ZAP Scanning Report

ZAP report for Guns for Hire.

Sites: https://api.twitch-radio.xyz https://twitch-radio.xyz

Generated on Sat, 18 Dec 2021 19:49:51

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	4
Informational	1

Alerts

Name	Risk Level	Number of Instances
CSP: Wildcard Directive	Medium	10
Cross-Domain Misconfiguration	Medium	8
X-Frame-Options Header Not Set	Medium	6
Incomplete or No Cache-control Header Set	Low	12
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	24
Timestamp Disclosure - Unix	Low	22
X-Content-Type-Options Header Missing	Low	13
Information Disclosure - Suspicious Comments	Informational	30

Alert Detail

Medium	CSP: Wildcard Directive
Description	The following directives either allow wildcard sources (or ancestors), are not defined, or are ove frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to d
URL	https://twitch-radio.xyz/home
Method	GET
Attack	
Evidence	default-src 'none'
URL	https://twitch-radio.xyz/home/
Method	GET
Attack	
Evidence	default-src 'none'

URL	https://twitch-radio.xyz/home/? code=AQBMWG6kJBRfJ6tBlfclUb3te_hJEBn1qd0uCyzIHmLAjPtMiXx12GSJdkLcFwWC2ug5m cNN97dNXacdc0FEartQxfTuXyZNgd5wyfZhjvFIzbAPITYQBay16HwmmIJ8zyard-jmfxp6d746V
Method	GET
Attack	
Evidence	default-src 'none'
URL	https://twitch-radio.xyz/profile
Method	GET
Attack	
Evidence	default-src 'none'
URL	https://twitch-radio.xyz/profile/
Method	GET
Attack	
Evidence	default-src 'none'
URL	https://twitch-radio.xyz/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'none'
URL	https://twitch-radio.xyz/sockjs-node
Method	GET
Attack	
Evidence	default-src 'none'
URL	https://twitch-radio.xyz/static
Method	GET
Attack	
Evidence	default-src 'none'
URL	https://twitch-radio.xyz/static/js
Method	GET
Attack	
Evidence	default-src 'none'
URL	https://twitch-radio.xyz/static/media
Method	GET
Attack	
Evidence	default-src 'none'
Instances	10
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet
CWE Id	693
WASC Id	15

Plugin Id	10055

Medium	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://api.twitch-radio.xyz/auth/me
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://api.twitch-radio.xyz/auth/token/verify
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://api.twitch-radio.xyz/twitch/findAllStreamers
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://api.twitch-radio.xyz/auth/me
Method	OPTIONS
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://api.twitch-radio.xyz/auth/spotify
Method	OPTIONS
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://api.twitch-radio.xyz/auth/token/verify
Method	OPTIONS
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://api.twitch-radio.xyz/twitch/findAllStreamers
Method	OPTIONS
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://api.twitch-radio.xyz/auth/spotify
Method	POST
Attack	
Evidence	Access-Control-Allow-Origin: *
Instances	8
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Medium	**X-Frame-Options Header Not Set**
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking'
URL	https://twitch-radio.xyz
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/home/?code=AQBMWG6kJBRfJ6tBlfclUb3te_hJEBn1qd0uCyzIHmLAjPtMiXx12GSJdkLcFwWC2ug5m cNN97dNXacdc0FEartQxfTuXyZNgd5wyfZhjvFIzbAPITYQBay16HwmmIJ8zyard-jmfxp6d746V
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/home/?code=AQC2K6lhMOIjnrSTFYsDIYd9jlC_tnAn1SCcmzeWKFMa6 i3F9UNETBIFpzZo4k2mWoLATb_ZLunh4EVY0NiKgj0WNboa3ZEm-vSb1tx1kRtcgCwH0Ktabq 20q1GeABxZEzL3J0Aqbuex89eOPZmOeLU5846eyAZYt0iRX
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/profile
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/sockjs-node
Method	GET
Attack	
Evidence	
Instances	6
Solution	Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all w server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you ne Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Low	**Incomplete or No Cache-control Header Set**

