

## **Web Application Hacking CSRF and XSS Combo Attack**

### **Objectives**

- Review lecture
- Complete lab on LFI

### **Lab CSRF and XSS combo attack**

#### Lab Prep

Open the link to <https://hack.me>

Choose “Start a hackme”

Scroll down and select “DVWA 1.0.7”

Accept the agreement after selecting “anonymous login”

## (Damn Vulnerable Web App (DVWA): Lesson 10)

{ Cross Site Request Forgery combined with curl }

### Section 0. Background Information

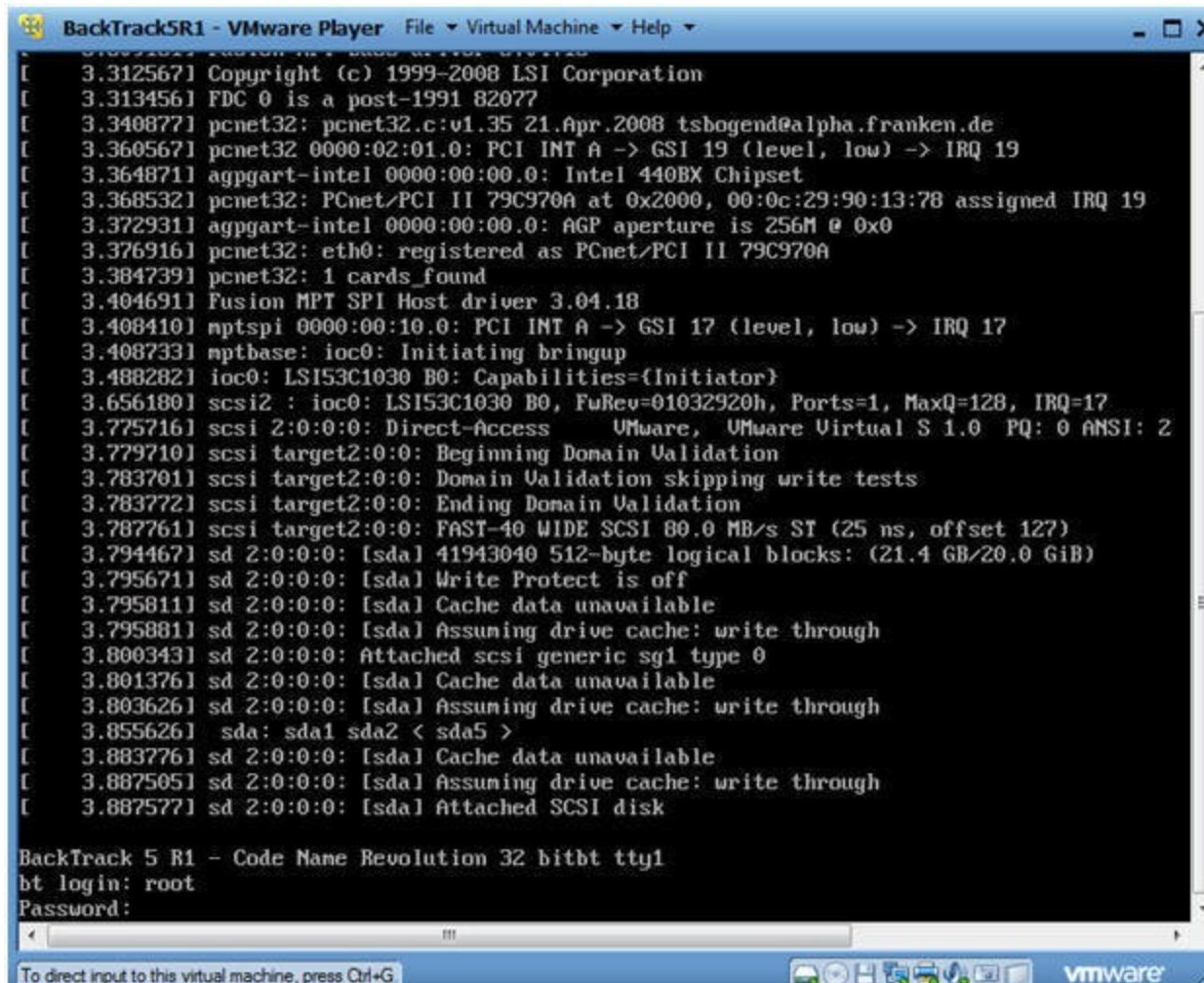
- What is Damn Vulnerable Web App (DVWA)?
  - Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable.
  - Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
- **Lab Notes**
  - In this lab we will do the following:
    1. We will test a basic Cross Site Request Forgery (XSRF) attack
    2. We will capture and manipulate a CSRF URL to change the admin password.
    3. We will obtain the session cookie string using a reflective XSS attack.
    4. We will create a curl CSRF string to change the admin password.

◦

1. Login to BackTrack

○ **Instructions:**

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



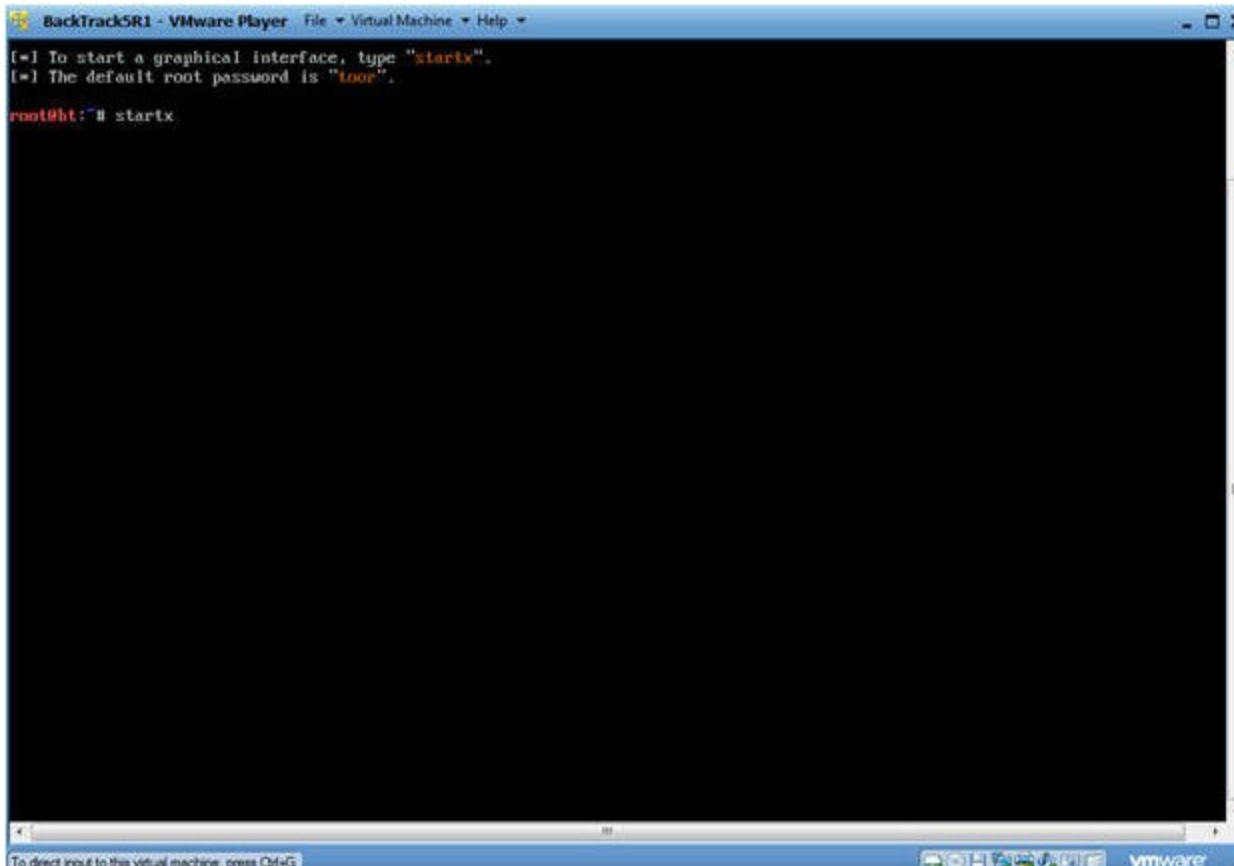
```
BackTrack5R1 - VMware Player  File  Virtual Machine  Help
[ 3.312567] Copyright (c) 1999-2008 LSI Corporation
[ 3.313456] FDC 0 is a post-1991 82077
[ 3.340877] pcnet32: pcnet32.c:v1.35 21.Apr.2008 tsbogend@alpha.franken.de
[ 3.360567] pcnet32 0000:02:01.0: PCI INT A -> GSI 19 (level, low) -> IRQ 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 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

○

2. Bring up the GNOME
  - **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



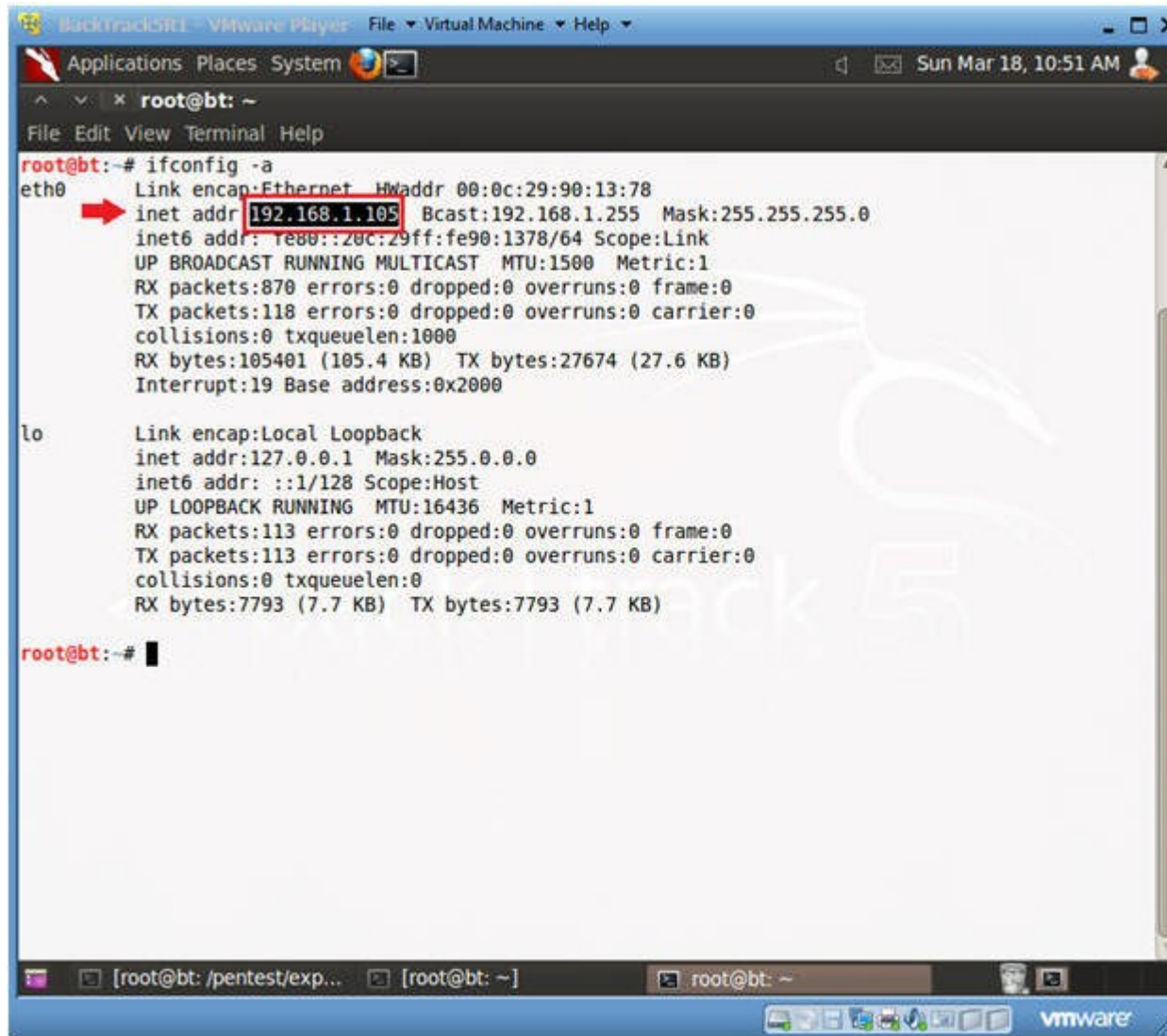
2. Get IP Address

- **Instructions:**

1. ifconfig -a

- **Notes:**

1. As indicated below, my IP address is 192.168.1.105.
2. Please record your IP address.



The screenshot shows a VMware Player window titled 'Backtrack5BT1 - VMware Player'. Inside, a terminal window is open with the prompt 'root@bt: ~'. The user has entered the command 'ifconfig -a'. The output shows details for two network interfaces: 'eth0' and 'lo'. The 'eth0' interface is an Ethernet card with MAC address '00:0c:29:90:13:78' and IP address '192.168.1.105', which is highlighted with a red box and a red arrow. The 'lo' interface is a local loopback with IP address '127.0.0.1'. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Terminal', and 'Help'. The VMware window has a menu bar with 'File', 'Virtual Machine', and 'Help', and a status bar at the bottom with 'Sun Mar 18, 10:51 AM' and a user icon.


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

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:7793 (7.7 KB)  TX bytes:7793 (7.7 KB)

root@bt:~#
```

