

# ZAP Scanning Report- authenticated\_scan\_part2

Sites: <https://fonts.gstatic.com> <https://ajax.googleapis.com> <https://code.getmdl.io> <https://fonts.googleapis.com> <https://cdnjs.cloudflare.com> <http://192.168.1.122>

Generated on Thu, 18 May 2023 13:16:17

## Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	8
Low	6
Informational	6

## Alerts

Name	Risk Level	Number of Instances
<a href="#">Cloud Metadata Potentially Exposed</a>	High	2
<a href="#">SQL Injection - SQLite</a>	High	1
<a href="#">Absence of Anti-CSRF Tokens</a>	Medium	3
<a href="#">CSP: Wildcard Directive</a>	Medium	1
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	11
<a href="#">Cross-Domain Misconfiguration</a>	Medium	33
<a href="#">Missing Anti-clickjacking Header</a>	Medium	9
<a href="#">Session ID in URL Rewrite</a>	Medium	23
<a href="#">Vulnerable JS Library</a>	Medium	2
<a href="#">XSLT Injection</a>	Medium	39
<a href="#">Cross-Domain JavaScript Source File Inclusion</a>	Low	4
<a href="#">Private IP Disclosure</a>	Low	1
<a href="#">Server Leaks Version Information via "Server" HTTP Response Header Field</a>	Low	53
<a href="#">Strict-Transport-Security Header Not Set</a>	Low	2
<a href="#">Timestamp Disclosure - Unix</a>	Low	5
<a href="#">X-Content-Type-Options Header Missing</a>	Low	25
<a href="#">Authentication Request Identified</a>	Informational	2
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	5
<a href="#">Modern Web Application</a>	Informational	1
<a href="#">Retrieved from Cache</a>	Informational	13
<a href="#">Session Management Response Identified</a>	Informational	4
<a href="#">User Agent Fuzzer</a>	Informational	241

## Alert Detail

High	Cloud Metadata Potentially Exposed
Description	<p>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.</p> <p>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.</p>
URL	<a href="http://192.168.1.122/latest/meta-data/">http://192.168.1.122/latest/meta-data/</a>
Method	POST
Attack	169.254.169.254
Evidence	
URL	<a href="http://192.168.1.122/latest/meta-data/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/latest/meta-data/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	169.254.169.254
Evidence	
Instances	2
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	<a href="https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/">https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">90034</a>

High	SQL Injection - SQLite
Description	SQL injection may be possible.
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	admin@juice-sh.op'('
Evidence	SQLITE_ERROR
Instances	1
Solution	<p>Do not trust client side input, even if there is client side validation in place.</p> <p>In general, type check all data on the server side.</p> <p>If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'</p> <p>If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.</p> <p>If database Stored Procedures can be used, use them.</p> <p>Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!</p> <p>Do not create dynamic SQL queries using simple string concatenation.</p>

	<p>Escape all data received from the client.</p> <p>Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input.</p> <p>Apply the principle of least privilege by using the least privileged database user possible.</p> <p>In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.</p> <p>Grant the minimum database access that is necessary for the application.</p>
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html</a>
CWE Id	<a href="#">89</a>
WASC Id	19
Plugin Id	<a href="#">40018</a>

Medium	Absence of Anti-CSRF Tokens
Description	<p>No Anti-CSRF tokens were found in a HTML submission form.</p> <p>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.</p> <p>CSRF attacks are effective in a number of situations, including:</p> <ul style="list-style-type: none"> <li>* The victim has an active session on the target site.</li> <li>* The victim is authenticated via HTTP auth on the target site.</li> <li>* The victim is on the same local network as the target site.</li> </ul> <p>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.</p>
URL	<a href="http://192.168.1.122/profile">http://192.168.1.122/profile</a>
Method	GET
Attack	
Evidence	<code>&lt;form action="/profile/image/file" style="margin-top:10%; width: 90%; margin-right: auto; margin-left: auto;" method="post" enctype="multipart/form-data"&gt;</code>
URL	<a href="http://192.168.1.122/profile">http://192.168.1.122/profile</a>
Method	GET
Attack	
Evidence	<code>&lt;form action="/profile/image/url" style="margin-top:5%; width: 90%; margin-right: auto; margin-left: auto;" method="post"&gt;</code>
URL	<a href="http://192.168.1.122/profile">http://192.168.1.122/profile</a>
Method	GET
Attack	
Evidence	<code>&lt;form action="/profile" method="post" style="width: 90%; margin-right: auto; margin-left: auto;"&gt;</code>

