GrimTheRipper Follow
Sep 28 · 2 min read · Listen

KLiK SocialMediaWebsite Version 1.0.1 — Stored XSS Vulnerability at reply-form

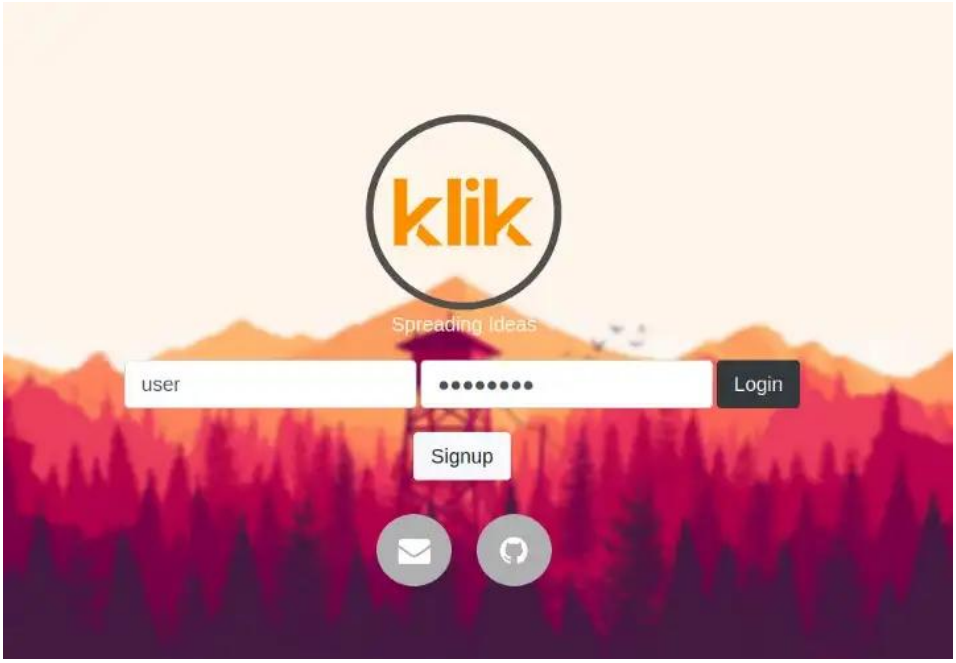
Vulnerability Explanation:
KLiK SocialMediaWebsite Version 1.0.1 has XSS vulnerabilities that allow attackers to store XSS via location input reply-form.

Affected Component:
http://[ip]/KLiK/posts.php?topic=[any]

