CS315 · Computer Security

Lab 11

胡玉斌 / 11712121

December 7, 2020

Task 1

Posting a Malicious Message to Display an Alert Window

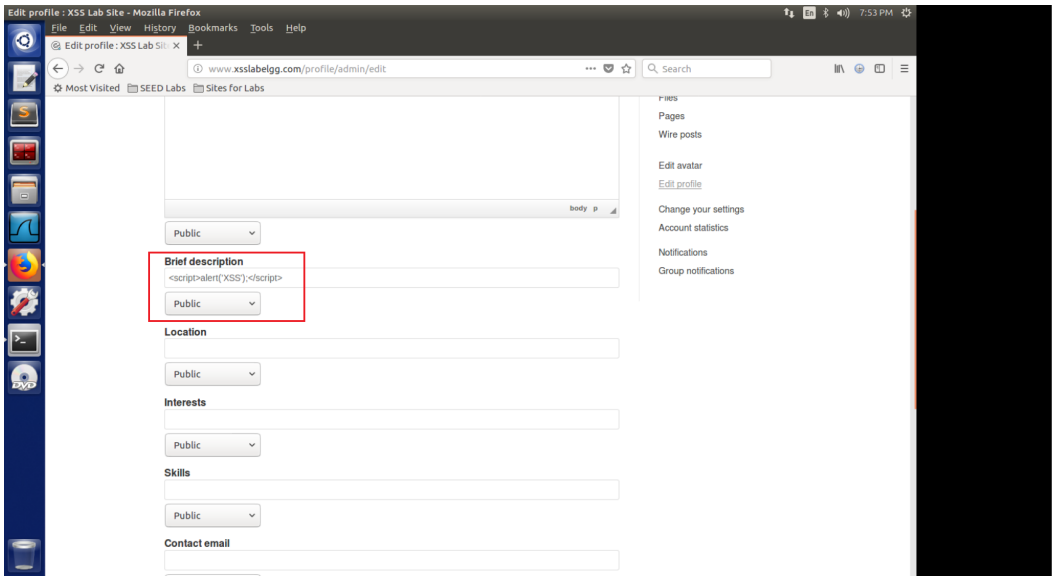

Figure 1: embed JavaScript code

