ZAP Scanning Report-active_scan_part2

Sites: https://cdnjs.cloudflare.com http://192.168.1.122

Generated on Thu, 18 May 2023 12:34:56

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	6
Low	5
Informational	4

Alerts

Name	Risk Level	Number of Instances
Cloud Metadata Potentially Exposed	High	1
Content Security Policy (CSP) Header Not Set	Medium	3
Cross-Domain Misconfiguration	Medium	17
Missing Anti-clickjacking Header	Medium	2
Session ID in URL Rewrite	Medium	5
Vulnerable JS Library	Medium	1
XSLT Injection	Medium	19
Cross-Domain JavaScript Source File Inclusion	Low	2
Private IP Disclosure	Low	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	20
Timestamp Disclosure - Unix	Low	5
X-Content-Type-Options Header Missing	Low	5
Information Disclosure - Suspicious Comments	Informational	4
Modern Web Application	Informational	1
Retrieved from Cache	Informational	3
User Agent Fuzzer	Informational	123

Alert Detail

High	Cloud Metadata Potentially Exposed
Description	The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure. All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.

URL	http://192.168.1.122/latest/meta-data/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	169.254.169.254
Evidence	
Instances	1
Solution	Do not trust any user data in NGINX configs. In this case it is probably the use of the $host variable which is set from the 'Host' header and can be controlled by an attacker.
Reference	https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/
CWE Id	
WASC Id	
Plugin Id	90034

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://192.168.1.122/
Method	GET
Attack	
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	
Evidence	
Instances	3
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 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	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	http://192.168.1.122/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/api/Challenges/?name=Score%20Board
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/api/Quantitys/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/assets/i18n/en.json
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/main.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/MaterialIcons-Regular.woff2
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/polyfills.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/rest/admin/application-configuration
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/rest/admin/application-version
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/rest/languages
Method	GET

Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/rest/products/search?q=
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/runtime.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/styles.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.122/vendor.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Instances	17
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

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://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
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

Medium	**Session ID in URL Rewrite**
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3z&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	
Evidence	Jz_kYE12zy7zDQ0GAAAZ
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	
Evidence	Jz_kYE12zy7zDQ0GAAAZ
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	
Evidence	Jz_kYE12zy7zDQ0GAAAZ
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	

Evidence	Jz_kYE12zy7zDQ0GAAAZ
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	
Evidence	Jz_kYE12zy7zDQ0GAAAZ
Instances	5
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html
CWE Id	200
WASC Id	13
Plugin Id	3

Medium	Vulnerable JS Library
Description	The identified library jquery, version 2.2.4 is vulnerable.
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	/2.2.4/jquery.min.js
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://github.com/jquery/jquery.com/issues/162
CWE Id	829
WASC Id	
Plugin Id	10003

Medium	XSLT Injection
Description	Injection using XSL transformations may be possible, and may allow an attacker to read system information, read and write files, or execute arbitrary code.
URL	http://192.168.1.122/api/Challenges/?name=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/rest/products/search?q=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache

URL	http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&transport=polling&t=OWkbRgj
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&t=OWkbRgj
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E

Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E
Method	POST
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E
Method	POST
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>

Evidence	Apache
Instances	19
Solution	Sanitize and analyze every user input coming from any client-side.
Reference	https://www.contextis.com/blog/xslt-server-side-injection-attacks
CWE Id	91
WASC Id	23
Plugin Id	90017

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://192.168.1.122/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.122/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Instances	2
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Low	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	http://192.168.1.122/rest/admin/application-configuration
Method	GET
Attack	
Evidence	192.168.99.100:3000
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Plugin Id	2

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

URL	http://192.168.1.122/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/api/Challenges/?name=Score%20Board
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/api/Quantitys/
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/assets/i18n/en.json
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/main.js
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/MaterialIcons-Regular.woff2
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/polyfills.js
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/rest/admin/application-configuration
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/rest/admin/application-version
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/rest/languages
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/rest/products/search?q=

Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/runtime.js
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3z&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/styles.css
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/vendor.js
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	