○

## Section 8. Login to DVWA

- 
1. Open the link to <https://hack.me>
  2. Choose “Start a hackme”
  3. Scroll down and select “DVWA 1.0.7”
  4. Accept the agreement after selecting “anonymous login”

○

## 5. Login to DVWA

### ○ **Instructions:**

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



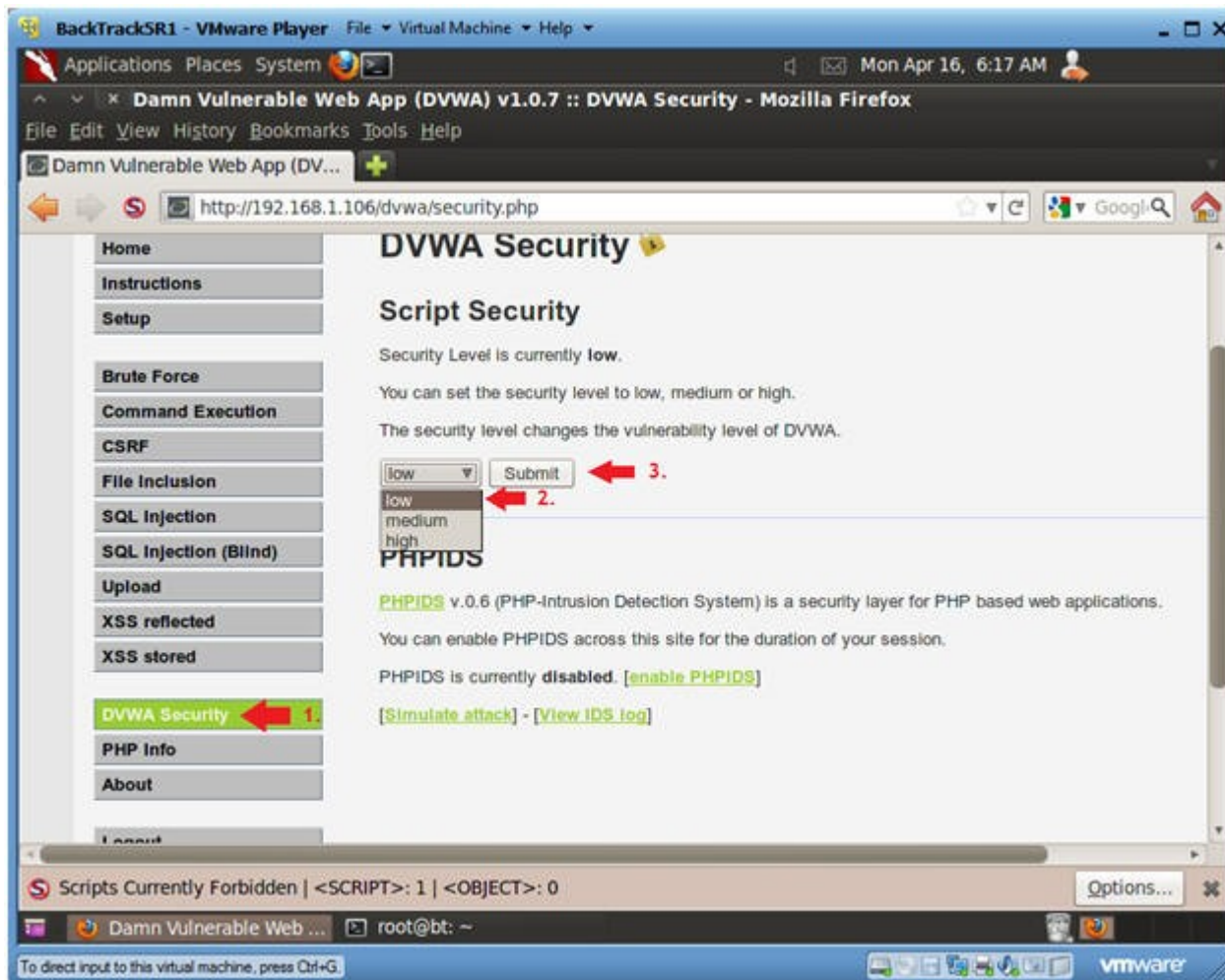


○

## Section 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

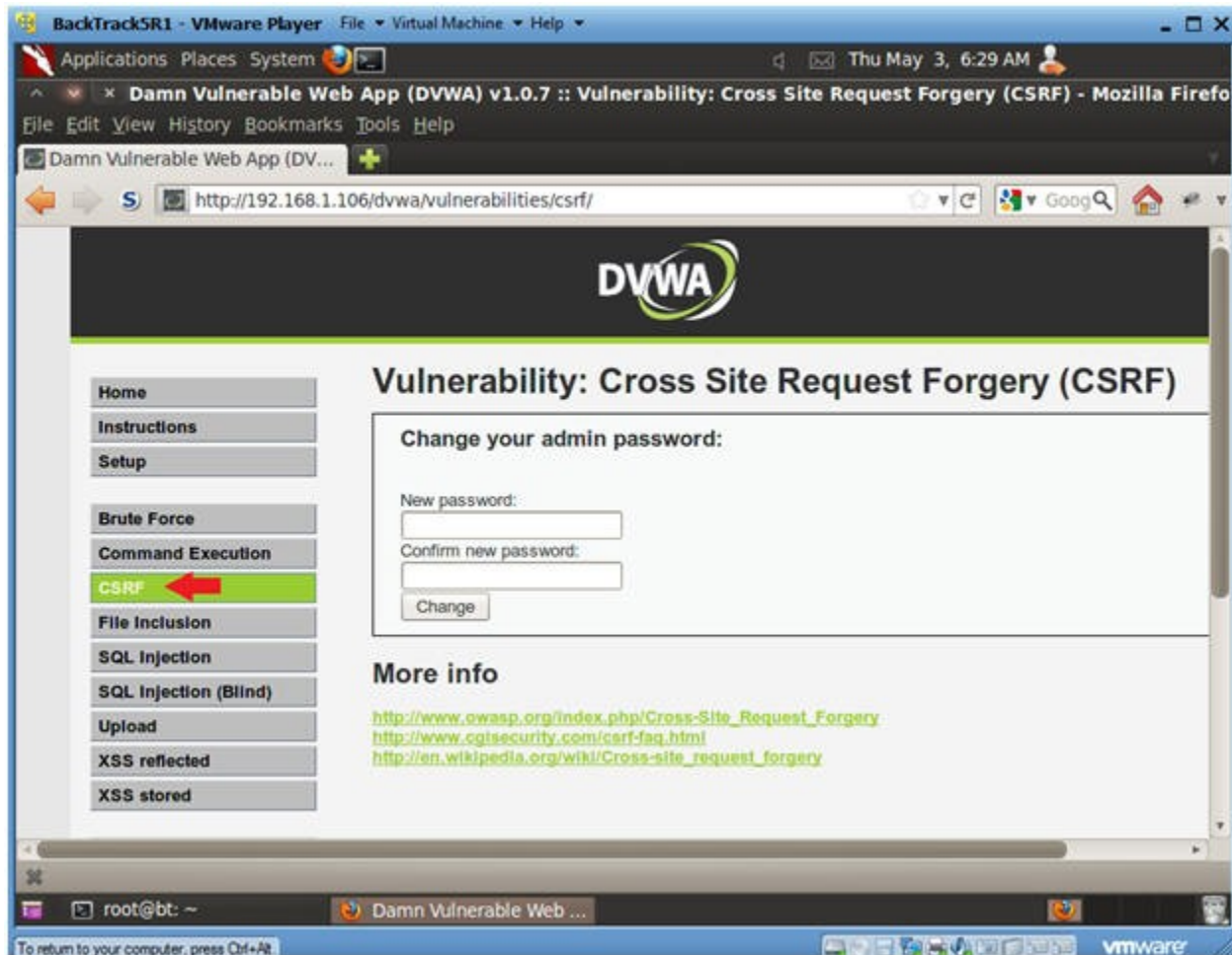


## Cross Site Request Forgery

1. CSRF Menu

- **Instructions:**

1. Select "CSRF" from the left navigation menu.



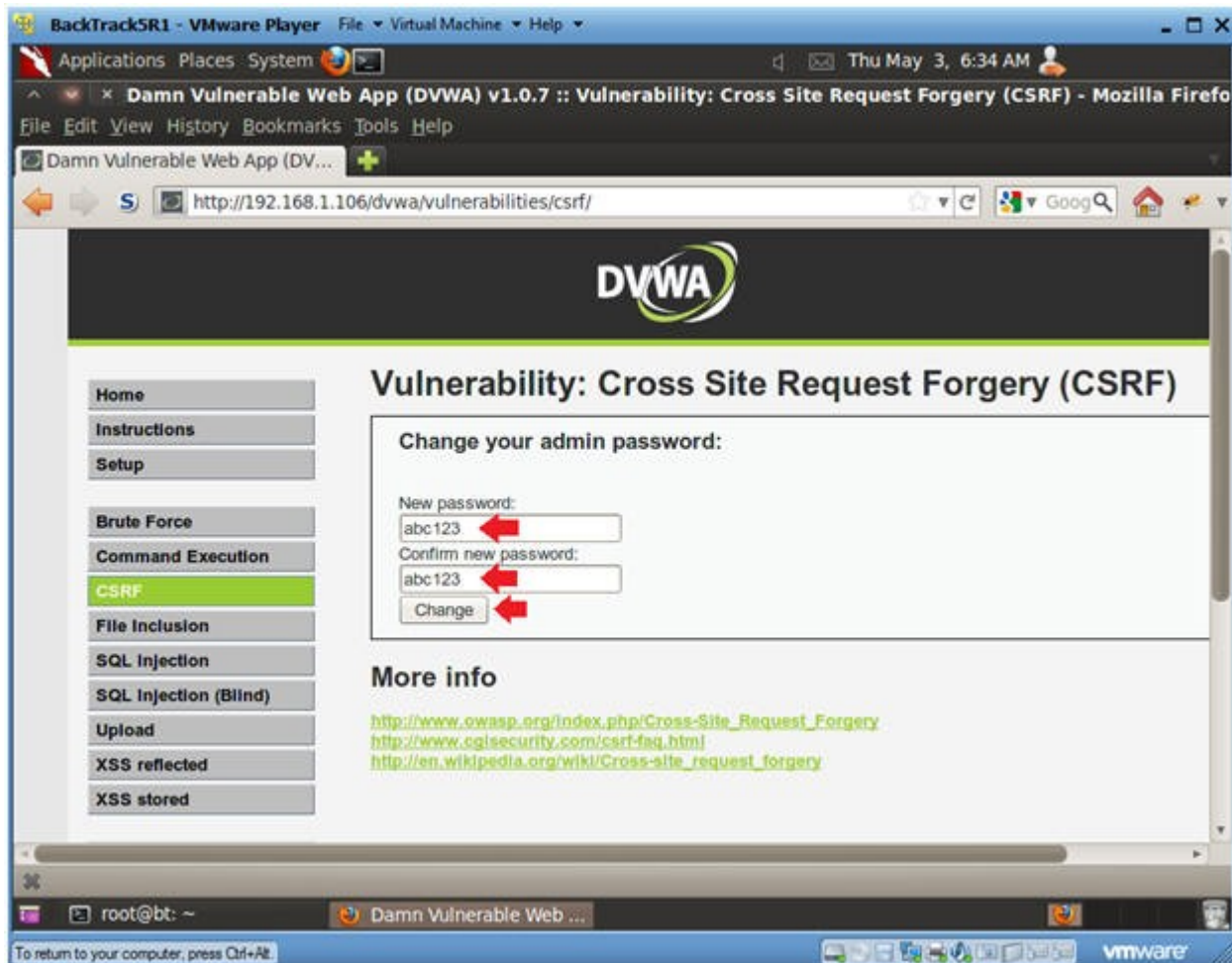
○

## 2. Basic CSRF Test

### ○ **Instructions:**

1. New password: abc123
2. Confirm new password: abc123

### 3. Click Change



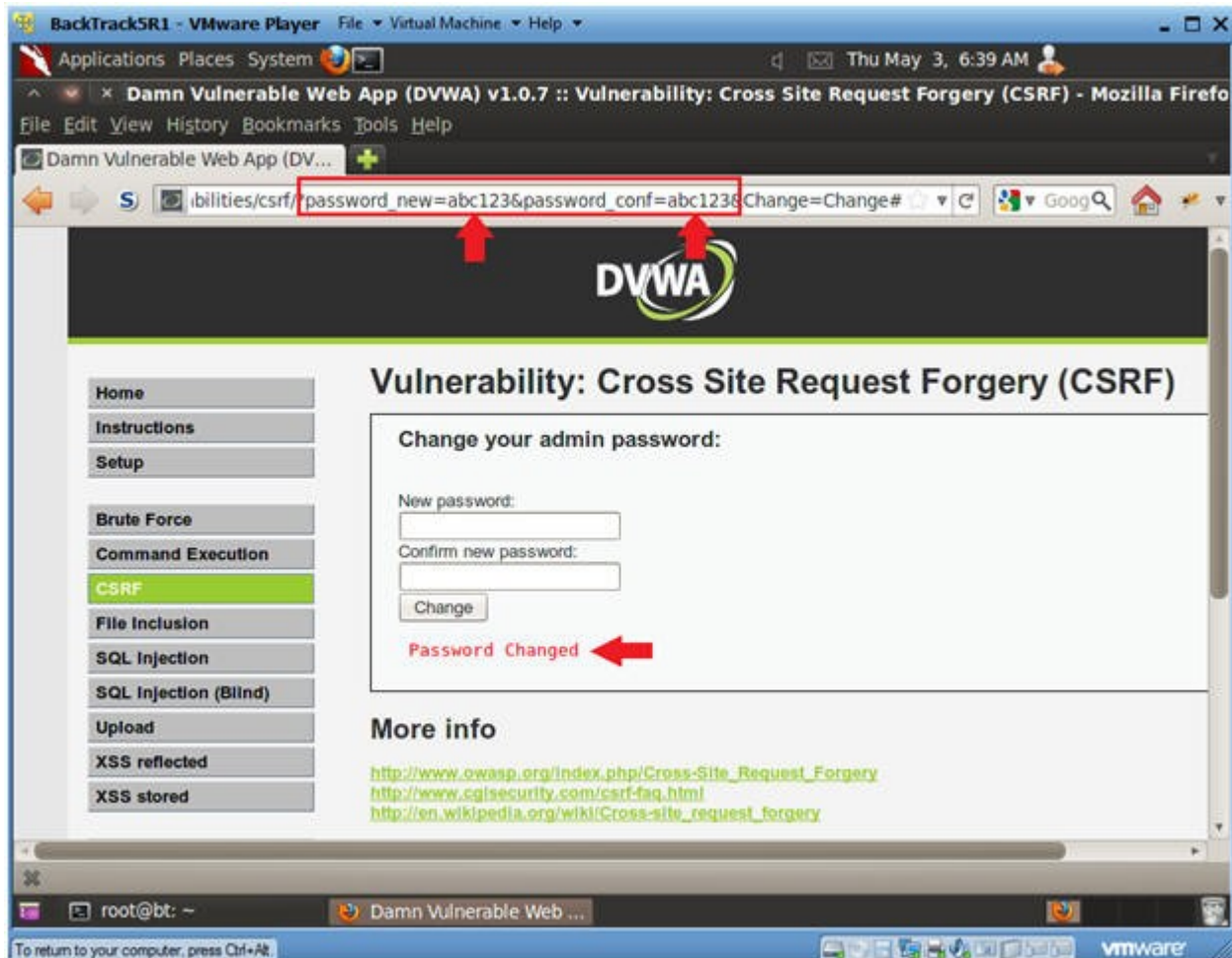
○