Instances	3
Solution	<p>Phase: Architecture and Design</p> <p>Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.</p> <p>For example, use anti-CSRF packages such as the OWASP CSRFGuard.</p> <p>Phase: Implementation</p> <p>Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.</p> <p>Phase: Architecture and Design</p> <p>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).</p> <p>Note that this can be bypassed using XSS.</p> <p>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.</p> <p>Note that this can be bypassed using XSS.</p> <p>Use the ESAPI Session Management control.</p> <p>This control includes a component for CSRF.</p> <p>Do not use the GET method for any request that triggers a state change.</p> <p>Phase: Implementation</p> <p>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.</p>
Reference	<a href="http://projects.webappsec.org/Cross-Site-Request-Forgery">http://projects.webappsec.org/Cross-Site-Request-Forgery</a> <a href="http://cwe.mitre.org/data/definitions/352.html">http://cwe.mitre.org/data/definitions/352.html</a>
CWE Id	<a href="#">352</a>
WASC Id	9
Plugin Id	<a href="#">10202</a>

Medium	<b>CSP: Wildcard Directive</b>
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	<a href="http://192.168.1.122/profile">http://192.168.1.122/profile</a>
Method	GET
Attack	
Evidence	img-src 'self' assets/public/images/uploads/defaultAdmin.png; script-src 'self' 'unsafe-eval' https://code.getmdl.io http://ajax.googleapis.com
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
	<a href="http://www.w3.org/TR/CSP2/">http://www.w3.org/TR/CSP2/</a>

Reference	<a href="http://www.w3.org/TR/CSP/">http://www.w3.org/TR/CSP/</a> <a href="http://caniuse.com/#search=content+security+policy">http://caniuse.com/#search=content+security+policy</a> <a href="http://content-security-policy.com/">http://content-security-policy.com/</a> <a href="https://github.com/shapesecurity/salvation">https://github.com/shapesecurity/salvation</a> <a href="https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources">https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</a>
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	<a href="http://192.168.1.122/">http://192.168.1.122/</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/assets/public/images/uploads/%F0%9F%98%BC-">http://192.168.1.122/assets/public/images/uploads/%F0%9F%98%BC-</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAEEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAEEu</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAEEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAEEu</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAEEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAEEu</a>
Method	POST

Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30q&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30q&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB7z&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB7z&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5x&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5x&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoHgq&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoHgq&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	
Instances	11
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy">https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy</a> <a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a> <a href="http://www.w3.org/TR/CSP/">http://www.w3.org/TR/CSP/</a> <a href="http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html">http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html</a> <a href="http://www.html5rocks.com/en/tutorials/security/content-security-policy/">http://www.html5rocks.com/en/tutorials/security/content-security-policy/</a> <a href="http://caniuse.com/#feat=contentsecuritypolicy">http://caniuse.com/#feat=contentsecuritypolicy</a> <a href="http://content-security-policy.com/">http://content-security-policy.com/</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10038</a>

<b>Medium</b>	<b>Cross-Domain Misconfiguration</b>
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	<a href="http://192.168.1.122/">http://192.168.1.122/</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/api/Challenges/?name=Score%20Board">http://192.168.1.122/api/Challenges/?name=Score%20Board</a>
Method	GET

Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/api/Feedbacks/">http://192.168.1.122/api/Feedbacks/</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/api/Quantitys/">http://192.168.1.122/api/Quantitys/</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/assets/i18n/en.json">http://192.168.1.122/assets/i18n/en.json</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/assets/public/css/userProfile.css">http://192.168.1.122/assets/public/css/userProfile.css</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/font-mfizz.woff">http://192.168.1.122/font-mfizz.woff</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/main.js">http://192.168.1.122/main.js</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/MaterialIcons-Regular.woff2">http://192.168.1.122/MaterialIcons-Regular.woff2</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/polyfills.js">http://192.168.1.122/polyfills.js</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/profile">http://192.168.1.122/profile</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/admin/application-configuration">http://192.168.1.122/rest/admin/application-configuration</a>
Method	GET
Attack	

Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/admin/application-version">http://192.168.1.122/rest/admin/application-version</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/basket/1">http://192.168.1.122/rest/basket/1</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/captcha/">http://192.168.1.122/rest/captcha/</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/chatbot/status">http://192.168.1.122/rest/chatbot/status</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/deluxe-membership">http://192.168.1.122/rest/deluxe-membership</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/languages">http://192.168.1.122/rest/languages</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/memories/">http://192.168.1.122/rest/memories/</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/user/whoami">http://192.168.1.122/rest/user/whoami</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/runtime.js">http://192.168.1.122/runtime.js</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *



URL	<a href="http://192.168.1.122/styles.css">http://192.168.1.122/styles.css</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/vendor.js">http://192.168.1.122/vendor.js</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js">https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css">https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="https://code.getmdl.io/1.3.0/material.min.css">https://code.getmdl.io/1.3.0/material.min.css</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="https://code.getmdl.io/1.3.0/material.min.js">https://code.getmdl.io/1.3.0/material.min.js</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="https://fonts.googleapis.com/icon?family=Material+Icons">https://fonts.googleapis.com/icon?family=Material+Icons</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="https://fonts.gstatic.com/s/materialicons/v140/flUhRq6tzZclQEJ-Vdg-IuiaDsNc.woff2">https://fonts.gstatic.com/s/materialicons/v140/flUhRq6tzZclQEJ-Vdg-IuiaDsNc.woff2</a>
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>

Method	POST
Attack	
Evidence	Access-Control-Allow-Origin: *
Instances	33
Solution	<p>Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).</p> <p>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.</p>
Reference	<a href="https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy">https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy</a>
CWE Id	<a href="#">264</a>
WASC Id	14
Plugin Id	<a href="#">10098</a>

<b>Medium</b>	<b>Missing Anti-clickjacking Header</b>
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30q&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30q&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	POST
Attack	

Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB7z&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB7z&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5x&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5x&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoHgq&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoHgq&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	
Instances	9
Solution	<p>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.</p> <p>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.</p>
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a>
CWE Id	<a href="#">1021</a>
WASC Id	15
Plugin Id	<a href="#">10020</a>

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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3z&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3z&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	
Evidence	Jz_kYE12zy7zDQ0GAAAZ
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	
Evidence	Jz_kYE12zy7zDQ0GAAAZ
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfll&amp;sid=_NVV98f7Trw1txqQAEEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfll&amp;sid=_NVV98f7Trw1txqQAEEu</a>
Method	GET
Attack	
Evidence	_NVV98f7Trw1txqQAEEu

URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflvT&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflvT&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	
Evidence	_NVV98f7Trw1txqQAAEu
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	
Evidence	_NVV98f7Trw1txqQAAEu
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30u&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30u&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	GET
Attack	
Evidence	jxCa-O8njmkwo8XzAAJF
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko375&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko375&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	GET
Attack	
Evidence	jxCa-O8njmkwo8XzAAJF
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB83&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB83&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	GET
Attack	
Evidence	Mh1p2UPvw5x_2UCfAAJH
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoBEc&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoBEc&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	GET
Attack	
Evidence	Mh1p2UPvw5x_2UCfAAJH
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5z&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5z&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	GET
Attack	
Evidence	Mh1p2UPvw5x_2UCfAAJH
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	
Evidence	_NVV98f7Trw1txqQAAEu
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	GET
Attack	
Evidence	jxCa-O8njmkwo8XzAAJF
	<a href="http://192.168.1.122/socket.io/?">http://192.168.1.122/socket.io/?</a>

URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	
Evidence	Jz_kYE12zy7zDQ0GAAAZ
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	GET
Attack	
Evidence	Mh1p2UPvw5x_2UCfAAJH
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	
Evidence	Jz_kYE12zy7zDQ0GAAAZ
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	
Evidence	Jz_kYE12zy7zDQ0GAAAZ
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	_NVV98f7Trw1txqQAAEu
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	_NVV98f7Trw1txqQAAEu
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	_NVV98f7Trw1txqQAAEu
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30q&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30q&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	POST
Attack	
Evidence	jxCa-O8njmkwo8XzAAJF
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB7z&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB7z&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	Mh1p2UPvw5x_2UCfAAJH
	<a href="http://192.168.1.122/socket.io/?">http://192.168.1.122/socket.io/?</a>

URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5x&amp;sid=Mh1p2UPvw5x_2UCfAAJH">EIO=4&amp;transport=polling&amp;t=OWkoH5x&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	Mh1p2UPvw5x_2UCfAAJH
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoHgg&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoHgg&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	Mh1p2UPvw5x_2UCfAAJH
Instances	23
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	<a href="http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html">http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html</a>
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">3</a>

<b>Medium</b>	<b>Vulnerable JS Library</b>
Description	The identified library jquery, version 2.2.4 is vulnerable.
URL	<a href="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js">https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js</a>
Method	GET
Attack	
Evidence	/3.3.1/jquery.min.js
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js</a>
Method	GET
Attack	
Evidence	/2.2.4/jquery.min.js
Instances	2
Solution	Please upgrade to the latest version of jquery.
Reference	<a href="https://github.com/jquery/jquery/issues/2432">https://github.com/jquery/jquery/issues/2432</a> <a href="http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/">http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/</a> <a href="http://research.insecurelabs.org/jquery/test/">http://research.insecurelabs.org/jquery/test/</a> <a href="https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/">https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-2019-11358">https://nvd.nist.gov/vuln/detail/CVE-2019-11358</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-2015-9251">https://nvd.nist.gov/vuln/detail/CVE-2015-9251</a> <a href="https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b">https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b</a> <a href="https://bugs.jquery.com/ticket/11974">https://bugs.jquery.com/ticket/11974</a> <a href="https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/">https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/</a> <a href="https://github.com/jquery/jquery.com/issues/162">https://github.com/jquery/jquery.com/issues/162</a>
CWE Id	<a href="#">829</a>
WASC Id	
Plugin Id	<a href="#">10003</a>

<b>Medium</b>	<b>XSLT Injection</b>
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	<a href="http://192.168.1.122/api/Challenges/?name=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E">http://192.168.1.122/api/Challenges/?name=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E</a>

Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/rest/products/search?q=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E">http://192.168.1.122/rest/products/search?q=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E</a>
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkbRgi">http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkbRgi</a>
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkfiTI">http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkfiTI</a>
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxsl%3Avalue-of+select%3D%22system-property%28%27xsl%3Avendor%27%29%22%2F%3E&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	<xsl:value-of select="system-property('xsl:vendor')"/>

Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkbRgj</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkfitI">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkfitI</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkfrac&amp;sid=NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkfrac&amp;sid=NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;sid=NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;sid=NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E</a>



URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E">3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E</a>
Method	GET
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAEEu">http://192.168.1.122/socket.io/?EIO=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAEEu</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAEEu">http://192.168.1.122/socket.io/?EIO=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAEEu</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>

Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>

Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=%3Cxml%3Avalue-of+select%3D%22system-property%28%27xml%3Avendor%27%29%22%2F%3E</a>
Method	POST
Attack	<xml:value-of select="system-property('xml:vendor')"/>
Evidence	Apache
Instances	39
Solution	Sanitize and analyze every user input coming from any client-side.
Reference	<a href="https://www.contextis.com/blog/xslt-server-side-injection-attacks">https://www.contextis.com/blog/xslt-server-side-injection-attacks</a>
CWE Id	<a href="#">91</a>
WASC Id	23
Plugin Id	<a href="#">90017</a>

<b>Low</b>	<b>Cross-Domain JavaScript Source File Inclusion</b>
Description	The page includes one or more script files from a third-party domain.
URL	<a href="http://192.168.1.122/">http://192.168.1.122/</a>
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	<a href="http://192.168.1.122/">http://192.168.1.122/</a>
Method	GET
Attack	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	<a href="http://192.168.1.122/profile">http://192.168.1.122/profile</a>

Method	GET
Attack	
Evidence	<script src="//ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	<a href="http://192.168.1.122/profile">http://192.168.1.122/profile</a>
Method	GET
Attack	
Evidence	<script src="https://code.getmdl.io/1.3.0/material.min.js"></script>
Instances	4
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	<a href="#">829</a>
WASC Id	15
Plugin Id	<a href="#">10017</a>

<b>Low</b>	<b>Private IP Disclosure</b>
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	<a href="http://192.168.1.122/rest/admin/application-configuration">http://192.168.1.122/rest/admin/application-configuration</a>
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	<a href="https://tools.ietf.org/html/rfc1918">https://tools.ietf.org/html/rfc1918</a>
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">2</a>

