Content Security Policy in Ezeelogin GUI

553 Nesvin KN November 18, 2022 General 1432

Content Security Policy (CSP) in the Ezeelogin web framework explained

Content-Security-Policy headers have been updated in the **Ezeelogin version 7.29.0**. Refer below article to update Ezeelogin to the latest version.

Upgrade the Ezeelogin Jumpserver to the latest version

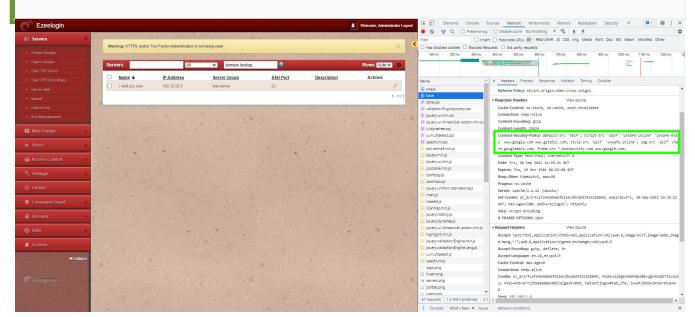
Ezeelogin GUI uses dynamic scripts and it needs to use **nonce**. But nonce needs to be dynamic and hence cannot be set in httpd.conf or any web server configuration because it is only static. **CSP headers are set from the Ezeelogin application itself**. Users need not set any headers in httpd.conf for Ezeelogin. Refer below screenshot to view the CSP header being set when the user accesses the Ezeelogin web panel - without any 'unsafe' option.

To view the **Content-Security-Policy**, use the **F12 key** or **right-click on the Ezeelogin software GUI** -> **Inspect** -> **Network** -> **base-> Headers** -> **Response Headers** -> **Content-Security-Policy**. Refer below screenshot.

zeelogin						Welcome, manu Logout		re log 🛛 🗆 Disable cache 🛛 No throttling 💌 😪	± ±	
vers 🔻	Servers find	All v domain lookup		p		Rows Auto V	Filter Invert Hide data URLs All Fetch/XHR JS CSS Img Media Font Doc WS Wasm Manifest Other Has blocked cookies Blocked Requests 3rd-party requests Srd-party S			
er Groups	□ Name ↓	IP Address	Server Group	SSH Port	Description	Actions	500 ms	1000 ms 1500 ms	2000 ms 2500 m	s 3000 m
er Groups	+ admod MDM	10.10.1.10	AdMod Servers	22		/ 🔳				
SSH Users			AdMod Servers							
H User Maps	+ admodserv1.com	10.10.1.2	AdMod Servers	2020	staffportal/wiki/idap/svn/nfsfileserver		Name	A Headers Preview Response In	tiator Timing Cookies	
	+ admodserv2.com	10.10.1.6	AdMod Servers	2020	gillab/ezlogin/Liveserversbackups	1	Check2	* General		
	+ admodserv3.admod.net	10.10.1.7	AdMod Servers	22	nfs file server/download.admod.net	/	📄 base	Request URL: https://10.10.1.6/in	iex.cho/base	
	+ admodserv3.adsssmod.net	10.10.1.5	AdMod Servers	2020	nfs file server/download.admod.net	1	style.css	Request Method: GET		
. 8							validationEngine.jquery.css	Status Code: 🖷 200 OK		
	+ secure.admod.net	10.10.1.18	AdMod Servers	22	ezloginmastersharedteam	1	jquery-ul.min.css Itatoickr.min.css	Remote Address: 10.10.1.6:443 Referrer Policy: strict-origin-when-cross-origin		
Web Portals	+ secureslave.admod.net	10.10.1.45	AdMod Servers	22	ezloginslaveservershared	1	vidynatree.css			
- 1 B						1-7/7	jquery.ukcmultiselect.css	* Response Headers	View source	
lsers 🕨						(5)	Spectrum.css	Cache-Control: no-store, no-cache,	must-revalidate, post-check=0, p	one-check=0
	The second second and				and provide the second second		🧧 ddr-ecma5.min.js	Connection: Keep-Alive		
							🤤 jqueryminijs	Content-Encoding: gzip		
							jquery-ui.min.js	Content-Length: 9691		
× 10							tooltipsy.is	Content-Security-Policy: default-src		
							🥃 zoombox.js	tw=='; img-src 'self' data: http: -uri 'self'	://chart.googleapis.com/chart; of	oject-src none; ba
							🥫 jquery.uniform.standalone.js	Content-Type: text/html: charset=	ITF-8	
- 83							🗟 mainjs	Date: Fri, 30 Sep 2022 14:28:12 G	мт	
							hattori_hanzo-webfont.woff	Expires: Thu, 19 Nov 1981 08:52:00	GMT	
							 base64,is ICanHazmin.is 	Keep-Alive: timeout=5, max=94		
1 A 1							jquery.history.js	Pragma: no-cache		
100							🥫 jquery.dynatree.js	Server: Apache/2.4.7 (Ubuntu)		
- 1 B			2 million and		and the second second		🔄 flatpickr.min.js	Set-Cookie: ez_ecsrf=2397e23dde8c1		30-Sep-2022 16:28
							🕞 highlight.min.js	GMT; Max-Age=7200; Path=%2F; Sec	ire; HttpOnly; SameSite=Strict	
							🧧 jquery.validationEngine.min.js	Vary: Accept-Encoding		
							jquery.validationEngine-lang.js	X-FRAME-OPTIONS: DENY		
	· · · · · · · · · · · · · · · · · · ·			1. C			jquery.uix.multiselect.js	* Request Headers	View source	
							spectrum.js	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif		e/avif,image/webp,
							logo.png	e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9		
		i inggring i hugang			Accept-Encoding: gzip, deflate, br					
							E servers.ong	 Accept-Language: en-US,en;q=0.9 		
							73 requests 1.4 MB transferred	22 4 Carbo Controls any nes 0		
						Console What's New X	Issues Network conditions			
and a second second second	Highlights from the Chrome 105 update									