### 3. View Password Change Results

#### ○ Notes:

1. Below the change button you will notice the message that says "Password Changed."

2. What I really want you to notice is the URL string.
3. See how the URL string has the below two parameters separated by a "&".
  - a. password\_new=abc123
  - b. password\_conf=abc123
4. This is DVWA's example of bad implementation of how to change a password on a web application for the following reasons:
  - a. http is being used instead of https, which means this password change was in clear text.
  - b. An attacker could manipulate the URL string using the address bar or curl to change the password.
5. Continue to next step



○

#### 4. Address Bar CSRF Test

- **Instructions:**

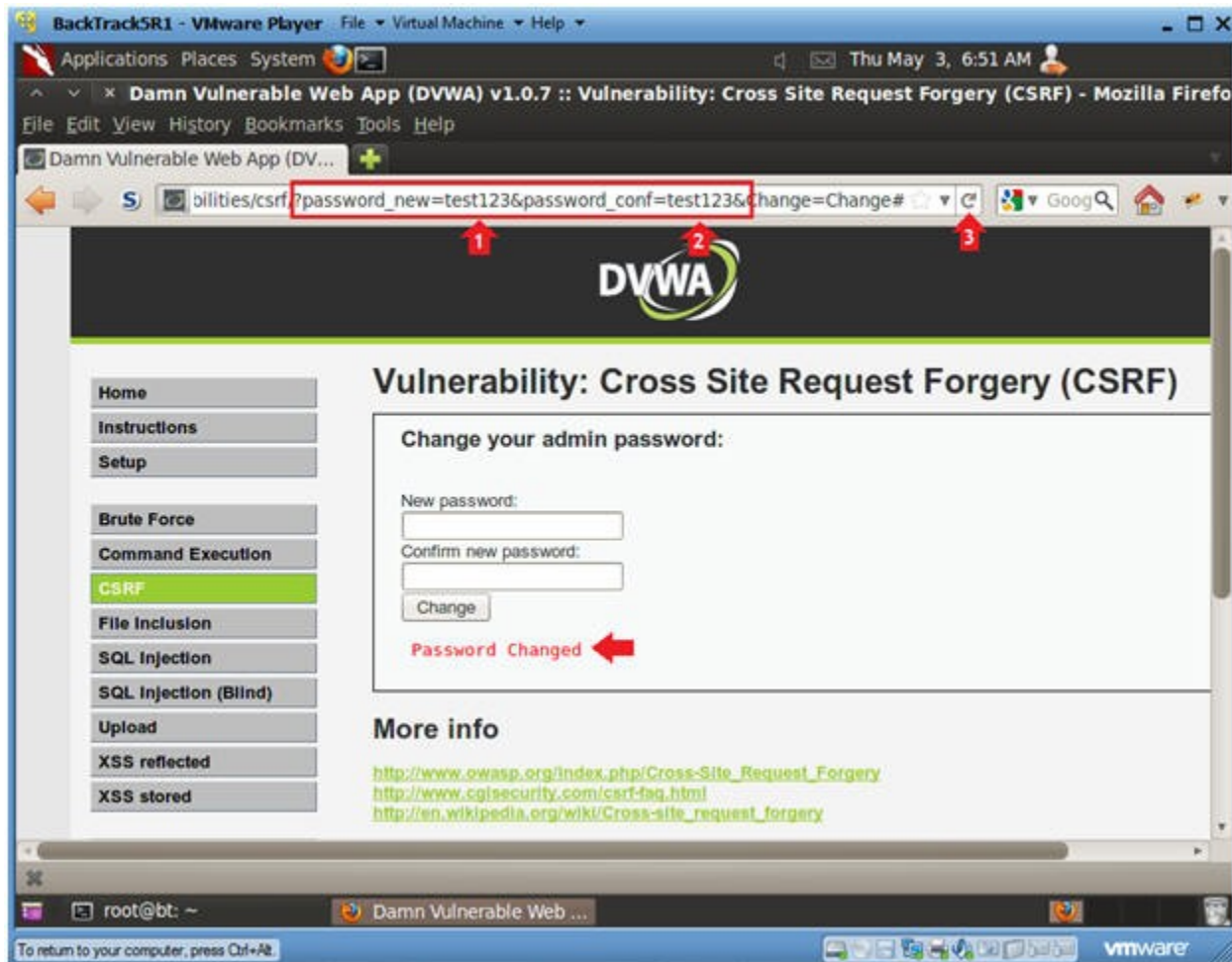
1. In the URL, after `password_new=`, replace `abc123` with `test123`.
2. In the URL, after `password_conf=`, replace `abc123` with `test123`.