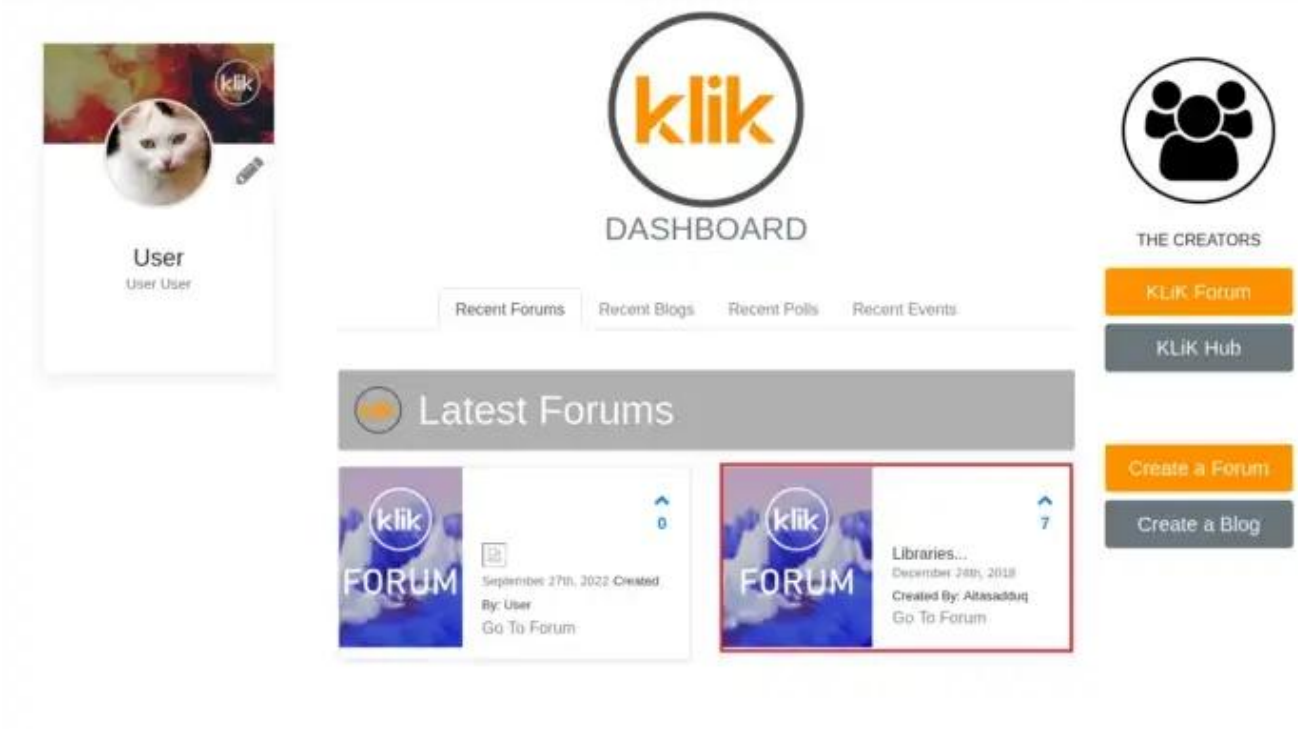
Payload :
<img src=”test” onerror=confirm(“Grim-The-Ripper-Team-by-SOSECURE-Thailand”)>

Tested on:
1. KLiK SocialMediaWebsite Version 1.0.1 https://github.com/msaad1999/KLiK-SocialMediaWebsite
2. Google Chrome Version 103.0.5060.114 (Official Build) (64-bit)

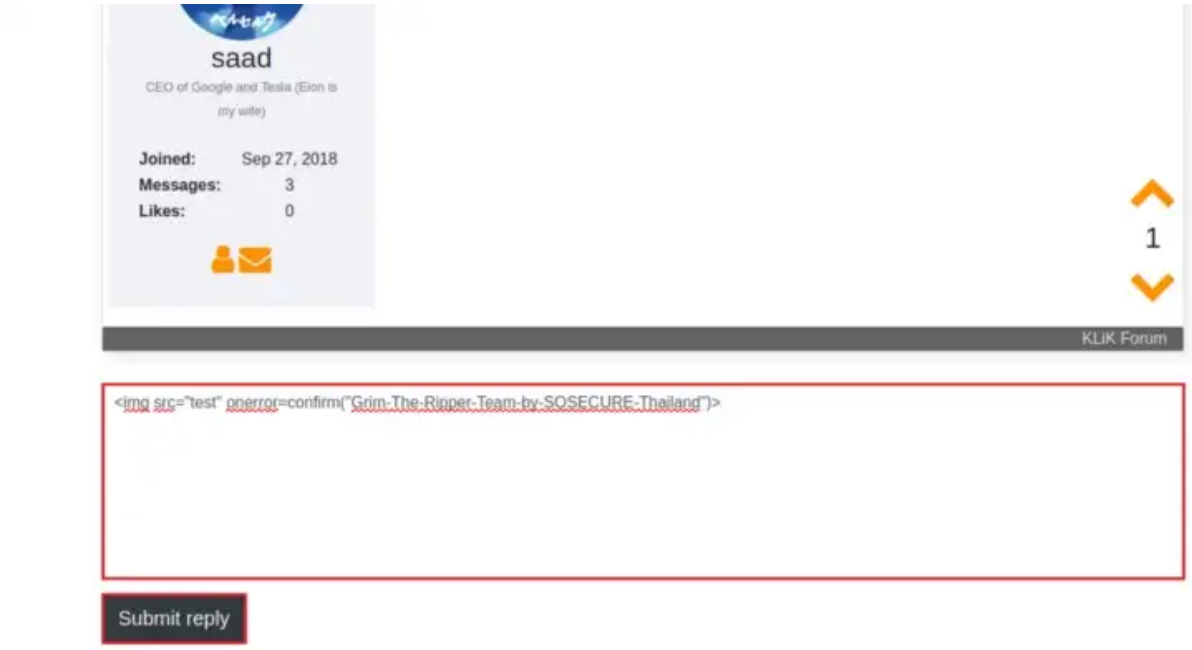
Steps to attack:
1. Login with user credentials.



