



Write ups

CTFVM 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** .



STORMLANDS

Login to Stormlands

Stannis is the legitimate king!!

Username

Password

☐ Remember login permanently?

Kita gak perlu men set lagi di file **"/etc/hosts"** dan masuk dengan u/p:
aryastark/N3ddl3_ls_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

Login: aryastark
Flag: ~/flag.txt
Search:

System Information
Logout

Search Webmin

Searching for a found 28 results :

Matching text	Source	Module	References
File Manager	Module name	File Manager	
Show files starting with a dot?	Configuration	File Manager	
Size of buttons in toolbar	Configuration	File Manager	
...tempt to use proper character set?	Configuration	File Manager	
...tract class files from JAR?	Configuration	File Manager	
Width for scaled images	Configuration	File Manager	
...ult archive mode for uploads	Configuration	File Manager	
Default user for uploads	Configuration	File Manager	
File extensions to edit as HTML	Configuration	File Manager	
Return to Webmin index.	User interface	File Manager	File Manager
Upload	User interface	File Manager	upform.cgi
...wser does not support java	User interface	File Manager	File Manager
File Manager	User interface	File Manager	File Manager

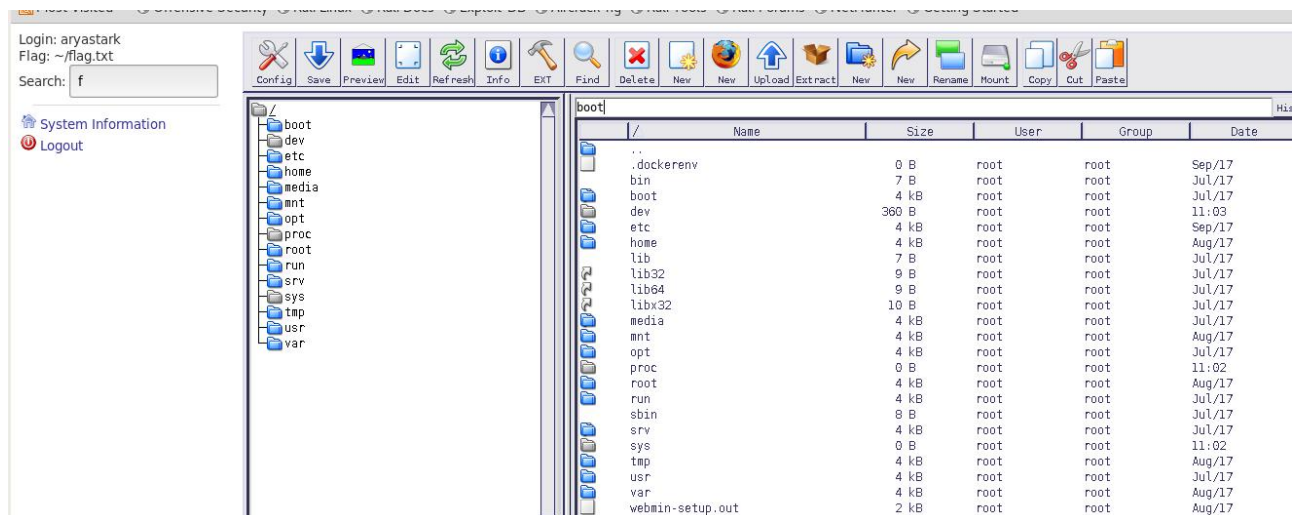
*It's work, . Nah kita sudah masuk dan disuruh mencari flag di file **flag.txt** . Mencoba menjelajahi.. Tetapi browser saya gk support dengan plugin lama (java)*

Login: aryastark
Flag: ~/flag.txt
Search:

This module requires java to function, but your browser does not support java

Mozilla, chrome & opera tidak support plugin java lagi.

Tapi coba lihat di browser ESR



Ini hanya tampilan, tapi kita tidak bisa menggunakannya. 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.

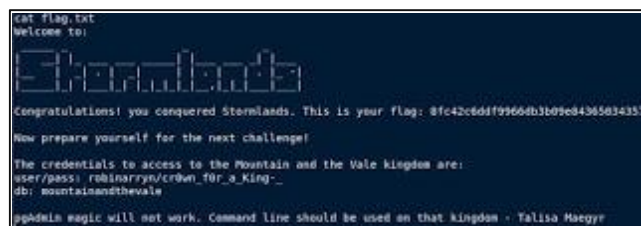
Untuk flag stormlands kita lewatkan dulu, dan saya pikir - pikir kita hanya mencari file flag.txt untuk mencari flag stromlands dan petunjuk selanjutnya.

