Write ups

CTF VM Game Of Thrones 1.0

Sulawesi I.T Security & iL7Team

Target sudah di set dengan :
Target : 192.168.56.102 - kindom.GOT.com
*Machine Target dijalankan di virtualBox dengan set jaringan **Host-only Adapter.***
Stormlands & Mountain_the vale

---

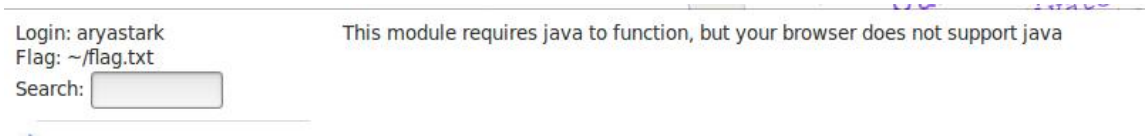
*kita mendapatkan flag iron islands dan kita sekarang dapat petunjuk baru yaitu **stormlands** yang jika liat dipeta kita masuk melalui **webmin** .*

*Kita gak perlu men set lagi di file "**/etc/hosts**" dan masuk dengan u/p: aryastark/N3ddl3_1s_a_g00d_sword*

*Jika sudah masuk ntar akan muncul **textbox** disudut kiri, ketika saya meng ketik beberapa huruf seperti **flag** ini tidak akan menampilkan apapun, hingga mencoba teknik XSS dan injection lainnya, tapi tetap gk ngaruh. tapi ketika mencoba 1 huruf*

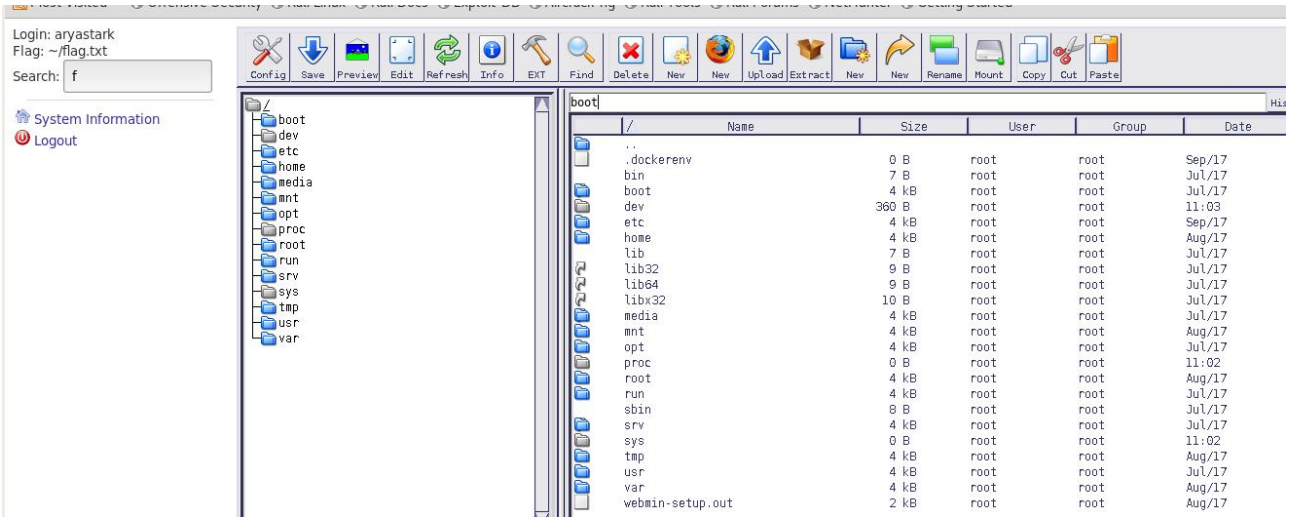
Create iL7Team with Sulawesi I.T Security

*It's work, . Nah kita sudah masuk dan disuruh mencari flag di file **flag.txt** . Mencoba menjelajahi.. Tetapi browser saya gk support dengan plugin lama (java)*



Mozilla, chrome & opera tidak support plugin java lagi.