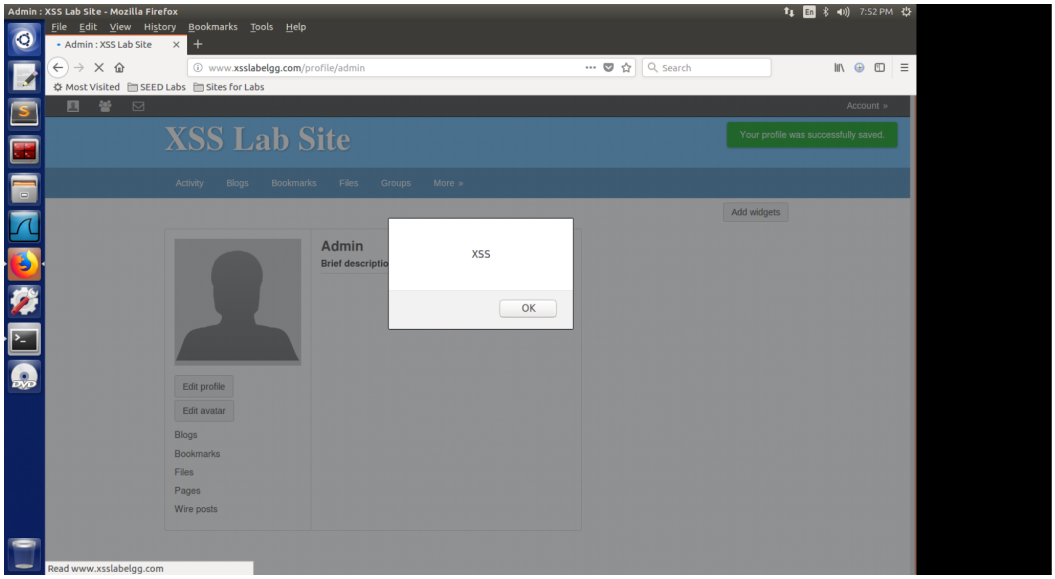

Figure 2: XSS

Task 2

Posting a Malicious Message to Display Cookies

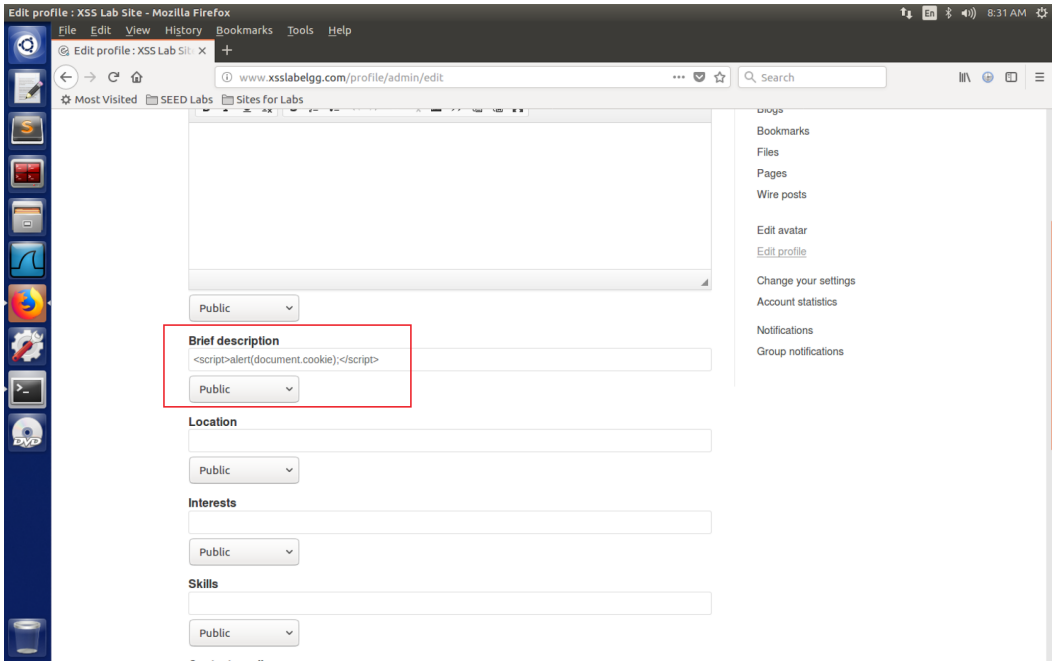

Figure 3: embed JavaScript code

