IN5290 - Home exam 4
Web hacking 2 – Parameter tampering, Cross Site Scripting, Session hijacking – Home exam

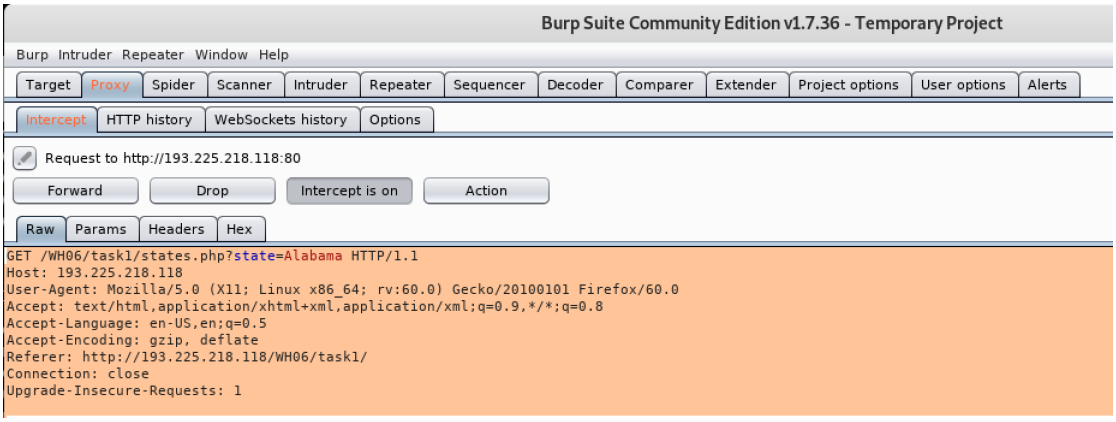
Tanusan Rajmohan - tanusanr@ulrik.uio.no