<b>Low</b>	<b>Server Leaks Version Information via "Server" HTTP Response Header Field</b>
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	<a href="http://192.168.1.122/">http://192.168.1.122/</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/api/Challenges/?name=Score%20Board">http://192.168.1.122/api/Challenges/?name=Score%20Board</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/api/Feedbacks/">http://192.168.1.122/api/Feedbacks/</a>
Method	GET

Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/api/Quantitys/">http://192.168.1.122/api/Quantitys/</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/assets/i18n/en.json">http://192.168.1.122/assets/i18n/en.json</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/assets/public/css/userProfile.css">http://192.168.1.122/assets/public/css/userProfile.css</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/assets/public/images/uploads/%F0%9F%98%BC-">http://192.168.1.122/assets/public/images/uploads/%F0%9F%98%BC-</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/font-mfizz.woff">http://192.168.1.122/font-mfizz.woff</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/main.js">http://192.168.1.122/main.js</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/MaterialIcons-Regular.woff2">http://192.168.1.122/MaterialIcons-Regular.woff2</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/polyfills.js">http://192.168.1.122/polyfills.js</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/profile">http://192.168.1.122/profile</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/admin/application-configuration">http://192.168.1.122/rest/admin/application-configuration</a>
Method	GET
Attack	

Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/admin/application-version">http://192.168.1.122/rest/admin/application-version</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/basket/1">http://192.168.1.122/rest/basket/1</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/captcha/">http://192.168.1.122/rest/captcha/</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/chatbot/status">http://192.168.1.122/rest/chatbot/status</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/deluxe-membership">http://192.168.1.122/rest/deluxe-membership</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/languages">http://192.168.1.122/rest/languages</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/memories/">http://192.168.1.122/rest/memories/</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/user/whoami">http://192.168.1.122/rest/user/whoami</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/runtime.js">http://192.168.1.122/runtime.js</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)

URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3z&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3z&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfllo&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfllo&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTl">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTl</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflvT&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflvT&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko2hu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko2hu</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30u&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30u&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko375&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko375&amp;sid=jxCa-O8njmkwo8XzAAJF</a>

Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoA-i">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoA-i</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB83&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB83&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoBEc&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoBEc&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5z&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5z&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/styles.css">http://192.168.1.122/styles.css</a>
Method	GET
Attack	



Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/vendor.js">http://192.168.1.122/vendor.js</a>
Method	GET
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30q&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30q&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB7z&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB7z&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)

URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5x&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5x&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoHgg&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoHgg&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	Apache/2.4.52 (Ubuntu)
Instances	53
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	<a href="http://httpd.apache.org/docs/current/mod/core.html#servertokens">http://httpd.apache.org/docs/current/mod/core.html#servertokens</a> <a href="http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007">http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007</a> <a href="http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx">http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx</a> <a href="http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html">http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html</a>
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">10036</a>

<b>Low</b>	<b>Strict-Transport-Security Header Not Set</b>
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	<a href="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js">https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js</a>
Method	GET
Attack	
Evidence	
URL	<a href="https://fonts.gstatic.com/s/materialicons/v140/flUhRq6tzZclQEJ-Vdg-IuiaDsNc.woff2">https://fonts.gstatic.com/s/materialicons/v140/flUhRq6tzZclQEJ-Vdg-IuiaDsNc.woff2</a>
Method	GET
Attack	
Evidence	
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a> <a href="http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security">http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security</a> <a href="http://caniuse.com/stricttransportsecurity">http://caniuse.com/stricttransportsecurity</a> <a href="http://tools.ietf.org/html/rfc6797">http://tools.ietf.org/html/rfc6797</a>
CWE Id	<a href="#">319</a>
WASC Id	15
Plugin Id	<a href="#">10035</a>

<b>Low</b>	<b>Timestamp Disclosure - Unix</b>
Description	A timestamp was disclosed by the application/web server - Unix

