IN5290 - Home exam 5
Web hacking 3 – SQL Injection, Xpath injection, Local File Inclusion – Home exam

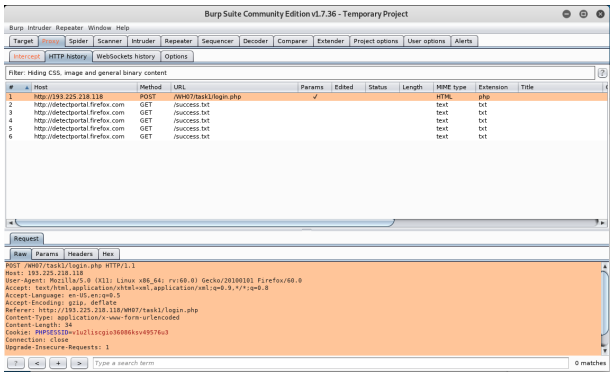
Tanusan Rajmohan - tanusanr@ulrik.uio.no

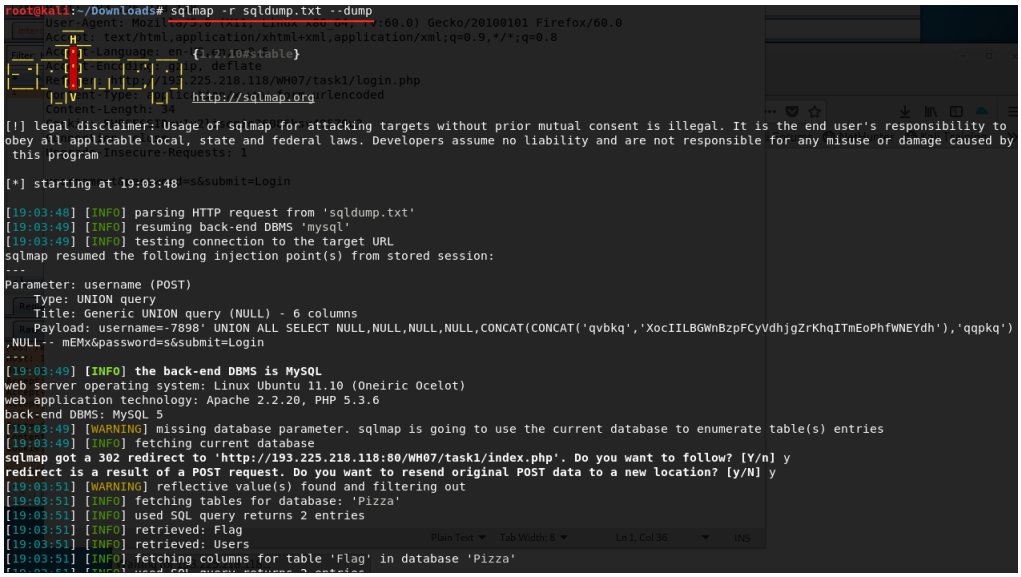
UNIVERSITETET I OSLO

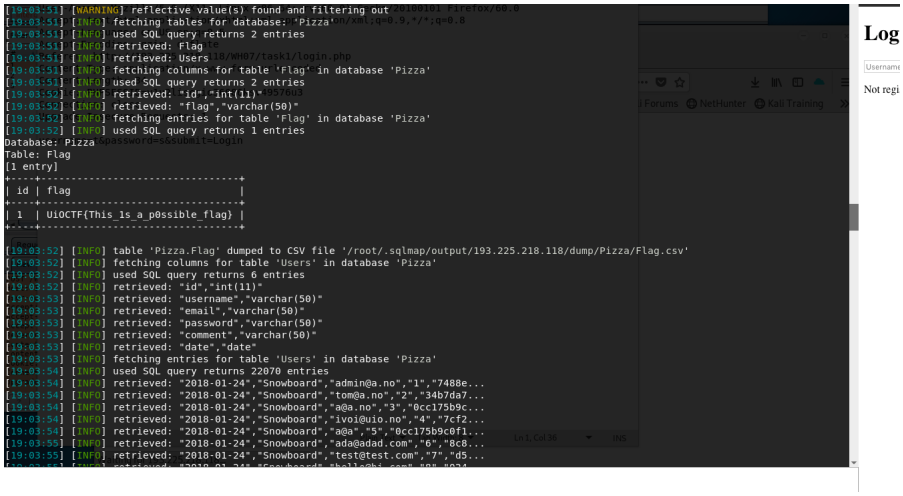
Høsten 2018

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

The flag in this assignment is: **UiOCTF{This_1s_a_p0ssible_flag}**.
This flag was found by trying different approaches, I tried blind boolean based sqli exploitation, exploitation with sqlmap and simple sql injection. None of these worked, so I tried dirb which lead to nothing. Then I used burp to see the post method and see which variables that was beeing sent. I saved the post information in a file and ran sqlmap -r with the filename which gave a lot of information and then the flag. When I used dirb, it gave me a file called "register" which downloaded a sql file wich lead me on the wrong path I think, but after using Burp I found the flag. See images below to see specific what I found, I changed the proxy to work with Burp.