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.
```

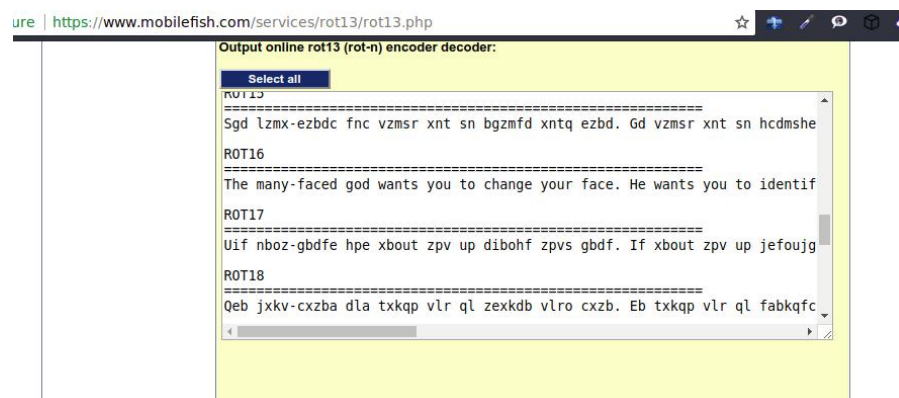
```
mountainandthevale-> \dt;
          List of relations
Schema |      Name      | Type  | Owner
-----+-----+-----+-----
public | alyas_kill_list | table | postgres
public | braavos_book    | table | postgres
public | eyrie           | table | postgres
public | popular_wisdom_book | table | postgres
(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
5 "A girl has no name" - Arya Stark
6 City of Braavos is ruled by the Sealord, an elected position.
7 "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
8 Dro wxxi-pkmon qyn gkxdc iye dy mrkxqo iye b pkmo. Ro gkxdc iye dy snoxdspl kc yxo yp iye b usvv vsacd. Covomd sd lkcon yx drsc lyyu'c vyced zkqo xewlob. Dro nkdcklco
9 dy myxxomd gsvv lo lbkkfyc knn iye b zkccgybn gsvv lo: FkvkbWbyqrevsc
(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: ValarMorphulis"

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

Langsung aja database braavos

Name	Owner	Encoding	Collate	Ctype	Access privileges
braavos	postgres	UTF8	en_US.utf8	en_US.utf8	=Tc/postgres +
mountainandthevale	postgres	UTF8	en_US.utf8	en_US.utf8	postgres=Ctc/postgres +
postgres	postgres	UTF8	en_US.utf8	en_US.utf8	=Tc/postgres +
template0	postgres	UTF8	en_US.utf8	en_US.utf8	=c/postgres +
template1	postgres	UTF8	en_US.utf8	en_US.utf8	postgres=Ctc/postgres +

```
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**.

```
mcmillan@xeCURITY:~$ psql -h 192.168.56.102 braavos WalderFrey
psql: FATAL: no pg_hba.conf entry for host "192.168.56.1", user "WalderFrey", da
mcmillan@xeCURITY:~$ psql -h 192.168.56.102 braavos CerseiLannister
psql: FATAL: no pg_hba.conf entry for host "192.168.56.1", user "CerseiLannister
mcmillan@xeCURITY:~$ psql -h 192.168.56.102 braavos TheMountain
psql: FATAL: no pg_hba.conf entry for host "192.168.56.1", user "TheMountain", d
mcmillan@xeCURITY:~$ psql -h 192.168.56.102 braavos TheHound
psql: FATAL: no pg_hba.conf entry for host "192.168.56.1", user "TheHound", data
mcmillan@xeCURITY:~$ psql -h 192.168.56.102 braavos TheRedWomanMelisandre
Password for user TheRedWomanMelisandre:
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.
braavos=>
1 WalderFrey
2 CerseiLannister
3 TheMountain
4 TheHound
5 TheRedWomanMelisandre
6 BericDondarrion
7 ThorosofMyr
8 IlynPayne
9 MerynTrant
10 JoffreyBaratheon
11 TywinLannister
12 Polliver
For ordering Ned Starks execution
For orchestrating the Red Wedding
For killing Lommy, stealing Needle and the torture at Harrenhal
```

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

```
braavos-> \dt
List of relations
Schema | Name | Type | Owner
-----+-----+-----+-----
public | temple_of_the_faceless_men | table | postgres
(1 row)

braavos-> SELECT * FROM temple_of_the_faceless_men;
```

Nah itu ada 1 table yang akan kita masukan.

```
flag | text
-----+-----
3f82c41a70a8b0cfec9052252d9fd721 | Congratulations. You've found the secret flag at City of Braavos. You've served well to any-Faced God.
(1 row)
```

Flag : **3f82c41a70a8b0cfec9052252d9fd721**