dk50u1 Follow
Nov 8 · 2 min read · Listen

Stored XSS in Zoneminder up to v1.36.12

CVE-2022-30768

Vulnerability Description:

Stored Cross Site Scripting (XSS) exists in ZoneMinder up to v1.36.12. This allows an attacker to execute malicious code via the “Username” vulnerable field when an Admin (or a user that can see other users logged on the platform) clicks to logout.

Affected Assets:

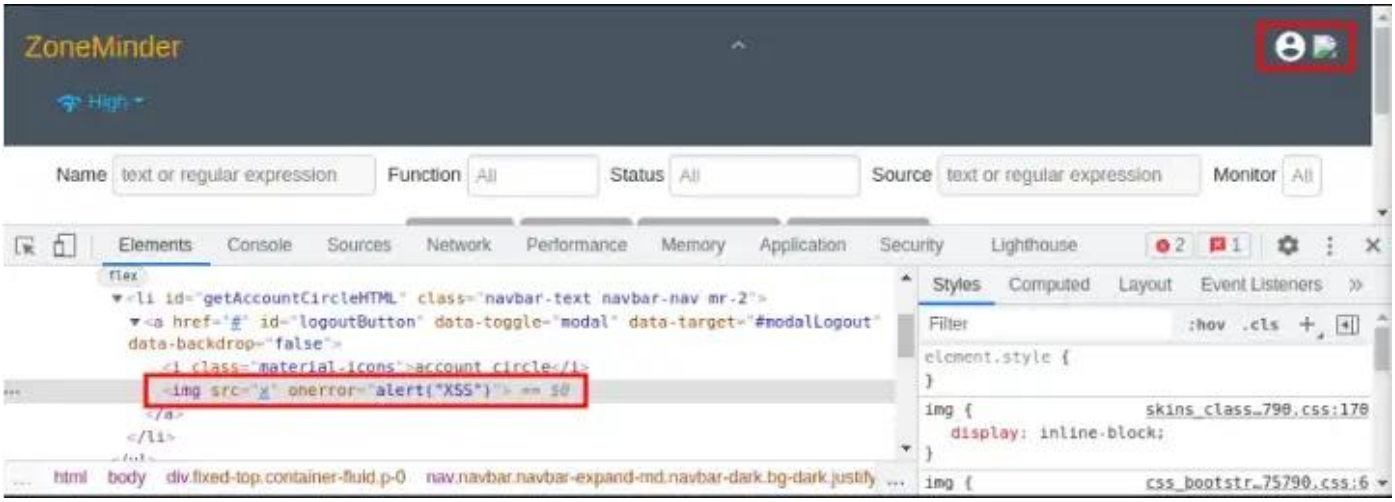
Username field and logout function.

Payload:

```
<img src=x onerror=alert(“XSS”)>
```

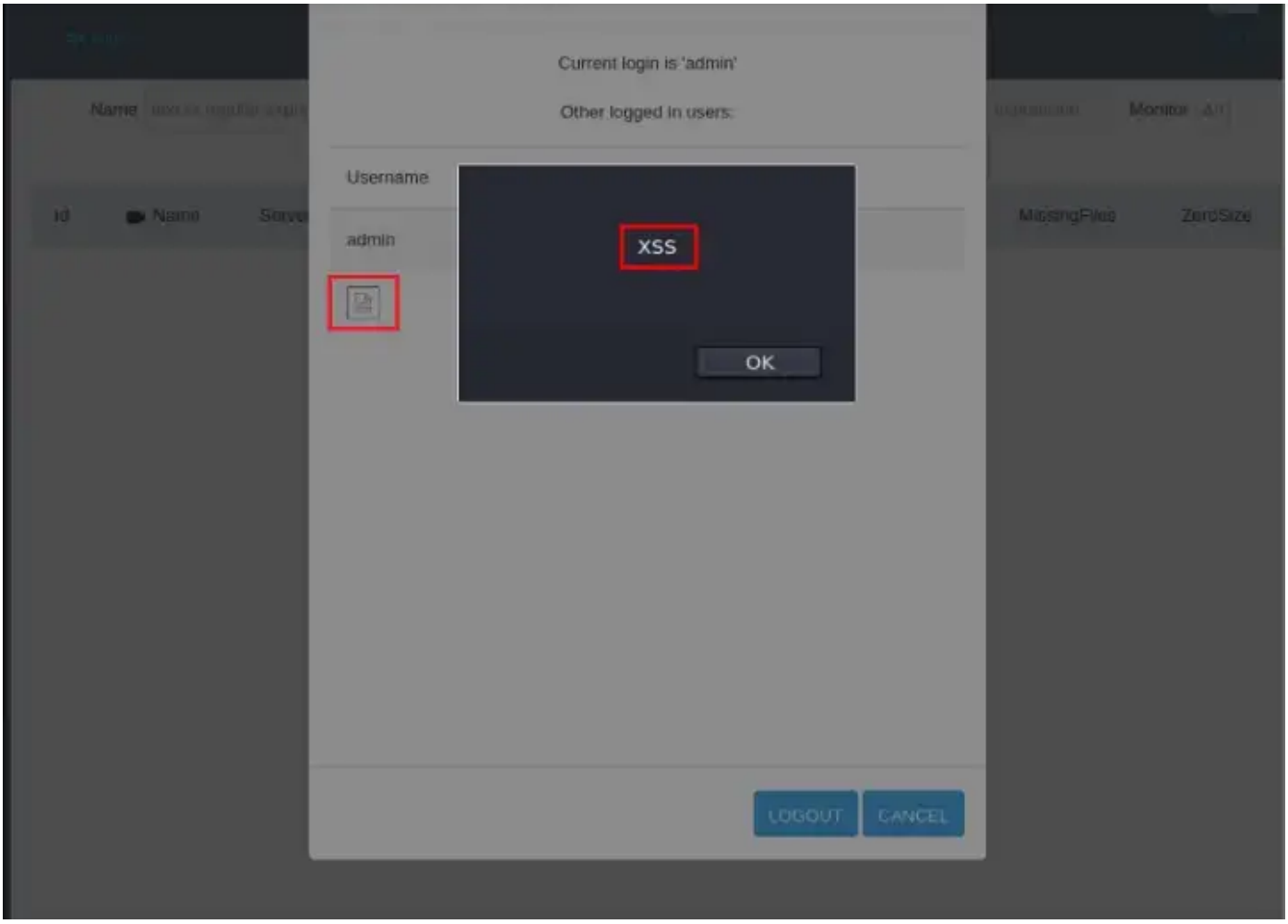
Details:

When a new user is created (or a user’s username is modified), if the “Username” field is set to an XSS payload (see Payload), at the next login with the modified username, if an Admin (or whoever has the proper permissions to see other users logged on the platform) want to logout from the web page, the “list of current user logged” triggers the payload and an you have an XSS. This works as long as the user with payload remains logged in.



Payload as username

2. Wait for the admin (or whoever has the ability to see logged in users) to log in and as long as you are logged in, if that user clicks to logout, the XSS is triggered because the logout function shows the users still logged on the platform and the code inside the username field is executed.



Admin logout and XSS triggered

That's all Folks.