**BITS3613 HACKING TECHNIQUES AND PREVENTION**

NAME: WAN MOHAMMAD FAISAL BIN SAMMIO

MATRIC NO: 3-BITZ B031720043

**Project**

**Hack The Box Instruction Report**

Contents

[Project : Hack The Box Instruction Report 4](#_Toc11406169)

[README FIRST!!! 4](#_Toc11406170)

[HTB – INVITE CODE 4](#_Toc11406171)

[MACHINE GAME 6](#_Toc11406172)

[1. ACTIVE MACHINE NETMON = 20 Points 6](#_Toc11406173)

[CHALLENGE GAME 7](#_Toc11406174)

[CRYPTO CHALLENGES 7](#_Toc11406175)

[1. KEYS = 40 POINTS 7](#_Toc11406176)

[2. DECEITFUL BATMAN = 10 POINTS 7](#_Toc11406177)

[3. CLASSIC YET COMPLICATED = 10 POINTS 8](#_Toc11406178)

[4. YOU CAN DO IT! = 10 POINTS 8](#_Toc11406179)

[5. BRAINY'S CIPHER = 30 POINTS 9](#_Toc11406180)

[6. \*INFINITE DESCENT\* = 90 POINTS 10](#_Toc11406181)

[7. \*EBOLA VIRUS =100 POINTS 12](#_Toc11406182)

[FORENSIC CHALLENGE 14](#_Toc11406183)

[1. MARSHALL IN THE MIDDLE = 40 Points 14](#_Toc11406184)

[2. DEADLY\_ARTHROPOD = 40 Points 17](#_Toc11406185)

[MISC CHALLENGE 18](#_Toc11406186)

[1. FSOCIETY = 30 POINTS 18](#_Toc11406187)

[2. INFERNO = 20 POINTS 18](#_Toc11406188)

[3. ART = 20 POINTS 19](#_Toc11406189)

[4. MISDIRECTION = 20 POINTS 20](#_Toc11406190)

[5. OLD IS GOLD = 10 POINTS 21](#_Toc11406191)

[6. BLACKHOLE = 20 POINTS 22](#_Toc11406192)

[7. LONGBOTTOM'S LOCKER = 20 POINTS 24](#_Toc11406193)

[8. ETERNAL LOOP = 20 POINTS 25](#_Toc11406194)

[REVERSING CHALLENGE 26](#_Toc11406195)

[1. IMPOSSIBLE PASSWORD = 30 POINTS 26](#_Toc11406196)

[2. SNAKE = 10 Points 26](#_Toc11406197)

[STEGO CHALLENGES 28](#_Toc11406198)

[1. FOREST = 40 POINTS 28](#_Toc11406199)

[2. RETRO = 50 Points 29](#_Toc11406200)

[3. DA VINCI = 30 Points 30](#_Toc11406201)

[4. DIGITALCUBE = 60 Points 32](#_Toc11406202)

[5. BEATLES = 40 Points 33](#_Toc11406203)

[6. UNIFIED = 20 Points 34](#_Toc11406204)

[7. PUSHEEN LOVES GRAPHS = 30 Points 35](#_Toc11406205)

[8. SENSELESS BEHAVIOUR = 50 Points 36](#_Toc11406206)

[WEB CHALLENGES 38](#_Toc11406207)

[1. HDC = 30 Points 38](#_Toc11406208)

[2. CARTOGRAPHER = 30 POINTS 41](#_Toc11406209)

[3. LERNAEAN = 20 POINTS 42](#_Toc11406210)

[4. \*I KNOW MAG1K\* = 50 Points 43](#_Toc11406211)