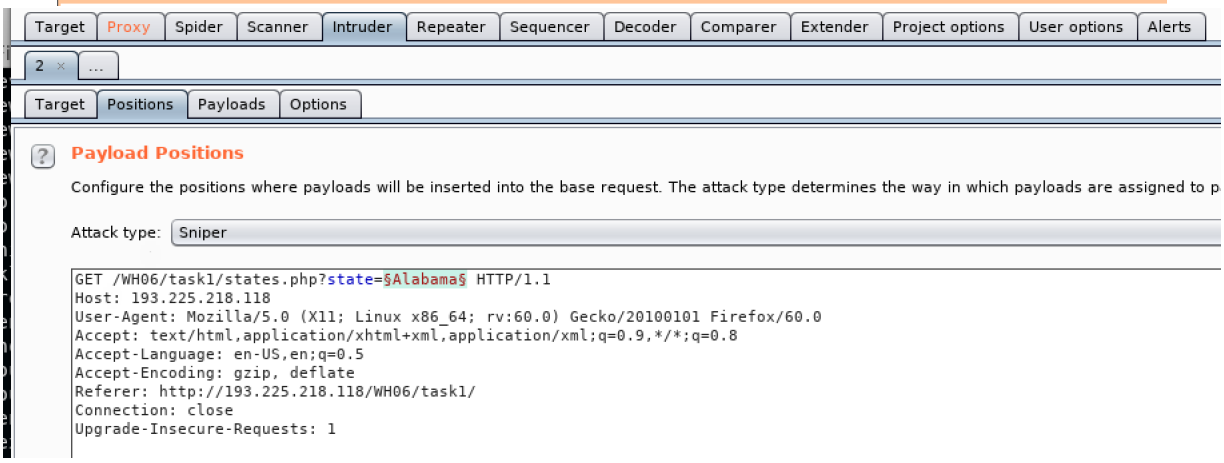
UNIVERSITETET I OSLO

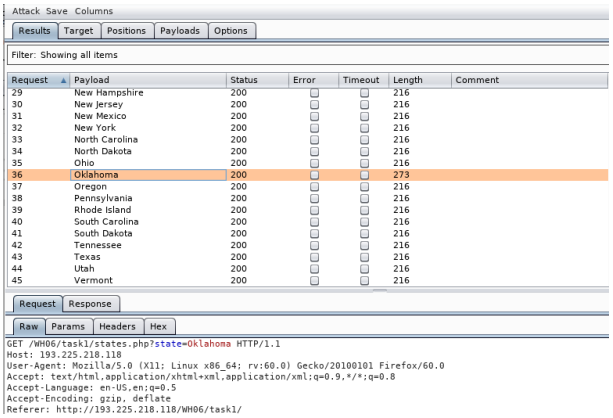
Høsten 2018

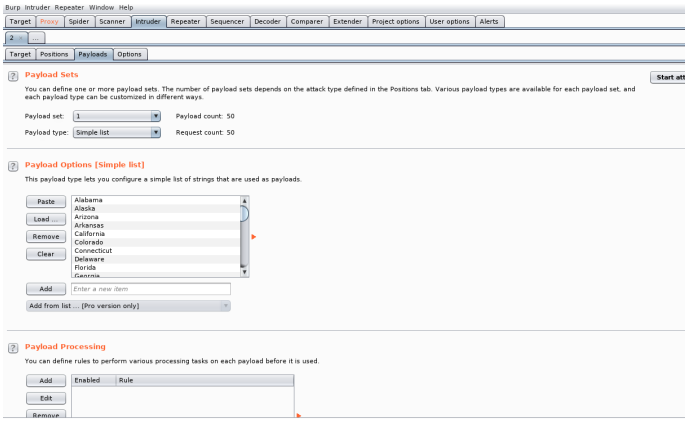
Find the flag on the site http://193.225.218.118/WH06/task1 (parameter tampering)

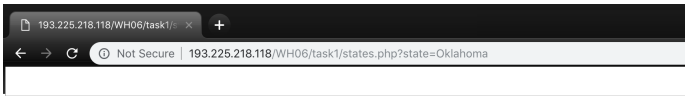
The flag is **UiOCTF{Where the Wind Comes Sweeping Down the Plain}**. This flag was found by using burp suit. I first used the proxy part to intercept the site when I clicked on a link. Then I pressed forward, so it gave me the information when a link was clicked. Then I right-clicked and sent it to 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.







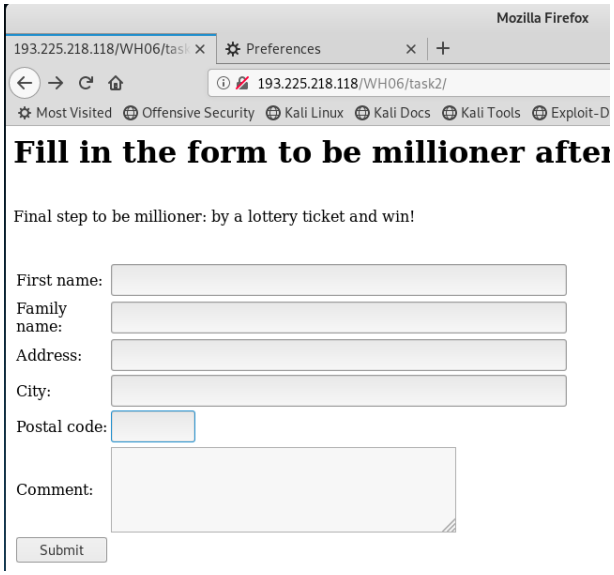


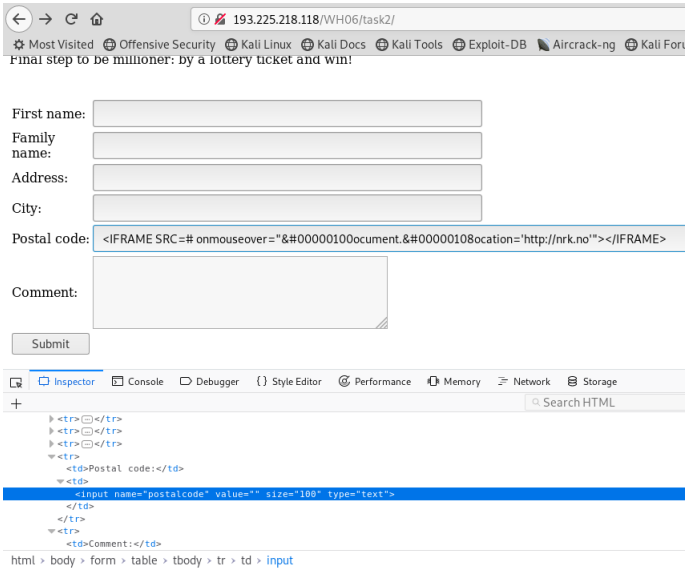


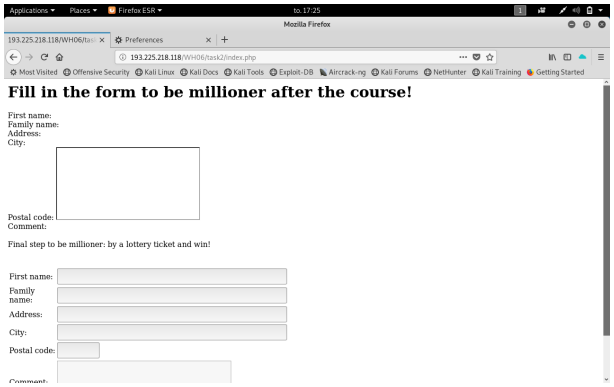
UiOCTF{Where the Wind Comes Sweeping Down the Plain}

