

COURSE: Ethical Hacking / Penetration Testing & Bug Bounty Hunting

Embark on a Journey of Ethical Hacking, Penetration Testing & Bug Bounty Hunting

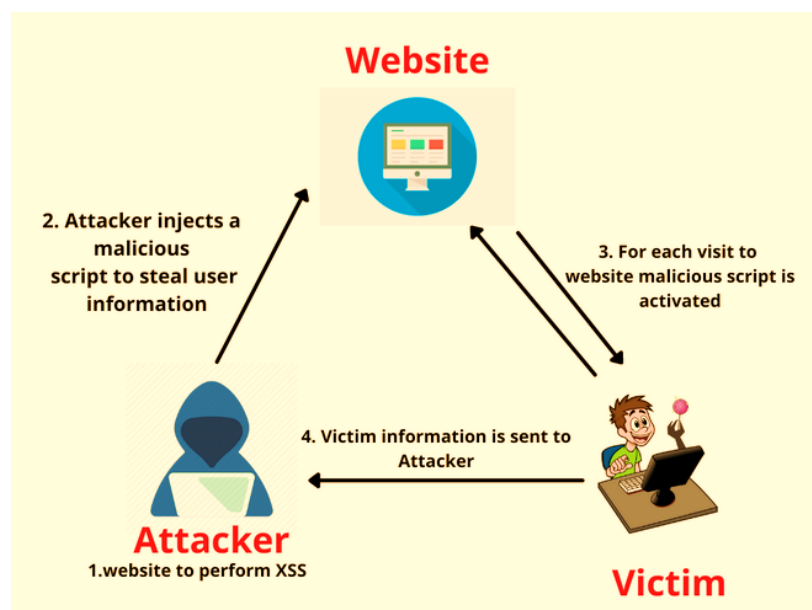


❖ Introduction:

In a world where digital landscapes are expanding at an unprecedented pace, the need for cybersecurity expertise has never been more vital. As organizations strive to safeguard their online assets, the demand for skilled ethical hackers, penetration testers, and bug bounty hunters are soaring. If you're intrigued by the idea of wielding your technical prowess for the greater good, then you're in the right place. Welcome to the comprehensive Udemmy course "Ethical Hacking / Penetration Testing & Bug Bounty Hunting." In this article, we will unravel the exciting facets of this course, showcasing the diverse topics covered to equip you with the skills to navigate the complex realm of cybersecurity.

❖ Introduction to XSS (Cross Site Scripting)

Cross-site scripting (XSS) is a web security vulnerability where malicious scripts are injected into a website and executed in the context of a user's browser, often leading to data theft or unauthorized actions.



❖ Lab from Portswigger for XSS

Link to the lab:-

<https://portswigger.net/web-security/cross-site-scripting/stored/lab-html-context-nothing-encoded>