# Project : Hack The Box Instruction Report

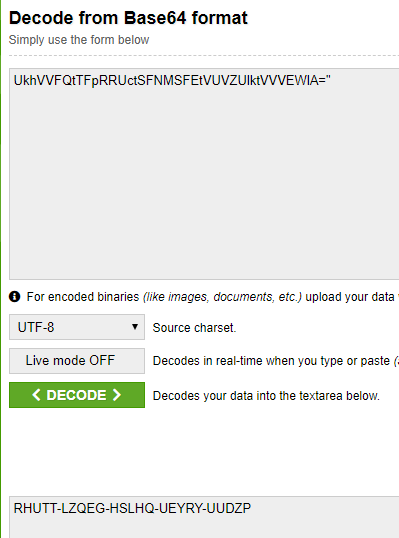
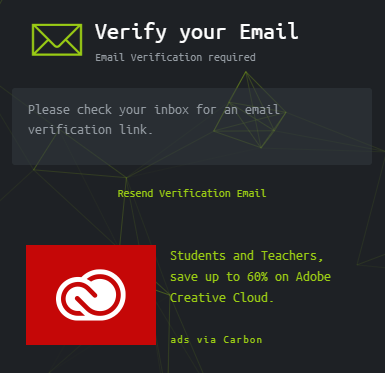
## README FIRST!!!

HTB has 2 type of games; Machine and Challenge. The Machine game is like attack and defence style. I need to hack the active machine to get 2 flags (user.txt and root.txt). User.txt file is a user flag that mean the user account has been pawned and root.txt file is mean a root account/machine has been pawned/owned. The second game is Challenge game that is likely to CTF style. In this challenge, I have to get the flag in the format of **HTB{flag\_here}**. Some of the challenge flags I just take screenshot to prevent from directly copy and paste of the flags from 3rd party. I have solved 31 challenges and 1 active machine recently.

## HTB – INVITE CODE

1. Go to inviteapi.min.js in developer mode
2. Search for makeInviteCode() and press enter.
3. You will get {  
    "0": 200,  
    "success": 1,  
    "data": {  
    "data": "SW4gb3JkZXIgdG8gZ2VuZXJhdGUgdGhlIGludml0ZSBjb2RlLCBtYWtlIGEgUE9TVCByZXF1ZXN0IHRvIC9hcGkvaW52aXRlL2dlbmVyYXRl",  
    "enctype": "BASE64"
4. Decode the data string base64 and we will get “In order to generate the invite code, make a POST request to /api/invite/generate”.
5. Open terminal and type curl -i -X POST <https://www.hackthebox.eu/api/invite/generate>



1. Decode the data string again and you will get the invite code in plain text..
2. Input the invite code and insert your detail and verify the email.

## MACHINE GAME

### ACTIVE MACHINE NETMON = 20 Points

|  |  |  |
| --- | --- | --- |
| 1 | First nmap the target machine. We discover open port 21 ftp. |  |
| 2 | Go to web browser and get to ftp://10.10.10.152 and click Users |  |
| 3 | Then, go to Public folder |  |
| 4 | Then, click **user.txt** to get the user flag |  |
| 5 | Yes, it is valid user flag and submit to HTB. I need to get root.txt to own the system. But, i did not managed to get root yet. |  |

## CHALLENGE GAME

## CRYPTO CHALLENGES

### KEYS = 40 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | The challenge contains an encrypted message |  |
| 2 | After googling in the forum, it is fernet encryption. So, go to <https://asecuritysite.com/encryption/ferdecode> and decode it. |  |
| 3 | Insert the token and key. Boomm!!  HTB{N0t\_A\_Fl1g!} |  |

### DECEITFUL BATMAN = 10 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | First unzip the folder and we found finale.txt file..it is baconian cipher exactly.. |  |
| 2 | Decode it online and get the flag. Put in htb format..HTB{NAPIER} |  |

### CLASSIC YET COMPLICATED = 10 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Unzip the folder and got ciphertext.txt..it is classic vigenere cipher |  |
| 2 | Decode it online and get this output. The hint is “the key is the flag”!! |  |
| 3 | The key is the flag..so put in the HTB flag format | HTB{helloworld} |

### YOU CAN DO IT! = 10 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Unzip and get the you\_can\_do\_it.txt file. It is unscramble text. Go and search for the tool online. |  |
| 2 | Decode it online..it is simple crack actually.. YOUSEETHATYOUCANDOIT! | HTB{YOUSEETHATYOUCANDOIT!} |