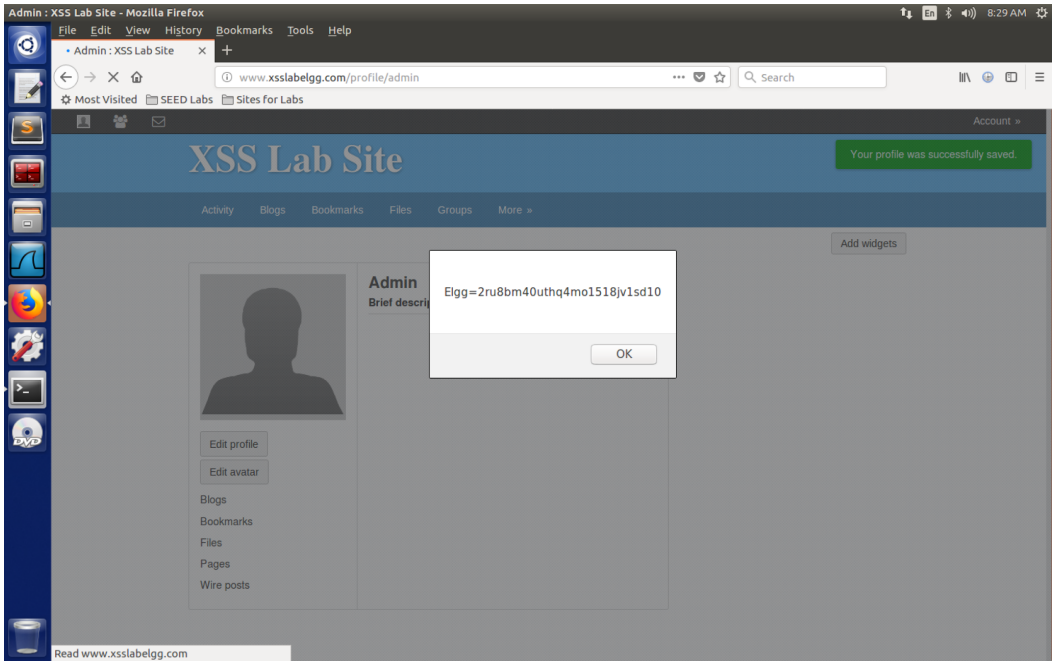

Figure 4: cookie

Task 3

Stealing Cookies from the Victim’s Machine

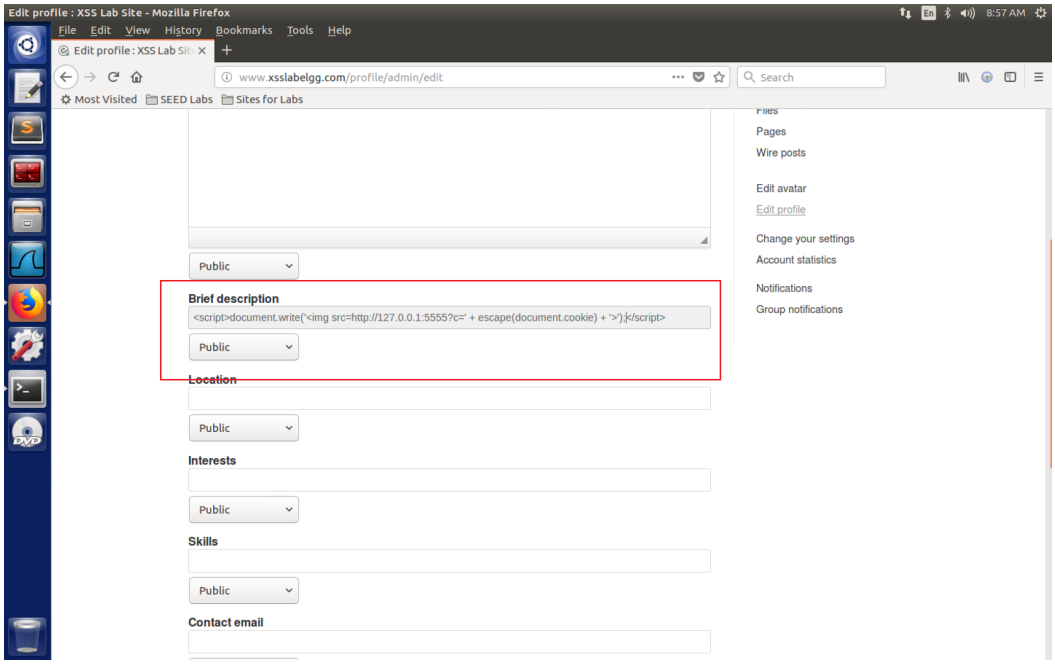

Figure 5: embed JavaScript code

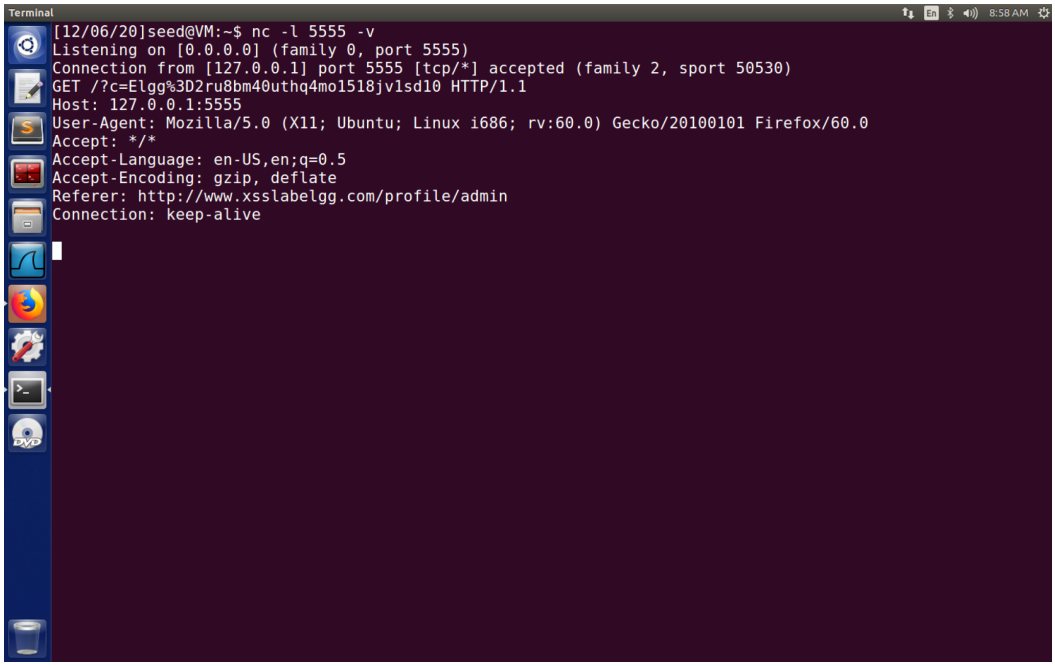