3. Click the Reload Current Page Arrow

○ **Notes:**

1. Notice the Password is changed



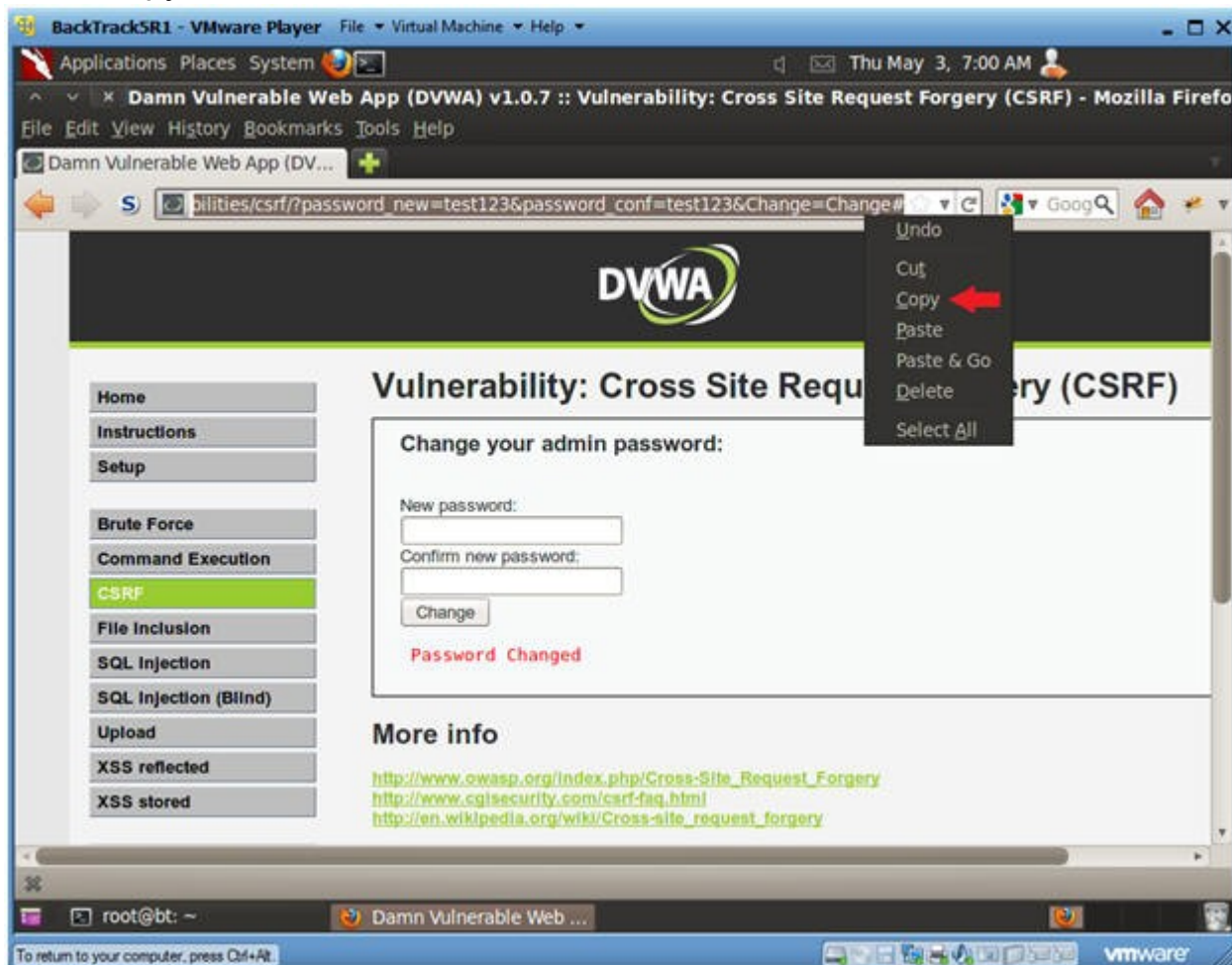
○

5. Copy CSRF URL



- **Instructions:**

1. Highlight the URL
2. Right Click
3. Copy

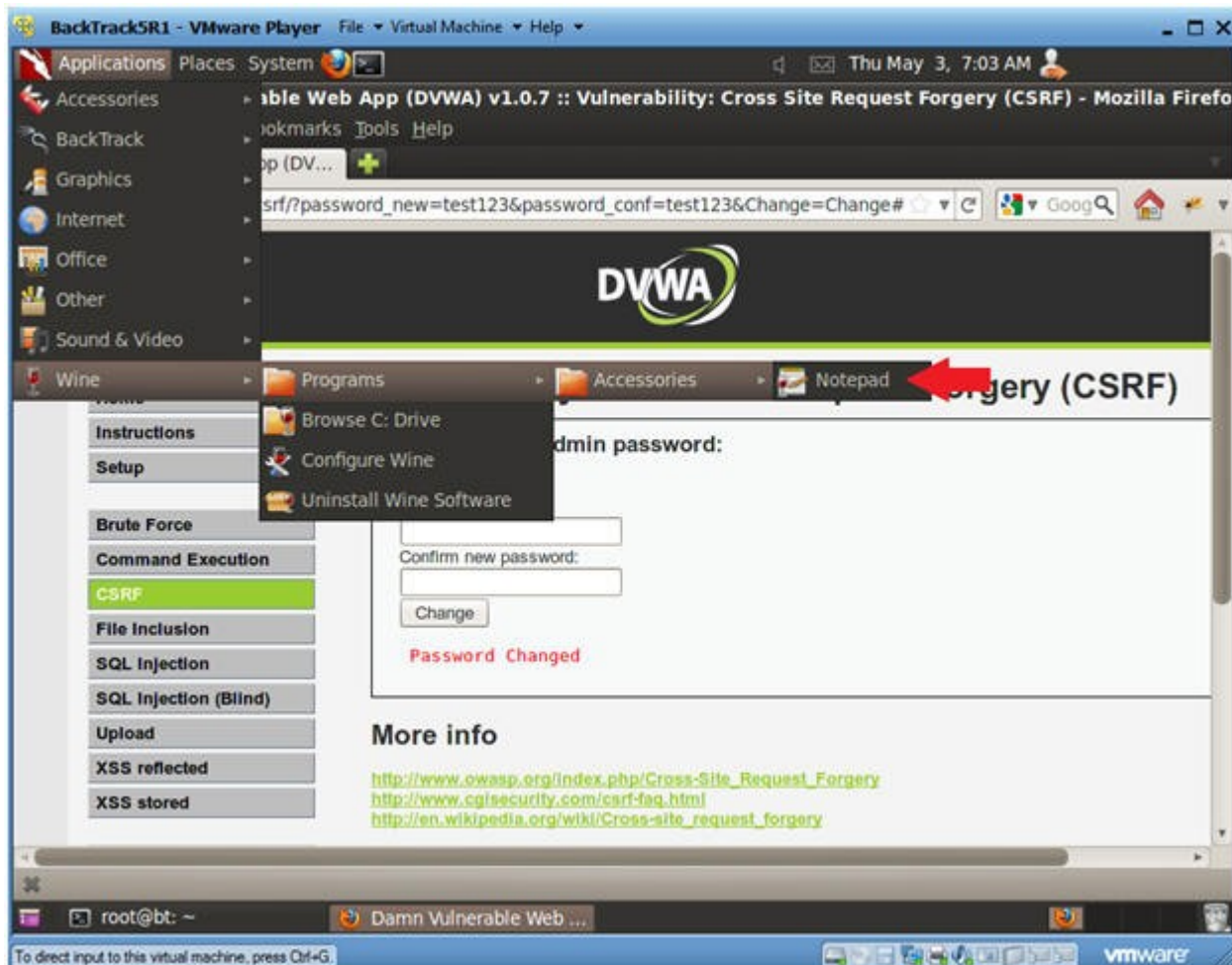


-

## 6. Start Notepad

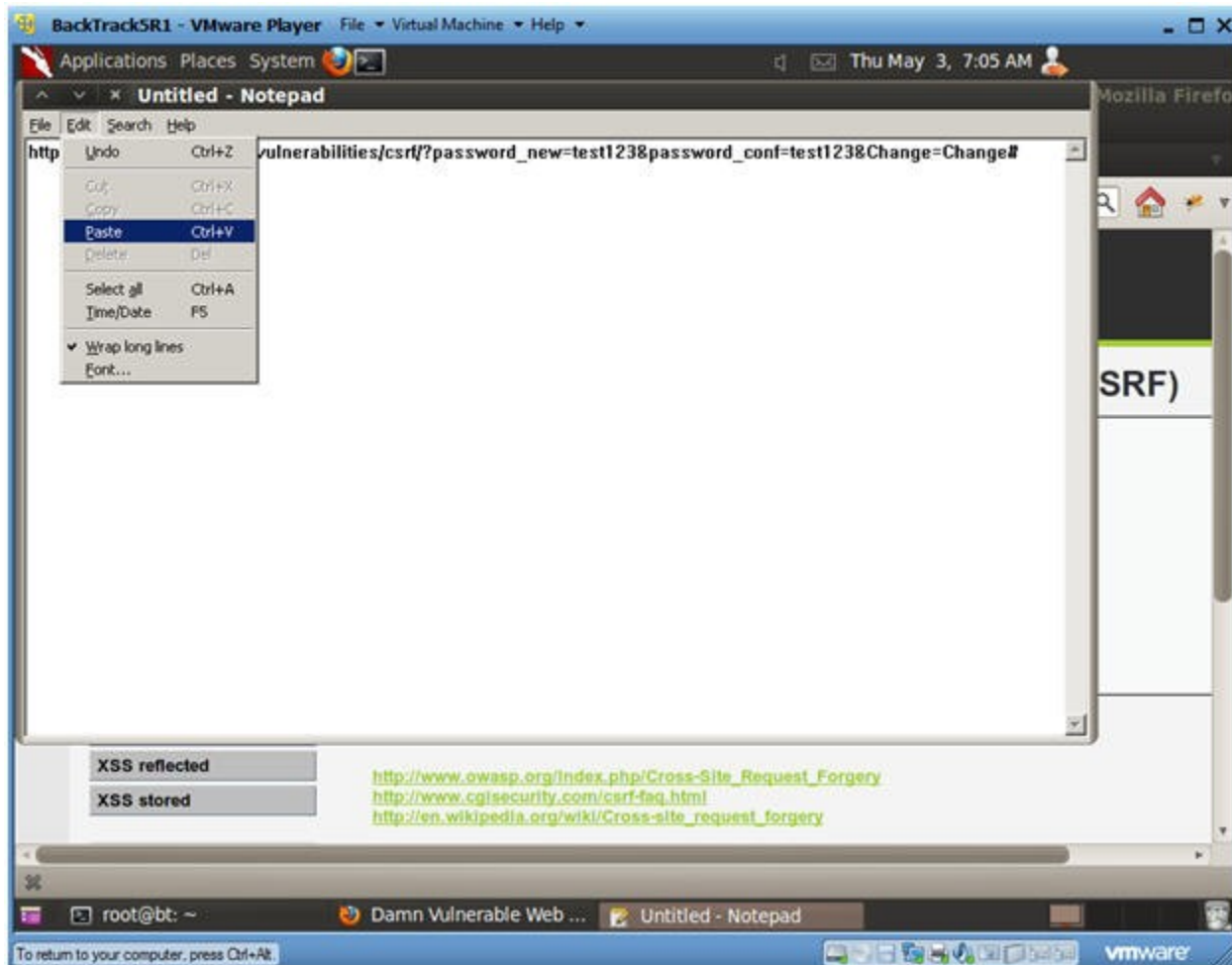
- **Instructions:**

- 1. Applications --> Wine --> Programs --> Notepad



- 
- 7. Paste URL into Notepad

- **Instructions:**
  1. Edit --> Paste



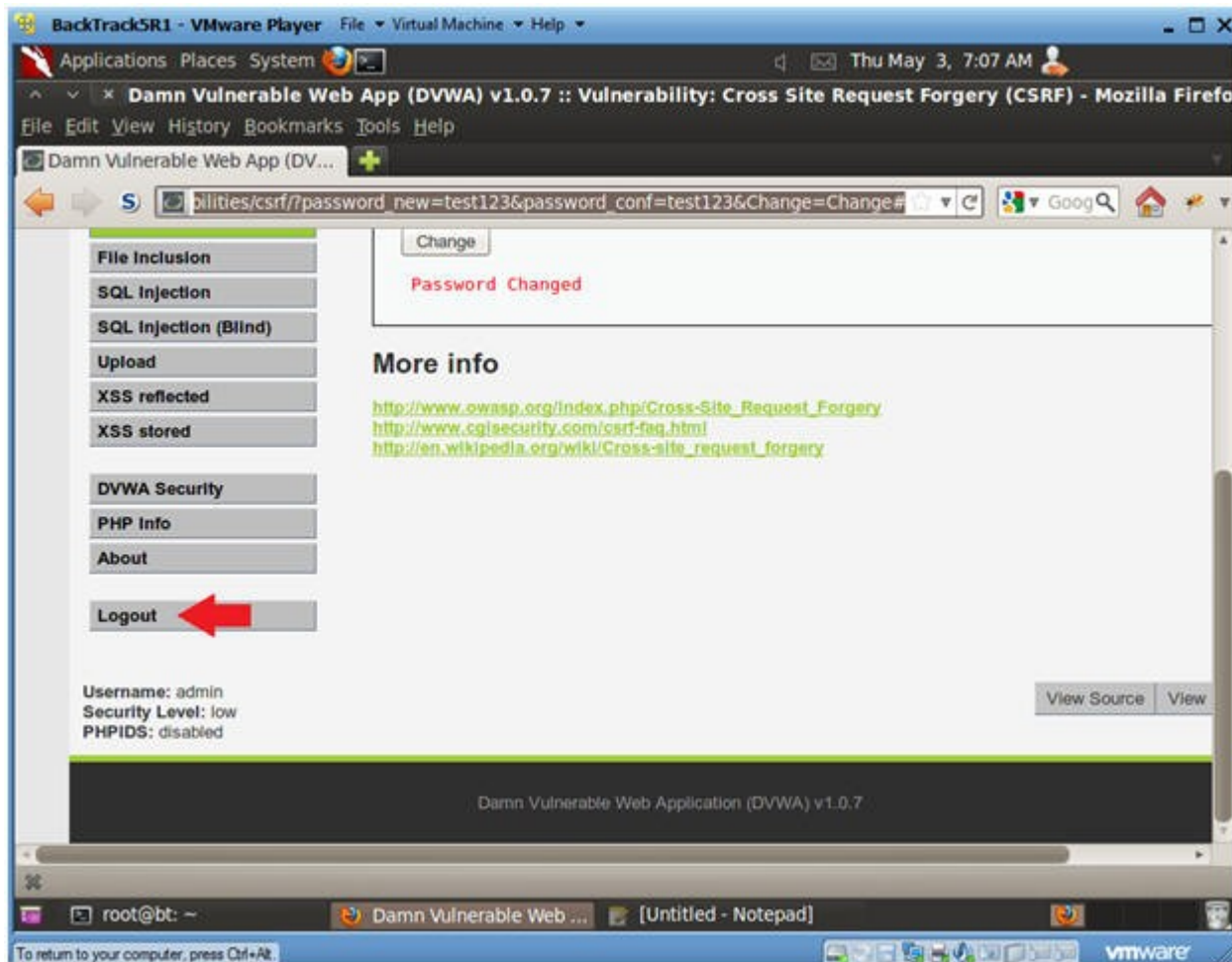
○

## Section 11. Test Password Change

## 1. Logout of DVWA

- **Instructions:**

- 1. In the Left Navigation Menu, Click Logout