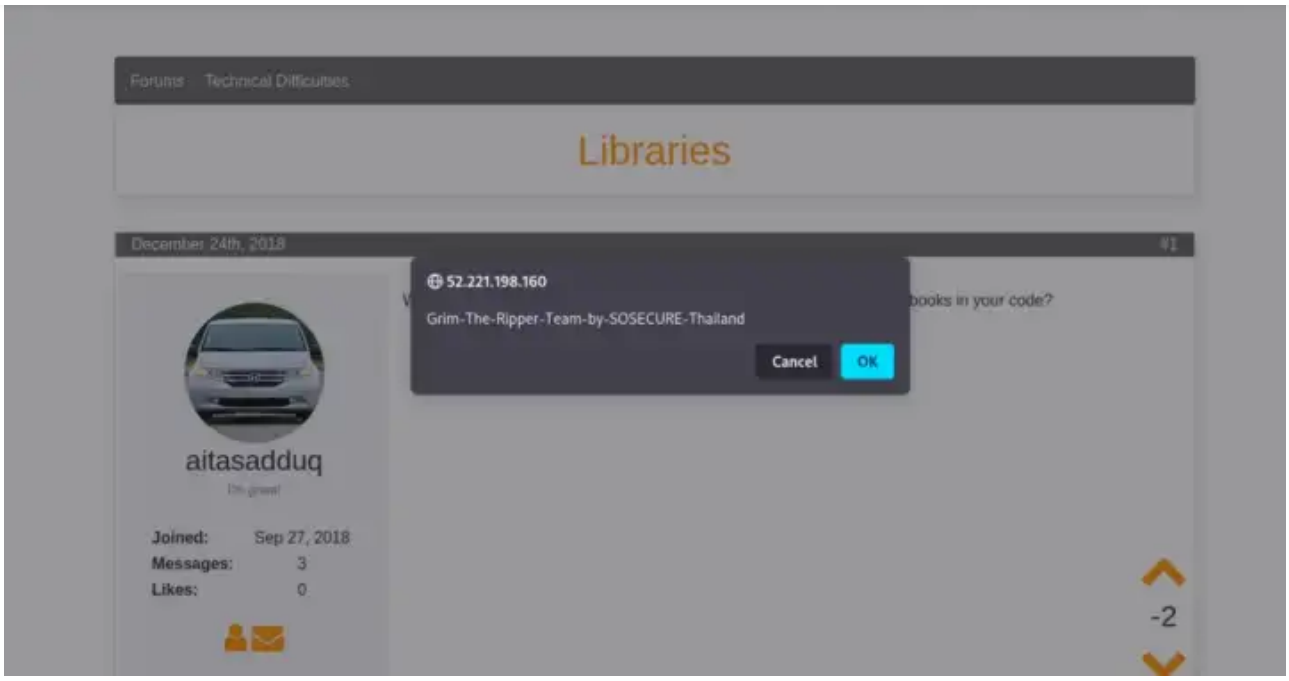
2. Go to the “Forum”(any forum) as show in the picture



3. Next, scroll down and click on the “reply-form” input then enter the XSS payload and press the Submit reply button.



4. After refresh this page The XSS payload will run immediately.



Discoverer:
Grim The Ripper Team by SOSECURE Thailand

Reference:
https://github.com/msaad1999/KLiK-SocialMediaWebsite