Fuzz Attack ZAP Scanning Report

Sites: https://beacons.gcp.gvt2.com https://clientservices.googleapis.com https://update.googleapis.com https://optimizationguide-pa.googleapis.com https://cdnjs.cloudflare.com http://192.168.1.80:3000 https://accounts.google.com

Generated on segunda, 30 maio 2022 17:45:16

Summary of Alerts

Risk Level	Number of Alerts
Alto	2
Médio	6
Baixo	7
Informational	6

Alertas

Name	Risk Level	Number of Instances
Advanced SQL Injection - AND boolean-based blind - WHERE or HAVING clause	Alto	1
SQL Injection - SQLite	Alto	1
Content Security Policy (CSP) Header Not Set	Médio	25
Cross-Domain Misconfiguration	Médio	42
Missing Anti-clickjacking Header	Médio	11
Session ID in URL Rewrite	Médio	35
Source Code Disclosure - Perl	Médio	1
Vulnerable JS Library	Médio	1
Cross-Domain JavaScript Source File Inclusion	Baixo	26
Dangerous JS Functions	Baixo	3
Deprecated Feature Policy Header Set	Baixo	20
Permissions Policy Header Not Set	Baixo	14
Private IP Disclosure	Baixo	1
Timestamp Disclosure - Unix	Baixo	18
X-Content-Type-Options Header Missing	Baixo	37
Base64 Disclosure	Informational	38
Information Disclosure - Suspicious Comments	Informational	5
Non-Storable Content	Informational	15
Re-examine Cache-control Directives	Informational	2
Storable and Cacheable Content	Informational	56
Storable but Non-Cacheable Content	Informational	23

Alert Detail

Alto	Advanced SQL Injection - AND boolean-based blind - WHERE or HAVING clause
Description	A SQL injection may be possible using the attached payload
URL	http://192.168.1.80:3000/rest/products/search?q=%25%27+AND+1440%3D1154+AND+%27%25%27%3D%27
Método	GET
Atacar	%' AND 9202=9202 AND '%'='
Evidence	
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the privilege of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	90018

Alto	SQL Injection - SQLite
Description	SQL injection may be possible.
URL	http://192.168.1.80:3000/rest/products/search?q=%27%28
Método	GET
Atacar	'(
Evidence	SQLITE_ERROR
Instances	1
	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side.

Solution	If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

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://192.168.1.80:3000/
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaVC
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaxW
Método	GET
Atacar	
Evidence	

URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXbU5
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXc42
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXdCK
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXeWD
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXfkm
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXgz-
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXiD5
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXjSG
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXkhS
Método	GET
Atacar	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1652706182349&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Método	GET
Atacar	
Evidence	

URL	http://192.168.1.80:3000/rest/user/login
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsP-&sid=vF1yivK7Yvj84POxACEs
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHy-H&sid=2hvZZ-gaXNmW0kz1ACEy
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyNO&sid=k7VALFK5jQ2FZxiTABDz
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv6u&sid=qSsfM_sP9l1WUMj9AAGo
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGGm&sid=wi5FC6uCPXkqXwo_AAv3
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4G8&sid=lTNxkvxbZfF5e4fHAAyK
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXllj&sid=l9bgom4JHm3ZoaD8AAyZ
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVd0&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	
	http://192.168.1.80:3000/socket.io/?

URL	EIO=4&transport=polling&t=O4LXX2b&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/? EIO=4&transport=polling&t=O4LXXEl&sid=dJ0XOAeV5pDMGzziAAyX
Método	POST
Atacar	
Evidence	
Instances	25
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP /Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

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://192.168.1.80:3000/
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/103.js
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaVC
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaxW

Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXbU5
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXc42
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXdCK
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXeWD
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXfkm
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXgz-
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXiD5
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXjSG
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXkhS
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/api/Challenges/?name=Score%20Board
Método	GET

Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/api/Feedbacks/
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/api/Quantitys/
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/assets/i18n/en.json
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/font-mfizz.woff
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/main.js
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/MaterialIcons-Regular.woff2
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/polyfills.js
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/admin/application-configuration
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/admin/application-version
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/captcha/
Método	GET
Atacar	

Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/continue-code
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/languages
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/products/1/reviews
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/products/24/reviews
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/products/33/reviews
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/products/42/reviews
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/products/6/reviews
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/products/search?q=
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/rest/user/whoami
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/runtime.js
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *

URL	http://192.168.1.80:3000/styles.css
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/tutorial.js
Método	GET
Atacar	
Evidence	Access-Control-Allow-Origin: *
URL	http://192.168.1.80:3000/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: *
URL	http://192.168.1.80:3000/rest/user/login
Método	POST
Atacar	
Evidence	Access-Control-Allow-Origin: *
Instances	42
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	**Missing Anti-clickjacking Header**
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
	https://optimizationguide-pa.googleapis.com/downloads?