Tapi coba lihat di browser ESR



Ini hanya tampilan, tapi kita tidak bisa menggnakannya. Saya sudah mencoba berkali - kali.

Tidak berputus asa saya mencoba menginstall browser lainnya, tapi tetap gk bisa. Dan jika kita lihat dokumentasi di virtualmin mereka gk support lagi ke browser tertentu.

Untuk flag stormlands kita lewatkan dulu, dan saya pikir - pikir kita hanya mencari file flag.txt untuk mencari flag stromlands dan petunjuk selanjutnya.

Kali ini coba kita lihat walktrought dari bule satu ini.

Click on the File Manager Module Link, Activate Java and Allow the app to launch.

Go to /home/aryastark/ and save the flag.txt file to your box.

We got the Stormlands flag : ***8fc42c6ddf9966db3b09e84365034357***

Now, we will have to play with the Postgresql service.

Our user/pass is ***robinarryn/cr0wn_f0r_a_King-_*** *and the db is* ***mountainandthevale***

Stormlands flag : ***8fc42c6ddf9966db3b09e84365034357***

U/p : ***robinarryn/cr0wn_f0r_a_King-_***

cr0wn_f0r_a_King-_

Database : ***mountainandthevale***

kita sudah mendapatkan petunjuk baru, jika kita lihat peta maka kita akan memasuki ***Mountain and the vale*** *yang mana kita masuk melalui* ***postgresql*** *.*

https://www.postgresql.org/docs/9.2/static/app-psql.html

Command psql sudah ada didalam, tinggal dibaca aja.

```
mcmillan@xeCURIty:~$ psql -h 192.168.56.102 mountainandthevale robinarryn
Password for user robinarryn:
psql (9.3.22, server 9.6.4)
WARNING: psql major version 9.3, server major version 9.6.
         Some psql features might not work.
Type "help" for help.
```

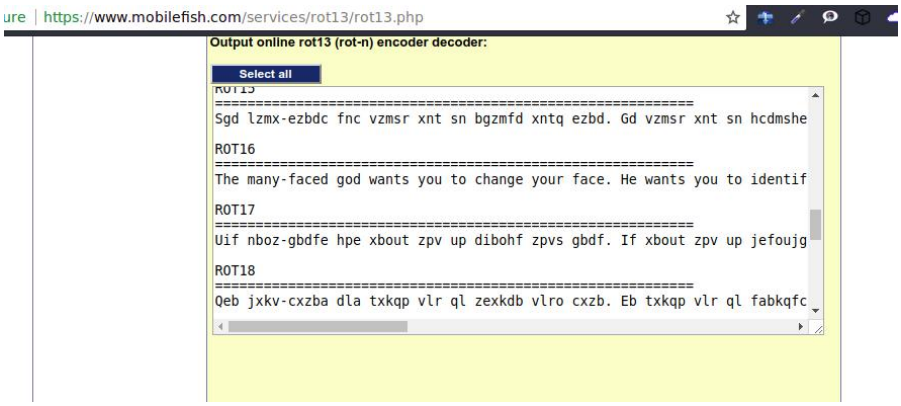
```
mountainandthevale-> \dt;
                List of relations
 Schema |         Name          | Type  |  Owner
--------+-----------------------+-------+----------
 public | aryas_kill_list       | table | postgres
 public | braavos_book          | table | postgres
 public | eyrie                 | table | postgres
 public | popular_wisdom_book   | table | postgres
(4 rows)
```