### BRAINY'S CIPHER = 30 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Unzip and got brainy.txt. It might be brainfuck encoder. |  |
| 2 | Decode the brainfuck and you will get this..it has p value,q ,dp,dq,c value respectively. |  |
| 3 | Get the rsa decoder in python online and insert the p,q,dp,dq,c value to decode the flag. |  |
| 4 | Decode it and flag appear. Put in htb format. |  |

### \*INFINITE DESCENT\* = 90 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Take a look at email.msg file. We have public key and message there. We can find the private key with help of public key…. |  |
| 2 | This is the decoded public key from ASN.1 JavaScript decoder online. |  |
| 3 | Then go to <http://www.mickybullock.com/blog/wp-content/RSA_Cryptography/ffactory.php> to find the factor of above number. Then we got the p,q number based of N. |  |
| 4 | Next, use the given fasterprimes.py and insert the p and q value based on above decoder. |  |
| 5 | Run fasterprimes.py and we got the decrypted message. |  |
| 6 | Go to given AESbootstrap.py and insert the decrypted message and do some coding. |  |
| 7 | So that script outputs a binary for each number. Hmmm |  |
| 8 | Lets convert the binary into ASCII. Here the result. It look like base64 format. |  |
| 9 | Decode it and get the flag. Put flag in the format of HTB{flag}. yesss!! |  |

### \*EBOLA VIRUS =100 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Go to <https://www.cryptool.org/en/cto-cryptanalysis/n-gram-analysis> to do frequency analysis and put the encrypted data. |  |
| 2 | We got this output.. |  |
| 3 | <https://www.semanticscholar.org/paper/Case-sensitive-letter-and-bigram-frequency-counts-Jones-Mewhort/722e190eed82279552905cb8ff8ac4967bacb04f> to get this |  |
| 4 | Then i try google for hints and got the sentence nearly same as the text from above. |  |
| 5 | This will help us a lot. So, more modifications and we got this. Looks like the flag is at the bottom. |  |
| 6 | 'N' should be a line break and we know that the flag format is HTB {flag}. Therefore, 'W' and 'J' can be easily substituted. But it looks like unreadable text. I try this flag and it failed. So it is not the flag. Need some modification. |  |
| 7 | 'M' looks like an underscore. And the flag reads something like '...know how to control...'. So, a bit more logical analysis and trial and errors, end up with the correct flag. |  |

## FORENSIC CHALLENGE

### MARSHALL IN THE MIDDLE = 40 Points

|  |  |  |
| --- | --- | --- |
| 1 | First, open the pcap file with NetworkMiner and i found anomalies here..it ARP spoofing |  |
| 2 | It has MAC address 080027D39CF8 and IP 10.10.99.42. Let’s find out. It is windows OS and has open port of TCP 53,TCP 443. |  |
| 3 | It fishy here. At host tab, I found linux machine? It maybe an attacker with Kali OS. it also has outgoing session to 10.10.99.42 TCP 53. It could be related to windows OS. |  |
| 4 | At the session tab, i found client host with 10.10.100.43 and 10.10.20.13(attacker might be) |  |
| 5 | So, i check who is 10.10.100.43 and it is Windows. It has outgoing session to 10.10.99.42 TCP 443. |  |
| 6 | After analyzing, 10.10.99.42 is a production web server.  10.10.100.43 is a client communicate with production web server. 10.10.20.13 is the attacker. The title look like MITM case. Question say “any data was stolen from web server”. | client<-->attacker<-->web server |
| 7 | Now let open pcap file with wireshark. That say traffic is encrypted with SSL/TLS, let decrypt the SSL protocol in wireshark with the key in secret.log |  |
| 8 | now , let filter ip add of attacker and look the first packet of filter list has TCP 53. Let check it out. select follow > TCP stream |  |
| 9 | Attacker have accessed credit card info detail. |  |
| 10 | we know that there was a POST call made, lets add that to the filter by ip.addr == 10.10.20.13 && http.request.method == POST |  |
| 11 | It seen 3rd packet has large number of length. Take a look at http stream and voilaa. The flag!!!!!!!!!! |  |

