CTF collection Vol.2

CTF collection Vol.2

Sharpening up your CTF skill with the collection. The second volume is about web-based CTF.

nmap-scan

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 1b:c2:b6:2d:fb:32:cc:11:68:61:ab:31:5b:45:5c:f4 (DSA)
|   2048 8d:88:65:9d:31:ff:b4:62:f9:28:f2:7d:42:07:89:58 (RSA)
|_  256 40:2e:b0:ed:2a:5a:9d:83:6a:6e:59:31:db:09:4c:cb (ECDSA)

80/tcp open  http    Apache httpd 2.2.22 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/DesKel_secret_base
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: 360 No Scope!

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

gobuster-scan

```
/index (Status: 200)
/login (Status: 301)
/button (Status: 200)
/static (Status: 200)
/cat (Status: 200)
/small (Status: 200)
/who (Status: 200)
/robots (Status: 200)
/iphone (Status: 200)
/game1 (Status: 301)
/egg (Status: 200)
/dinner (Status: 200)
/ty (Status: 200)
/ready (Status: 301)
/saw (Status: 200)
/game2 (Status: 301)
/wel (Status: 200)
/free_sub (Status: 301)
/nicole (Status: 200)
/server-status (Status: 403)
```

[Task 1] Author note

Welcome, welcome and welcome to another CTF collection. This is the second installment of the CTF collection series. For your information, the second serious focuses on the web-based challenge. There are a total of 20 easter eggs a.k.a flags can be found within the box. Let see how good is your CTF skill.
Now, deploy the machine and collect the eggs!
Warning: The challenge contains seizure images and background. If you feeling uncomfortable, try removing the background on <style> tag.

Note: All the challenges flag are formatted as `THM{flag}`, unless stated otherwise

#1

Fact: Eggs contain the highest quality protein you can buy.

No answer needed

[Task 2] Easter egg

Submit all your easter egg right here. Gonna find it all!

click me
Easter 1

found in /robots.txt hex string:
45 61 73 74 65 72 20 31 3a 20 54 48 4d 7b 34 75 37 30 62 30 37 5f 72 30 6c 6c 5f 30 75 37 7d

THM{4u70b07_r0ll_0u7}

click me
Easter 2

found in /robots.txt Disallow: /
VlNCcElFSWdTQ0JKSUVZZ1dTQm5JR1VnYVNCQ0lGUWdTU0JFSUVrZ1p5QldJR2tnUWlCNklFa2dSaUJuSUdjZ1RTQjVJRUlnV
Cyberchef recipe --- base64 -> URL-decode -> base64 -> remove-spaces -> base64 -> remove-spaces -> base64

THM{f4ll3n_b453}

click me
Easter 3

found in source code of /login page

THM{y0u_c4n'7_533_m3}

click me
Easter 4

found using sqlmap by dumping DB named ‘THM_f0und_m3', table ‘nothing_inside’, column 'Easter'

THM{1nj3c7_l1k3_4_b055}

click me
Easter 5

found by using md5 hash and username found in sqlmap with crackstation, and logging into /login page with DesKel:cutie

THM{wh47_d1d_17_c057_70_cr4ck_7h3_5ql}

click me
Easter 6

found in header of home page as value of Busted: parameter ("Busted: Hey, you found me, take this Easter 6: THM{l37'5_p4r7y_h4rd}")

THM{l37'5_p4r7y_h4rd}

click me
Easter 7

change value of cookie named ‘Invited’ from a 0 to a 1 and refresh page

THM{w3lc0m3!_4nd_w3lc0m3}

click me
Easter 8

found by changing user agent to “Mozilla/5.0 (iPhone; CPU iPhone OS 13_1_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.0.1 Mobile/15E148 Safari/604.1”

THM{h3y_r1ch3r_wh3r3_15_my_k1dn3y}

click me

Easter 9

found by catching /ready page in ZAP before redirect

THM{60nn4_60_f457}

click me

Easter 10

found by sending GET request with ‘Referer: tryhackme.com’ parameter set

THM{50rry_dud3}

click me

Easter 11

found by altering the HTML code in ‘menu’ area, by changing value from ‘salad’ to ‘egg’

THM{366y_b4k3y}

click me

Easter 12

found in the hidden JS file ‘jquery-9.1.2.js’ by decoding hex string ‘4561737465722031322069732054484d7b68316464336e5f6a355f66316c337d’

THM{h1dd3n_j5_f1l3}

click me

Easter 13

found in /ready/gone.php page

THM{1_c4n'7_b3l13v3_17}

click me

Easter 14

in source code theres an image that is encoded into base64. Decode that and save as png. Flag will show up in image

THM{d1r3c7_3mb3d)

click me

Easter 15

got flag by decoding message by inputting both upper and lowercase letters to get a numerical value. 51 89 77 93 126 14 93 10 in plaintext is G a m e O v e r
enter GameOver and get flag

THM{ju57_4_64m3}

click me

Easter 16

got the flag by adding the following data to the POST request in Burpsuite - “button1=button1&button2=button2&button3=button3”

THM{73mp3r_7h3_h7ml}

click me

Easter 17

decoded with the following Python script:

```
b =
'10001010110000101110011011101000110010101110010001000000011000100110111001110100010000001010100010010000100110101-
111011011010100011010101011111011010100011010101011111011010110011001101110000010111110110010000110011011000110011-
0000011001000011001101111101'
d = int(b, 2)
h = hex(d)[2:]
print(bytes.fromhex(h).decode('ASCII'))
```

THM{j5_j5_k3p_d3c0d3}

click me

Easter 18

added ‘egg: Yes’ parameter into request header

THM{70ny_r0ll_7h3_366}

click me

Easter 19

got flag by going to http://<machine-IP>/small.png

THM{700_5m4ll_3yy}

click me

Easter 20

found flag by changing GET request to a POST request and adding the following data parameters: ‘username=DesKel&password=heisDumb’

THM{17_w45_m3_4ll_4l0n6}