ada 4 list tables disitu, mari kita lihat satu persatu didalam nya.

```
 id |         name          |                                  why
----+-----------------------+-----------------------------------------------------------------------
  1 | WalderFrey            | For orchestrating the Red Wedding
  2 | CerseiLannister       | For her role in Ned Starks death
  3 | TheMountain           | For the torture at Harrenhal
  4 | TheHound              | For killing Mycah, the butchers boy
  5 | TheRedWomanMelisandre | For kidnapping Gendry
  6 | BericDondarrion       | For selling Gendry to Melisandre
  7 | ThorosofMyr           | For selling Gendry to Melisandre
  8 | IlynPayne             | For executing Ned Stark
  9 | MerynTrant            | For killing Syrio Forel
 10 | JoffreyBaratheon      | For ordering Ned Starks execution
 11 | TywinLannister        | For orchestrating the Red Wedding
 12 | Polliver              | For killing Lommy, stealing Needle and the torture at Harrenhal
 13 | Rorge                 | For the torture at Harrenhal and threatening to rape her
```

```
 1 | City of Braavos is a very particular place. It is not so far from here.
 2 | "There is only one god, and his name is Death. And there is only one thing we say to Death: Not today" - Syrio Forel
 3 | Braavos have a lot of curious buildings. The Iron Bank of Braavos, The House of Black and White, The Titan of Braavos, etc.
 4 | "A man teaches a girl. -Valar Dohaeris- All men must serve. Faceless Men most of all" - Jaqen H'ghar
 6 | "A girl has no name" - Arya Stark
 7 | City of Braavos is ruled by the Sealord, an elected position.
 8 | "That man's life was not yours to take. A girl stole from the Many-Faced God. Now a debt is owed" - Jaqen H'ghar
 9 | Dro wkxi-pkmon qyn gkxdc iye dy mrkxqo iyeb pkmo. Ro gkxdc iye dy snoxdspi kc yxo yp iyeb usvv vscd. Covomd sd lkcon yx drsc lyyu'c vycd zkqo xewlob. Dro nkdklkco
dy myxxomd gsvv lo lbkkfyc kxn iyeb zkccgybn gsvv lo: FkvkbWybqrevsc
(8 rows)
```

Sepertinya itu ter encode, mari kita encode
https://www.mobilefish.com/services/rot13/rot13.php



"The many-faced god wants you to change your face. He wants you to identify as one of your kill list. Select it based on this book's lost page number. The database to connect will be braavos and your password will be: ValarMorghulis"

*Ternyata ada database tersembunyi "**braavos"** password nya : **ValarMorghulis***

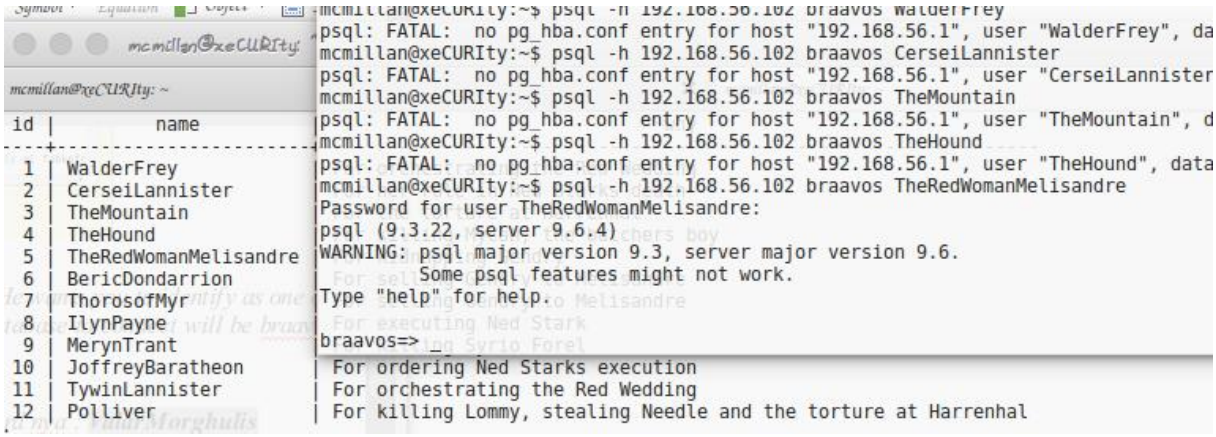
Langsung aja database braavos

```
                                  List of databases
    Name     |  Owner   | Encoding |  Collate   |   Ctype    |   Access privileges
-------------+----------+----------+------------+------------+-----------------------
braavos      | postgres | UTF8     | en_US.utf8 | en_US.utf8 | =Tc/postgres         +
             |          |          |            |            | postgres=CTc/postgres
mountainandthevale | postgres | UTF8     | en_US.utf8 | en_US.utf8 | =Tc/postgres         +
             |          |          |            |            | postgres=CTc/postgres
postgres     | postgres | UTF8     | en_US.utf8 | en_US.utf8 | =Tc/postgres         +
             |          |          |            |            | postgres=CTc/postgres
template0    | postgres | UTF8     | en_US.utf8 | en_US.utf8 | =c/postgres          +
             |          |          |            |            | postgres=CTc/postgres
template1    | postgres | UTF8     | en_US.utf8 | en_US.utf8 | =c/postgres          +
             |          |          |            |            | postgres=CTc/postgres
5 rows)
```