Description	The cache-control header has not been set properly or is missing, allowing the browser and pro
URL	https://api.twitch-radio.xyz/auth/me
Method	GET
Attack	
Evidence	
URL	https://api.twitch-radio.xyz/auth/token/verify
Method	GET
Attack	
Evidence	
URL	https://api.twitch-radio.xyz/twitch/findAllStreamers
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/home/?code=AQBMWG6kJBRfJ6tBlfclUb3te_hJEBn1qd0uCyzIHmLAjPtMiXx12GSJdkLcFwWC2ug5m cNN97dNXacdc0FEartQxfTuXyZNgd5wyfZhjvFIzbAPITYQBay16HwmmIJ8zyard-jmfxp6d746V
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/home/?code=AQC2K6lhMOIjnrSTFYsDIYd9jlC_tnAn1SCcmzeWKFMa6 i3F9UNETBIFpzZo4k2mWoLATb_ZLunh4EVY0NiKgj0WNboa3ZEm-vSb1tx1kRtcgCwH0Ktabq 20q1GeABxZEzL3J0Aqbuex89eOPZmOeLU5846eyAZYt0iRX
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/manifest.json
Method	GET
Attack	
Evidence	public, max-age=0
URL	https://twitch-radio.xyz/profile
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/robots.txt

Method	GET
Attack	
Evidence	public, max-age=0
URL	https://twitch-radio.xyz/sockjs-node
Method	GET
Attack	
Evidence	
URL	https://api.twitch-radio.xyz/auth/spotify
Method	POST
Attack	
Evidence	
Instances	12
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control
CWE Id	525
WASC Id	13
Plugin Id	10015

Low	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP respor /components your web application is reliant upon and the vulnerabilities such components may
URL	https://twitch-radio.xyz
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/favicon.ico
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/home
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/home/
Method	GET
Attack	
Evidence	X-Powered-By: Express
	https://twitch-radio.xyz/home/?

URL	code=AQBMWG6kJBRfJ6tBlfclUb3te_hJEBn1qd0uCyzIHmLAjPtMiXx12GSJdkLcFwWC2ug5m cNN97dNXacdc0FEartQxfTuXyZNgd5wyfZhjvFIzbAPITYQBay16HwmmIJ8zyard-jmfxp6d746V
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/home/?code=AQC2K6lhMOIjnrSTFYsDIYd9jlC_tnAn1SCcmzeWKFMa6 i3F9UNETBIFpzZo4k2mWoLATb_ZLunh4EVY0NiKgj0WNboa3ZEm-vSb1tx1kRtcgCwH0Ktabq 20q1GeABxZEzL3J0Aqbuex89eOPZmOeLU5846eyAZYt0iRX
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/logo192.png
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/manifest.json
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/profile
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/profile/
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/robots.txt
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/sitemap.xml
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/sockjs-node
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/static
Method	GET
Attack	

Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/static/js
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/static/js/bundle.js
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/static/js/main.chunk.js
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://twitch-radio.xyz/static/media
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://api.twitch-radio.xyz/auth/me
Method	OPTIONS
Attack	
Evidence	X-Powered-By: Express
URL	https://api.twitch-radio.xyz/auth/spotify
Method	OPTIONS
Attack	
Evidence	X-Powered-By: Express
URL	https://api.twitch-radio.xyz/auth/token/verify
Method	OPTIONS
Attack	
Evidence	X-Powered-By: Express
URL	https://api.twitch-radio.xyz/twitch/findAllStreamers
Method	OPTIONS
Attack	
Evidence	X-Powered-By: Express
Instances	24
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.a http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200

WASC Id	13
Plugin Id	10037

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	https://api.twitch-radio.xyz/auth/me
Method	GET
Attack	
Evidence	1639852428
URL	https://api.twitch-radio.xyz/auth/me
Method	GET
Attack	
Evidence	48130127
URL	https://api.twitch-radio.xyz/auth/token/verify
Method	GET
Attack	
Evidence	1639852428
URL	https://api.twitch-radio.xyz/twitch/findAllStreamers
Method	GET
Attack	
Evidence	1639852428
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	0123456789
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	1073741823
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	1073741824
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	1073741825
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	134217727

URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	134217728
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	20090320
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	20121025
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	20131105
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	2147483647
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	254874553
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	268435456
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	33554432
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	62914560
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	67108864
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js

Method	GET
Attack	
Evidence	805306368
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	86400000
URL	https://api.twitch-radio.xyz/auth/spotify
Method	POST
Attack	
Evidence	1639852428
Instances	22
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows old potentially causing the response body to be interpreted and displayed as a content type other th declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://twitch-radio.xyz
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/favicon.ico
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/home/?code=AQBMWG6kJBRfJ6tBlfclUb3te_hJEBn1qd0uCyzIHmLAjPtMiXx12GSJdkLcFwWC2ug5m cNN97dNXacdc0FEartQxfTuXyZNgd5wyfZhjvFIzbAPITYQBay16HwmmIJ8zyard-jmfxp6d746V
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/home/?code=AQC2K6lhMOIjnrSTFYsDIYd9jlC_tnAn1SCcmzeWKFMa6 i3F9UNETBIFpzZo4k2mWoLATb_ZLunh4EVY0NiKgj0WNboa3ZEm-vSb1tx1kRtcgCwH0Ktabq 20q1GeABxZEzL3J0Aqbuex89eOPZmOeLU5846eyAZYt0iRX
Method	GET

