

[Open in app](#)[Get started](#)

GrimTheRipper

[Follow](#)

Sep 28 · 2 min read ·

[Listen](#)

Save



KLik SocialMediaWebsite Version 1.0.1 — Stored XSS Vulnerability at Forum Subject

Vulnerability Explanation:

KLik SocialMediaWebsite Version 1.0.1 has XSS vulnerabilities that allow attackers to store XSS via location Forum Subject input.

Affected Component:

[http://\[ip\]/KLik/create-topic.php](http://[ip]/KLik/create-topic.php)

Payload :

```

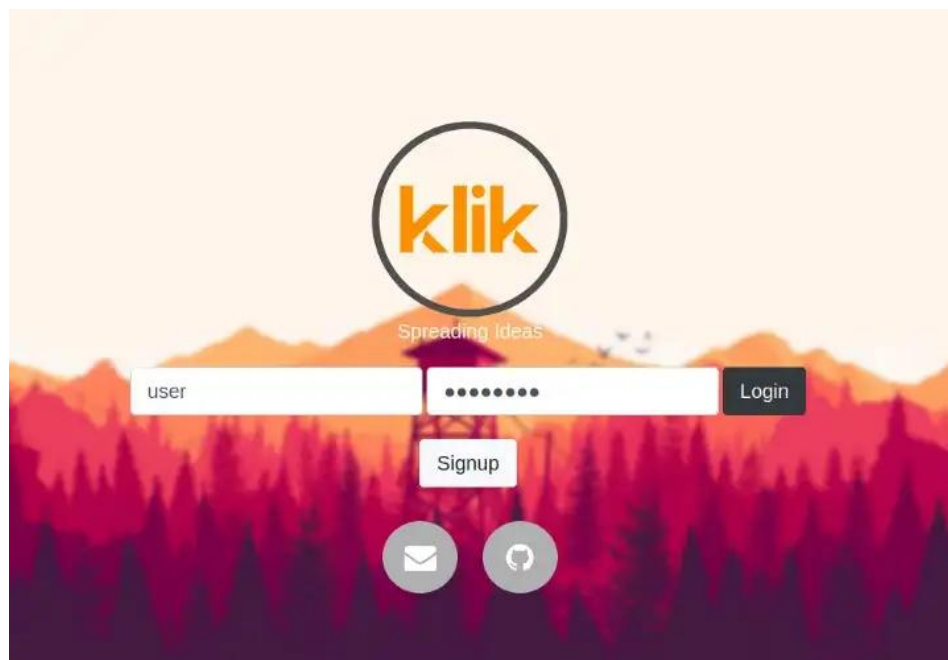
```

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)

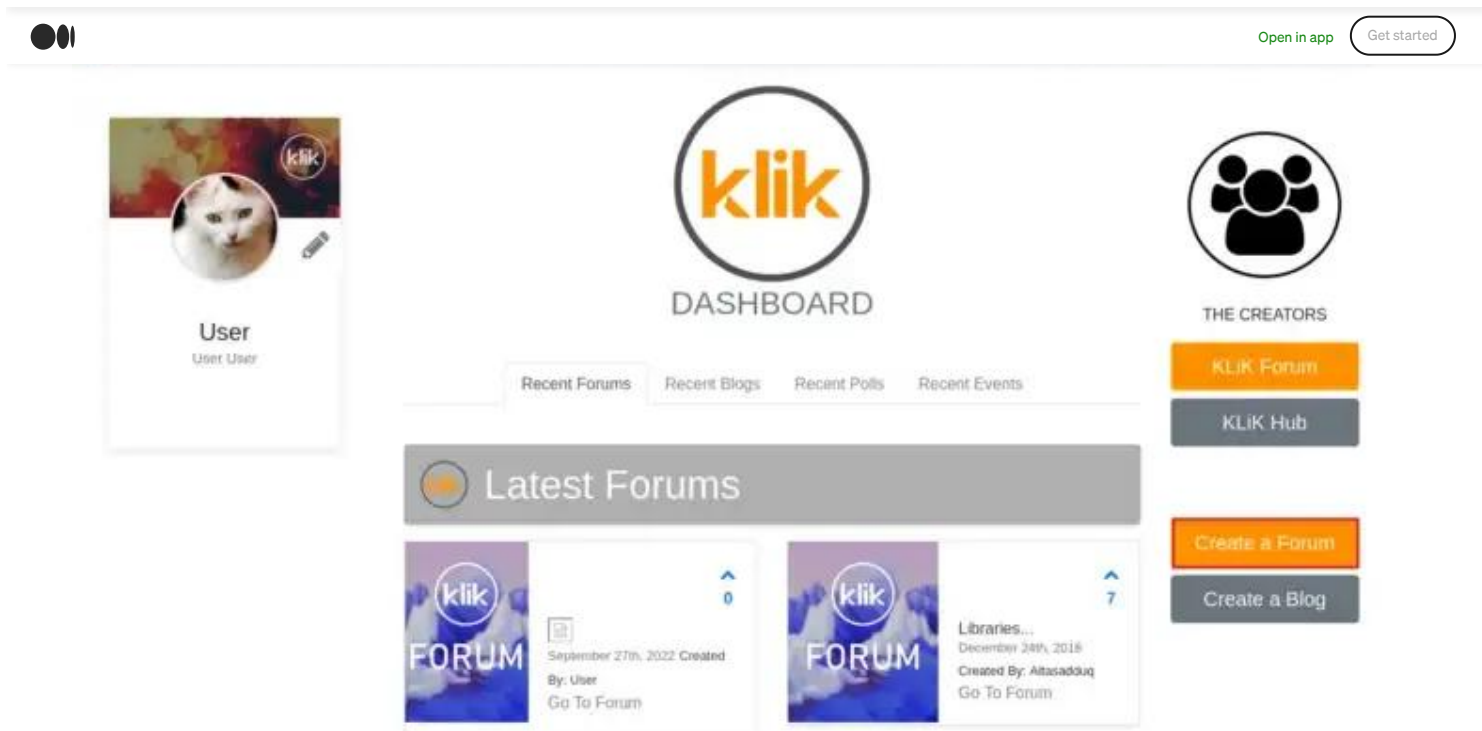
Steps to attack:

