Active Scan ZAP Scanning Report

Sites: https://content-autofill.googleapis.com https://cdnjs.cloudflare.com http://localhost https://accounts.google.com

Generated on quarta, 24 mai. 2023 18:03:02

Summary of Alerts

Risk Level	Number of Alerts
Alto	0
Médio	4
Baixo	6
Informational	5

Alertas

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Médio	14
Cross-Domain Misconfiguration	Médio	17
Session ID in URL Rewrite	Médio	16
Vulnerable JS Library	Médio	1
Cross-Domain JavaScript Source File Inclusion	Baixo	2
Private IP Disclosure	Baixo	1
Server Leaks Version Information via "Server" HTTP Response Header Field	Baixo	36
Strict-Transport-Security Header Not Set	Baixo	3
Timestamp Disclosure - Unix	Baixo	5
X-Content-Type-Options Header Missing	Baixo	9
Information Disclosure - Suspicious Comments	Informational	4
Modern Web Application	Informational	1
Re-examine Cache-control Directives	Informational	3
Retrieved from Cache	Informational	3
User Agent Fuzzer	Informational	96

Alert Detail

Médio	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

URL	http://localhost/
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=websocket&sid=2-5FBl90I8w_pNoIAAiD
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=websocket&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=websocket&sid=VPX8e4aDhKtZ4qAZAAh_
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNi0&sid=VPX8e4aDhKtZ4qAZAAh_
Método	POST
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNR-&sid=VPX8e4aDhKtZ4qAZAAh_
Método	POST
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNwr&sid=cF2a6v9-nJLcU6pFAAiA
Método	POST
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNy5&sid=cF2a6v9-nJLcU6pFAAiA
Método	POST
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOeN&sid=EV5uIvC3E3hRAqGqAAiC
Método	POST
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOHz&sid=VlaeWDzlA8iwozlAAAiB
Método	POST

Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOIN&sid=VlaeWDzlA8iwozlAAAiB
Método	POST
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOta&sid=2-5FBl90I8w_pNoIAAiD
Método	POST
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOuD&sid=2-5FBl90I8w_pNoIAAiD
Método	POST
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP63&sid=5MH03bjZREF2A4SCAAiE
Método	POST
Atacar	
Evidence	
Instances	14
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Médio	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	http://localhost/
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/api/Challenges/?name=Score%20Board
Método	GET
Atacar	

Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/api/Quantitys/
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/assets/i18n/en.json
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/main.js
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/MaterialIcons-Regular.woff2
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/polyfills.js
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/rest/admin/application-version
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/rest/languages
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/rest/products/search?q=
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://localhost/runtime.js
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *

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

Médio	Session ID in URL Rewrite
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNS5&sid=VPX8e4aDhKtZ4qAZAAh_
Método	GET
Atacar	
Evidence	VPX8e4aDhKtZ4qAZAAh_
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNws&sid=cF2a6v9-nJLcU6pFAAiA
Método	GET
Atacar	

Evidence	cF2a6v9-nJLcU6pFAAiA
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	
Evidence	VlaeWDzlA8iwozlAAAiB
URL	http://localhost/socket.io/?EIO=4&transport=websocket&sid=2-5FBl90I8w_pNoIAAiD
Método	GET
Atacar	
Evidence	2-5FBl90I8w_pNoIAAiD
URL	http://localhost/socket.io/?EIO=4&transport=websocket&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	
Evidence	VlaeWDzlA8iwozlAAAiB
URL	http://localhost/socket.io/?EIO=4&transport=websocket&sid=VPX8e4aDhKtZ4qAZAAh_
Método	GET
Atacar	
Evidence	VPX8e4aDhKtZ4qAZAAh_
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNi0&sid=VPX8e4aDhKtZ4qAZAAh_
Método	POST
Atacar	
Evidence	VPX8e4aDhKtZ4qAZAAh_
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNR-&sid=VPX8e4aDhKtZ4qAZAAh_
Método	POST
Atacar	
Evidence	VPX8e4aDhKtZ4qAZAAh_
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNwr&sid=cF2a6v9-nJLcU6pFAAiA
Método	POST
Atacar	
Evidence	cF2a6v9-nJLcU6pFAAiA
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNy5&sid=cF2a6v9-nJLcU6pFAAiA
Método	POST
Atacar	
Evidence	cF2a6v9-nJLcU6pFAAiA
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOen&sid=EV5ulvC3E3hRAqGqAAiC
Método	POST
Atacar	
Evidence	EV5ulvC3E3hRAqGqAAiC
	http://localhost/socket.io/?