URL	name=1652706182349&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsP-&sid=vF1yivK7Yvj84POxACEs
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHy-H&sid=2hvZZ-gaXNmW0kz1ACEy
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyNO&sid=k7VALFK5jQ2FZxiTABDz
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv6u&sid=qSsfM_sP9l1WUMj9AAGo
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGGm&sid=wi5FC6uCPXkqXwo_AAv3
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4G8&sid=lTNxkvxbZfF5e4fHAAyK
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXllj&sid=l9bgom4JHm3ZoaD8AAyZ
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVd0&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	
	http://192.168.1.80:3000/socket.io/?

URL	EIO=4&transport=polling&t=O4LXX2b&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXEl&sid=dJ0XOAeV5pDMGzziAAyX
Método	POST
Atacar	
Evidence	
Instances	11
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

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://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsft&sid=vF1yivK7Yvj84POxACEs
Método	GET
Atacar	
Evidence	vF1yivK7Yvj84POxACEs
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsQB&sid=vF1yivK7Yvj84POxACEs
Método	GET
Atacar	
Evidence	vF1yivK7Yvj84POxACEs
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHy-M&sid=2hvZZ-gaXNmW0kz1ACEy
Método	GET
Atacar	
Evidence	2hvZZ-gaXNmW0kz1ACEy
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyNT&sid=k7VALFK5jQ2FZxiTABDz
Método	GET
Atacar	
Evidence	k7VALFK5jQ2FZxiTABDz
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyPz&sid=k7VALFK5jQ2FZxiTABDz

Método	GET
Atacar	
Evidence	k7VALFK5jQ2FZxiTABDz
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv6-&sid=qSsfM_sP9l1WUMj9AAGo
Método	GET
Atacar	
Evidence	qSsfM_sP9l1WUMj9AAGo
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPvEU&sid=qSsfM_sP9l1WUMj9AAGo
Método	GET
Atacar	
Evidence	qSsfM_sP9l1WUMj9AAGo
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGGt&sid=wi5FC6uCPXkqXwo_AAv3
Método	GET
Atacar	
Evidence	wi5FC6uCPXkqXwo_AAv3
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGIt&sid=wi5FC6uCPXkqXwo_AAv3
Método	GET
Atacar	
Evidence	wi5FC6uCPXkqXwo_AAv3
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4GD&sid=lTNxkvxbZfF5e4fHAAyK
Método	GET
Atacar	
Evidence	lTNxkvxbZfF5e4fHAAyK
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4Jz&sid=lTNxkvxbZfF5e4fHAAyK
Método	GET
Atacar	
Evidence	lTNxkvxbZfF5e4fHAAyK
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXllx&sid=l9bgom4JHm3ZoaD8AAyZ
Método	GET
Atacar	
Evidence	l9bgom4JHm3ZoaD8AAyZ
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXlq9&sid=l9bgom4JHm3ZoaD8AAyZ
Método	GET
Atacar	
Evidence	l9bgom4JHm3ZoaD8AAyZ
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVd7&sid=HUX7BubfMXm3f-7sAAyV

Método	GET
Atacar	
Evidence	HUX7BubfMXm3f-7sAAyV
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVhd&sid=HUX7BubfMXm3f-7sAAyV
Método	GET
Atacar	
Evidence	HUX7BubfMXm3f-7sAAyV
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXEr&sid=dJ0XOAeV5pDMGzziAAyX
Método	GET
Atacar	
Evidence	dJ0XOAeV5pDMGzziAAyX
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXHb&sid=dJ0XOAeV5pDMGzziAAyX
Método	GET
Atacar	
Evidence	dJ0XOAeV5pDMGzziAAyX
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=2hvZZ-gaXNmW0kz1ACEy
Método	GET
Atacar	
Evidence	2hvZZ-gaXNmW0kz1ACEy
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=dJ0XOAeV5pDMGzziAAyX
Método	GET
Atacar	
Evidence	dJ0XOAeV5pDMGzziAAyX
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=k7VALFK5jQ2FZxiTABDz
Método	GET
Atacar	
Evidence	k7VALFK5jQ2FZxiTABDz
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=l9bgom4JHm3ZoaD8AAyZ
Método	GET
Atacar	
Evidence	l9bgom4JHm3ZoaD8AAyZ
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=lTNxkvxbZfF5e4fHAAyK
Método	GET
Atacar	
Evidence	lTNxkvxbZfF5e4fHAAyK
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=qSsfM_sP9l1WUMj9AAGo

