Adminer Bugs and Features

Database management in a single PHP file
Brought to you by: jakubvrana

#775 XSS Reflected

Milestone: 4.7.8 **Status:** closed-fixed **Owner:** Jakub Vrána **Labels:** XSS (2), Security Issue (2)
Priority: 7
Updated: 2021-02-10 **Created:** 2020-12-28 **Creator:** morphine0x4 **Private:** No

There is a security issue, in particular a Reflected XSS, on "history" parameter. The issue affected the latest version of Adminer and priors.

Using the following request:
/adminer/?username=root&sql=&history='-alert('XSS')-'
is possible to execute javascript.

I applied for a CVE, assigned with the id "CVE-2020-35572".

As attachment a screenshot of the issue.

Discussion

morphine0x4 - *2021-01-24*
Updates?

Jakub Vrána - *2021-02-06*
- **status**: open --> closed-fixed

Jakub Vrána - *2021-02-06*
I'm sorry for not responding sooner, I've missed this bug in triage.
There's no attachment and I can't reproduce it because browsers encode URL parameters so the `'` is actually sent to server as `%27`.
But I see what you mean and I've fixed the possible issue.

Jakub Vrána - *2021-02-07*
- **private**: Yes --> No

morphine0x4 - *2021-02-09*
No problem and thanks for the fix.
I try to upload again the proof of the XSS.
If you reproduce it with Edge, you can trigger the XSS easily. Edge doesn't sanitize the input in the address bar.

adminerXSS.png

Jakub Vrána - *2021-02-10*
Published at https://github.com/vrana/adminer/security/advisories/GHSA-9pgx-gcph-mpqr.

Log in to post a comment.

Company

About
Team
SourceForge Headquarters
225 Broadway Suite 1600
San Diego, CA 92101
+1 (858) 454-5900

Resources

Support
Site Documentation
Site Status