Figure 6: nc -l 5555 -v

Task 4

Becoming the Victim’s Friend

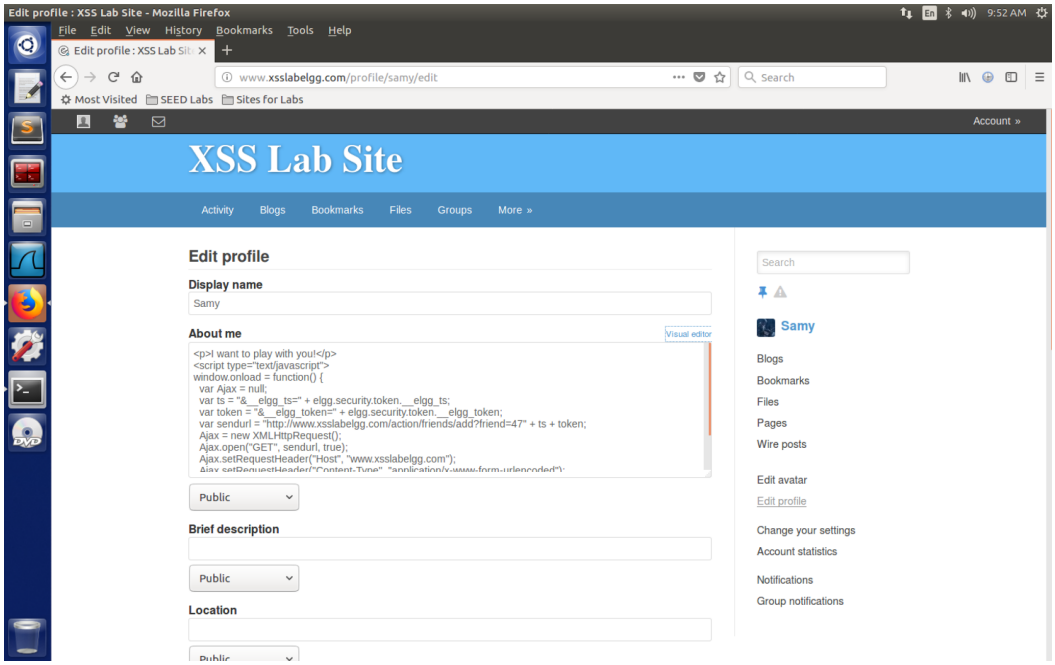

Figure 7: embed JavaScript code

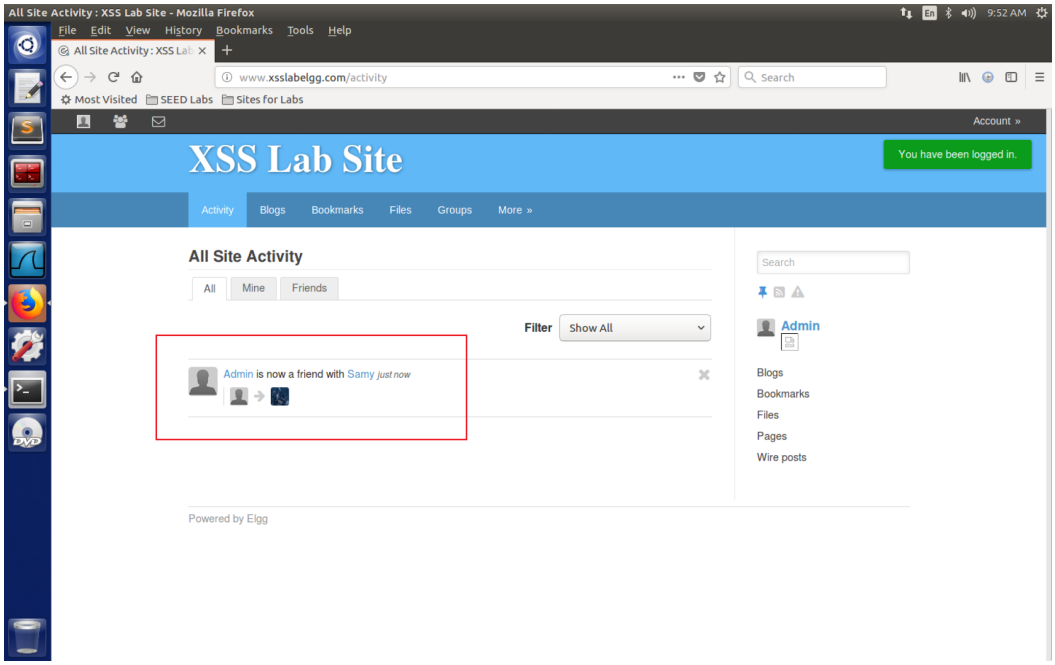

Figure 8: add friends

Q1

`ts` and `token` are used for authentication. So that the operate can be succeed.

Q2

No, we cannot launch a successful attack, because we cannot have a HTML entry in `"About me"`