- 

## 2. Login to DVWA

- **Instructions:**

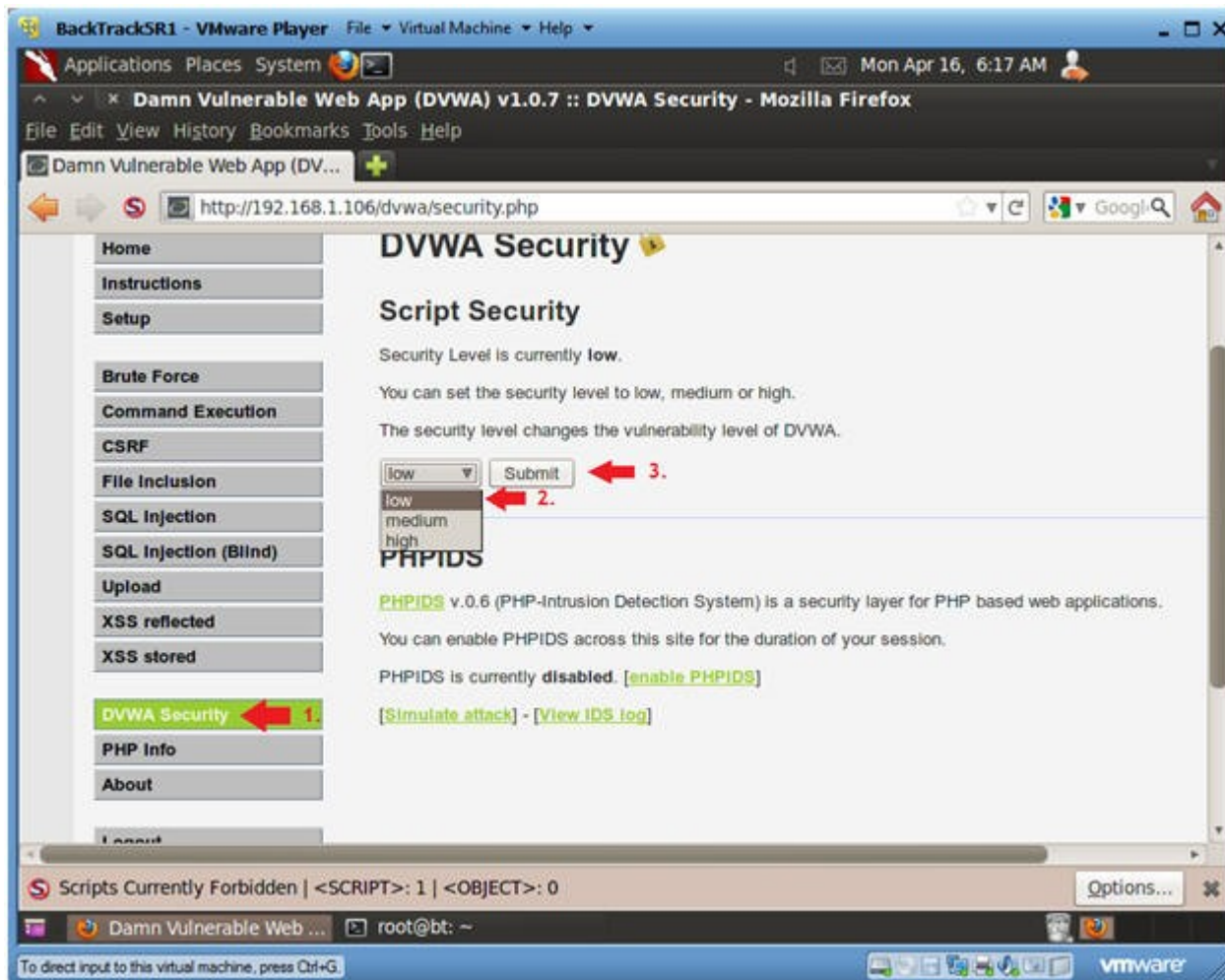
1. Username: admin
2. Password: test123



- 
- 3. Set DVWA Security Level



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

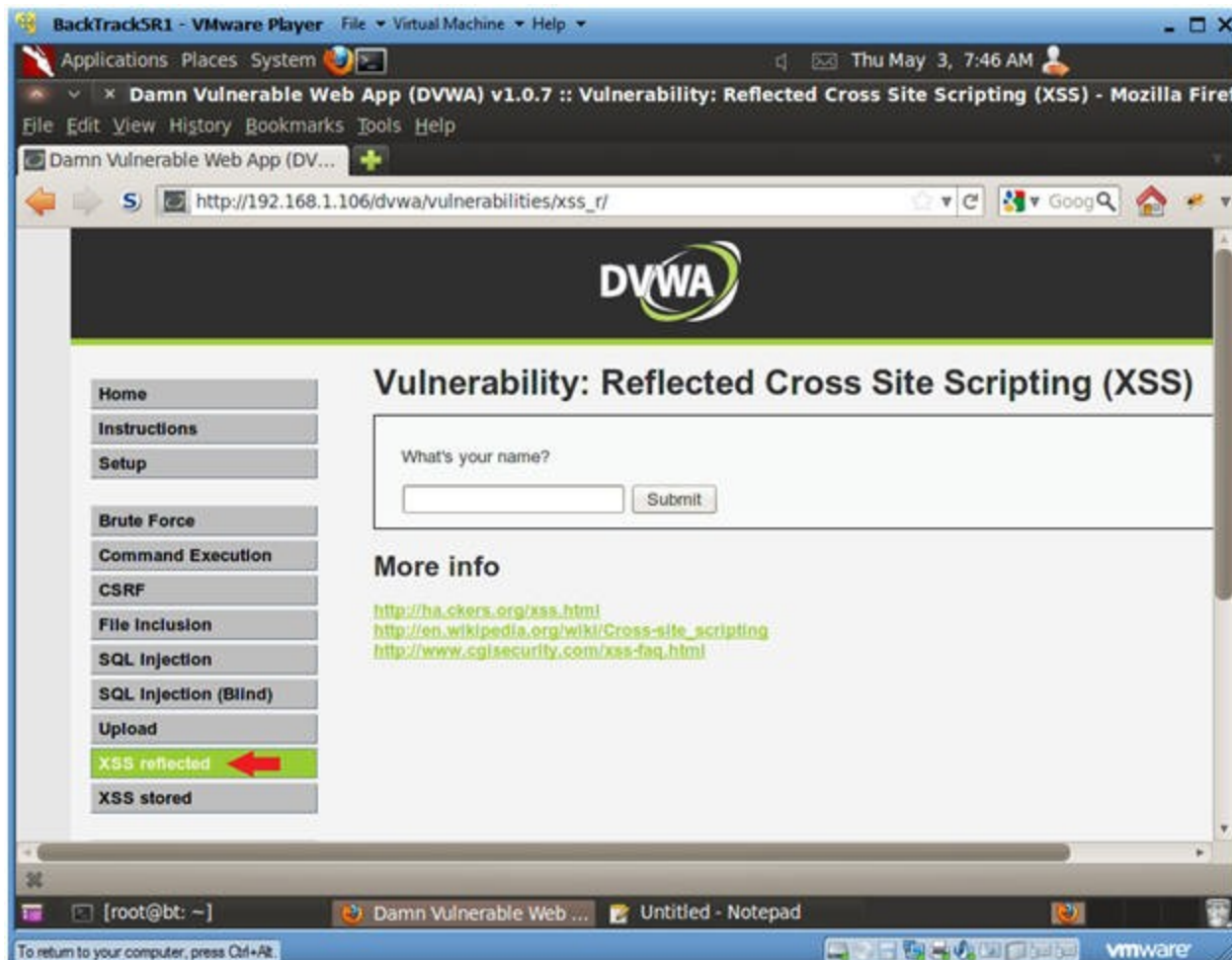


## Section 12. XSS reflected

1. XSS reflected

- **Instructions:**

1. Select "XSS reflected" from the left menu navigation.

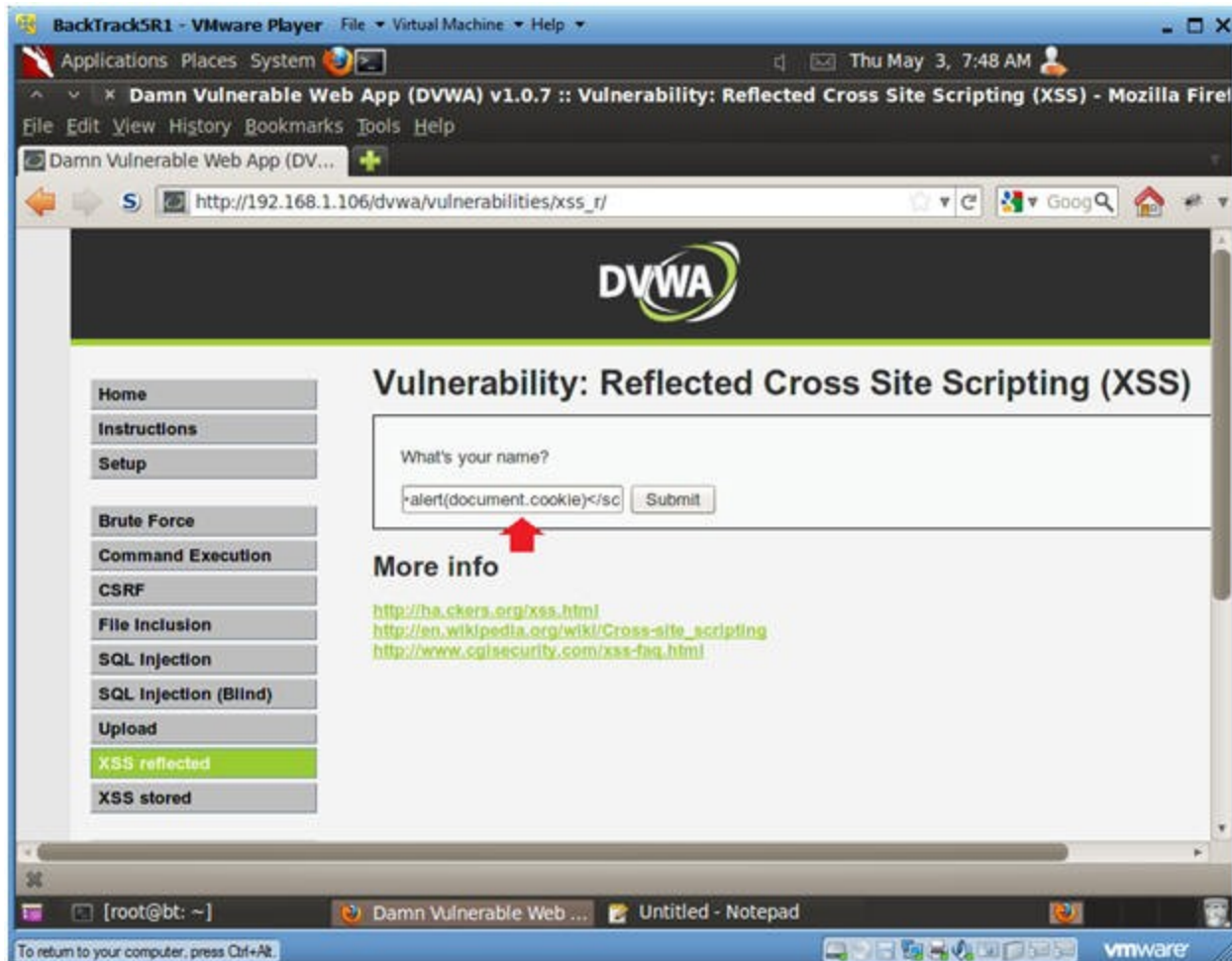


- 
- 2. Submit cookie XSS attack

- **Instructions:**

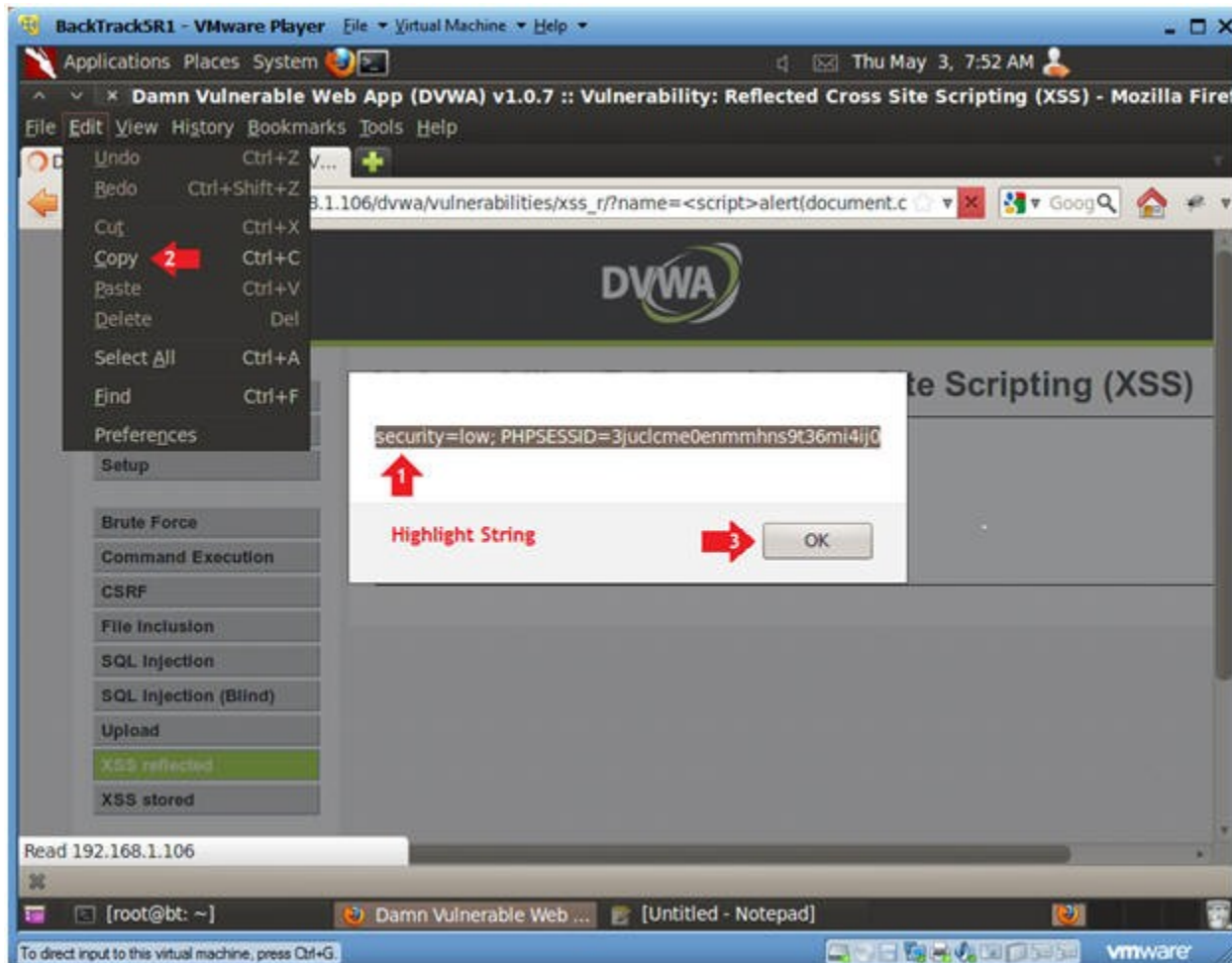
- 1. What's your Name? `<script>alert(document.cookie)</script>`
    - 2. Click Submit





