WEB EXPLOITS

1) Robocorp

There was nothing to be found on the webpage robocorp.

So i just added /robots.txt path in the url and found that a particular path was disallowed. copy pasted it in the url and got the flag

Flag - inctfj{th3\_r0b0\_exclusi0n\_pr0t0c0l} --- robocorp

2)- Favourite Cookie

When i opened the webpage and checked the cookies,i saw a cookie named “time” with some random value and i saw a cookie named favcookie which had value “xxx” which i felt weird

I used burpsuite and got a Hint in the header saying “oreo is my favourite”. I changed the value of favcookie to oreo. And a text appeared on the webpage saying that the flag will be shown at a particular time, so i changed the value of the time cookie to that value and got the flag.

# 3)Client Auth

open inspect element you will find a javascript

Run that function in your ide to get the id and password

# 4)No-Rclick

Use Control + Shift I

Or you can use ctrl+shft+c in firefox to open the console and you will find the flag there

# 5)Wrath of the Romans

When you see the python code you fell that it is shifting letters so it should be Ceasar cipher

But its just a normal question so run the python code using the values

bpztugttsdbaphiiwthidgb

key : 15

inctfj{makefreedomlastthestorm}

https://www.dcode.fr/caesar-cipher

FOREINSICS:

# 6)Angry Steve

strings Angry\_f0b4b562-106e-4ac8-8876-73a939faf723.jpg | grep inctf

inctfj{string5\_m4keth\_fl4gs}

# 7)Con-The-Cat

THE png file should end at iend but there is too much data after that

the first line after iend is JFIF so it means a jpg file may be hidden after i end

correct the magic number of new png file

you can see some flag but you still cannot open it, the file is very large because of .......

send the file to someone on whatsapp, it will auto convert it

inctfj{y0u\_c4nt\_s33\_m3!!}

# 8) S3cr3t

use sonic visualizer you will see that wav file is like a morse code.

https://morsecode.world/international/decoder/audio-decoder-adaptive.html

first time you run the online tool, you will get a garbage output, run it twice

inctf{M0RS3C0D3I5C001}

CRYPTOGRAPHY:

# 9) XOR is Easy

# 10)Vinegar-v1

key is given: abcxyz

ioeqdi{siwcdke\_tjrdelf\_uesefmg}

https://www.dcode.fr/vigenere-cipher

inctfj{shuffle\_shuffle\_shuffle}

# 11)Vinegar v2

https://www.dcode.fr/vigenere-cipher

use the length:6

wecgln{mfu\_pgr\_rvcbji\_hyif\_qimcefy}

inctfj{you\_can\_decode\_this\_keyless}

# 12)Single byte X0r

use the key z

https://www.dcode.fr/xor-cipher

inctfj{x0r\_c4n't\_b3\_e4sily\_br0k3n}

# 13)SimpleRSA

./RsaCtfTool.py --uncipher 484661494807973176484841550022162356056969394230726278907827156279573785417739620605749085238379352332325669223692676583758711843467179784519220209212809010990483 -n 6823097956559906304718047559434503772935670794168872682087986860491266565197938988585578012131795379682740793915178580560097648572207445450501957620442660379247761 -e 65537

Pwning

1- break me

The downloaded file was a shell script.

When I downloaded and executed it was running in a loop. I figured that shellshock attack can be done and searched about it to find what to do. I gave bash –c “cat flag” as input to get the flag

2- integer overflow

I used gdb and found a flag printing line and before that a line with cmp, I added a breakpoint at that address and ran the program.

And at the break point I checked the value of the comparing variables, one of them was the value I entered and the other was the correct password for flag

3- connect

Connected using netcat and it asked to use bash commands. Just did ls and saw a flag.txt file and did cat flag.txt

Reversing

1- replicants

I just used strings on the file to get the flag inside the file

2- may the force be with you

Just ran the force program and tried giving different password and I found that the result was based on only the first letter of the strings given. Since its about force, I went on to try brute force and gave characters one by one as input. When I gave ‘h’ character I got the flag