Refer below screenshot to find Content-Security-Policy with "unsafeinline" in prior Ezeelogin version 7.29.0. To view the **Content-Security-Policy**, use the **F12** key or **right-click on the Ezeelogin software GUI** -> **Inspect** -> **Network** -> **base-> Headers** -> **Response Headers** -> **Content-Security-Policy**. Refer below screenshot.

Header always set Content-Security-Policy "default-src 'self'; style-src 'self' '**unsafe-inline**'; frameancestors 'self'; script-src 'self' '**unsafe-inline**';"



Error when enabling **Header always set Content-Security-Policy** "default-src 'self'; frame-ancestors 'self';" in httpd.conf.

Refer below screenshot for the browser console error when **Header always set Content-Security-Policy ''default-src 'self'; frame-ancestors 'self';''** is enabled in **httpd.conf**.

♥ Refused to execute inline script because it violates the following Content Security Policy directive: "script-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-qwI7/vd6+Mphox1gZyeQf2XaV6cSTh6iTRk8lzTli7g='), or a nonce ('nonce') is required to enable inline execution.	<u>jquery.min.js:2</u> ℚ
Incaught (in promise) unknown action process discovery con	tent script.js:2 🔍
Refused to execute inline script because it violates the following Content Security Policy directive: "script-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-B31Cj9nClObyN+fkIAqsYryghnruuDjH0MSRSUmeivQ='), or a nonce ('nonce') is required to enable inline execution.	j <u>query.min.js:2</u> @
Refused to execute inline script because it violates the following Content Security Policy directive: "script-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-JxtD4T2IsYXd2MCt5JVnfjE6HK1H/zAnr2iwbuKtP4Q='), or a nonce ('nonce') is required to enable inline execution.	j <u>query.min.js:2</u> @
Refused to execute inline script because it violates the following Content Security Policy directive: "script-src 'self'". Either the 'unsafe-inline' keyword, a hash ('sha256-B31Cj9nClObyN+fkIAqsYryghnruuDjH0MSRSUmeivQ='), or a nonce ('nonce') is required to enable inline execution.	jquery.min.js:2 🔍

Online URL: https://www.ezeelogin.com/kb/article/content-security-policy-in-ezeelogin-gui-553.html

>