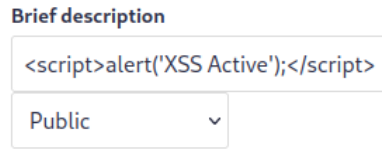
Liam Brew
02 Feb 2022

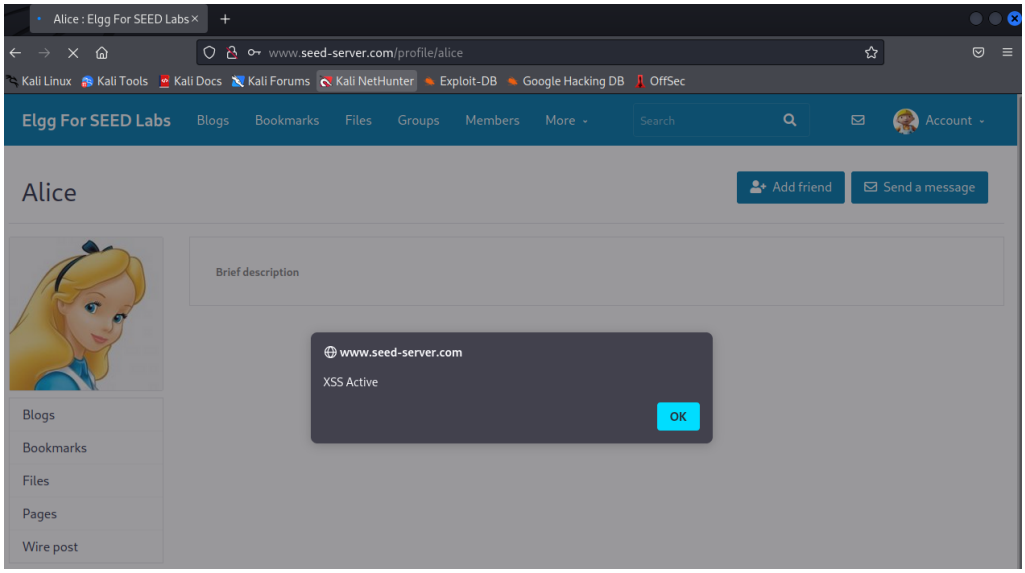
Lab 03: XSS

Task 1: Malicious XSS Message

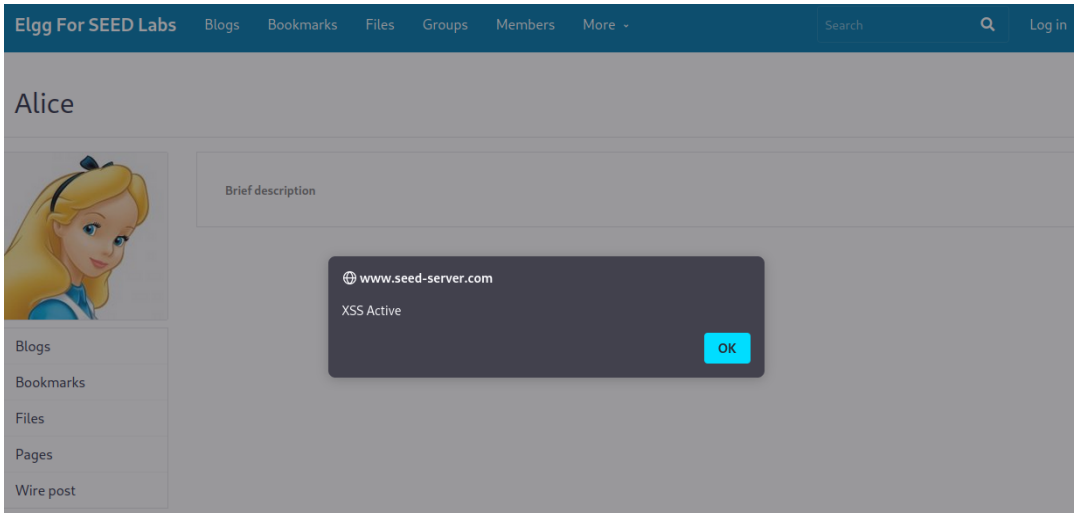
Code:



XSS Triggering on user Boby:



XSS Triggering on no user (not currently logged in):