1. Login with user credentials.

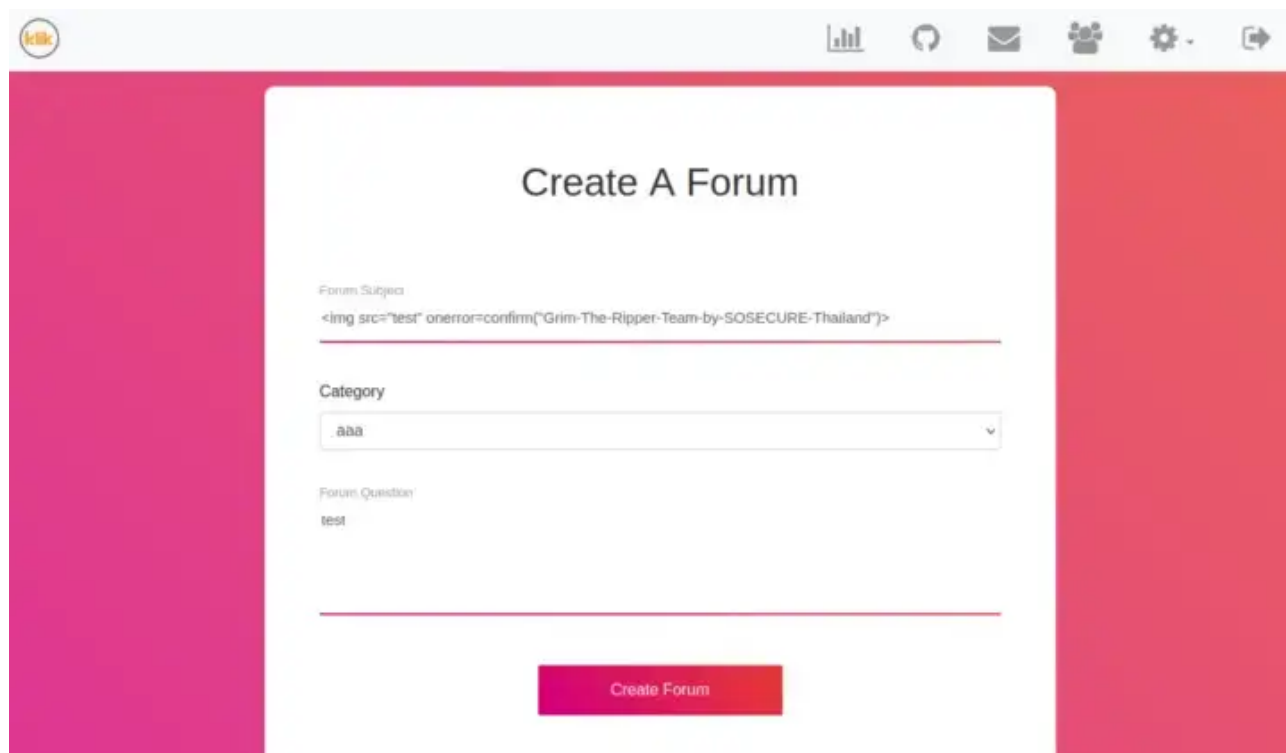



2. Go to the "Forum"(any forum) as show in the picture





3. Next, click on the “Forum Subject” input then enter the XSS payload and press the Create Forum button then there will be a message saying that the forum has been successfully created as in the picture.



Open in appGet started

Create A Forum

*Forum successfully created

Form Subject

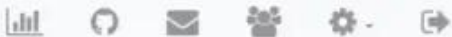

Category


aaa


Forum Question

Create Forum


4. Next, go back to the index.php page and you will see that a new forum has been created.