URL	EIO=4&transport=polling&t=OXEiOHz&sid=VlaeWDzlA8iwozlAAAiB
Método	POST
Atacar	
Evidence	VlaeWDzlA8iwozlAAAiB
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOIN&sid=VlaeWDzlA8iwozlAAAiB
Método	POST
Atacar	
Evidence	VlaeWDzlA8iwozlAAAiB
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOta&sid=2-5FBl90I8w_pNoIAAiD
Método	POST
Atacar	
Evidence	2-5FBl90I8w_pNoIAAiD
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOuD&sid=2-5FBl90I8w_pNoIAAiD
Método	POST
Atacar	
Evidence	2-5FBl90I8w_pNoIAAiD
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP63&sid=5MH03bjZREF2A4SCAAiE
Método	POST
Atacar	
Evidence	5MH03bjZREF2A4SCAAiE
Instances	16
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html
CWE Id	200
WASC Id	13
Plugin Id	3

Médio	**Vulnerable JS Library**
Description	The identified library jquery, version 2.2.4 is vulnerable.
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Método	GET
Atacar	
Evidence	/2.2.4/jquery.min.js
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	https://github.com/jquery/jquery/issues/2432 http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ http://research.insecurelabs.org/jquery/test/ https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://nvd.nist.gov/vuln/detail/CVE-2015-9251 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b

	https://bugs.jquery.com/ticket/11974 https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://github.com/jquery/jquery.com/issues/162
CWE Id	829
WASC Id	
Plugin Id	10003

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

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

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

Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/api/Challenges/?name=Score%20Board
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/api/Quantitys/
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/assets/i18n/en.json
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/main.js
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/MaterialIcons-Regular.woff2
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/polyfills.js
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/rest/admin/application-version
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/rest/languages
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/rest/products/search?q=
Método	GET
Atacar	

Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/runtime.js
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNMd
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNS5&sid=VPX8e4aDhKtZ4qAZAAh_
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNsM
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNws&sid=cF2a6v9-nJLcU6pFAAiA
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOe7
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOEe
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOqy
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET

Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=websocket&sid=2-5FBl90I8w_pNoIAAiD
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=websocket&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=websocket&sid=VPX8e4aDhKtZ4qAZAAh_
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/styles.css
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/vendor.js
Método	GET
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNi0&sid=VPX8e4aDhKtZ4qAZAAh_
Método	POST
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNR-&sid=VPX8e4aDhKtZ4qAZAAh_
Método	POST
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNwr&sid=cF2a6v9-nJLcU6pFAAiA
Método	POST
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNy5&sid=cF2a6v9-nJLcU6pFAAiA
Método	POST
Atacar	
Evidence	Apache/2.4.6 (CentOS)
	http://localhost/socket.io/?