Task 2: XSS Cookie

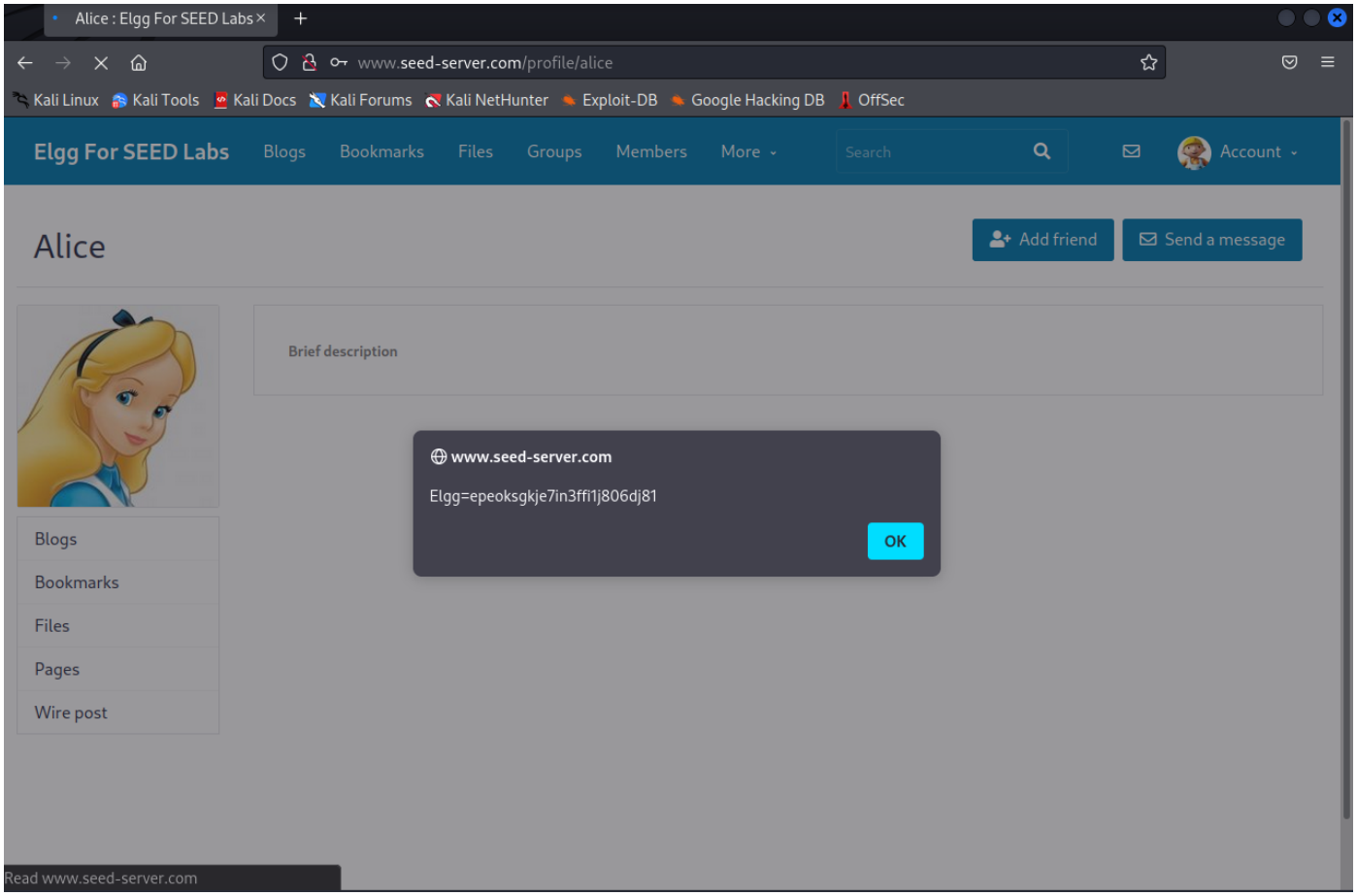
Code:

Brief description

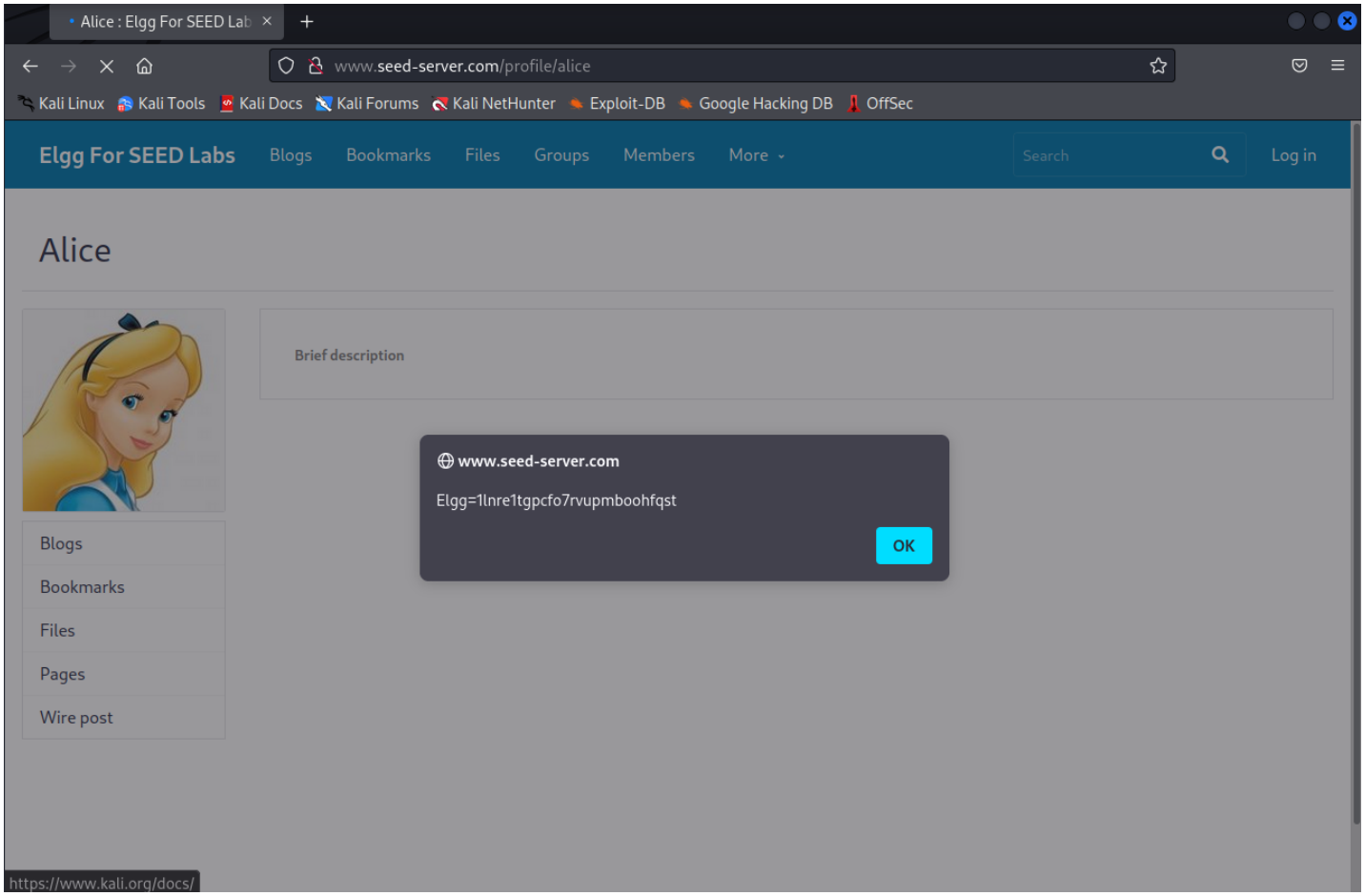
```
<script>alert(document.cookie);</script>
```

Public

XSS Triggering on user Boby:



XSS Triggering on no user (not currently logged in):



Explanation

This incident represents attackers using the forms on the profile to inject malicious scripts onto the web page. Once successfully injected and stored, this script will have the same source as the other content that is trusted. This means that it will be executed as if it was legitimate code.

This type of attack represents a stored XSS attack. This is because the script is being saved in the relevant database entry for a user's 'brief description' field. As the victim navigates the website and loads the page where this data is pulled from, the script is loaded and executed.

This XSS attack is possible because the website does not seem to utilize input validation on these form fields. If these forms were in some way sanitized, such as limiting the length or restricting certain characters, or using some of the language-dependent security options for the website (such as the *eval()* method in Javascript).