Método	GET
Atacar	
Evidence	qSsfM_sP9l1WUMj9AAGo
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=vF1yivK7Yvj84POxACEs
Método	GET
Atacar	
Evidence	vF1yivK7Yvj84POxACEs
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=wi5FC6uCPXkqXwo_AAv3
Método	GET
Atacar	
Evidence	wi5FC6uCPXkqXwo_AAv3
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsP-&sid=vF1yivK7Yvj84POxACEs
Método	POST
Atacar	
Evidence	vF1yivK7Yvj84POxACEs
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHy-H&sid=2hvZZ-gaXNmW0kz1ACEy
Método	POST
Atacar	
Evidence	2hvZZ-gaXNmW0kz1ACEy
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyNO&sid=k7VALFK5jQ2FZxiTABDz
Método	POST
Atacar	
Evidence	k7VALFK5jQ2FZxiTABDz
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv6u&sid=qSsfM_sP9l1WUMj9AAGo
Método	POST
Atacar	
Evidence	qSsfM_sP9l1WUMj9AAGo
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGGm&sid=wi5FC6uCPXkqXwo_AAv3
Método	POST
Atacar	
Evidence	wi5FC6uCPXkqXwo_AAv3
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4G8&sid=lTNxkvxbZfF5e4fHAAyK
Método	POST
Atacar	
Evidence	lTNxkvxbZfF5e4fHAAyK
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXllj&sid=l9bgom4JHm3ZoaD8AAyZ

Método	POST
Atacar	
Evidence	l9bgom4JHm3ZoaD8AAyZ
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVd0&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	HUX7BubfMXm3f-7sAAyV
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXX2b&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	HUX7BubfMXm3f-7sAAyV
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXEl&sid=dJ0XOAeV5pDMGzziAAyX
Método	POST
Atacar	
Evidence	dJ0XOAeV5pDMGzziAAyX
Instances	35
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	**Source Code Disclosure - Perl**
Description	Application Source Code was disclosed by the web server - Perl
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1652706182349&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Método	GET
Atacar	
Evidence	$#rx2m
Instances	1
Solution	Ensure that application Source Code is not available with alternative extensions, and ensure that source code is not present within other files or data deployed to the web server, or served by the web server.
Reference	http://blogs.wsj.com/cio/2013/10/08/adobe-source-code-leak-is-bad-news-for-u-s-government/
CWE Id	540
WASC Id	13
Plugin Id	10099

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/
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://192.168.1.80:3000/
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaVC
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaVC
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>

URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaxW
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaxW
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXbU5
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXbU5
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXc42
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXc42
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXdCK
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXdCK
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXeWD
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXeWD
Método	GET

Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXfkm
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXfkm
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXgz-
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXgz-
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXiD5
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXiD5
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXjSG
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXjSG
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXkhS
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js"></script>

URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXkhS
Método	GET
Atacar	
Evidence	<script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js"></script>
Instances	26
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	**Dangerous JS Functions**
Description	A dangerous JS function seems to be in use that would leave the site vulnerable.
URL	http://192.168.1.80:3000/main.js
Método	GET
Atacar	
Evidence	bypassSecurityTrustHtml
URL	http://192.168.1.80:3000/vendor.js
Método	GET
Atacar	
Evidence	bypassSecurityTrustHtml
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Método	GET
Atacar	
Evidence	eval
Instances	3
Solution	See the references for security advice on the use of these functions.
Reference	https://angular.io/guide/security
CWE Id	749
WASC Id	
Plugin Id	10110

Baixo	**Deprecated Feature Policy Header Set**
Description	The header has now been renamed to Permissions-Policy.
URL	http://192.168.1.80:3000/
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/103.js
Método	GET
Atacar	
Evidence	Feature-Policy

URL	http://192.168.1.80:3000/admin
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaVC
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaxW
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXbU5
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXc42
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXdCK
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXeWD
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXfkm
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXgz-
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXiD5
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXjSG

Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXkhS
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/main.js
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/polyfills.js
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/runtime.js
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/tutorial.js
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/vendor.js
Método	GET
Atacar	
Evidence	Feature-Policy
URL	http://192.168.1.80:3000/rest/user/login
Método	POST
Atacar	
Evidence	Feature-Policy
Instances	20
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header instead of the Feature-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy
CWE Id	16
WASC Id	15
Plugin Id	10063

Baixo	**Permissions Policy Header Not Set**
Description	Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that

	allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Método	GET
Atacar	
Evidence	
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Método	GET
Atacar	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1652706182349&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsP-&sid=vF1yivK7Yvj84POxACEs
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHy-H&sid=2hvZZ-gaXNmW0kz1ACEy
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyNO&sid=k7VALFK5jQ2FZxiTABDz
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv6u&sid=qSsfM_sP9l1WUMj9AAGo
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGGm&sid=wi5FC6uCPXkqXwo_AAv3
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4G8&sid=lTNxkvxbZfF5e4fHAAyK
Método	POST
Atacar	
Evidence	

URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXllj&sid=l9bgom4JHm3ZoaD8AAyZ
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVd0&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXX2b&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXEl&sid=dJ0XOAeV5pDMGzziAAyX
Método	POST
Atacar	
Evidence	
URL	https://beacons.gcp.gvt2.com/domainreliability/upload
Método	POST
Atacar	
Evidence	
Instances	14
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy https://developers.google.com/web/updates/2018/06/feature-policy https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	693
WASC Id	15
Plugin Id	10063

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://192.168.1.80:3000/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	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	http://192.168.1.80:3000/main.js
Método	GET
Atacar	
Evidence	1734944650
URL	http://192.168.1.80:3000/main.js
Método	GET
Atacar	
Evidence	384948954
URL	http://192.168.1.80:3000/main.js
Método	GET
Atacar	
Evidence	435235279
URL	http://192.168.1.80:3000/rest/admin/application-configuration
Método	GET
Atacar	
Evidence	1969196030
URL	http://192.168.1.80:3000/rest/admin/application-configuration
Método	GET
Atacar	
Evidence	1970691216
URL	http://192.168.1.80:3000/rest/admin/application-configuration
Método	GET
Atacar	
Evidence	771984076
URL	http://192.168.1.80:3000/rest/products/search?q=
Método	GET
Atacar	
Evidence	1969196030
URL	http://192.168.1.80:3000/rest/products/search?q=
Método	GET
Atacar	
Evidence	1970691216
URL	http://192.168.1.80:3000/styles.css
Método	GET
Atacar	

Evidence	00000005
URL	http://192.168.1.80:3000/styles.css
Método	GET
Atacar	
Evidence	00000024
URL	http://192.168.1.80:3000/styles.css
Método	GET
Atacar	
Evidence	00000042
URL	http://192.168.1.80:3000/styles.css
Método	GET
Atacar	
Evidence	00000061
URL	http://192.168.1.80:3000/tutorial.js
Método	GET
Atacar	
Evidence	771984076
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Método	GET
Atacar	
Evidence	16777216
URL	https://update.googleapis.com/service/update2/json?cup2key=12:GVpR_h7eBH8BF4Yb4FsikZoYLwDuRgPtyiZ0LRTwj5A&cup2hreq=8d90ae05099844480b9ec8
Método	POST
Atacar	
Evidence	1652906823
URL	https://update.googleapis.com/service/update2/json?cup2key=12:GVpR_h7eBH8BF4Yb4FsikZoYLwDuRgPtyiZ0LRTwj5A&cup2hreq=8d90ae05099844480b9ec8
Método	POST
Atacar	
Evidence	20220505
URL	https://update.googleapis.com/service/update2/json?cup2key=12:z6A9eyE_kpCCbdpYIZcC5bbpRuabfuCmAfwysNK4A0Q&cup2hreq=7156d2ba94e1a2347a5f1
Método	POST
Atacar	
Evidence	1652906823
URL	https://update.googleapis.com/service/update2/json?cup2key=12:z6A9eyE_kpCCbdpYIZcC5bbpRuabfuCmAfwysNK4A0Q&cup2hreq=7156d2ba94e1a2347a5f1
Método	POST
Atacar	
Evidence	20220505
Instances	18
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregat

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://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsDp
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsft&sid=vF1yivK7Yvj84POxACEs
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsQB&sid=vF1yivK7Yvj84POxACEs
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHy-M&sid=2hvZZ-gaXNmW0kz1ACEy
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHywV
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyHx
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyNT&sid=k7VALFK5jQ2FZxiTABDz
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyPz&sid=k7VALFK5jQ2FZxiTABDz

Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv3O
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv6-&sid=qSsfM_sP9l1WUMj9AAGo
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPvEU&sid=qSsfM_sP9l1WUMj9AAGo
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVG6x
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGGt&sid=wi5FC6uCPXkqXwo_AAv3
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGIt&sid=wi5FC6uCPXkqXwo_AAv3
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4A6
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4GD&sid=lTNxkvxbZfF5e4fHAAyK
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4Jz&sid=lTNxkvxbZfF5e4fHAAyK
Método	GET
Atacar	

Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXlfS
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXllx&sid=l9bgom4JHm3ZoaD8AAyZ
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXlq9&sid=l9bgom4JHm3ZoaD8AAyZ
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVd7&sid=HUX7BubfMXm3f-7sAAyV
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVhd&sid=HUX7BubfMXm3f-7sAAyV
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVYo
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXAL
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXEr&sid=dJ0XOAeV5pDMGzziAAyX
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXHb&sid=dJ0XOAeV5pDMGzziAAyX
Método	GET
Atacar	
Evidence	
	https://optimizationguide-pa.googleapis.com/downloads?

URL	name=1652706182349&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsP-&sid=vF1yivK7Yvj84POxACEs
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHy-H&sid=2hvZZ-gaXNmW0kz1ACEy
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyNO&sid=k7VALFK5jQ2FZxiTABDz
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv6u&sid=qSsfM_sP9l1WUMj9AAGo
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGGm&sid=wi5FC6uCPXkqXwo_AAv3
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4G8&sid=lTNxkvxbZfF5e4fHAAyK
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXllj&sid=l9bgom4JHm3ZoaD8AAyZ
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVd0&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	
	http://192.168.1.80:3000/socket.io/?

URL	EIO=4&transport=polling&t=O4LXX2b&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXEl&sid=dJ0XOAeV5pDMGzziAAyX
Método	POST
Atacar	
Evidence	
Instances	37
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	**Base64 Disclosure**
Description	Base64 encoded data was disclosed by the application/web server. Note: in the interests of perf /developer(s).
URL	http://192.168.1.80:3000/api/Challenges/?name=Score%20Board
Método	GET
Atacar	
Evidence	270-oF8UL2LpXfd471G1zDdQho6+PYw
URL	http://192.168.1.80:3000/api/Challenges/?name=Score%20Board
Método	GET
Atacar	
Evidence	270-wuNeKg7DdoJ5kqAfGlV1qYaFngI
URL	http://192.168.1.80:3000/api/Feedbacks/
Método	GET
Atacar	
Evidence	59e-Zj0bH8lN6+GTuOeGXE+GUpvI9Pg
URL	http://192.168.1.80:3000/api/Quantitys/
Método	GET
Atacar	
Evidence	1767-+IoqtIxLfTWo0sHtYN3RjZ0N4W8
URL	http://192.168.1.80:3000/api/Quantitys/
Método	GET
Atacar	
Evidence	1767-/Fuz2BXkI/Hs7vlAOkql6UY/0To

URL	http://192.168.1.80:3000/main.js
Método	GET
Atacar	
Evidence	com/forms/d/e/1FAIpQLSdaNEuz0dzFA2sexCa0AJ4QOb2OYdEL04eQOLFD2Y4T-BW6ag/viev
URL	http://192.168.1.80:3000/rest/admin/application-configuration
Método	GET
Atacar	
Evidence	4960-UblYT53fkD34usU3X+ie//t9sL0
URL	http://192.168.1.80:3000/rest/admin/application-version
Método	GET
Atacar	
Evidence	14-2RV/f91Hh4CfWUoOYAGBlgRuO80
URL	http://192.168.1.80:3000/rest/captcha/
Método	GET
Atacar	
Evidence	32-yBf3TSqiwPsCdKV5ptz6VMkxccM
URL	http://192.168.1.80:3000/rest/continue-code
Método	GET
Atacar	
Evidence	4f-M1P/NQ9a4ULA1qLqGf5OaO9bW6k
URL	http://192.168.1.80:3000/rest/languages
Método	GET
Atacar	
Evidence	11ad-TJkT3i/P3LSnNL8jWkn9DoCXGvE
URL	http://192.168.1.80:3000/rest/products/1/reviews
Método	GET
Atacar	
Evidence	ac-ME514Rrm1IXQlnDjFHLZtlBcLqU
URL	http://192.168.1.80:3000/rest/products/24/reviews
Método	GET
Atacar	
Evidence	1e-JkPcI+pGj7BBTxOuZTVVIm91zaY
URL	http://192.168.1.80:3000/rest/products/33/reviews
Método	GET
Atacar	
Evidence	1e-JkPcI+pGj7BBTxOuZTVVIm91zaY
URL	http://192.168.1.80:3000/rest/products/42/reviews
Método	GET
Atacar	
Evidence	19d-3X2HjG0fNiHdt/HSkwvc3OB+JVU
URL	http://192.168.1.80:3000/rest/products/6/reviews

