ZAP by Checkmarx Scanning Report

Sites: https://alfaplus.demo.hmsbox.it http://alfaplus.demo.hmsbox.it

Generated on Wed, 19 Mar 2025 10:08:07

ZAP Version: 2.16.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	3
Informational	8

Alerts

Name	Risk Level	Number of Instances
CSP: Wildcard Directive	Medium	13
CSP: script-src unsafe-eval	Medium	13
CSP: script-src unsafe-inline	Medium	13
CSP: style-src unsafe-inline	Medium	13
Cookie No HttpOnly Flag	Low	7
Cookie Without Secure Flag	Low	6
X-Content-Type-Options Header Missing	Low	1
Authentication Request Identified	Informational	3
Re-examine Cache-control Directives	Informational	3
Session Management Response Identified	Informational	7
Tech Detected - Django	Informational	2
Tech Detected - HSTS	Informational	2
Tech Detected - Nginx	Informational	2
User Agent Fuzzer	Informational	12
User Controllable HTML Element Attribute (Potential XSS)	Informational	14

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	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/admin/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/admin/password_reset/done/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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://alfaplus.demo.hmsbox.it/admin/password_reset/
Method	POST
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; 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	13
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	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfaplus.demo.hmsbox.it/
Method	GET

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

URL	https://alfaplus.demo.hmsbox.it/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
URL	https://alfaplus.demo.hmsbox.it/admin/password_reset/
Method	POST
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-eval.
Instances	13
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	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfaplus.demo.hmsbox.it/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfaplus.demo.hmsbox.it/admin/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other	

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

Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	script-src includes unsafe-inline.
Instances	13
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	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfaplus.demo.hmsbox.it/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfaplus.demo.hmsbox.it/admin/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:

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

Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
URL	https://alfaplus.demo.hmsbox.it/admin/password_reset/
Method	POST
Attack	
Evidence	img-src 'self'; style-src 'self' 'unsafe-inline'; frame-src www.canva.com; connect-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-inline'; default-src 'none'; font-src 'self' data:
Other Info	style-src includes unsafe-inline.
Instances	13
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

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

URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfaplus.demo.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
Instances	7
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://alfaplus.demo.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken

Other Info	
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfaplus.demo.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	Set-Cookie: csrftoken
Other Info	
Instances	6
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**
	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

Description	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://alfaplus.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://alfaplus.demo.hmsbox.it/admin/login/?next=/
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=ZAP passwordParam=password referer=https://alfaplus.demo.hmsbox.it/admin/login/?next=/ csrfToken=csrfmiddlewaretoken
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=ZAP passwordParam=password referer=https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/ csrfToken=csrfmiddlewaretoken
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	password
Other Info	userParam=username userValue=ZAP passwordParam=password referer=https://alfaplus.demo.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	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://alfaplus.demo.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfaplus.demo.hmsbox.it/admin/password_reset/done/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alfaplus.demo.hmsbox.it/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
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	http://alfaplus.demo.hmsbox.it/
Method	GET

Attack	
Evidence	mF5ccLyrmAKJSSB9GiGer5m0XGpQanOf
Other Info	cookie:csrftoken
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	SdXUGo1xr6jxXsBKT3YLZWqETzVTO7H9
Other Info	cookie:csrftoken
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	zJaSWzf9zSidGJW1GaQxs29IWr1Dz5Xz
Other Info	cookie:csrftoken
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	GET
Attack	
Evidence	zJaSWzf9zSidGJW1GaQxs29IWr1Dz5Xz
Other Info	cookie:csrftoken
URL	https://alfaplus.demo.hmsbox.it/admin/password_reset/
Method	GET
Attack	
Evidence	zJaSWzf9zSidGJW1GaQxs29IWr1Dz5Xz
Other Info	cookie:csrftoken
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	zJaSWzf9zSidGJW1GaQxs29IWr1Dz5Xz
Other Info	cookie:csrftoken
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/sitemap.xml
Method	POST
Attack	
Evidence	zJaSWzf9zSidGJW1GaQxs29IWr1Dz5Xz
Other Info	cookie:csrftoken
Instances	7
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	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	
Evidence	<input type="hidden" name="csrfmiddlewaretoken" value=" 3yQvbtTaT2T7rzoCA1h13NOa3CaEfydZf3Lxd4hr5stG9hPB69N5kI00Q8pkfLR4">
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:djangoproject:django:*:*: *:*:*:*:*:*
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/
Method	GET
Attack	
Evidence	<input type="hidden" name="csrfmiddlewaretoken" value=" fT3uHzL4F4HgbxIZZ67j6Npwq31cZ7h7XWQedNCrW0QDYP9zIZVUVzF09sMVD4O6">
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:djangoproject:django:*:*: *:*:*:*:*:*
Instances	2
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	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	
Evidence	Strict-Transport-Security
Other Info	
URL	https://alfaplus.demo.hmsbox.it/
Method	GET
Attack	
Evidence	Strict-Transport-Security
Other Info	

Instances	2
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	http://alfaplus.demo.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:*:*:*:*:*:*:*:*
URL	https://alfaplus.demo.hmsbox.it/robots.txt
Method	GET
Attack	
Evidence	nginx
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:*
Instances	2
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	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	

Other Info	
URL	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://alfaplus.demo.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	http://alfaplus.demo.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	http://alfaplus.demo.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	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://alfaplus.demo.hmsbox.it/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other	

Info	
URL	http://alfaplus.demo.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	http://alfaplus.demo.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	http://alfaplus.demo.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://alfaplus.demo.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://alfaplus.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://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	GET
Attack	
Evidence	
Other	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://alfaplus.demo.hmsbox.it

Info	/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://alfaplus.demo.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://alfaplus.demo.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://alfaplus.demo.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://alfaplus.demo.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://alfaplus.demo.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://alfaplus.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://alfaplus.demo.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://alfaplus.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://alfaplus.demo.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://alfaplus.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/password_reset/
URL	https://alfaplus.demo.hmsbox.it/admin/login/?next=/admin/
Method	POST
Attack	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://alfaplus.demo.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://alfaplus.demo.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://alfaplus.demo.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://alfaplus.demo.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://alfaplus.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://alfaplus.demo.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://alfaplus.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
URL	https://alfaplus.demo.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://alfaplus.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://alfaplus.demo.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://alfaplus.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: password=ZAP The user-controlled value was: zap
URL	https://alfaplus.demo.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://alfaplus.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: username=ZAP The user-controlled value was: zap
Instances	14
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