URL	<a href="http://192.168.1.122/main.js">http://192.168.1.122/main.js</a>
Method	GET
Attack	
Evidence	1734944650
URL	<a href="http://192.168.1.122/rest/admin/application-configuration">http://192.168.1.122/rest/admin/application-configuration</a>
Method	GET
Attack	
Evidence	1969196030
URL	<a href="http://192.168.1.122/rest/admin/application-configuration">http://192.168.1.122/rest/admin/application-configuration</a>
Method	GET
Attack	
Evidence	1970691216
URL	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
Method	GET
Attack	
Evidence	1969196030
URL	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
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	<a href="http://projects.webappsec.org/w/page/13246936/Information%20Leakage">http://projects.webappsec.org/w/page/13246936/Information%20Leakage</a>
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">10096</a>

<b>Low</b>	<b>X-Content-Type-Options Header Missing</b>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3z&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3z&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	
Evidence	

URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfll&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfll&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflvT&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflvT&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko2hu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko2hu</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30u&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30u&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko375&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko375&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoA-i">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoA-i</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB83&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB83&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>

Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoBEc&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoBEc&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5z&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5z&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	GET
Attack	
Evidence	
URL	<a href="https://code.getmdl.io/1.3.0/material.min.css">https://code.getmdl.io/1.3.0/material.min.css</a>
Method	GET
Attack	
Evidence	
URL	<a href="https://code.getmdl.io/1.3.0/material.min.js">https://code.getmdl.io/1.3.0/material.min.js</a>
Method	GET
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST

Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30q&amp;sid=jxCa-O8njmkwo8XzAAJF">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWko30q&amp;sid=jxCa-O8njmkwo8XzAAJF</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB7z&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoB7z&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5x&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoH5x&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoHgq&amp;sid=Mh1p2UPvw5x_2UCfAAJH">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkoHgq&amp;sid=Mh1p2UPvw5x_2UCfAAJH</a>
Method	POST
Attack	
Evidence	
Instances	25
Solution	<p>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.</p> <p>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.</p>
Reference	<a href="http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx">http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10021</a>

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	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	
Evidence	password
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	

Evidence	password
Instances	2
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10111</a>

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	<a href="http://192.168.1.122/main.js">http://192.168.1.122/main.js</a>
Method	GET
Attack	
Evidence	query
URL	<a href="http://192.168.1.122/vendor.js">http://192.168.1.122/vendor.js</a>
Method	GET
Attack	
Evidence	query
URL	<a href="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js">https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js</a>
Method	GET
Attack	
Evidence	username
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js</a>
Method	GET
Attack	
Evidence	db
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js</a>
Method	GET
Attack	
Evidence	select
Instances	5
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">10027</a>

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	<a href="http://192.168.1.122/">http://192.168.1.122/</a>
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	<a href="#">10109</a>

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	<a href="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js">https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js</a>
Method	GET
Attack	
Evidence	Age: 394128
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css">https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css</a>
Method	GET
Attack	
Evidence	Age: 1079384
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css">https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css</a>
Method	GET
Attack	
Evidence	Age: 1080514
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css">https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css</a>
Method	GET
Attack	
Evidence	Age: 1082690
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js</a>
Method	GET
Attack	
Evidence	Age: 11441
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js</a>
Method	GET
Attack	
Evidence	Age: 12571
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js">https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js</a>
Method	GET
Attack	



Evidence	Age: 14747
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js</a>
Method	GET
Attack	
Evidence	Age: 140813
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js</a>
Method	GET
Attack	
Evidence	Age: 141943
URL	<a href="https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js">https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js</a>
Method	GET
Attack	
Evidence	Age: 144119
URL	<a href="https://code.getmdl.io/1.3.0/material.min.css">https://code.getmdl.io/1.3.0/material.min.css</a>
Method	GET
Attack	
Evidence	Age: 59371
URL	<a href="https://code.getmdl.io/1.3.0/material.min.js">https://code.getmdl.io/1.3.0/material.min.js</a>
Method	GET
Attack	
Evidence	Age: 525425
URL	<a href="https://fonts.gstatic.com/s/materialicons/v140/flUhRq6tzZclQEJ-Vdg-IuiaDsNc.woff2">https://fonts.gstatic.com/s/materialicons/v140/flUhRq6tzZclQEJ-Vdg-IuiaDsNc.woff2</a>
Method	GET
Attack	
Evidence	Age: 433357
Instances	13
Solution	<p>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:</p> <p>Cache-Control: no-cache, no-store, must-revalidate, private</p> <p>Pragma: no-cache</p> <p>Expires: 0</p> <p>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.</p>
Reference	<a href="https://tools.ietf.org/html/rfc7234">https://tools.ietf.org/html/rfc7234</a> <a href="https://tools.ietf.org/html/rfc7231">https://tools.ietf.org/html/rfc7231</a> <a href="http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html">http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html</a> (obsoleted by rfc7234)
CWE Id	
WASC Id	
Plugin Id	<a href="#">10050</a>