DASHBOARD

Recent ForumsRecent BlogsRecent PollsRecent Events


Latest Forums


FORUM

September 27th, 2022 Created
By: User
Go To Forum


FORUM

September 27th, 2022 Created
By: User
Go To Forum


THE CREATORS

KLK Forum

KLK Hub

Create a Forum

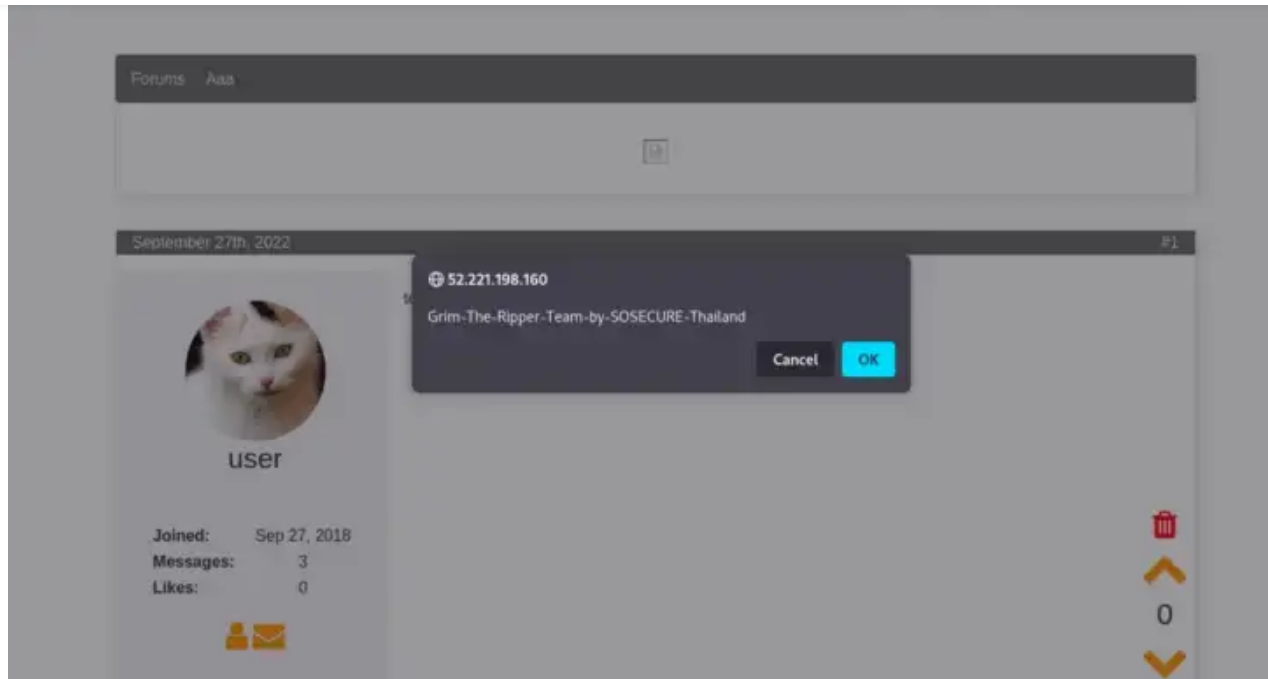
Create a Blog

5. After, go to that forum The XSS payload will run immediately.



Open in app

Get started



Discoverer:

Grim The Ripper Team by SOSECURE Thailand

Reference:

<https://github.com/msaad1999/KLiK-SocialMediaWebsite>

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