### DEADLY\_ARTHROPOD = 40 Points

|  |  |  |
| --- | --- | --- |
| 1 | use tshark to strip out only the keyscans. Then we got the keystroke at outputfile043.txt |  |
| 2 | clear out empty whitespaces from the capture file by “cat outputfile043.txt | awk 'NF' > pipe;cat pipe > outputfile043.txt” |  |
| 3 | I got python script from github to convert the keystroke. |  |
| 4 | After convert, i got this.. |  |
| 5 | ***follow the keystrokes, '<' is left arrow, and '>' is right arrow.*** |  |
| 6 | If follow the keystroke correctly will get the final flag. | HTB{If\_It\_Quack5\_It'5\_a\_K3yb0ard...} |

## MISC CHALLENGE

### FSOCIETY = 30 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Crack the zip with fcrackzip |  |
| 2 | Extract new file and show it.. |  |
| 3 | Decode it with base64 and the output is binary |  |
| 4 | Decode the binary to text and Here the flag...put in HTB format |  |

### INFERNO = 20 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | decode the inferno.txt message to base64 and here is output |  |
| 2 | Then convert the output to Malbolge programming language and the flag is appear.  **HTB{!1t\_1s\_just\_M4lb0lg3\_l4ngu4g3!}** |  |

### ART = 20 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | It is a piet program image.. |  |
| 2 | So, decode it with tool online <https://www.bertnase.de/npiet/npiet-execute.php> and flag is here. |  |

### MISDIRECTION = 20 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Extract the folder and delete the folder that has no file in each folder |  |
| 2 | Show the hidden file. From here you need to arrange the number and decode to get the flag. Let say 1=S, 2=R, 3=R and so on.. |  |
| 3 | After arrange it look like this |  |
| 4 | Then decode base64 as usual and…. |  |

### OLD IS GOLD = 10 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Crack the pdf first and found the passwd. |  |
| 2 | The output of the cracked pdf file. Wait it has small morse code below the image..so enlarge it and decode it. |  |
| 3 | Decode the morse code and flag is here. Put in the correct format HTB{}... |  |

### BLACKHOLE = 20 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Determine type of file and rename to correct file type. It is jpeg |  |
| 2 | That is the correct file type appear. |  |
| 3 | Steghide the file with correct password is hawking. |  |
| 4 | Steghide extract it and flag.txt appear in base64. Decode flag.txt in 2 times until caesar cipher text appear. |  |
| 5 | This is the caesar cipher text after converting from base64 in 2 times. |  |
| 6 | Flag after decrypting from cipher text |  |

### LONGBOTTOM'S LOCKER = 20 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | File all to view file type |  |
| 2 | We apply convert and We see that both files have different sizes, so we apply binwalk with -e. A folder \_socute.jpg.extracted a file named 'donotshare' that contains a strange text |  |
| 3 | I came to the conclusion that it is a banner and should be used python pickle: save this code as pick.py and convert the donotshare file. |  |
| 4 | The output is ... |  |
| 5 | Then go to index.html and insert the output as password to get this flag. |  |

### ETERNAL LOOP = 20 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | First, must make a script / program to decompress recursively inside the zip files. Go online and search for the script. |  |
| 2 | Run the script and found the last zip. The last zip dont found the passwd. So had to crack |  |
| 3 | Run fcrackzip for the last zip and get the passwd. |  |
| 4 | Go to the last zip and enter the sqlite3 database and find the flag. |  |

## REVERSING CHALLENGE

### IMPOSSIBLE PASSWORD = 30 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Make a script with the enc and xor\_key |  |
| 2 | Flag appear!! |  |

### SNAKE = 10 Points

|  |  |  |
| --- | --- | --- |
| 1 | In the python code, we know that slither has username |  |
| 2 | So convert the “aa + db + nn + ef + rr + gh + lr + ty” to (\x61\x6e\x61\x63\x6f\x6e\x64\x61) |  |
| 3 | Decode the Hex value to ASCII and value is anaconda. It is for username. |  |
| 4 | Decode all the Hex value to get hint for the question. On the right are the converted hex. | 1. Chains = this is a troll (15) 2. Keys = password (10) 3. Password = its not that easy 4. Auth = keep trying |
| 5 | Add this code to get the password |  |
| 6 | Run the snake.py and we get 25 characters of password but the hint said it is 10 chars long. So take only first 10 chars which is **udvvrjwa$$** and we get the right password.  The flag is **HTB{anaconda:udvvrjwa$$}** |  |