Informational	Session Management Response Identified
---------------	--

Description	The given response has been identified as containing a session management token. The 'Other
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	
Evidence	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9. eyJzdGF0dXMiOiJzdWNjZXRzIiwiaWF0IjE6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6I JrF3TXOGgVw8JOsiZg5RKumEK3SE1XyzDvO8YcPTZassrDULM3-OzFfifhsK2kYvdgQESKvh
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	
Evidence	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9. eyJzdGF0dXMiOiJzdWNjZXRzIiwiaWF0IjE6eyJpZCI6MSwidXNlcm5hbWUiOiJkZW1IMjAiLCJlb Tt6XmUwVE-S4nnuXuB8At_P-6WWJJQeCC3nUMj1mBvKrl6u1ABE0cbRCMhKSnU5DP8IREi
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	
Evidence	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9. eyJzdGF0dXMiOiJzdWNjZXRzIiwiaWF0IjE6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6I JrF3TXOGgVw8JOsiZg5RKumEK3SE1XyzDvO8YcPTZassrDULM3-OzFfifhsK2kYvdgQESKvh
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	
Evidence	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9. eyJzdGF0dXMiOiJzdWNjZXRzIiwiaWF0IjE6eyJpZCI6MSwidXNlcm5hbWUiOiJkZW1IMjAiLCJlb Tt6XmUwVE-S4nnuXuB8At_P-6WWJJQeCC3nUMj1mBvKrl6u1ABE0cbRCMhKSnU5DP8IREi
Instances	4
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10112</a>

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	<a href="http://192.168.1.122/api/Quantitys/">http://192.168.1.122/api/Quantitys/</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/api/Quantitys/">http://192.168.1.122/api/Quantitys/</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/api/Quantitys/">http://192.168.1.122/api/Quantitys/</a>
Method	GET

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

Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
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	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
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	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
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	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
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	<a href="http://192.168.1.122/assets">http://192.168.1.122/assets</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
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	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
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	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	

Evidence	
URL	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
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	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
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	<a href="http://192.168.1.122/assets/i18n">http://192.168.1.122/assets/i18n</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
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	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
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	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
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	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
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	<a href="http://192.168.1.122/assets/public">http://192.168.1.122/assets/public</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/assets/public/images">http://192.168.1.122/assets/public/images</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/assets/public/images">http://192.168.1.122/assets/public/images</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/assets/public/images">http://192.168.1.122/assets/public/images</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/assets/public/images">http://192.168.1.122/assets/public/images</a>

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



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

Evidence	
URL	<a href="http://192.168.1.122/rest/languages">http://192.168.1.122/rest/languages</a>
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	<a href="http://192.168.1.122/rest/languages">http://192.168.1.122/rest/languages</a>
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	<a href="http://192.168.1.122/rest/languages">http://192.168.1.122/rest/languages</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
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	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
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	<a href="http://192.168.1.122/rest/products/search?q=">http://192.168.1.122/rest/products/search?q=</a>
Method	GET

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

Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbRgj</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSAM&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflTI</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfITl">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfITl</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfITl">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfITl</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfITl">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfITl</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfITl">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfITl</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfITl">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfITl</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>



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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfrac&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	

URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=websocket&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
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	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
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	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
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	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
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	<a href="http://192.168.1.122/rest/user/login">http://192.168.1.122/rest/user/login</a>
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbS3t&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST

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

Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkbSyv&amp;sid=Jz_kYE12zy7zDQ0GAAAZ</a>
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkflli&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>

URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	

Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfraa&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
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	<a href="http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu">http://192.168.1.122/socket.io/?EIO=4&amp;transport=polling&amp;t=OWkfsVJ&amp;sid=_NVV98f7Trw1txqQAAEu</a>
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Instances	241
Solution	
Reference	<a href="https://owasp.org/wstg">https://owasp.org/wstg</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10104</a>