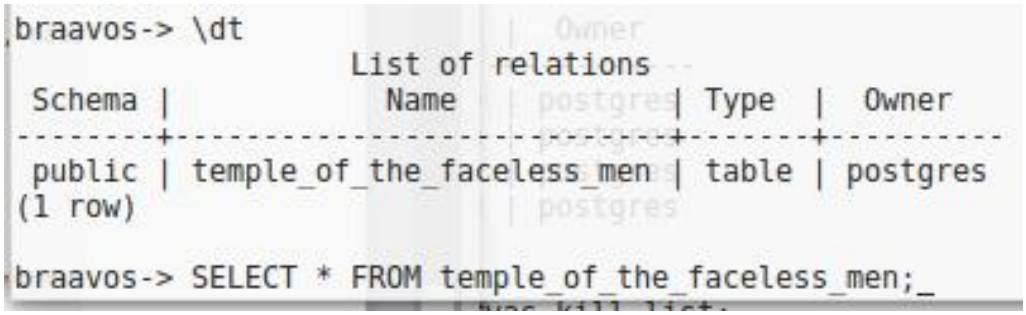
```
mcmillan@xeCURIty:~$ psql -h 192.168.56.102 braavos robinarryn
psql: FATAL:  pg_hba.conf rejects connection for host "192.168.56.1", user "robinarryn", database "braavos", SSL off
```

Tapi apa yang terjadi, ini sebuah kesalahan username dan tidak mungkin kesalahan nama database.

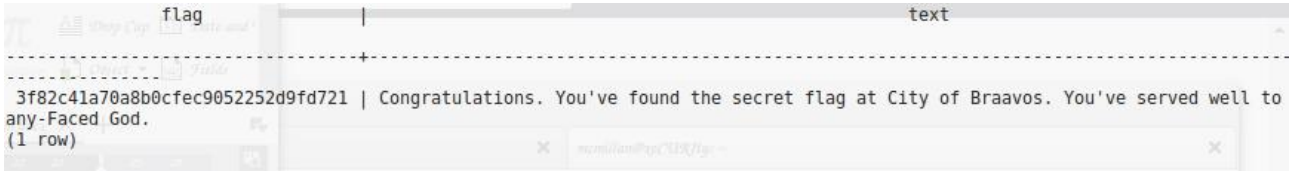
*Jadi saya menggunakan username yang terdaftar di table **aryas_kill_list .***



Kekekekeeh.. Username it's TheRedWomanMelisandre & password nya :
ValarMorghulis



Nah itu ada 1 table yang akan kita masukin.



Flag : 3f82c41a70a8b0cfec9052252d9fd721