- 
- 3. Copy Cookie String
  - **Instructions:**
    1. Highlight The Cookie String
    2. Edit --> Copy

3. Click the OK button

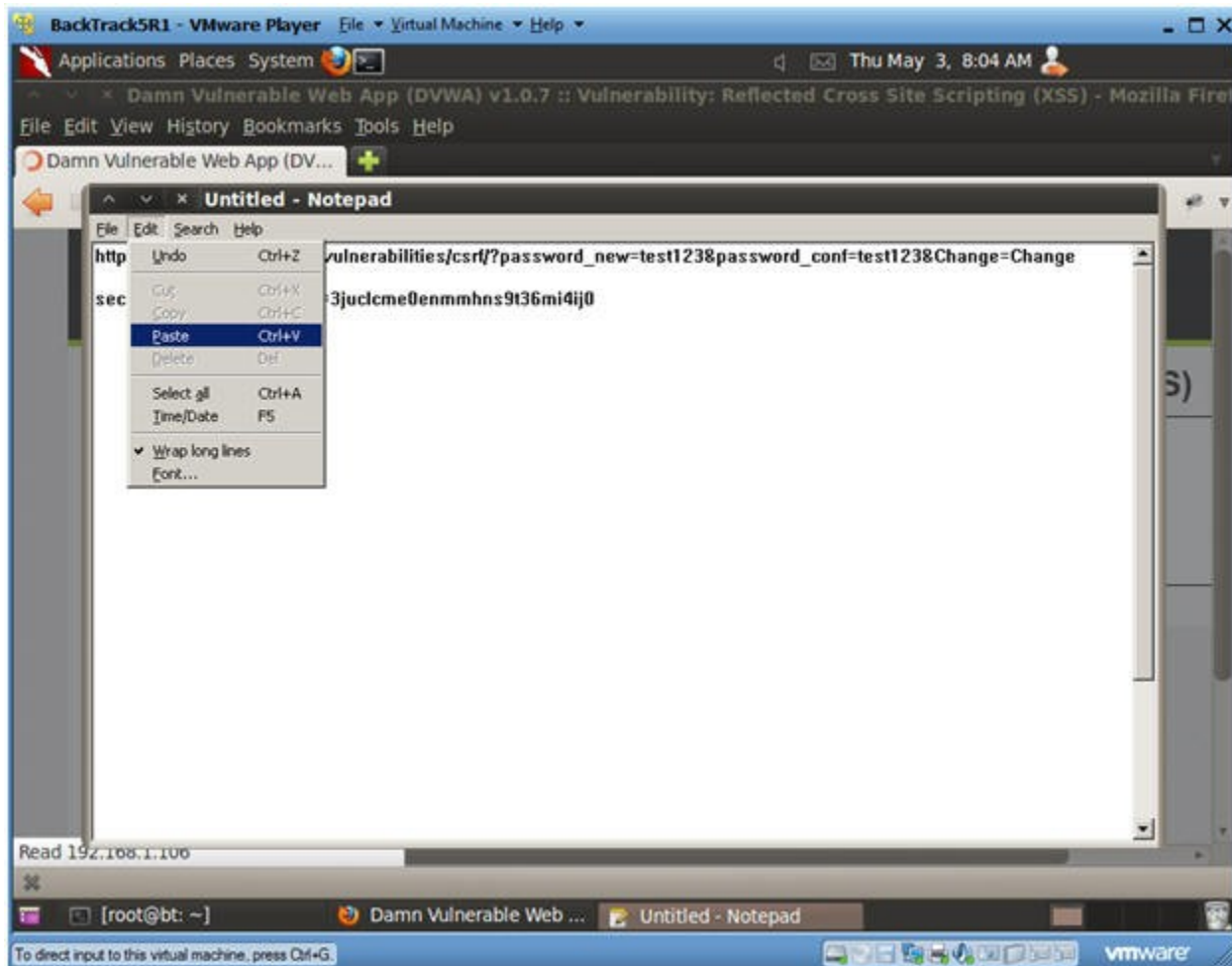


4. Paste Cookie into Notepad

○ **Instructions:**

1. Go back to your notepad

## 2. Edit --> Paste



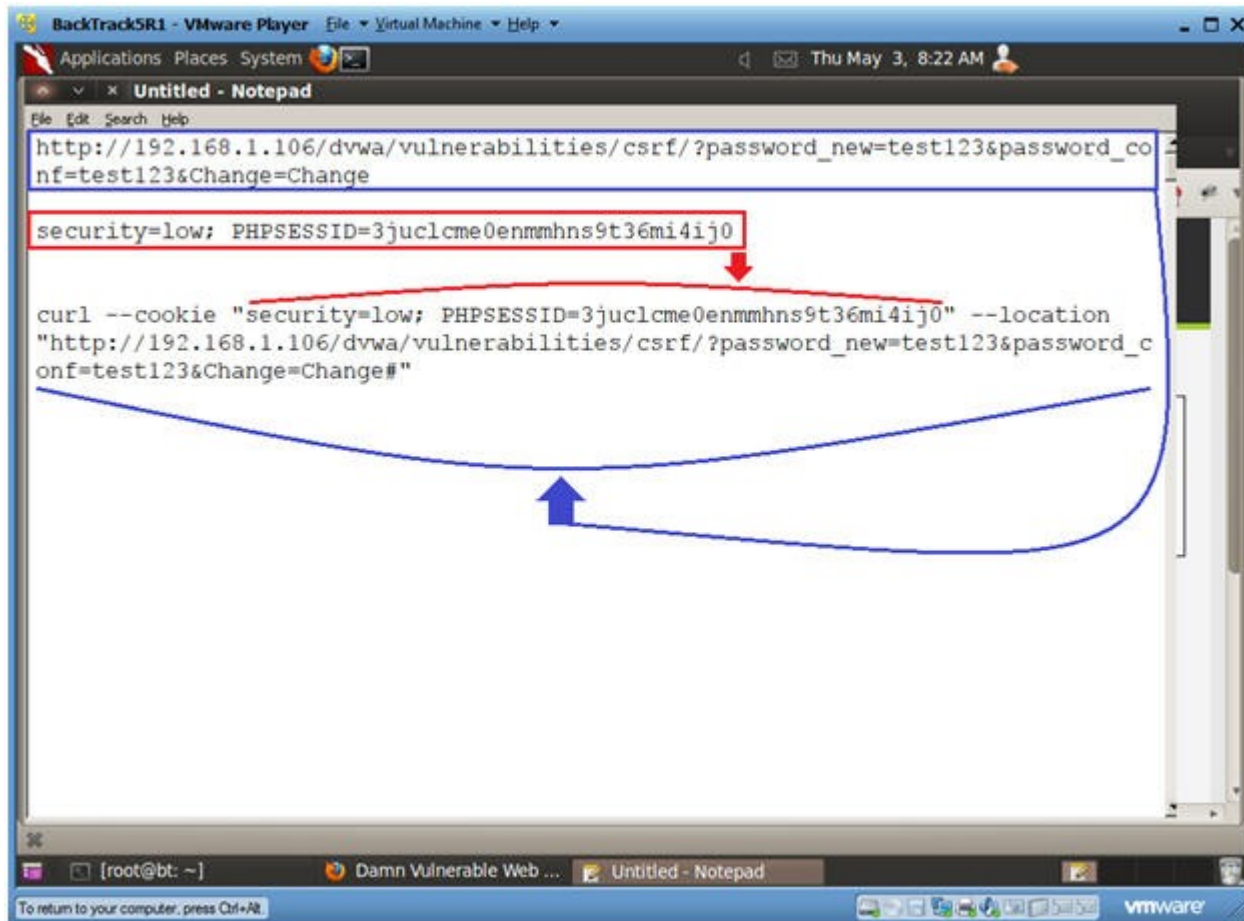
○

## Section 13. Build Curl String

1. Open a console terminal

○ **Instructions:**

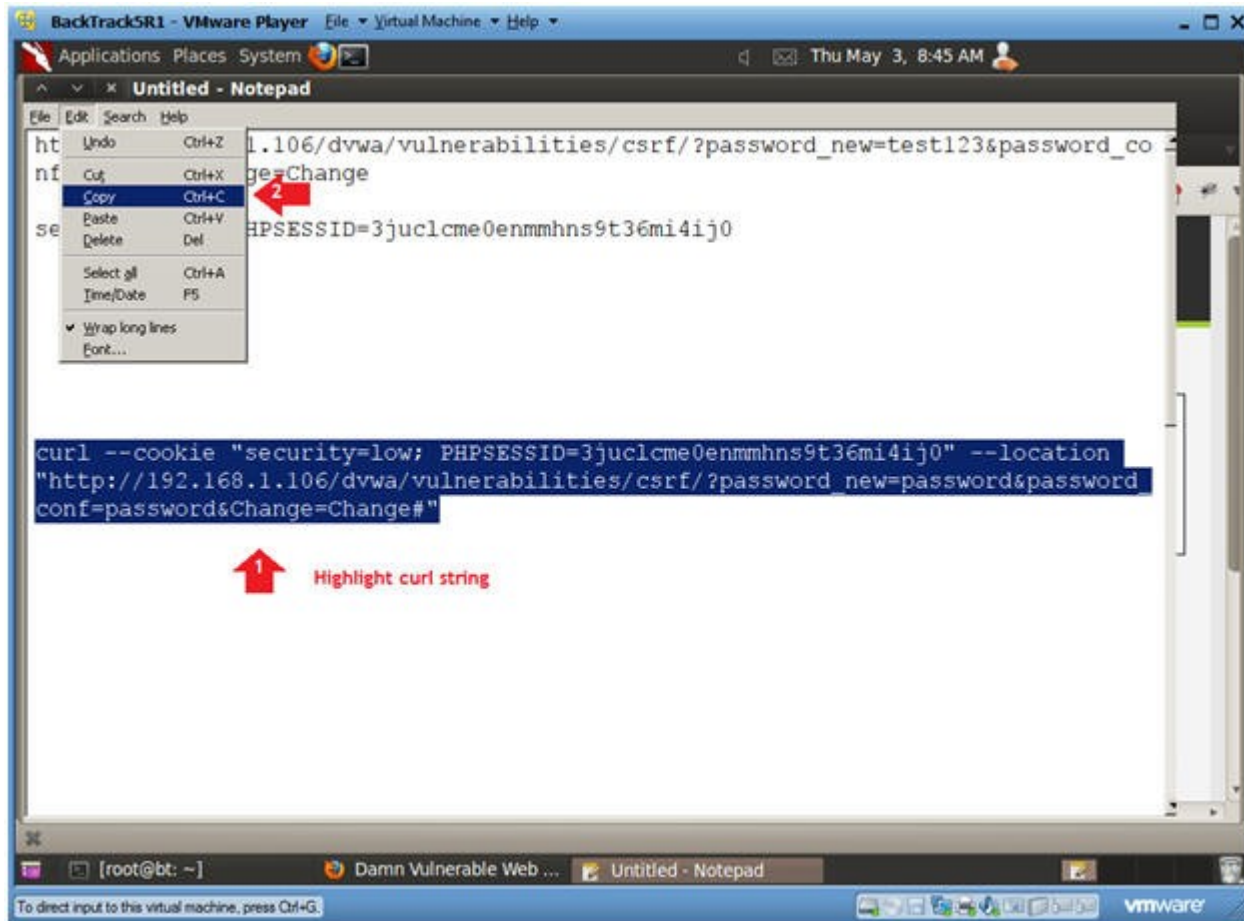
1. **Go to notepad**
2. **In notepad type the following**
  - a. `curl --cookie "" --location ""`
  - b. Place the cookie string between the quotes after the `--cookie` tag.
  - c. Place the html string between the quotes after the `--location` tag.
3. **Your string should now look like the below line and picture**
  - a. `curl --cookie "security=low; PHPSESSID=3juclme0enmmhns9t36mi4ij0" --location "http://<yourIPhere>/dvwa/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#"`
4. **Replace the "test123" password with "password"**
  - a. `curl --cookie "security=low; PHPSESSID=3juclme0enmmhns9t36mi4ij0" --location "http://<yourIPaddresshere>/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change#"`



