ZAP Scanning Report

Sites: https://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com

Generated on Mon, 27 Jun 2022 08:38:44

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	1
Informational	1
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	2
Anti-CSRF Tokens Check	Medium	2
Buffer Overflow	Medium	1
Content Security Policy (CSP) Header Not Set	Medium	2
HTTP Only Site	Medium	1
Missing Anti-clickjacking Header	Medium	2
X-Content-Type-Options Header Missing	Low	2
User Agent Fuzzer	Informational	35

Alert Detail

Medium	**Absence of Anti-CSRF Tokens**
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET
Parameter	
Attack	
Evidence	<form action="add" method="POST">
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	
Attack	
Evidence	<form action="add" method="POST">
Instances	2

Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium **Anti-CSRF Tokens Check**

Description	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET
Parameter	
Attack	
Evidence	<form action="add" method="POST">
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	
Attack	
Evidence	<form action="add" method="POST">
Instances	2
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	20012

Medium **Buffer Overflow**

Description	Buffer overflow errors are characterized by the overwriting of memory spaces of the background web process, which should have never been modified intentionally or unintentionally. Overwriting values of the IP (Instruction Pointer), BP (Base Pointer) and other registers causes exceptions, segmentation faults, and other process errors to occur. Usually these errors end execution of the application in an unexpected way.
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/add
Method	POST

Parameter	text
Attack	FxSgKbBbonQeFasqMPORGiTHhASLJQJseiLQovdAWtFKkCKSiOZCAdNcqWpMEYVrgSWLTWuxYMGIWKcDiJCUTFPKUnpwTmdoNY JXWQYqsTYrLHZZYIyHRfbiMbVWYrTNcVyyeAmLqRAateACqOdbWNcqspyoMKjucstIGFSgteuVgDrOGBkBGDmtQrVqTvexjqulxrTNwIe OCRlTXCGiMPoISIHMwEsdaACLakDUKdPoIhLuYiCsHewcxZEZHUSbqLJQrymNDYyLwjdggdnuCGGebeHPxXuWCMPUECHyUQtwjNM lRmxdcCqsqLhnutBmXAmOBEvvvhqmMCXIkDcBShwFTJfgBMxknYtLdXFCfrdLVdsEXyoCdWgycEMEEttXDmZZcXVioxAhyuTactcJlMgG SnlJKXkflFUmEvMJdAldGgpOXuthmrEUgZOiVfAZjrQeeHLghQLaOSVQLGCcqqSXcvxMbpxKCEZUZCrqFVDvLTXEGHfUvYopJuUYDTxr MjsSUtGcJbkRdbUaSKBgKIOXcYxhosmAVhkntUsMmjPVmNudclVQqgtBsypBHItJhuISUpCAAMaBRHmxUjtVwVbNefIrnPAaFCbbljOoHX qnJKkucJOllevmSQUFoadDdRNHSAajlFhWOUaeahvLEoNjfPBGVjehOerLjwnXMVwQepLdvPgRNGJYUdQQQIFvHhyLoXyRtfyEaJPvYb oCRbMyJjwqchtgNwhSCPQMnHqUPPBMDLhorLfvbocLnkyiovjoPTcNKEsqdALIxGfxgXmbYeXUWVXMqjLleuhCGEfXgaQqoTlqUUVfsqQ UnRrtteuTbEKtFLvtvtGJAvZpeDdIJvCYVcJTxwRcLbtJWQJgAGbVRanRbWPmPPbtWJASNhcGSbjpNamRVhWLaQvMoEBMUeqaKLwT YEEoyEyuwepligJCLByfWIiOkCqZumYdYwVxIXuTJlMlaxbaNPCQvyiGbKLeElBtkrhEJNiSaUlyfdewhBtuhHxWUuinhMfoaAQIVANHQZOa kUpVFVRFITcgmymLMOlbYoBbtaYEqZEvLMrxpiHtHZCwqwCSaiXxCVaPMkdLbTyfALMlmhUbLBAtKUiwyNIRMxZLBABUuNmtttJdWMlhx BKUbPLTviGsTSNpAZiyESngniJZXhhsKqPUXcWPngPdCogTERVEGfiTgtNFEeYZRJbAmdRdsyDZnXKqTSZTIpnEdtvRuXLuojeeAkVhujj mFHgSBHxlWmFfsbhJZOaIrjaiISffBwAcHUGqdmIjOdCxHmLUVSejrNjuOXQAVbHNXXysngPotLAWVGIEZhqVNvCsnLLXuodHdEtCeMeL pESUHgLbxilqfwdjWCuOITUTrPwHbeBuFUoKklbDhsnHHbQNhQaBWVPESFmUJcWbChNTIuvtXLTOQrXuxlUYWaZCbaTCqwVRRVGn BrTLGmuCHZIKElyssamTVMebNhCVGKoyPcWvmVPVdJtFMnOelvkAtULlNHnJAOWqJfLIZYpZJclvTZeZAwWNJoJoVrLjYKBxigHnpOrwy jkqmOnqIrOjrpoqWiyhitrDMRvkIcmuxIqrIDhTNsYHHpLiEtQHvljvwbrpSGfaxtLKyjcrxXhVwpklulbRidXjOLmSPjZbZXoHNyGRclGQfbaRTyI GYNtpgyKJfGNnuGCHjmFHDqgTvLqqnYSEBrGZuPhFbRHxTrYOusrhvbZGSHmWNUNQxATwfIFiHLRuMLeiMCbTdmVaxuyWfaXKovHV KjGIQEBvhMFpFtLeNoUVWkoRGpgikvysnSaouSLJlcZATWjIeICoJJxEuaMGfLPWKIIZpLdwHpTDxXAkeeFrvuQicDkBKVPhixjCYCJRMM ReQUHTYcYmkRJKDvUyyeYXmWFHWYTFlLuiUbIdyTBQIfjlyFknJmXWOGjgamOBhYSuAhGWRwLWMISGIyjOKQreICIVydDavMERvIW CjyIHUsjGTsZcqsQOEYGfhPNOgTssFMrgMjEOVTmnIyvNYxXFgpCjJEjXhefxWjiZAdHBREViMhLHWrvYkIBBERBFQRlJpohgDvkTyffFJxg GcQNCnlbrpSWE
Evidence	Connection: close
Instances	1
Solution	Rewrite the background program using proper return length checking. This will require a recompile of the background executable.
Reference	https://owasp.org/www-community/attacks/Buffer_overflow_attack
CWE Id	120
WASC Id	7
Plugin Id	30001

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	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com

Method	GET
Parameter	
Attack	
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	
Attack	
Evidence	
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**HTTP Only Site**
Description	The site is only served under HTTP and not HTTPS.
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/add
Method	POST
Parameter	
Attack	
Evidence	

Instances	1
Solution	Configure your web or application server to use SSL (https).
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html https://letsencrypt.org/
CWE Id	311
WASC Id	4
Plugin Id	10106

Medium	**Missing Anti-clickjacking Header**
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET
Parameter	X-Frame-Options
Attack	
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	X-Frame-Options
Attack	
Evidence	
Instances	2
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15

Plugin Id	10020
Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	X-Content-Type-Options
Attack	
Evidence	
Instances	2
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021
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://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	

URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/sitemap.xml
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/add
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/add
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/add
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/add
Method	POST
Parameter	Header User-Agent

Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/add
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/add
Method	POST
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://ec2-3-69-178-222.eu-central-1.compute.amazonaws.com/add
Method	POST
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Instances	35
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104