Evidence	Apache/2.4.52 (Ubuntu)
Instances	20
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10036

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	http://192.168.1.122/main.js
Method	GET
Attack	
Evidence	1734944650
URL	http://192.168.1.122/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1969196030
URL	http://192.168.1.122/rest/admin/application-configuration
Method	GET
Attack	
Evidence	1970691216
URL	http://192.168.1.122/rest/products/search?q=
Method	GET
Attack	
Evidence	1969196030
URL	http://192.168.1.122/rest/products/search?q=
Method	GET
Attack	
Evidence	1970691216
Instances	5
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10096

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

Description	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://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
Method	GET
Attack	
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3z&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	
Evidence	
Instances	5
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	**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	http://192.168.1.122/main.js
Method	GET
Attack	
Evidence	query

URL	http://192.168.1.122/vendor.js
Method	GET
Attack	
Evidence	query
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	db
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	select
Instances	4
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	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://192.168.1.122/
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
Instances	1
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Method	GET
Attack	
Evidence	Age: 1079384

URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Method	GET
Attack	
Evidence	Age: 11441
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Method	GET
Attack	
Evidence	Age: 140813
Instances	3
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	
WASC Id	
Plugin Id	10050

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://192.168.1.122/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.1.122/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.1.122/assets
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.1.122/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence	
URL	http://192.168.1.122/assets
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	
URL	http://192.168.1.122/assets
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	
URL	http://192.168.1.122/assets
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.1.122/assets
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.1.122/assets
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.1.122/assets
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	
URL	http://192.168.1.122/assets
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	
URL	http://192.168.1.122/assets
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.1.122/assets/i18n
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.1.122/assets/i18n
Method	GET

Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.1.122/assets/i18n
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.1.122/assets/i18n
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.1.122/assets/i18n
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	
URL	http://192.168.1.122/assets/i18n
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	
URL	http://192.168.1.122/assets/i18n
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.1.122/assets/i18n
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.1.122/assets/i18n
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.1.122/assets/i18n
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	
URL	http://192.168.1.122/assets/i18n
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	
URL	http://192.168.1.122/assets/i18n

Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.1.122/assets/public
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.1.122/assets/public
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.1.122/assets/public
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.1.122/assets/public
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.1.122/assets/public
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	
URL	http://192.168.1.122/assets/public
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	
URL	http://192.168.1.122/assets/public
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.1.122/assets/public
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.1.122/assets/public
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.1.122/assets/public

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	
URL	http://192.168.1.122/assets/public
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	
URL	http://192.168.1.122/assets/public
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.1.122/assets/public/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.1.122/assets/public/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.1.122/assets/public/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.1.122/assets/public/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.1.122/assets/public/images
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	
URL	http://192.168.1.122/assets/public/images
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	
URL	http://192.168.1.122/assets/public/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

URL	http://192.168.1.122/assets/public/images
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.1.122/assets/public/images
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.1.122/assets/public/images
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	
URL	http://192.168.1.122/assets/public/images
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	
URL	http://192.168.1.122/assets/public/images
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.1.122/assets/public/images/products
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.1.122/assets/public/images/products
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.1.122/assets/public/images/products
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.1.122/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.1.122/assets/public/images/products
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	
URL	http://192.168.1.122/assets/public/images/products
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	
URL	http://192.168.1.122/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.1.122/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.1.122/assets/public/images/products
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.1.122/assets/public/images/products
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	
URL	http://192.168.1.122/assets/public/images/products
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	
URL	http://192.168.1.122/assets/public/images/products
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.1.122/rest/languages
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	
URL	http://192.168.1.122/rest/languages
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.1.122/rest/languages
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj

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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbRgj
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
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	
	http://192.168.1.122/socket.io/?

URL	EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSAM&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	

URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=websocket&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	GET

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ

Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
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://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbS3t&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
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	

URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
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	
URL	http://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
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://192.168.1.122/socket.io/?EIO=4&transport=polling&t=OWkbSyv&sid=Jz_kYE12zy7zDQ0GAAAZ
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Instances	123
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104