- 
- 2. Copy Curl String

- **Instructions:**

- 1. Highlight Curl String
    - 2. Edit --> Copy



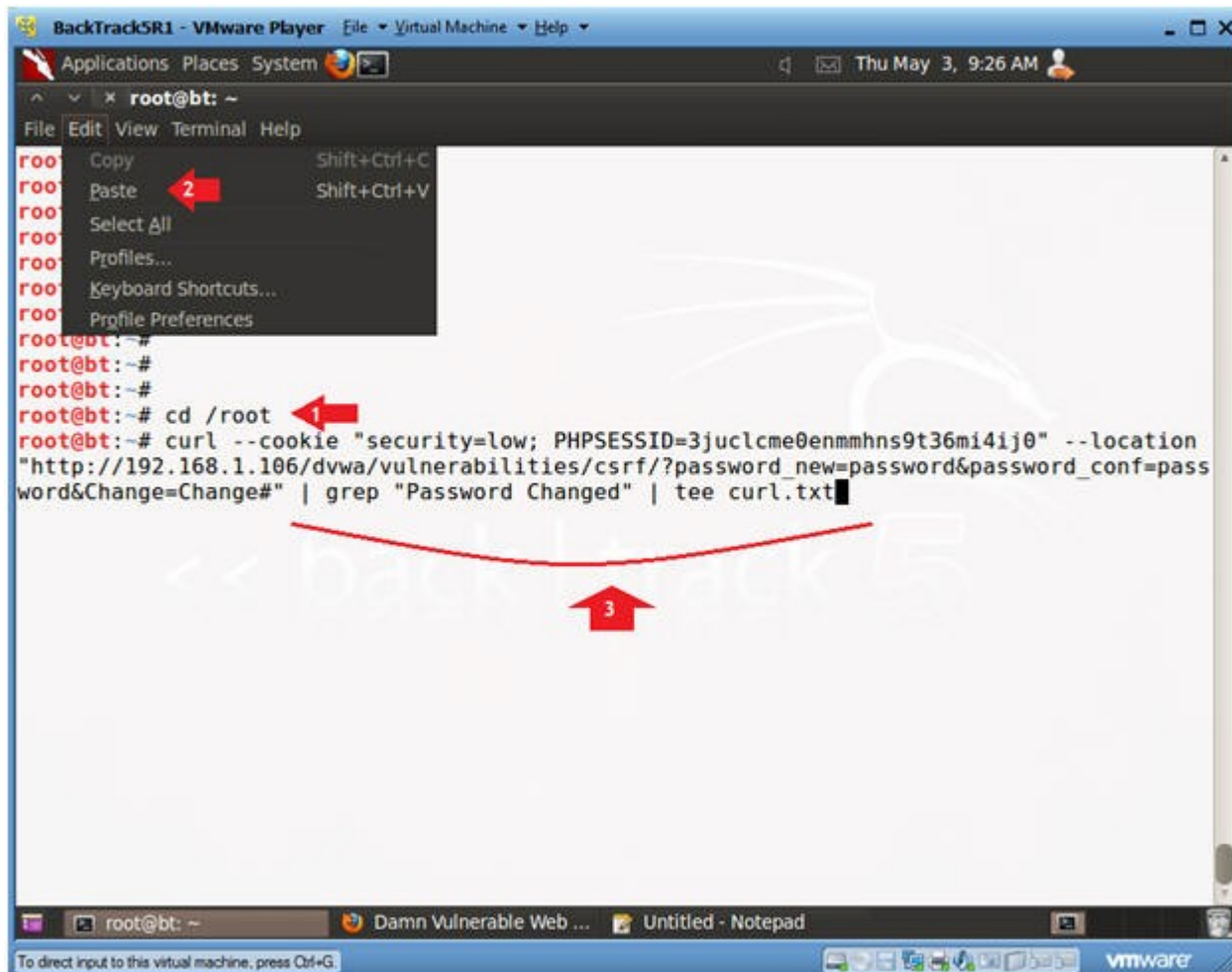
- 
- 3. Open a console terminal
  - **Instructions:**
    1. Click on the console terminal





- 
- 4. Execute Curl String
  - **Instructions:**
    1. cd /root

- 

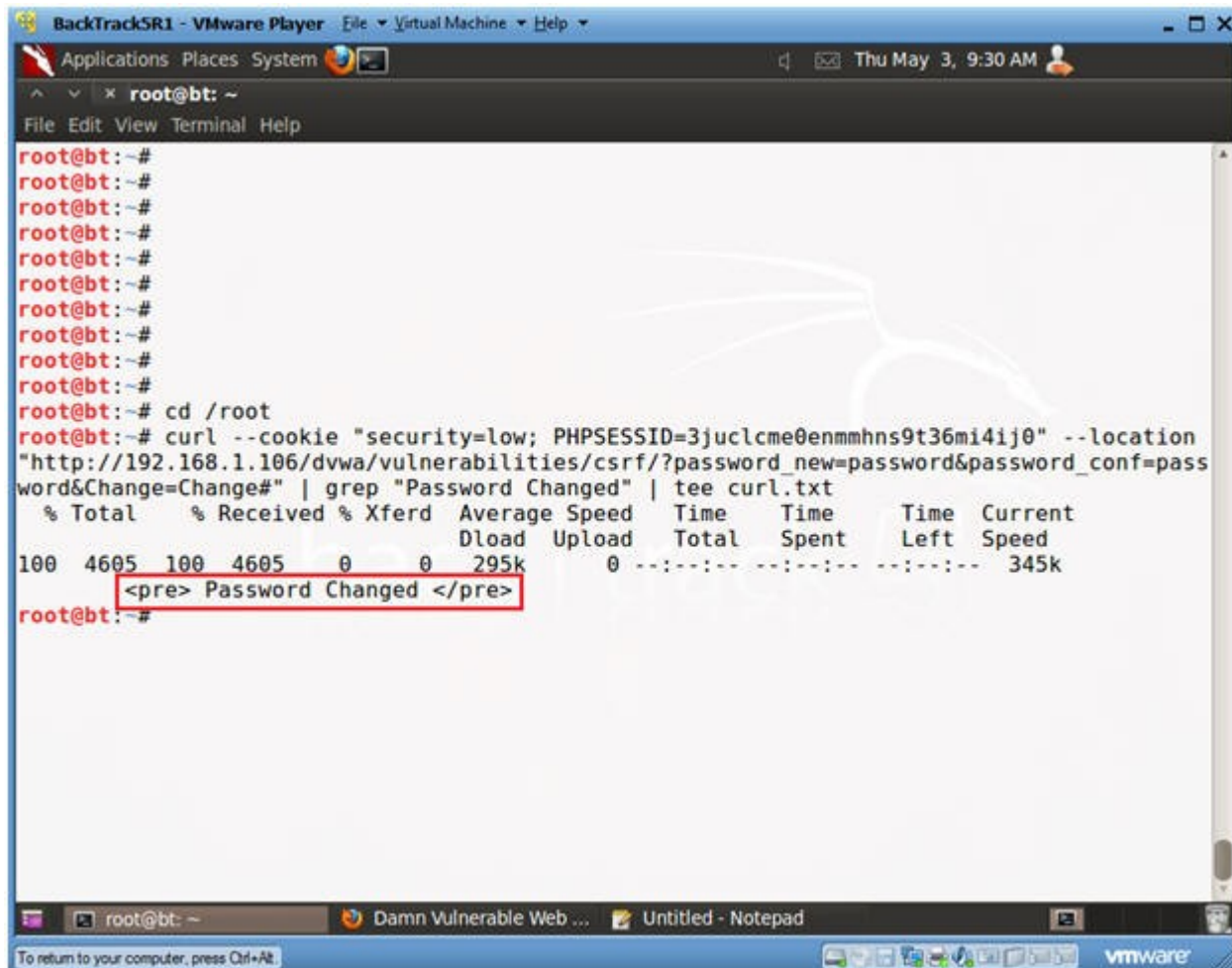




## 2. Verify Curl Results

- **Notes:**

1. You should see the Password Changed message you saw earlier, when you changed your password using the CSRF menu.



The screenshot shows a terminal window titled "BackTrackSR1 - VMware Player". The terminal prompt is "root@bt: ~". The user has entered a curl command to perform a CSRF attack on a DVWA instance. The output shows a successful request with a "Password Changed" message. The message is highlighted with a red box.

```
root@bt: ~  
File Edit View Terminal Help  
root@bt: ~#  
root@bt: ~#  
root@bt: ~#  
root@bt: ~#  
root@bt: ~#  
root@bt: ~#  
root@bt: ~#  
root@bt: ~#  
root@bt: ~#  
root@bt: ~#  
root@bt: ~#  
root@bt: ~#  
root@bt: ~# cd /root  
root@bt: ~# curl --cookie "security=low; PHPSESSID=3juclcme0enmmhns9t36mi4ij0" --location  
"http://192.168.1.106/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=pass  
word&Change=Change#" | grep "Password Changed" | tee curl.txt  
% Total % Received % Xferd Average Speed Time Time Time Current  
Dload Upload Total Spent Left Speed  
100 4605 100 4605 0 0 295k 0 --:--:-- --:--:-- --:--:-- 345k  
<pre> Password Changed </pre>  
root@bt: ~#
```

