Description

Summary

A Stored Cross-Site Scripting (XSS) vulnerability in the API-Access page allows authenticated users to inject arbitrary JavaScript through the "description" parameter when creating a new API token. This vulnerability can result in the execution of malicious code in the context of other users' sessions, compromising their accounts and enabling unauthorized actions.

Details

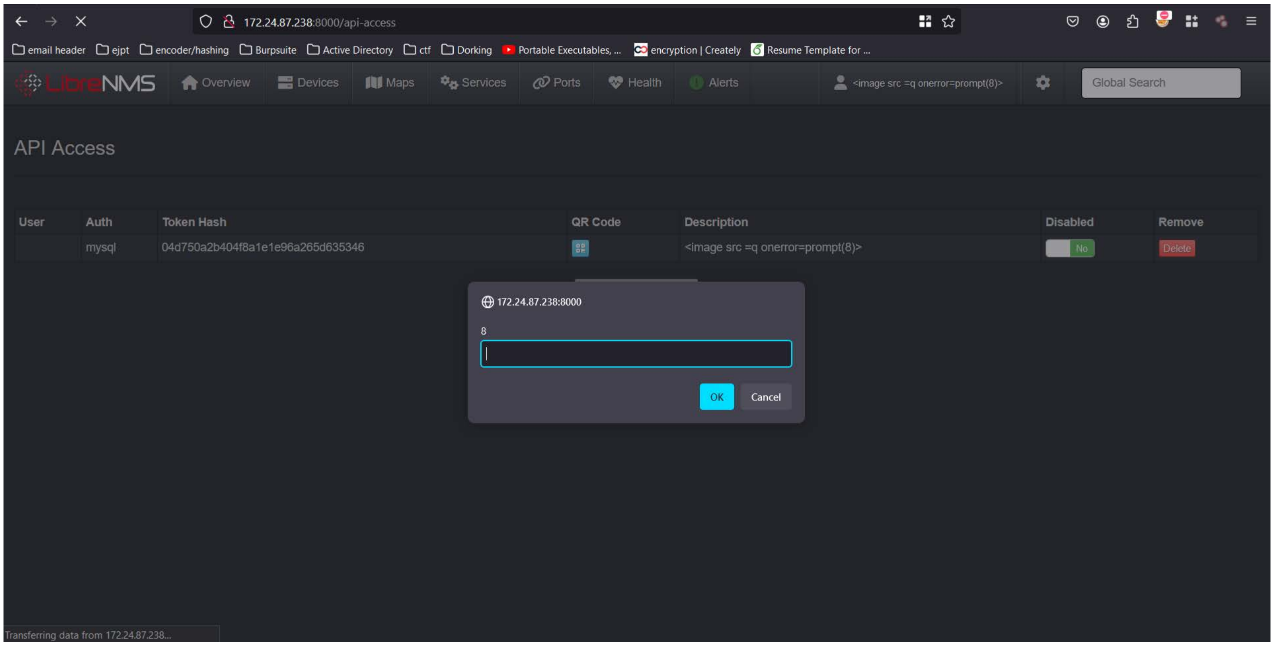
The vulnerability occurs when creating a new API Token. An attacker can inject arbitrary JavaScript into the "description" parameter, which is then executed when the API Access page is visited.

The payload used to exploit this vulnerability is: <image src =q onerror=prompt(8)>

Note: The payload leverages an tag with the onerror attribute to execute arbitrary JavaScript code when the image fails to load. By utilizing a crafted src value, the payload triggers the onerror event, which can be used to execute a proof-of-concept (POC) XSS attack or any arbitrary JavaScript code. This technique is effective in exploiting XSS vulnerabilities in applications that fail to properly sanitize user input, and the payload can be further customized to fetch malicious scripts from a remote domain to bypass input length restrictions or deliver more complex attacks.

PoC

Create a new API token with the following payload in the "description" parameter: <image src =q onerror=prompt(8)>
Save the token.
Navigate to the API Access page.
Observe that the injected script executes.



API Access

User	Auth	Token Hash	QR Code	Description	Disabled	Remove
	mysql	04d750a2b404f8a1e1e96a265d635346		<image src =q onerror=prompt(8)>	No	Delete

172.24.87.238:8000

8

Impact

The vulnerability allows authenticated users to execute arbitrary JavaScript code in the context of other users' sessions. This can lead to account compromise and enable unauthorized actions on behalf of the impacted users.