Task 5

Modifying the Victim’s Profile

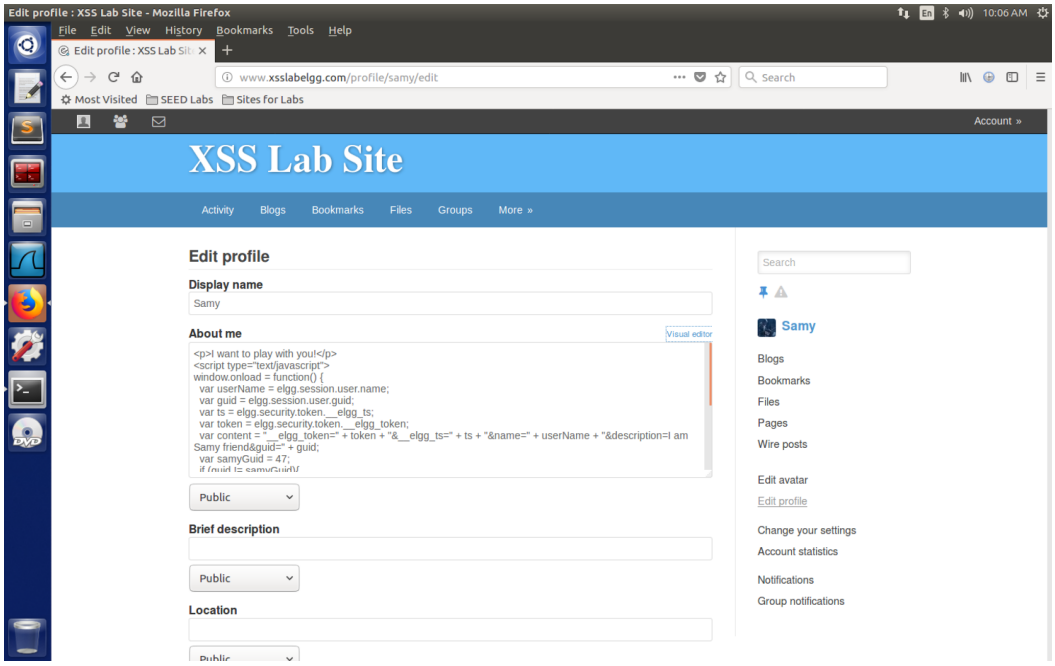

Figure 9: embed JavaScript code

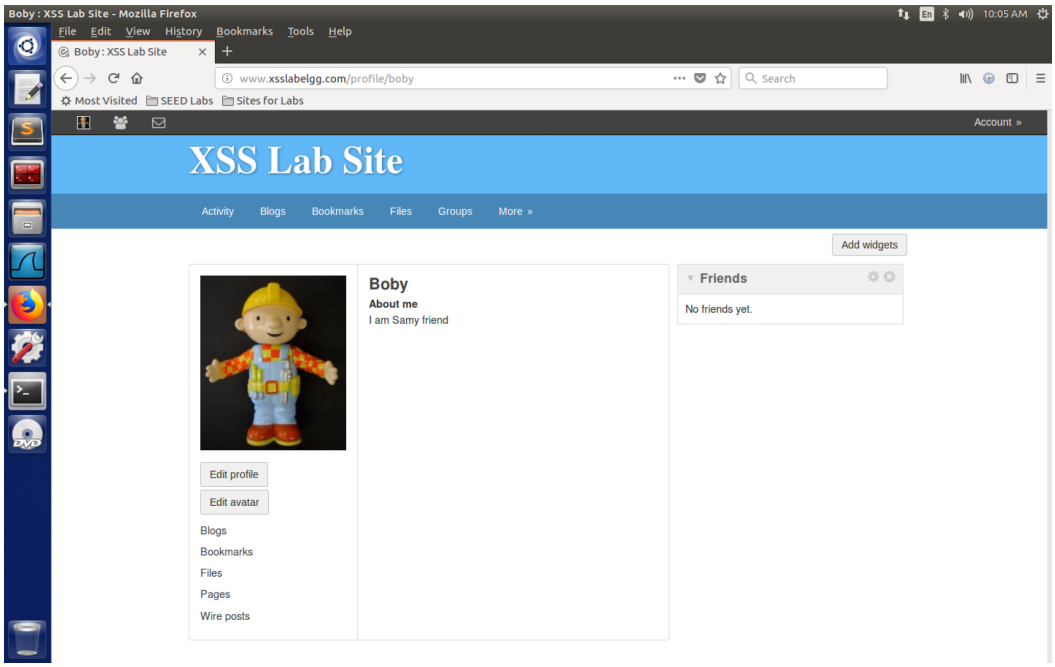

Figure 10: modify profile

Q3

This line is needed, otherwise Samy will modify his own profile and overwrite the JavaScript code.