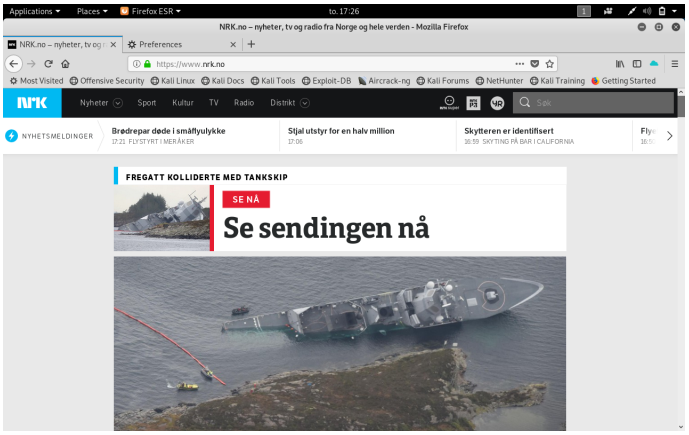
Redirect the following page to http://nrk.no (XSS) http://193.225.218.118/WH06/task2

This was done by testing a couple of scripting phrases, which lead to the command: $< IFRAMESRC = \#onmouseover = $"&#00000100ocument.&#00000108ocation =' 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 se the whole line).







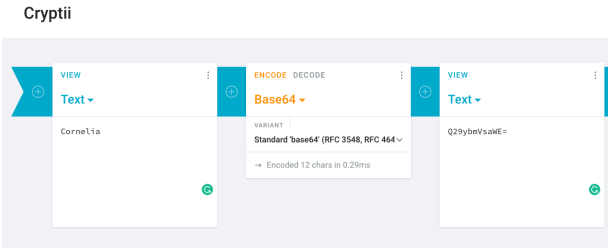


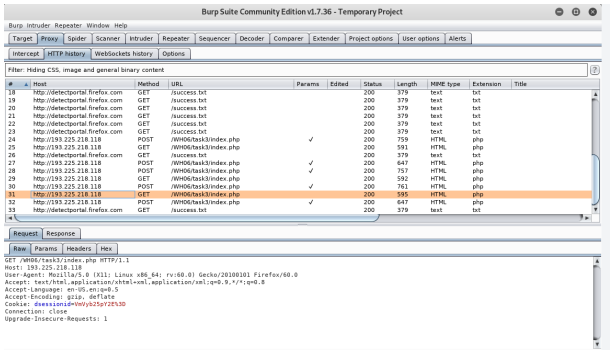
I also used these pages for look up and additional information:
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet
http://www.asciitable.com/

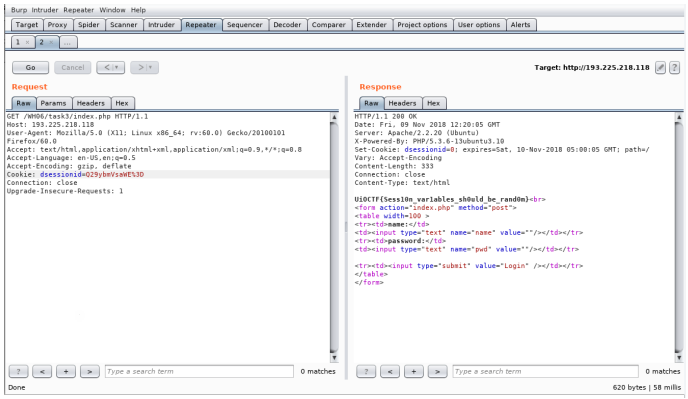
Find the flag on the site http://193.225.218.118/WH06/task3 4 users are already logged in (they have valid sessions): Nora/flowers, Stine/Hedgedog, Veronica/Halifax, Kari/sunshine There's another logged in user: Cornelia

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	$Tm9yYQ\%3D\%3D$
Stine	$U3RpbmU\%3D$
Veronica	$VmVyb25pY2E\%3D$
Kari	$S2FyaQ\%3D\%3D$
Cornelia	$Tm9yYQ\%3D\%3D$







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.