1. Description of the Lab

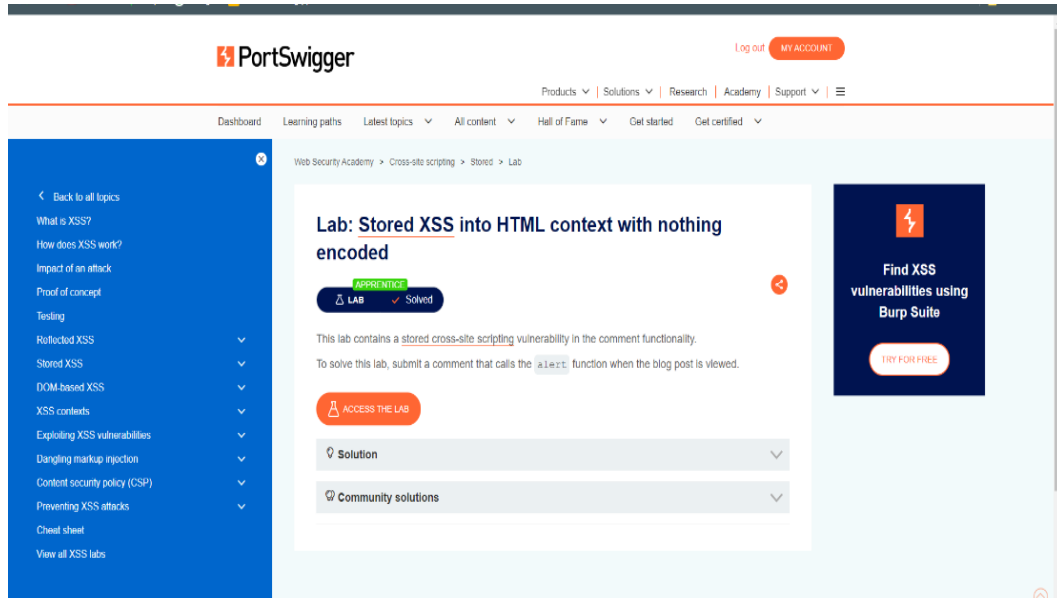


Figure 1 :-

The above Figure shows the Description of the Lab

2. Click on View Post

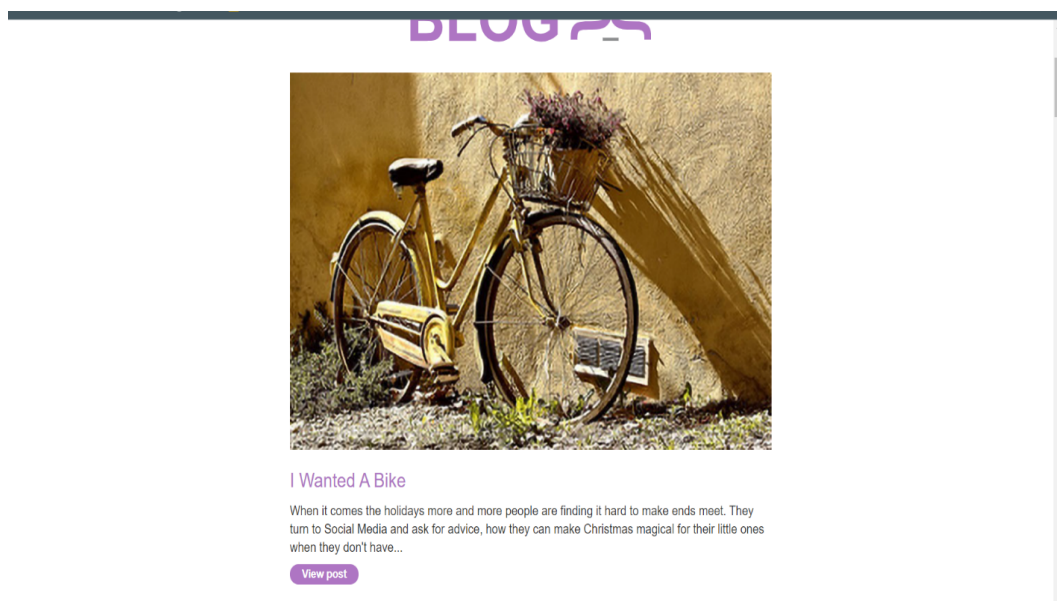
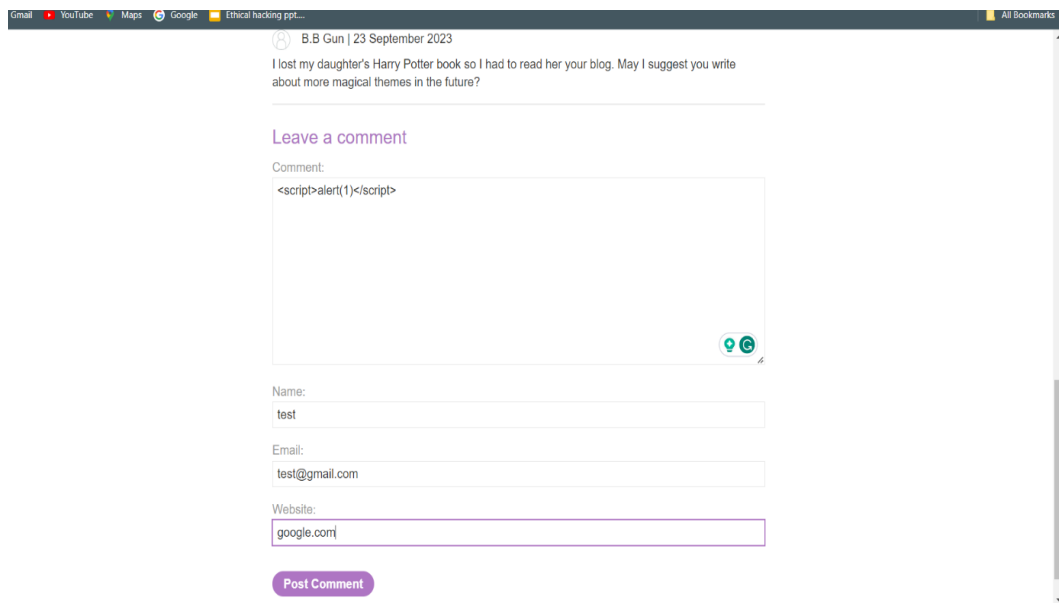


Figure 2 :-

The above figure shows that we have to click on View Post button.

3. Fill up the Details and in Comment Section Write XSS Payload “ <script>alert(1)</script> “



The screenshot shows a web browser window with a blog post by 'B.B Gun' dated '23 September 2023'. The post content is: 'I lost my daughter's Harry Potter book so I had to read her your blog. May I suggest you write about more magical themes in the future?'. Below the post is a 'Leave a comment' section. The 'Comment:' text area contains the XSS payload: '<script>alert(1)</script>'. Below the comment field are three input fields: 'Name:' with 'test', 'Email:' with 'test@gmail.com', and 'Website:' with 'google.com'. A 'Post Comment' button is at the bottom of the form.

Figure 3:-

The above figure shows that we have to fill up all the details but in comment field we have to write XSS payload

4. And the XSS will Pop up.

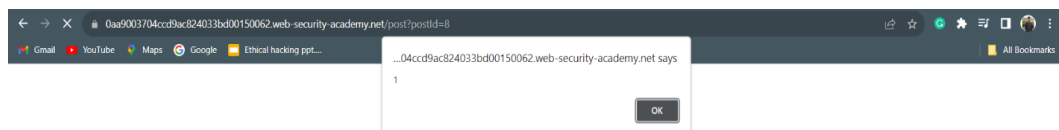


Figure 4 :-

The above figure shows that the XSS pop has come and the payload was executed successfully