Task 6

Writing a Self-Propagating XSS Worm

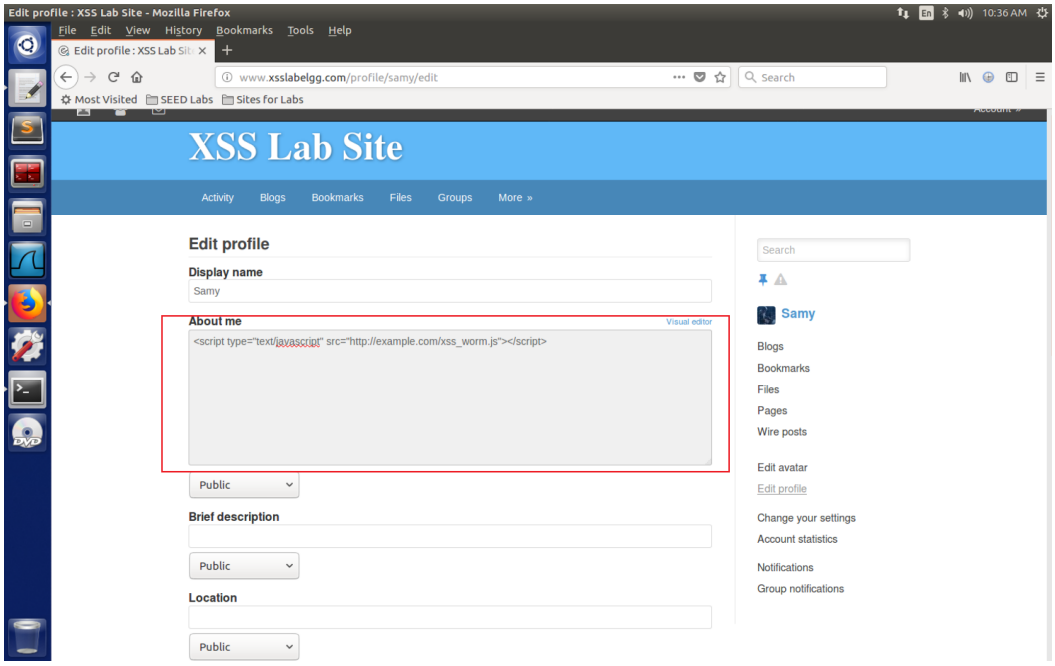

Figure 11: XSS Worm

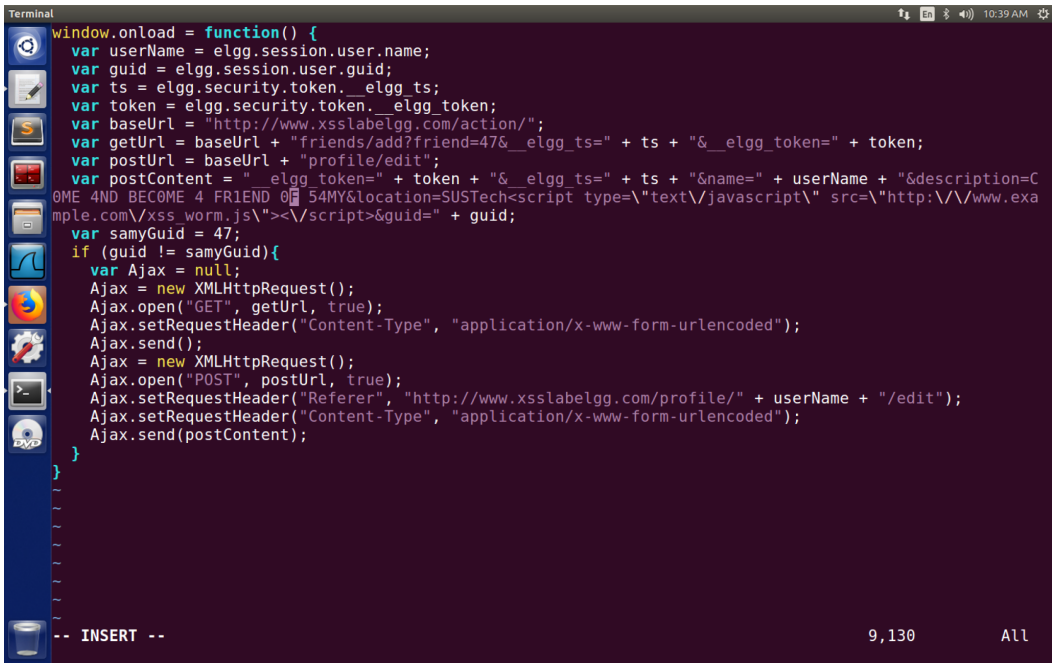

Figure 12: XSS Worme

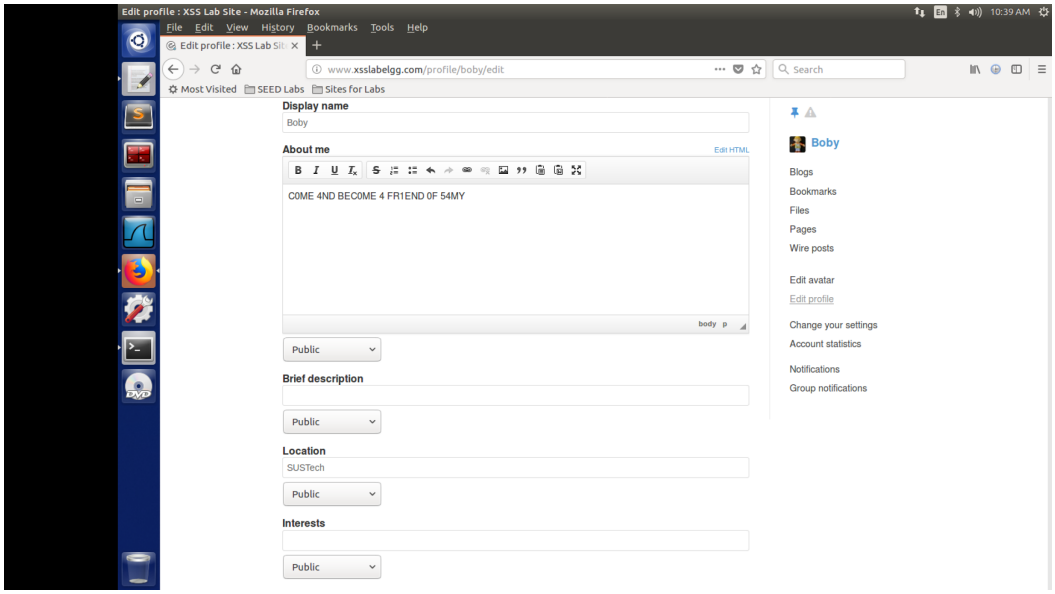