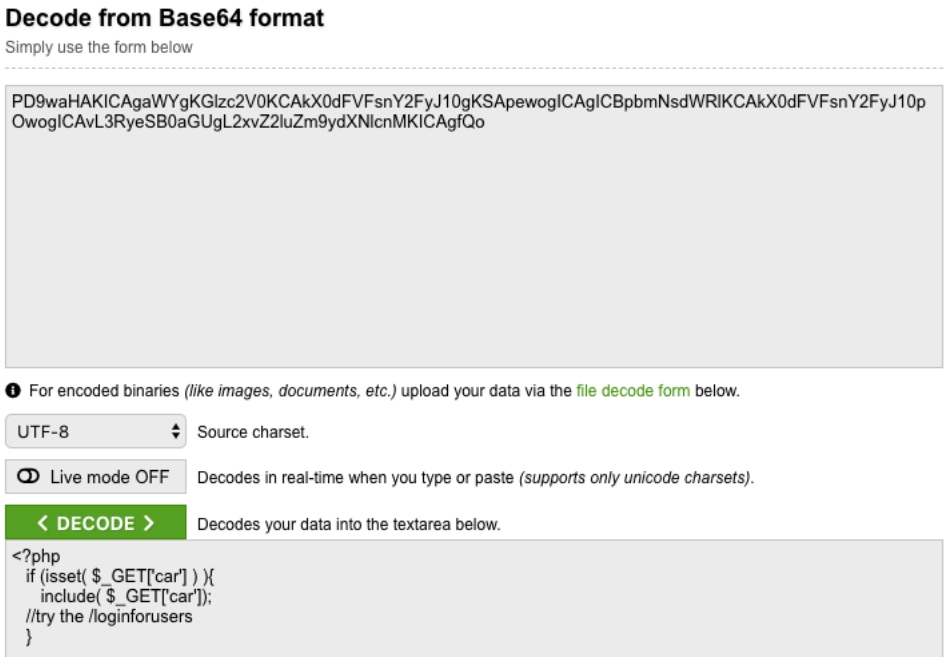
Find the flag on the site http://193.225.218.118/WH07/task2

The flag in this site is **UiOCTF{Getting_the_flag_needs_multiple_vulnerabilities_sometimes}**. This was found with a couple of steps. I first started to fool around with the webpage, then I tried the php filter and found out that the command:

$http://193.225.218.118/WH07/task2/index.php?car=php://filter/convert.base64-encode/resource=index.php$

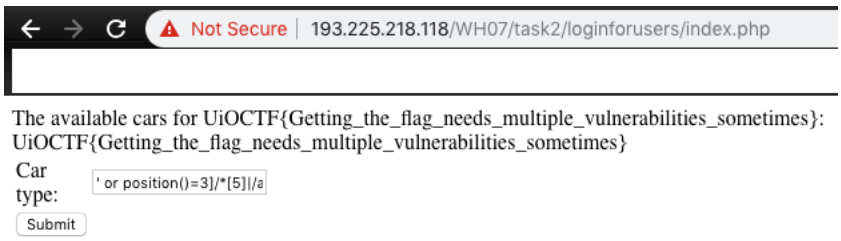
Which gave me the hash:
PD9waHAKICAgaWYgKGlzc2V0KCAkX0dFVFsnY2FyJ10gKSApewogICAgICBpbmNsdWRlKCAkX0dFVFsnY2FyJ10pOwogICAvL3RyeSB0aGUgL2xvZ2luZm9ydXNlcnMKICB9Cg==

I decoded this and got the subfolder and the message you see below.



After this I got redirected to a page to submit car types which only took "audi" in the input field. After a bit I found out that xpath injection could be used. I tried several xpath injections and ended up with sentence:

' or position()=3]/*[5]—/a['



This lead to the flag as you can see above.