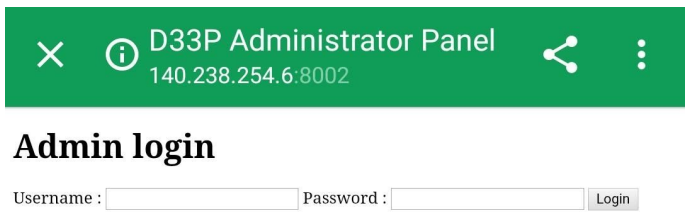
# DeepCTF - Writeup

Team WOW6 - Thanks to @dvirus @andreamarin @Jexus909

## WEB Challenges

### Oh JS! 120

This is the most secure login form on earth.
We use SECURITY BY OBSCURITY in order to prevent hackers from finding our flags.
I dare you to login.
http://140.238.254.6:8002



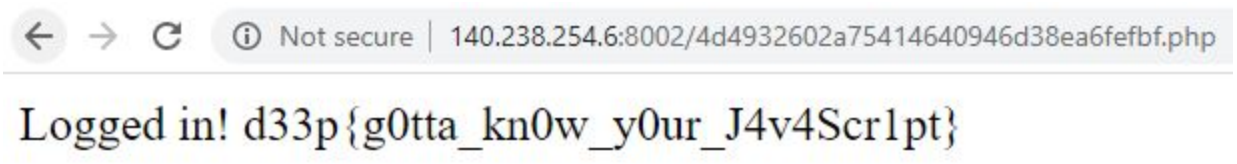

Seeking in the page's source code we can see a obfuscated code which look like:

```
function validate() {
[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]][([][(![]+[])[+[]]+([!
[]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]+[])[!+[]+!+[]+!+[]]+(!![]+[][(![]+[])[+[]
]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[+!+[]+[+[]]]+([][[]]+[])[+!+[]]+([
]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+[]]+(!![]+[])[+!+[]]+([][[]]+[])[+[]]+([][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!![]+[])[+[]]...
```

JSFuck is an esoteric and educational programming style based on the atomic parts of JavaScript. It uses only six different characters to write and execute code.
By decoding this code, credentials are obtained to enter the website

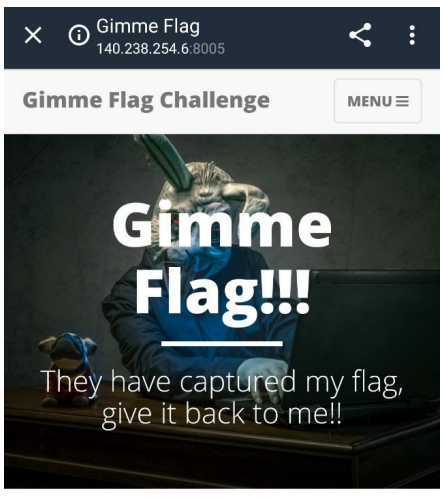
```
if (document.forms[0].username.value == "corb3nik" && document.forms[0].password.value == "chickenachos") document.location =
"4d4932602a75414640946d38ea6fefbf.php"
```

So that we got our flag:




### Did You Got Trolled? 120

An army of hackers has stolen the flag from our rabbits. Security experts have failed to capture the flag and some have even gone mad.
Please…GIMME THE FLAG!!
http://140.238.254.6:8005




**Follow the White Rabbit releases his first CTF Challenge!**

Comments in the code can be good development practice, but sometimes they reveal filenames, links, usernames or, in this case, our key1:

```
/*
 * What is this doing here?
 * Key1 = gimme0x.....
 */
```

Each post directs redirect to the following URL: http://140.238.254.6:8005/post.html again, looking in the source code we get a hint:

```
<span class="subheading">deep.php?page=debug.html</span>
<!--Creds in /home/ubuntu/key2.txt -->
```