Figure 13: modify profile

Task 7

Countermeasures

- Enabling HTMLawed, the HTML tags are removed in editors
- Uncommenting htmlspecialchars , the attack no longer works.

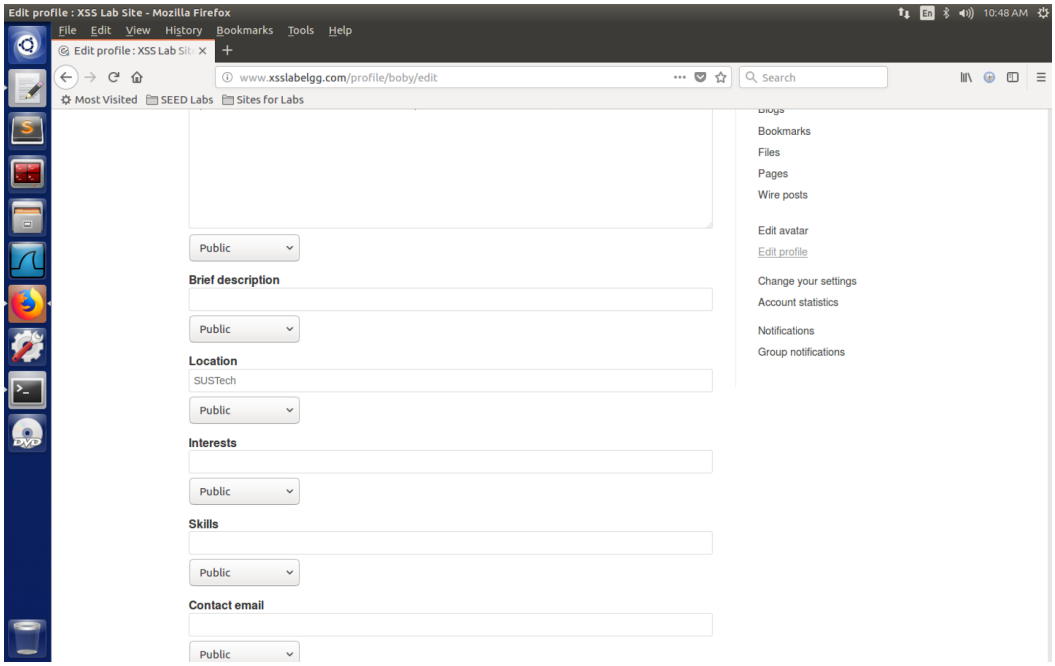

Figure 14: Countermeasures