Content Security Policy in Ezeelogin GUI

553 Nesvin KN March 20, 2025 General 3553

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

Overview: This article explains the updated CSP headers in Ezeelogin 7.29.0, where dynamic scripts use nonce set by the application. Users no longer need to configure CSP headers in httpd.conf to secure the GUI.

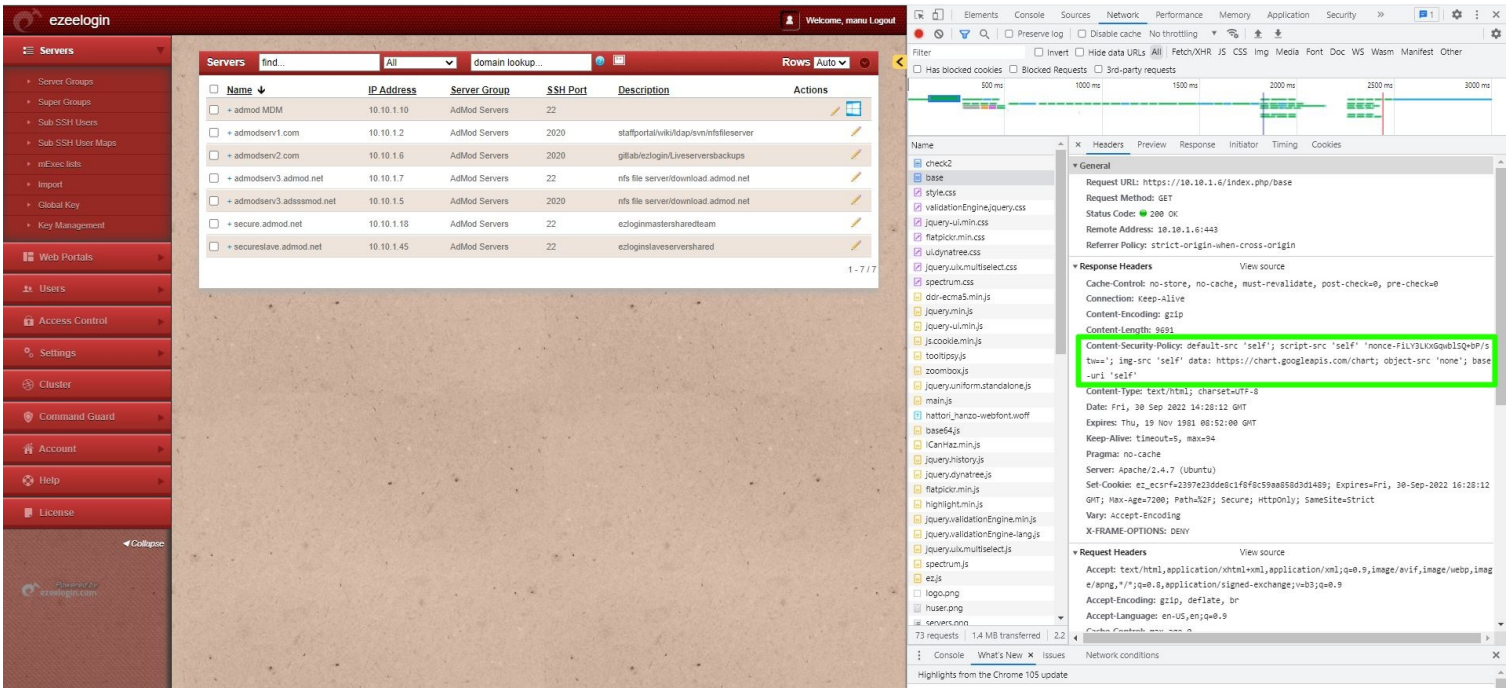
Note:

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

Note: 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.



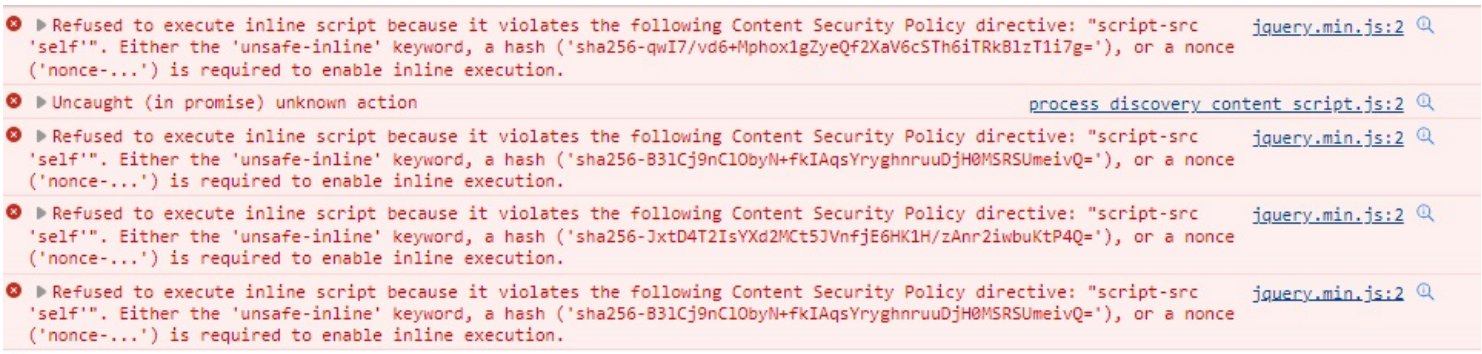
Refer below screenshot to find Content-Security-Policy with **"unsafe-inline"** in prior Ezeelogin version 7.29.0.

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**'; frame-ancestors '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**.



Related Articles:

Best Practices for Ezeelogin: A Guide to Standard Security Configurations

How to ensure that ssh jump host users are not using previous password set to meet security compliances such as PCI DSS , SOX, HIPAA , NIST , MAS, SOC2, FFIEC, NERC CIP , ISO 27001

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