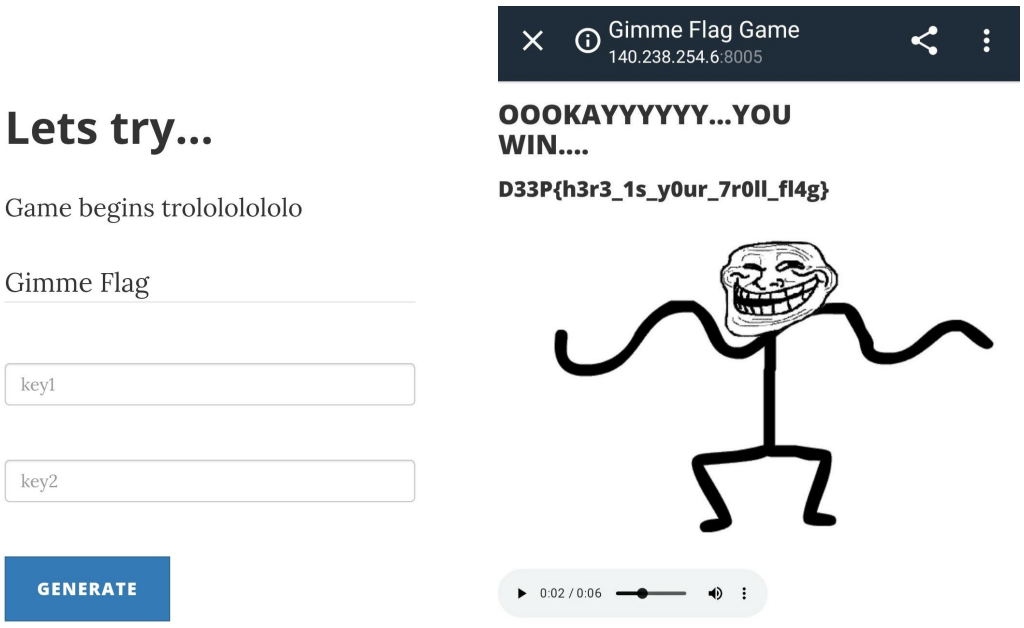
So, with LFI we got our second key:




**MAINTENANCE**

**key2 = flag0x085927**

with these values we obtained the flag:




Claro que si, guapi http://140.238.254.6:8005/img/guapi.mp3 xD

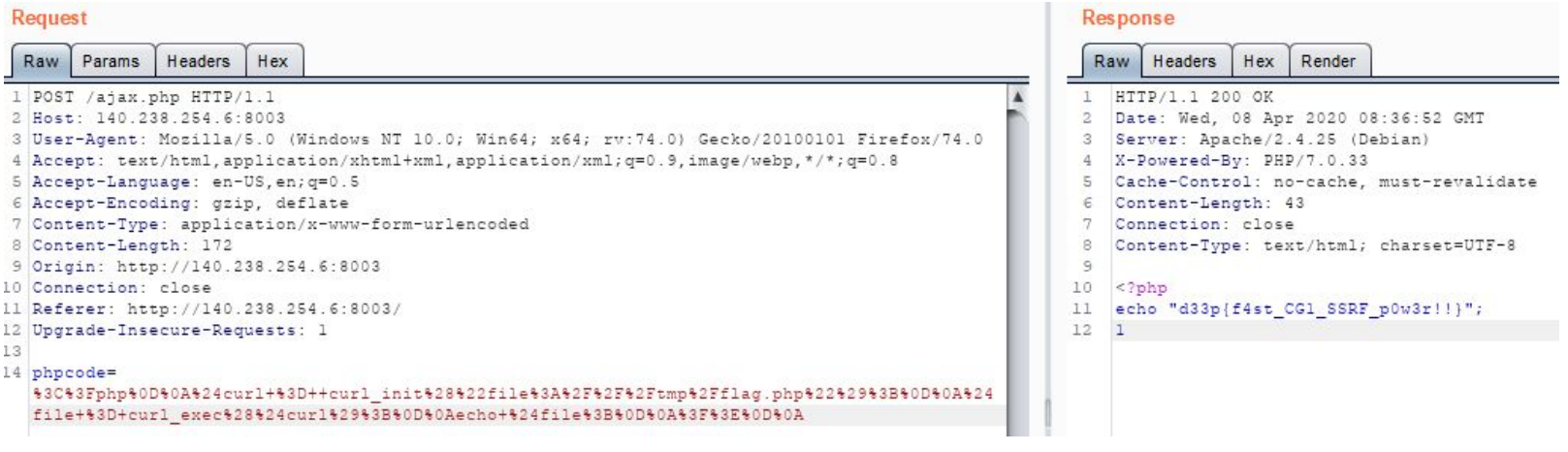
## Nothing is Impossible 160

One of our rabbits has lost the keys of his server to access his flag. He is crying desperately as he only remembers that the flag was in the path: /tmp/flag.php but he don't know how to get there. Our friend BugsBunny was performing reconnaissance tasks when suddenly found a web that could help you, please bring me back his flag.
Author; whitex
http://140.238.254.6:8003

In this challenge, we know it's about LFI the first step is to check if file exists:


and then I tried to get the file's content:


Apparently it is an LFI but the server but the inclusion was done using the require_once function of PHP, hence, I used cURL to bypass this filter so that I could read the flag:



# CRYPTO Challenges

## WarmUp 50

Get Ready For Crypto Fight. Here A Challenge Just For Your WarmUp.