Método	GET
Atacar	
Evidence	aa-gVpSGvx7URQeqShKTEEYP0yzbS0
URL	http://192.168.1.80:3000/rest/products/search?q=
Método	GET
Atacar	
Evidence	325f-OiJBFFIvvcRBikbrUJnuTa5Wsa0
URL	http://192.168.1.80:3000/rest/products/search?q=
Método	GET
Atacar	
Evidence	325f-in4AoE4qq1hEn7O9E/2ZIw9g81M
URL	http://192.168.1.80:3000/vendor.js
Método	GET
Atacar	
Evidence	0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Método	GET
Atacar	
Evidence	EI6MsSjWdGNNMUJZY9PJWWPAQh7n0g0wYgdOrOayXjZJs78FTGuppEbilOd
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Método	GET
Atacar	
Evidence	2BBfSmZO37YcaXSg5u8DR5umNJBG3wFbQf
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Método	GET
Atacar	
Evidence	2F1PIyxAJQEjwfRFlu9twNtqL0bsnr7X
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Método	GET
Atacar	
Evidence	2FOuClm4THVJsTeygbmkA0cI0fT6nLiOJqqL89Q4vr5q9rwcBgn9CeJ2CJfDh3onmmVpe4EEYc
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Método	GET
Atacar	
Evidence	2FlGENA0I1V7CT1Sr9zhboTp2CMCFTWQHXUHAAbiTDFhsS23Ih9AzLbKI8snpo77
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Método	GET
Atacar	
Evidence	NO3B350aYY33a9awwqQWq5uzKzsp9ovdvgPDKCbN4aTN6tq2Mkqz
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Método	GET

Atacar	
Evidence	ONwLLMhoYJd4Xjbe9ttefH6egn3OVVkyxomkCz0u2jxWx6ymIdrFtEJg2sPqoakZtvaggveG4LGk
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Método	GET
Atacar	
Evidence	fzXwti8EefIePuslzdZjaUNoMQaGeegvlGIK4VuPbiYxfzLGhuE4BX1gtwqBlMHdh1a
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Método	GET
Atacar	
Evidence	2B0j7SBalutklBrW0Bmq31bLTxSAb91fIxS5ll5r4WURGN0G
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Método	GET
Atacar	
Evidence	F8CJ35o2KwZuRPrqA6hBwD2cgiK0Nd6
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Método	GET
Atacar	
Evidence	2BjrQTfeVA1UDklrmC7wM167V4IgMaZ5798CLpF9mh
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Método	GET
Atacar	
Evidence	2F5MqotFRzsr20Wn7fbFNz2157n3eC60lMYPnU
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1652706182349&target=OPTIM
Método	GET
Atacar	
Evidence	ADPycdtNjJwjBw76xQceOaPyha3L5lwgbL_Efk1XmMyvQ9D-RW_k9T3xN2rFtp84y6xqwPjZE2h
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1652706182349&target=OPTIM
Método	GET
Atacar	
Evidence	ADPycdtWp5kST9uIPe46er5FFBuDIQEL_FlIATbV4PyZUt54uqCMapdcGuw94fVC2LkwkLQTIS
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1652706182349&target=OPTIM
Método	GET
Atacar	
Evidence	ADPycdtXLYnD7hqH678PX1S5lFfStKOlOcaVgb7MwCSLBz_t9mX6oUwFP_IU-pFpXHoxGr7ac
URL	http://192.168.1.80:3000/rest/user/login
Método	POST
Atacar	
Evidence	1a-ARJvVK+smzAF3QQve2mDSG+3Eus
URL	https://beacons.gcp.gvt2.com/domainreliability/upload
Método	POST
Atacar	