## STEGO CHALLENGES

### FOREST = 40 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | Open the image and brighten it in Image Magick to discover hidden text. Here the hidden text. |  |
| 2 | Run command “steghide extract -sf forest.jpg” and enter the passphrase as the hidden text. |  |
| 3 | after success you see nothinghere.txt and open it and copy the text to decode it. |  |
| 4 | Go to <https://www.dcode.fr/caesar-cipher> and paste the text to decode. The shift key is 13. |  |
| 5 | Then see the flag in format HTB{texthere} as below. |  |

### RETRO = 50 Points

|  |  |  |
| --- | --- | --- |
| 1 | Extract binary file from image and got retro.jpg |  |
| 2 | Decode wave file with turggen |  |
| 3 | Go to tab,tools>turbo decoder and select the retro.wav file and select the output directory.  Set the jump to 341365 and click “decode until EOF”. |  |
| 4 | Set the jump to 87266 and click “decode one file” |  |
| 5 | Open terminal in output directory of retro wav, and type “string \*.tm” and flag is appear. |  |

### DA VINCI = 30 Points

|  |  |  |
| --- | --- | --- |
| 1 | The password is TOM at the image of people. |  |
| 2 | “steghide extract -sf Thepassword\_is\_the\_small\_name\_of\_the\_actor\_named\_Hanks.jpg” and insert the password |  |
| 3 | Let decode the md5 hash from the extracted data.. (key:020e60c6a84db8c5d4c2d56a4e4fe082) and found “leonardo” |  |
| 4 | Check string at Plan.jpg file; “strings Plan.jpg” and found the youtube link and open. The title of youtube is Guernica |  |
| 5 | Check the monalisa img “binwalk -e monalisa.jpg” and got file zip. |  |
| 6 | Extract the famous.zip with md5 decoded password and Mona.jpg appear. |  |
| 7 | Steghide the image and use “Guernica” as password and key file appear. |  |
| 8 | Show the key. It is base64 |  |
| 9 | Decode the base64 key online. Decode three time of each value to show the final flag |  |

### DIGITALCUBE = 60 Points

|  |  |  |
| --- | --- | --- |
| 1 | Extract and found digitalcube.txt and it is binary so let convert it to image. The output is barcode. |  |
| 2 | We got qrcode and let scan it |  |
| 3 | Barcode reader online and scan it to view the flag |  |
| 4 | The flag is………. |  |

### BEATLES = 40 Points

|  |  |  |
| --- | --- | --- |
| 1 | Open m3ss@g#\_f0r\_pAuL file. Here we got random message. I think it is caesar cipher text . |  |
| 2 | So , i decode it with shift key 13 and get this message |  |
| 3 | So let attack passphrase with dictionary file; “fcrackzip -u -D -p /usr/share/wordlists/fasttrack.txt BAND.zip” and found something!! |  |
| 4 | Lets use steghide at the current image; “steghide extract -sf BAND.JPG -p THEBEATLES” |  |
| 5 | Let try to strings the testabeatle.out file; and we get message to Paul. it has base64 message as well. |  |
| 6 | Let decode to base64 and what we got!!! |  |

### UNIFIED = 20 Points

|  |  |  |
| --- | --- | --- |
| 1 | Extract the file and got BOD\_30079.txt. Open it. |  |
| 2 | Oh, it UTF character. Let decode in burpsuite. |  |
| 3 | The output is ... |  |
| 4 | Here is the flag; **HTB{tr1th3m1u5\_1499}** |  |

### PUSHEEN LOVES GRAPHS = 30 Points

|  |  |  |
| --- | --- | --- |
| 1 | Extract the file and we got Pusheen file. |  |
| 2 | Dissemble it in IDA. but,we got error when load the exe file. The error is the max amount of nodes is 1000. So, i change it to 20000. Boom, some text appear. |  |
| 3 | The flag format is HTB{text\_here}. So , just completed the format as well. | **HTB{fUn\_w17h\_CFGz}** |