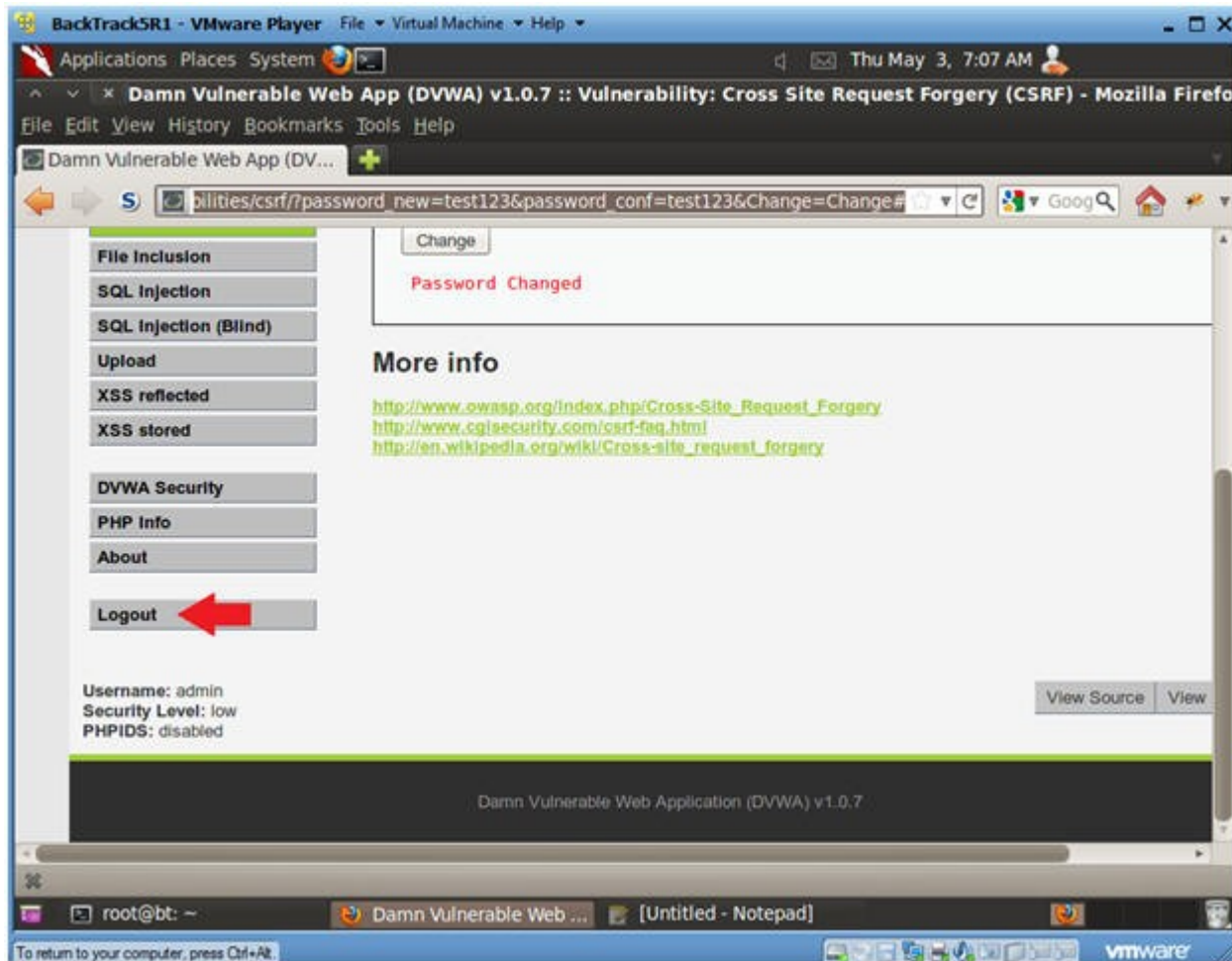
○

## Section 14. Test Curl String Password Change

### 1. Logout of DVWA

- **Instructions:**

- 1. In the Left Navigation Menu, Click Logout

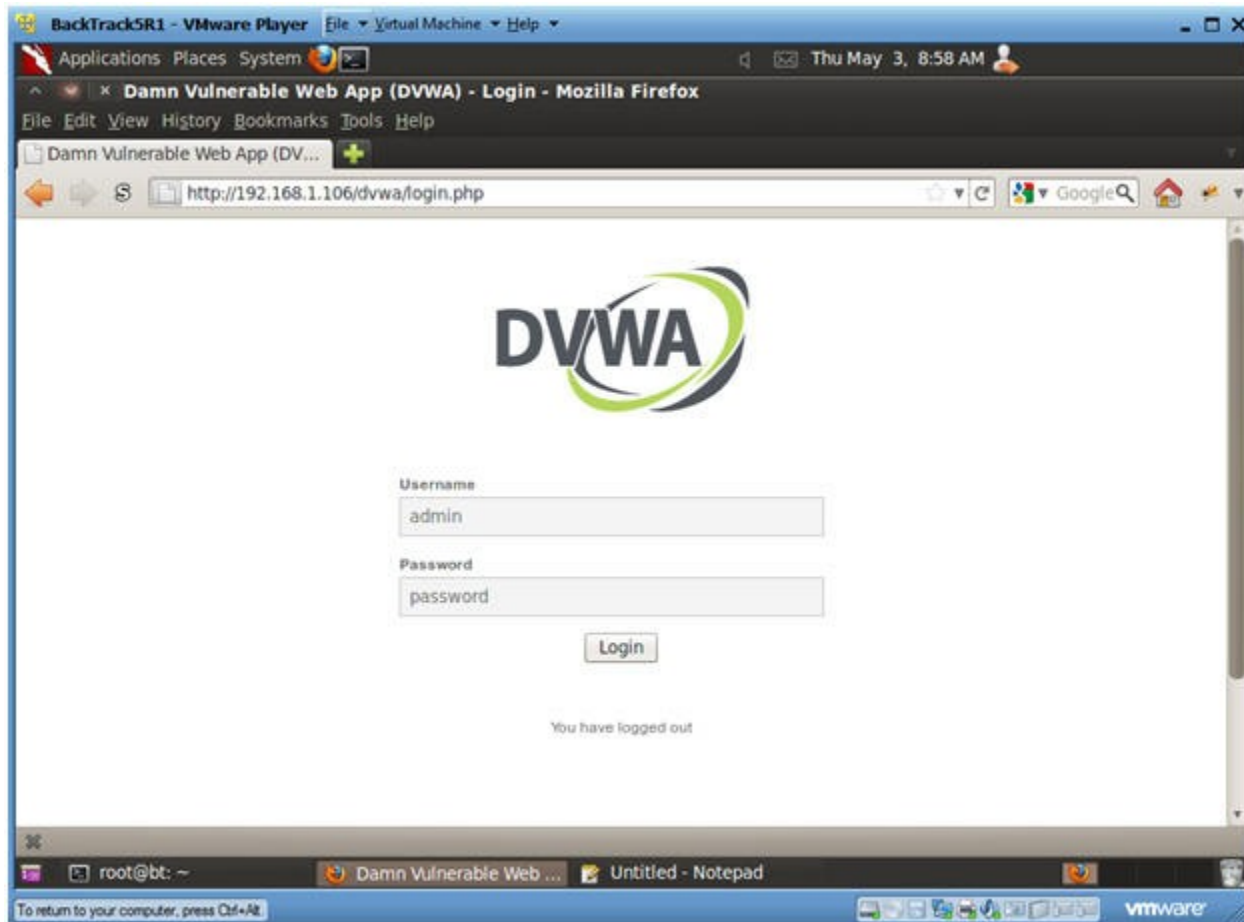


-

## 2. Login to DVWA

- **Instructions:**

1. Username: admin
2. Password: password

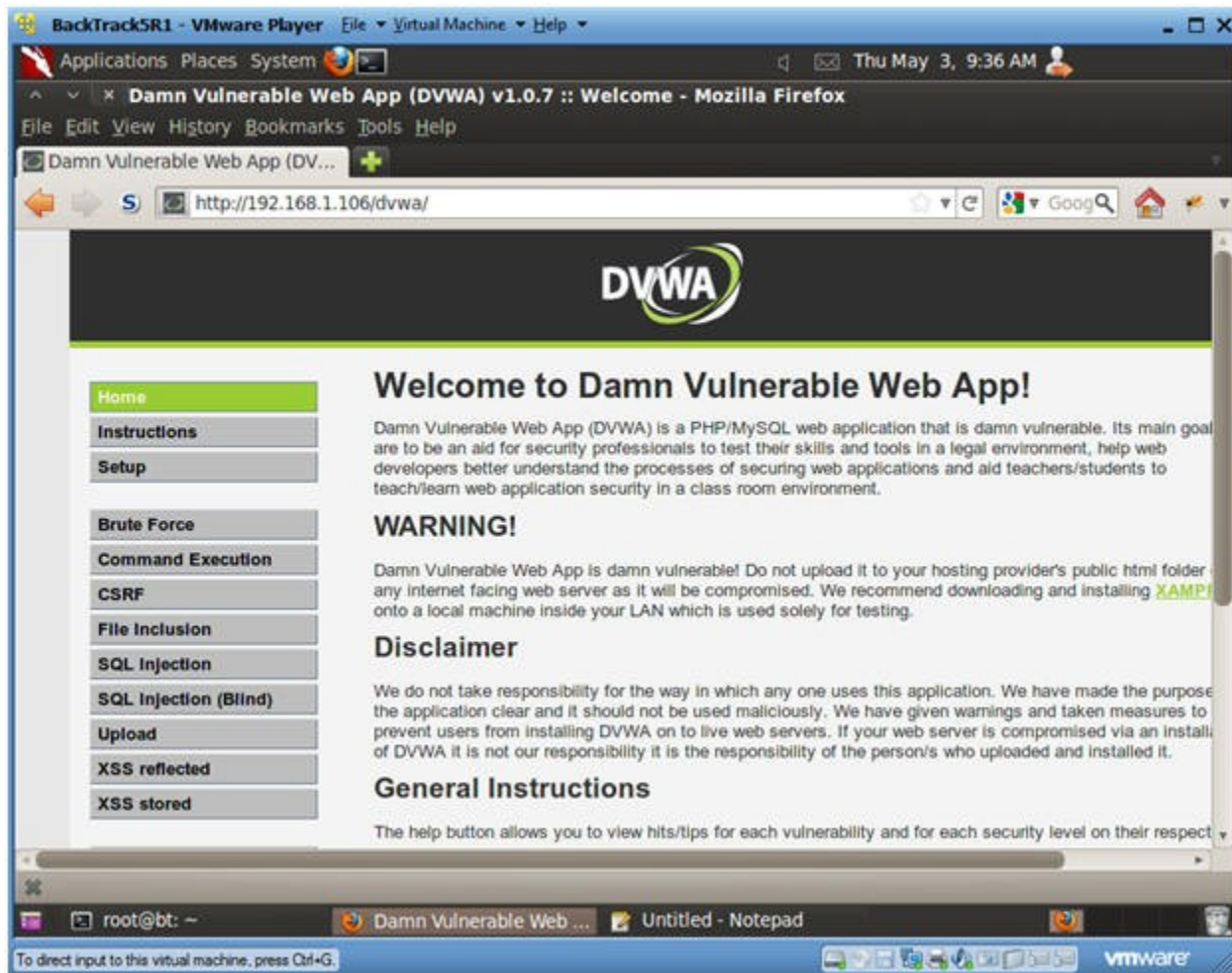


○

### 3. Welcome to DVWA

- **Notes:**

1. If you see the Welcome Screen, then you have successfully use curl to change the password remotely without a browser.



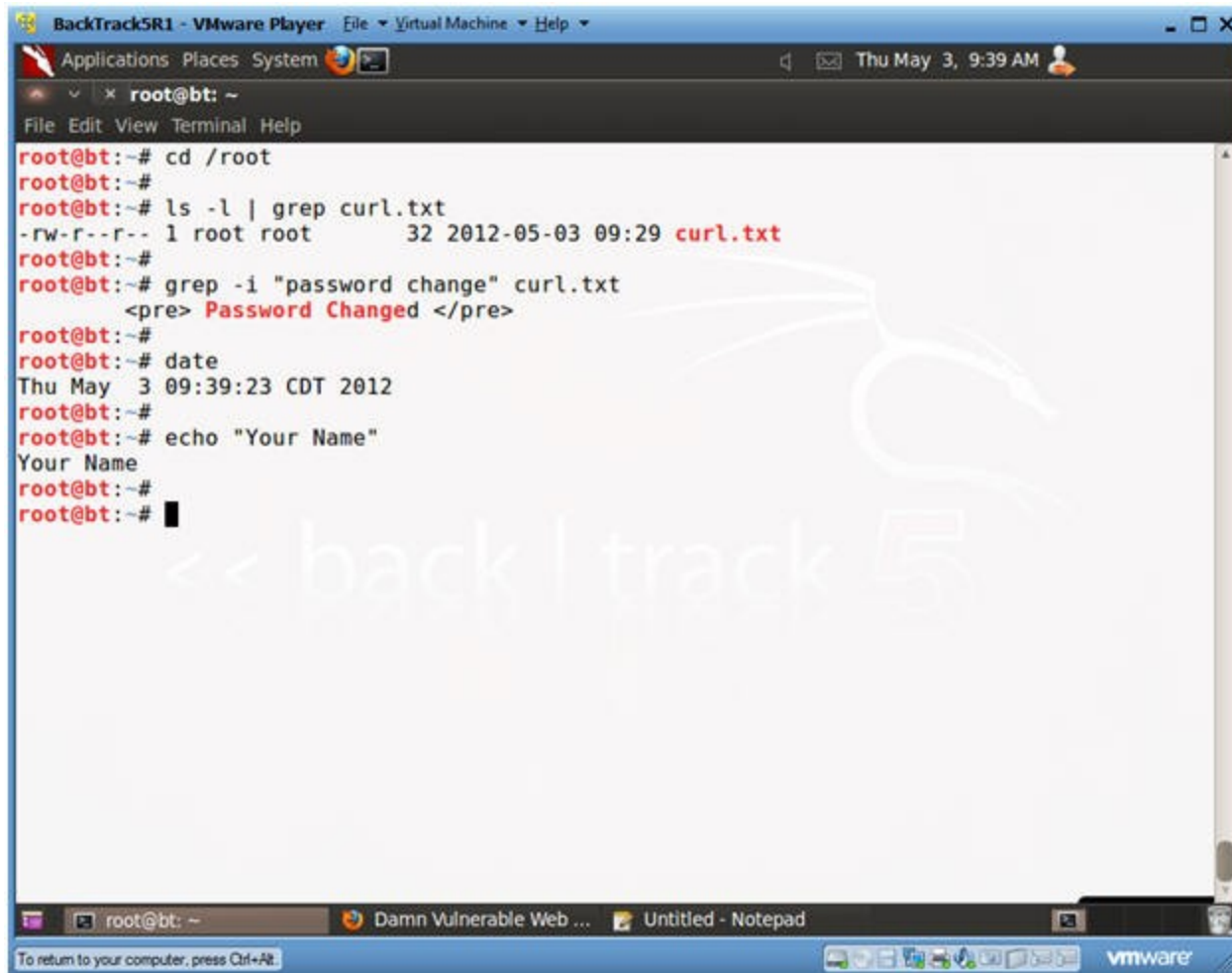
○

## Proof of Lab

### 1. Proof of Lab

- **Proof of Lab Instructions:**

1. Pull up a BackTrack Terminal Window
2. `cd /root`
3. `ls -l | grep curl.txt`
4. `grep -i "password change" curl.txt`
5. `date`
6. `echo "Your Name"`
  - Replace the string "Your Name" with your actual name.
  - e.g., `echo "Octavius Walton"`
7. Do a <PrtScn>
8. Paste into a word document
9. Upload to TeamBox



```
BackTrack5R1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: ~
File Edit View Terminal Help
root@bt:~# cd /root
root@bt:~#
root@bt:~# ls -l | grep curl.txt
-rw-r--r-- 1 root root      32 2012-05-03 09:29 curl.txt
root@bt:~#
root@bt:~# grep -i "password change" curl.txt


```
 Password Changed 
```


root@bt:~#
root@bt:~# date
Thu May  3 09:39:23 CDT 2012
root@bt:~#
root@bt:~# echo "Your Name"
Your Name
root@bt:~#
root@bt:~#
```

backtrack 5

root@bt: ~ Damn Vulnerable Web ... Untitled - Notepad

To return to your computer, press Ctrl+Alt

○

