments	Informational	11
Re-examine Cache-control Directives	Informational	2
Session Management Response Identified	Informational	8
Tech Detected - Django	Informational	1
Tech Detected - Nginx	Informational	1
User Agent Fuzzer	Informational	12
User Controllable HTML Element Attribute (Potential XSS)	Informational	16

Alert Detail

Medium	CSP: Wildcard Directive
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.aslfoggia.hmsbox.it/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding

	them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/done/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-

Evidence	inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
Instances	12
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://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
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.aslfoggia.hmsbox.it/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	GET
Attack	

Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/done/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/

Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
Instances	12
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://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
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.aslfoggia.hmsbox.it/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/
Method	GET

Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/done/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.

URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
Instances	12
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://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
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.aslfoggia.hmsbox.it/

Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/done/
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other	

Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	POST
Attack	
Evidence	img-src 'self'; connect-src 'self'; default-src 'none'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
Instances	12
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://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

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://alfarate.aslfoggia.hmsbox.it/robots.txt
Method	GET
Attack	
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/Security/CSP/Introducing_Content_Security_Policy 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

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.aslfoggia.hmsbox.it/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	

Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
Instances	8
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.aslfoggia.hmsbox.it/
Method	GET

Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken

Other Info	
Instances	8
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	**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://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	

Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/done/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/static/admin/css/base.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/static/admin/css/dark_mode.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/static/admin/css/forms.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/static/admin/css/login.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/static/admin/css/nav_sidebar.css
Method	GET
Attack	
Evidence	
Other Info	

URL	https://alfarate.aslfoggia.hmsbox.it/static/admin/css/responsive.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/static/admin/js/nav_sidebar.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/static/admin/js/theme.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	
Other Info	
Instances	18
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

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.aslfoggia.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=ZAP passwordParam=password referer=https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/ csrfToken=csrfmiddlewaretoken
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=ZAP passwordParam=password referer=https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/ csrfToken=csrfmiddlewaretoken
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=ZAP passwordParam=password referer=https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml csrfToken=csrfmiddlewaretoken
Instances	3
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	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://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script src="/static/admin/js/theme.js" defer></script>", see evidence field for the suspicious comment/snippet.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	GET
Attack	

Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script src="/static/admin/js/theme.js" defer></script>", see evidence field for the suspicious comment/snippet.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script src="/static/admin/js/theme.js" defer></script>", see evidence field for the suspicious comment/snippet.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script src="/static/admin/js/theme.js" defer></script>", see evidence field for the suspicious comment/snippet.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script src="/static/admin/js/theme.js" defer></script>", see evidence field for the suspicious comment/snippet.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/done/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script src="/static/admin/js/theme.js" defer></script>", see evidence field for the suspicious comment/snippet.
URL	https://alfarate.aslfoggia.hmsbox.it/static/admin/js/nav_sidebar.js
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 4 times, the first in the element starting with: " let navSidebarIsOpen = localStorage.getItem('django.admin.navSidebarIsOpen');", see evidence field for the suspicious comment/snippet.
URL	https://alfarate.aslfoggia.hmsbox.it/static/admin/js/theme.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: " Array.from(buttons).forEach((btn) => {", see evidence field for the suspicious comment/snippet.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/

Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script src="/static/admin/js/theme.js" defer></script>", see evidence field for the suspicious comment/snippet.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script src="/static/admin/js/theme.js" defer></script>", see evidence field for the suspicious comment/snippet.
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script src="/static/admin/js/theme.js" defer></script>", see evidence field for the suspicious comment/snippet.
Instances	11
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

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.aslfoggia.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/done/
Method	GET
Attack	
Evidence	
Other Info	
Instances	2

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/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.aslfoggia.hmsbox.it/
Method	GET
Attack	
Evidence	TteQpxDz5xFxQrFsUvb1GaIUeFR47G1y
Other Info	cookie:csrftoken
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	vM5hKQ1R6h5XFy5Qs8zy2CVGX7pNeFpb
Other Info	cookie:csrftoken
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	vM5hKQ1R6h5XFy5Qs8zy2CVGX7pNeFpb
Other Info	cookie:csrftoken
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	vM5hKQ1R6h5XFy5Qs8zy2CVGX7pNeFpb
Other Info	cookie:csrftoken
URL	https://alfarate.aslfoggia.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	vM5hKQ1R6h5XFy5Qs8zy2CVGX7pNeFpb
Other Info	cookie:csrftoken

URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	vM5hKQ1R6h5XFy5Qs8zy2CVGX7pNeFpb
Other Info	cookie:csrftoken
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	vM5hKQ1R6h5XFy5Qs8zy2CVGX7pNeFpb
Other Info	cookie:csrftoken
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	vM5hKQ1R6h5XFy5Qs8zy2CVGX7pNeFpb
Other Info	cookie:csrftoken
Instances	8
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.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	<input type="hidden" name="csrfmiddlewaretoken" value=" 95Gz9s9xabtnrWFgJebiKh7MIkZt7w7JuHBGJ80e6ioaWkAW1cAGCJSivhe6b1mK">
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 - Nginx**
	The following "Web servers, Reverse proxies" technology was identified: Nginx.

Description	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.aslfoggia.hmsbox.it/sitemap.xml
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.aslfoggia.hmsbox.it/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	

URL	https://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	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://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	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://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	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://alfarate.aslfoggia.hmsbox.it/
Method	GET
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
Evidence	
Other Info	

URL	https://alfarate.aslfoggia.hmsbox.it/
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	12
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

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.aslfoggia.hmsbox.it/admin/login/?next=/admin/
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.aslfoggia.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.aslfoggia.hmsbox.it/admin/login/?next=/admin/
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.aslfoggia.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/password_reset/
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
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.aslfoggia.hmsbox.it /admin/login/?next=/admin/ appears to include user input in: a(n) [form] tag [action] attribute The user input found was: next=/admin/ The user-controlled value was: /admin/login/?next= /admin/
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
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.aslfoggia.hmsbox.it /admin/login/?next=/admin/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: next=/admin/ The user-controlled value was: /admin/
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
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.aslfoggia.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.aslfoggia.hmsbox.it/admin/login/?next=/
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.aslfoggia.hmsbox.it /admin/login/?next=/ 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.aslfoggia.hmsbox.it/admin/login/?next=/
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.aslfoggia.hmsbox.it /admin/login/?next=/ 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
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
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.aslfoggia.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.aslfoggia.hmsbox.it/admin/login/?next=/admin/
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.aslfoggia.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/password_reset/
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
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.aslfoggia.hmsbox.it /admin/login/?next=/admin/ appears to include user input in: a(n) [form] tag [action] attribute The user input found was: next=/admin/ The user-controlled value was: /admin/login/?next= /admin/
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
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.aslfoggia.hmsbox.it /admin/login/?next=/admin/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: next=/admin/ The user-controlled value was: /admin/
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/admin/
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.aslfoggia.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.aslfoggia.hmsbox.it/admin/login/?next=/admin/
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.aslfoggia.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
URL	https://alfarate.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
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.aslfoggia.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.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
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.aslfoggia.hmsbox.it /admin/login/?next=/sitemap.xml 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.aslfoggia.hmsbox.it/admin/login/?next=/sitemap.xml
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.aslfoggia.hmsbox.it /admin/login/?next=/sitemap.xml 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	16
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