### SENSELESS BEHAVIOUR = 50 Points

|  |  |  |
| --- | --- | --- |
| 1 | Let bruteforce the meow.wav file with steg\_brute.py. We got password and extracted file name meow\_flag.txt |  |
| 2 | The output is text with random character. It might be base64 format.let remove unwanted character and letter. |  |
| 3 | So , we will get the cleartext64.png as output .png file. |  |
| 4 | Now, use stegsolve. Open the output file and find the interesting info. |  |
| 5 | Wow, after navigating, i found braille text. |  |
| 6 | Let decode the braille and see what happen. It is “blindasabat”. Change it to **HTB{blindasabat}** format. |  |

## WEB CHALLENGES

### HDC = 30 Points

|  |  |  |
| --- | --- | --- |
| 1 | Go to http://docker.hackthebox.eu:47479/ |  |
| 2 | so i press f12 and digging around, i saw two hidden inputs and when we submit the form it triggers the doProcess() function |  |
| 3 | Then, i saw a custom js myscripts. I think it maybe scripted by the owner. It related to the submit function of hidden inputs. |  |
| 4 | So, i decided to explore the jquery-321.js and search for doProcess and found value for input name1 and name2. It look like credential. |  |
| 5 | Let try login with the credential. look , we success to login!! |  |
| 6 | Based on the question hint; |  |
| 7 | so now i had to find the mail of the individual.  i clicked at **Mailbox of Special Customers** and i got this |  |
| 8 | based my little experience in ctf, I learned to check the path and the source code of the images so i decided to check the small image that appears in the right side in the page title. i opened the image on a new tap and i found url???!!. |  |
| 9 | Here im try to traverse thru link backward and found interesting file. |  |
| 10 | Click the mails.txt and got this!! |  |
| 11 | Based on other question hint; hmmm. one thing come into my head !!Burpsuite!! |  |
| 12 | i intercepted the request, sent it to Intruder added the list of emails as payload and click attack. now after the attack completed i stated analyse all the request’s and and yeah!! I finally got the Flag :D |  |
| 13 | So i enter the email and what !!  The flag is in this picture!! |  |

### CARTOGRAPHER = 30 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | First, i press f12 to see the code. Get the username and password field but there’s no action parameter?? |  |
| 2 | Then,im looking for hint in the forum and i try to make sqli. Lulz..it work! |  |
| 3 | Here is the url changed |  |
| 4 | But, i dont know what to do yet. Looking for clue and it just change the link to what we are looking for?? It is flag broo! Just by changing info=home to info=flag... |  |

### LERNAEAN = 20 POINTS

|  |  |  |
| --- | --- | --- |
| 1 | This is the login page. There is also Error message of invalid password. The error message is useful to bruteforce the password. |  |
| 2 | Try to ping to look for IP |  |
| 3 | Now, im tried hydra to bruteforce with info about the website needed. Haha, got the password. So, let try login |  |
| 4 | Success login but get this message. What the?? It say im too slow? What does it mean? I think we have to grab the request and look at the reply? Burpsuite again? |  |
| 5 | Let try BS and intercept request. Use repeater and check the response. Nah...what we got there??  **HTB{lik3\_4\_b0s5\_s0n}** |  |

### \*I KNOW MAG1K\* = 50 Points

|  |  |  |
| --- | --- | --- |
| 1 | First create new account |  |
| 2 | By logging into the system with the user information created, the interfaces and request contents sent in the application are started to be examined. |  |
| 3 | After successful login, only session value görülmek iknowmag1k at is assigned to the user. |  |
| 4 | Then, decode the base64 of the session value and got this.... |  |
| 5 | Then use padbuster and change to user: admin and role: admin. the session value created with the role value “admin m is obtained -“LDRCU61StZbYrdIXPROTGIprI45i7IsYMAovrw2IGp8AAAAAAAAAA% 3D% 3D” |  |
| 6 | The session value obtained in the last step is placed into the pr /profile.php ”request in the“ Burp Suite - Repeater ”tab and access to the“ admin ”profile screen. Now, we got the final **flag**..yess |  |