URL	EIO=4&transport=polling&t=OXEiOen&sid=EV5uIvC3E3hRAqGqAAiC
Método	POST
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOHz&sid=VlaeWDzlA8iwozlAAAiB
Método	POST
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOIN&sid=VlaeWDzlA8iwozlAAAiB
Método	POST
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOta&sid=2-5FBl90I8w_pNoIAAiD
Método	POST
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOuD&sid=2-5FBl90I8w_pNoIAAiD
Método	POST
Atacar	
Evidence	Apache/2.4.6 (CentOS)
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP63&sid=5MH03bjZREF2A4SCAAiE
Método	POST
Atacar	
Evidence	Apache/2.4.6 (CentOS)
Instances	36
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10036

Baixo	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web serv with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IET
URL	https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTEzLjAuNTY3Mi4xMjcSEAr
Método	GET
Atacar	

Evidence	
URL	https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTEzLjAuNTY3Mi4xMjcSFwl
Método	GET
Atacar	
Evidence	
URL	https://content-autofill.googleapis.com/v1/pages /ChVDaHJvbWUvMTEzLjAuNTY3Mi4xMjcSSAm05qxeQf5lthIFDQbtu_8SBQ0G7bv_EgUNBu2 alt=proto
Método	GET
Atacar	
Evidence	
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Stri
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Baixo	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	http://localhost/main.js
Método	GET
Atacar	
Evidence	1734944650
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	
Evidence	1969196030
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	
Evidence	1970691216
URL	http://localhost/rest/products/search?q=
Método	GET
Atacar	
Evidence	1969196030
URL	http://localhost/rest/products/search?q=
Método	GET
Atacar	
Evidence	1970691216

Instances	5
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10096

Baixo	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNMd
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNS5&sid=VPX8e4aDhKtZ4qAZAAh_
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNsM
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiNws&sid=cF2a6v9-nJLcU6pFAAiA
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOe7
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOEe
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	
Evidence	

URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOqy
Método	GET
Atacar	
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	
Evidence	
Instances	9
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://localhost/main.js
Método	GET
Atacar	
Evidence	query
URL	http://localhost/vendor.js
Método	GET
Atacar	
Evidence	query
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Método	GET
Atacar	
Evidence	db
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Método	GET
Atacar	
Evidence	select
Instances	4
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200

WASC Id	13
Plugin Id	10027

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

Informational	Re-examine Cache-control Directives
Description	The cache-control header has not been set properly or is missing, allowing the browser and pro intended, however, the resources should be reviewed to ensure that no sensitive content will be
URL	https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTEzLjAuNTY3Mi4xMjcSEAr
Método	GET
Atacar	
Evidence	private,max-age=604800
URL	https://content-autofill.googleapis.com/v1/pages/ChVDaHJvbWUvMTEzLjAuNTY3Mi4xMjcSFwl
Método	GET
Atacar	
Evidence	private,max-age=604800
URL	https://content-autofill.googleapis.com/v1/pages /ChVDaHJvbWUvMTEzLjAuNTY3Mi4xMjcSSAm05qxeQf5lthIFDQbtu_8SBQ0G7bv_EgUNBu2 alt=proto
Método	GET
Atacar	
Evidence	private,max-age=604800
Instances	3
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, mus max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	Retrieved from Cache

Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Método	GET
Atacar	
Evidence	Age: 203860
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Método	GET
Atacar	
Evidence	Age: 64169
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Método	GET
Atacar	
Evidence	Age: 33316
Instances	3
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	
WASC Id	
Plugin Id	10050

Informational	**User Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence	
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://localhost/assets
Método	GET
Atacar	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://localhost/assets
Método	GET

Atacar	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://localhost/assets/i18n
Método	GET

Atacar	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://localhost/assets/i18n
Método	GET
Atacar	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://localhost/assets/public
Método	GET
Atacar	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0

Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://localhost/assets/public/images
Método	GET
Atacar	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET

Atacar	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://localhost/assets/public/images/products
Método	GET
Atacar	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://localhost/rest/admin/application-configuration

Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	

URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://localhost/rest/admin/application-configuration
Método	GET
Atacar	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiOH_&sid=VlaeWDzlA8iwozlAAAiB
Método	GET
Atacar	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r

Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://localhost/socket.io/?EIO=4&transport=polling&t=OXEiP5r
Método	GET
Atacar	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Instances	96
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104