File: w4rmup.txt

Content: 64 33 33 70 01111011 01001010 01110101 00110101 01110100 01011111 00110100 01011111 01001110 00110000 01110010 01101101 00110100 01101100 95 67 104 52 108 108 95 95 111 163 156 140 164 137 61 164 77 175
Solution: In order to get the flag the text was decoded using HEX, Binary, and Ascii Table
d33p{Ju5t_4_N0rm4l_Ch4ll__Isn`t_1t?}

## Ali3nAgain 100

SPD force needs your help again...!!!!
Flag Format: d33p{UPPERCASE}
File: spdvsalien.png
Solution: Use **https://www.dafont.com/es/futurama.font**
d33p{POWERRANGERSPDFORCEWON}

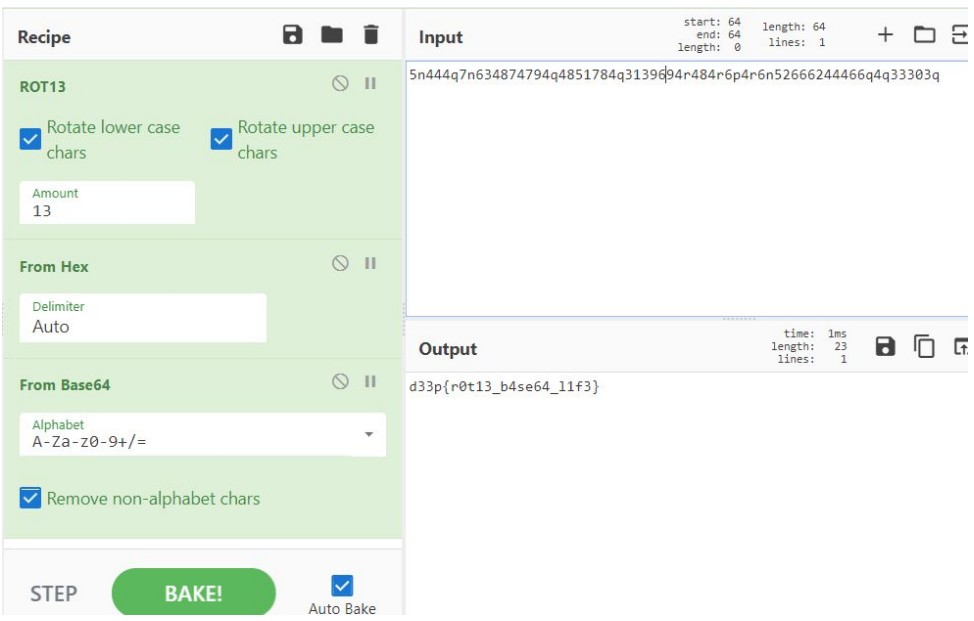
## WierdText 100

I Need A New Keyboard..!!
File: w1erdc1ph3r.txt
Content: c4co"Lct5-vec+H2efw)G-"Ve+$2;5zeef+
Solution: Keyboard Shifting Cipher consists in typing a letter close to another on a computer keyboard. The shift can be on the right, the left, up or down.
d33p{K3yb04rd_N33ds_T0_B3_R3p41r3d}

# MISC Challenges

## Weirdo 120

We got some wierdo text, we need to decode it to read the secret flag. I think you can do it. I tried my best but didn't get anything.
File: w1erdc1ph3r.txt
Content:
5nd33p44d33p4qd33p7nd33p63d33p48d33p74d33p79d33p4qd33p48d33p51d33p78d33p4qd33p31d33p39d33p69d33p4rd33p48d33p4rd33p6pd33p4rd33p6nd33p52d33p66d33p62d33p44d33p46d33p6qd33p4qd33p33d33p30d33p3q
Hint: 13 - 0x - 64
Solution: In order to get the flag the text was decoded using ROT13, HEX and Base64




# OSINT Challenges

## History 80

Where did it happen?
'Drunk Hackers'
P.S. Hackers love that place
Flag format - d33p{xxxxxx}
Solution: Drunk Hackers History is a famous space at DefCon @DrunkHackerHist
d33p{defcon}