Evidence	goog/upload/1 /AHDprHrfFq6G0tIFIm4Ej1TThpWABvG_5G8VR95ew91tI511anKe7WqJkmwrQdceDn4aph7Bv WAncz9UKA0_NPJrLmWOhW9xO8bwxBK1z9t9CT7urACaZ
URL	https://update.googleapis.com/service/update2/json?cup2key=12:GVpR_h7eBH8BF4Yb4FsikZ
Método	POST
Atacar	
Evidence	com/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvYjFkQUFWdmlaXy12MHFUTG
URL	https://update.googleapis.com/service/update2/json?cup2key=12:z6A9eyE_kpCCbdpYIZcC5bb
Método	POST
Atacar	
Evidence	com/chromewebstore/L2Nocm9tZV9leHRlbnNpb24vYmxvYnMvYjFkQUFWdmlaXy12MHFUTG
Instances	38
Solution	Manually confirm that the Base64 data does not leak sensitive information, and that the data ca
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10094

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://192.168.1.80:3000/main.js
Método	GET
Atacar	
Evidence	query
URL	http://192.168.1.80:3000/tutorial.js
Método	GET
Atacar	
Evidence	query
URL	http://192.168.1.80:3000/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	5
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	Non-Storable Content
Description	The response contents are not storable by caching components such as proxy servers. If the re specific information, it may benefit from being stored and cached, to improve performance.
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=2hvZZ-gaXNmW0kz1AC
Método	GET
Atacar	
Evidence	101
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=dJ0XOAeV5pDMGzziAA
Método	GET
Atacar	
Evidence	101
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=k7VALFK5jQ2FZxiTABD
Método	GET
Atacar	
Evidence	101
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=l9bgom4JHm3ZoaD8AA
Método	GET
Atacar	
Evidence	101
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=lTNxkvxbZfF5e4fHAAyK
Método	GET
Atacar	
Evidence	101
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=qSsfM_sP9l1WUMj9AAC
Método	GET
Atacar	
Evidence	101
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=vF1yivK7Yvj84POxACEs
Método	GET
Atacar	
Evidence	101
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=websocket&sid=wi5FC6uCPXkqXwo_AA
Método	GET
Atacar	
Evidence	101
URL	http://192.168.1.80:3000/rest/user/login
Método	POST

Atacar	
Evidence	401
URL	https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard
Método	POST
Atacar	
Evidence	no-store
URL	https://clientservices.googleapis.com/uma/v2
Método	POST
Atacar	
Evidence	private
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBOti4mM-6x9WDnZIjIe
Método	POST
Atacar	
Evidence	private
URL	https://update.googleapis.com/service/update2/json
Método	POST
Atacar	
Evidence	no-store
URL	https://update.googleapis.com/service/update2/json?cup2key=12:GVpR_h7eBH8BF4Yb4FsikZoYLwDuRgPtyiZ0LRTwj5A&cup2hreq=8d90ae05099844480b9ec8
Método	POST
Atacar	
Evidence	no-store
URL	https://update.googleapis.com/service/update2/json?cup2key=12:z6A9eyE_kpCCbdpYIZcC5bbpRuabfuCmAfwysNK4A0Q&cup2hreq=7156d2ba94e1a2347a5f11
Método	POST
Atacar	
Evidence	no-store
Instances	15
Solution	The content may be marked as storable by ensuring that the following conditions are satisfied: The request method must be understood by the cache and defined as being cacheable ("GET", cacheable) The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, o The "no-store" cache directive must not appear in the request or response header fields For caching by "shared" caches such as "proxy" caches, the "private" response directive must n For caching by "shared" caches such as "proxy" caches, the "Authorization" header field must n explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control res In addition to the conditions above, at least one of the following conditions must also be satisfied It must contain an "Expires" header field It must contain a "max-age" response directive For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive

	It must contain a "Cache Control Extension" that allows it to be cached It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301
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	524
WASC Id	13
Plugin Id	10049

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1652706182349&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Método	GET
Atacar	
Evidence	public, max-age=86400
URL	https://clientservices.googleapis.com/uma/v2
Método	POST
Atacar	
Evidence	private
Instances	2
Solution	Whenever possible ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**Storable and Cacheable Content**
Description	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. 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 "shared" 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	http://192.168.1.80:3000/api/Challenges/?name=Score%20Board
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/api/Feedbacks/

Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/api/Quantitys/
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/admin/application-configuration
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/admin/application-version
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/captcha/
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/continue-code
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/languages
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/products/1/reviews
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/products/24/reviews
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/products/33/reviews
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/products/42/reviews
Método	GET

Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/products/6/reviews
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/products/search?q=
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/rest/user/whoami
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsDp
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsft&sid=vF1yivK7Yvj84POxACEs
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsQB&sid=vF1yivK7Yvj84POxACEs
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHy-M&sid=2hvZZ-gaXNmW0kz1ACEy
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHywV
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyHx
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyNT&sid=k7VALFK5jQ2FZxiTABDz

Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyPz&sid=k7VALFK5jQ2FZxiTABDz
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv3O
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv6-&sid=qSsfM_sP9l1WUMj9AAGo
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPvEU&sid=qSsfM_sP9l1WUMj9AAGo
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVG6x
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGGt&sid=wi5FC6uCPXkqXwo_AAv3
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGIt&sid=wi5FC6uCPXkqXwo_AAv3
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4A6
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4GD&sid=lTNxkvxbZfF5e4fHAAyK
Método	GET
Atacar	

Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4Jz&sid=lTNxkvxbZfF5e4fHAAyK
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXlfS
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXllx&sid=l9bgom4JHm3ZoaD8AAyZ
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXlq9&sid=l9bgom4JHm3ZoaD8AAyZ
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVd7&sid=HUX7BubfMXm3f-7sAAyV
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVhd&sid=HUX7BubfMXm3f-7sAAyV
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVYo
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXAL
Método	GET
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXEr&sid=dJ0XOAeV5pDMGzziAAyX
Método	GET
Atacar	
Evidence	

URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXHb&sid=dJ0XOAeV5pDMGzziAAyX
Método	GET
Atacar	
Evidence	
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css
Método	GET
Atacar	
Evidence	max-age=30672000
URL	https://cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js
Método	GET
Atacar	
Evidence	max-age=30672000
URL	https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Método	GET
Atacar	
Evidence	max-age=30672000
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1652706182349&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Método	GET
Atacar	
Evidence	max-age=86400
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHsP-&sid=vF1yivK7Yvj84POxACEs
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LHy-H&sid=2hvZZ-gaXNmW0kz1ACEy
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LkyNO&sid=k7VALFK5jQ2FZxiTABDz
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LPv6u&sid=qSsfM_sP9l1WUMj9AAGo
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LVGGm&sid=wi5FC6uCPXkqXwo_AAv3

Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LW4G8&sid=lTNxkvxbZfF5e4fHAAyK
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXllj&sid=l9bgom4JHm3ZoaD8AAyZ
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXVd0&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXX2b&sid=HUX7BubfMXm3f-7sAAyV
Método	POST
Atacar	
Evidence	
URL	http://192.168.1.80:3000/socket.io/?EIO=4&transport=polling&t=O4LXXEl&sid=dJ0XOAeV5pDMGzziAAyX
Método	POST
Atacar	
Evidence	
URL	https://beacons.gcp.gvt2.com/domainreliability/upload
Método	POST
Atacar	
Evidence	
Instances	56
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	524
WASC Id	13
Plugin Id	10049

Informational	**Storable but Non-Cacheable Content**
Description	The response contents are storable by caching components such as proxy servers, but will not be retrieved directly from the cache, without validating the request upstream, in response to similar requests from other users.
URL	http://192.168.1.80:3000/
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/103.js
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaVC
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXaxW
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXbU5
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXc42
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXdCK
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXeWD
Método	GET

Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXfkm
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXgz-
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXiD5
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXjSG
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/admin/socket.io/?EIO=4&transport=polling&t=O4LXkhS
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/assets/i18n/en.json
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/font-mfizz.woff
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/main.js
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/MaterialIcons-Regular.woff2
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/polyfills.js
Método	GET
Atacar	

Evidence	max-age=0
URL	http://192.168.1.80:3000/runtime.js
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/styles.css
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/tutorial.js
Método	GET
Atacar	
Evidence	max-age=0
URL	http://192.168.1.80:3000/vendor.js
Método	GET
Atacar	
Evidence	max-age=0
Instances	23
Solution	
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	524
WASC Id	13
Plugin Id	10049