Attack	
Evidence	
URL	https://twitch-radio.xyz/logo192.png
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/manifest.json
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/profile
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/robots.txt
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/sockjs-node
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/static/js/bundle.js
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/static/js/main.chunk.js
Method	GET
Attack	
Evidence	
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	
Instances	13
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it s If possible, ensure that the end user uses a standards-compliant and modern web browser that 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: Matc
URL	https://twitch-radio.xyz/static/js/bundle.js
Method	GET
Attack	
Evidence	bugs
URL	https://twitch-radio.xyz/static/js/bundle.js
Method	GET
Attack	
Evidence	from
URL	https://twitch-radio.xyz/static/js/bundle.js
Method	GET
Attack	
Evidence	later
URL	https://twitch-radio.xyz/static/js/bundle.js
Method	GET
Attack	
Evidence	TODO
URL	https://twitch-radio.xyz/static/js/main.chunk.js
Method	GET
Attack	
Evidence	from
URL	https://twitch-radio.xyz/static/js/main.chunk.js
Method	GET
Attack	
Evidence	user
URL	https://twitch-radio.xyz/static/js/main.chunk.js
Method	GET
Attack	
Evidence	username
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	bug
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	bugs
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js

Method	GET
Attack	
Evidence	FIXME
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	from
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	later
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	query
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	select
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	TODO
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	user
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	username
URL	https://twitch-radio.xyz/static/js/vendors~main.chunk.js
Method	GET
Attack	
Evidence	where
URL	https://twitch-radio.xyz
Method	GET
Attack	
Evidence	from
URL	https://twitch-radio.xyz
Method	GET

Attack	
Evidence	user
URL	https://twitch-radio.xyz/
Method	GET
Attack	
Evidence	from
URL	https://twitch-radio.xyz/
Method	GET
Attack	
Evidence	user
URL	https://twitch-radio.xyz/home/? code=AQBMWG6kJBRfJ6tBlfclUb3te_hJEBn1qd0uCyzIHmLAjPtMiXx12GSJdkLcFwWC2ug5m cNN97dNXacdc0FEartQxfTuXyZNgd5wyfZhjvFIzbAPITYQBay16HwmmIJ8zyard-jmfxp6d746V
Method	GET
Attack	
Evidence	from
URL	https://twitch-radio.xyz/home/? code=AQBMWG6kJBRfJ6tBlfclUb3te_hJEBn1qd0uCyzIHmLAjPtMiXx12GSJdkLcFwWC2ug5m cNN97dNXacdc0FEartQxfTuXyZNgd5wyfZhjvFIzbAPITYQBay16HwmmIJ8zyard-jmfxp6d746V
Method	GET
Attack	
Evidence	user
URL	https://twitch-radio.xyz/home/?code=AQC2K6lhMOIjnrSTFYsDIYd9jlC_tnAn1SCcmzeWKFMa6 i3F9UNETBIFpzZo4k2mWoLATb_ZLunh4EVY0NiKgj0WNboa3ZEm-vSb1tx1kRtcgCwH0Ktabq 20q1GeABxZEzL3J0Aqbuex89eOPZmOeLU5846eyAZYt0iRX
Method	GET
Attack	
Evidence	from
URL	https://twitch-radio.xyz/home/?code=AQC2K6lhMOIjnrSTFYsDIYd9jlC_tnAn1SCcmzeWKFMa6 i3F9UNETBIFpzZo4k2mWoLATb_ZLunh4EVY0NiKgj0WNboa3ZEm-vSb1tx1kRtcgCwH0Ktabq 20q1GeABxZEzL3J0Aqbuex89eOPZmOeLU5846eyAZYt0iRX
Method	GET
Attack	
Evidence	user
URL	https://twitch-radio.xyz/profile
Method	GET
Attack	
Evidence	from
URL	https://twitch-radio.xyz/profile
Method	GET
Attack	
Evidence	user
URL	https://twitch-radio.xyz/sockjs-node
Method	GET

Attack	
Evidence	from
URL	https://twitch-radio.xyz/sockjs-node
Method	GET
Attack	
Evidence	user
Instances	30
Solution	Remove all comments that return information that may help an attacker and fix any underlying p
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027