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

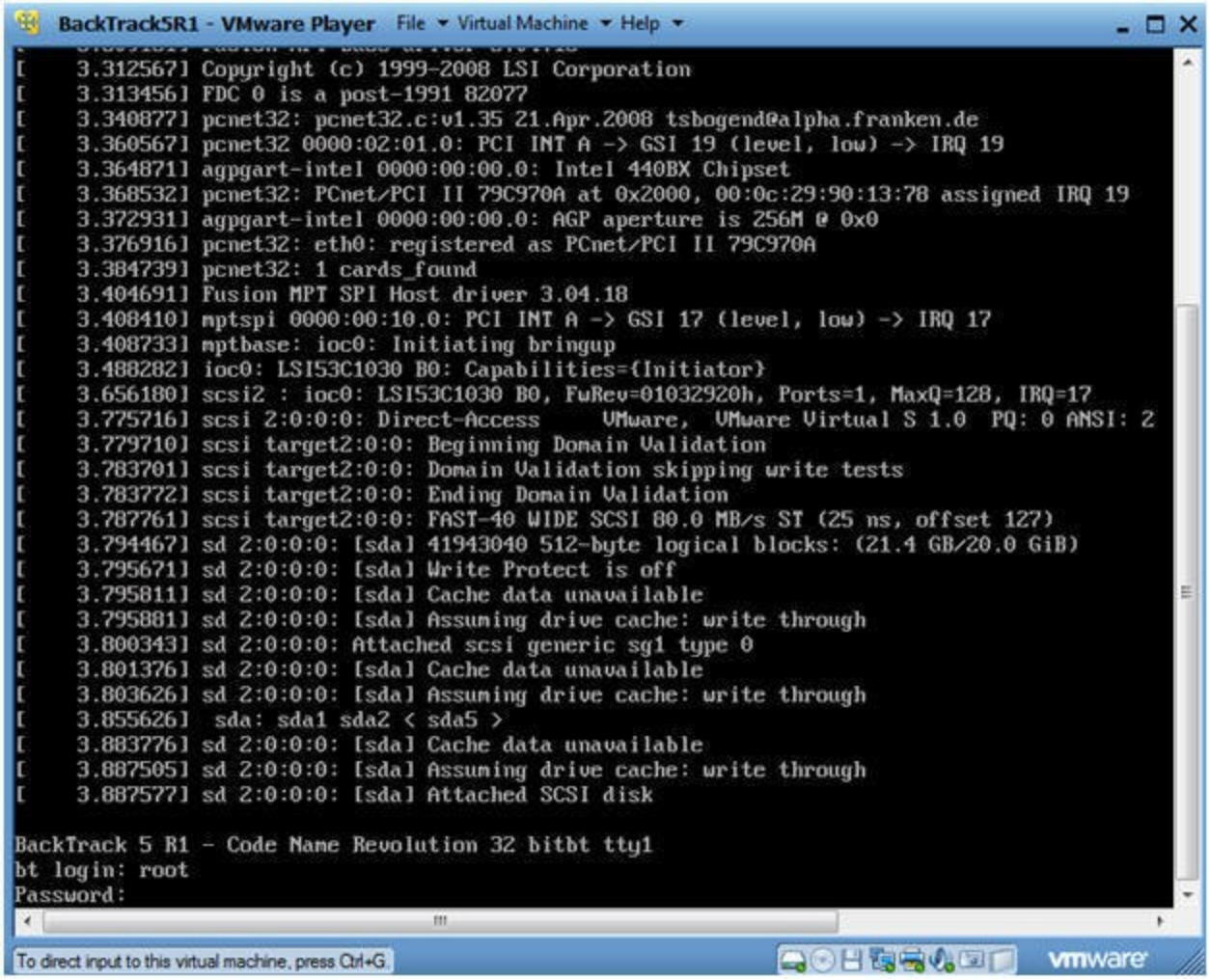
- What is Damn Vulnerable Web App (DVWA)?
  - Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable.
  - Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes 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.

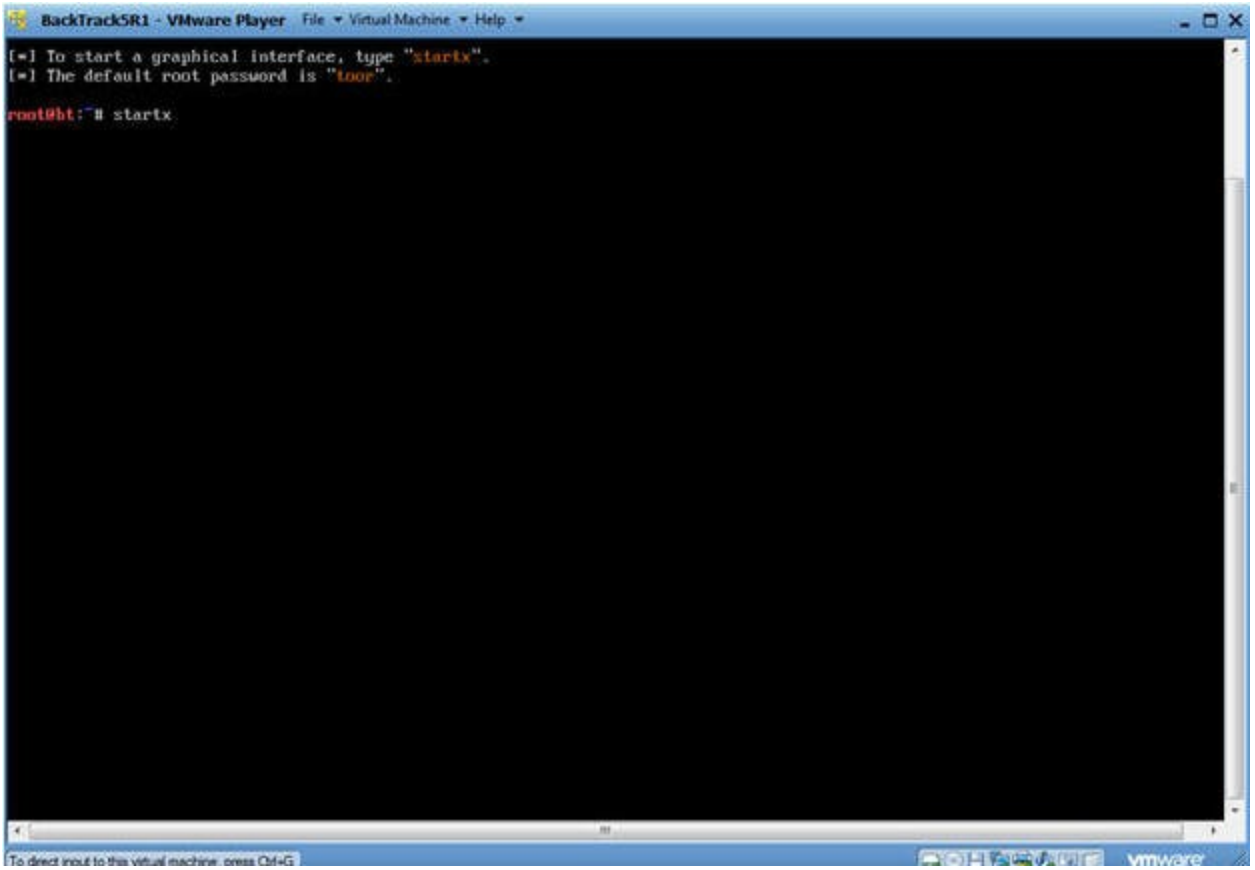
  -

1. Login to BackTrack

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

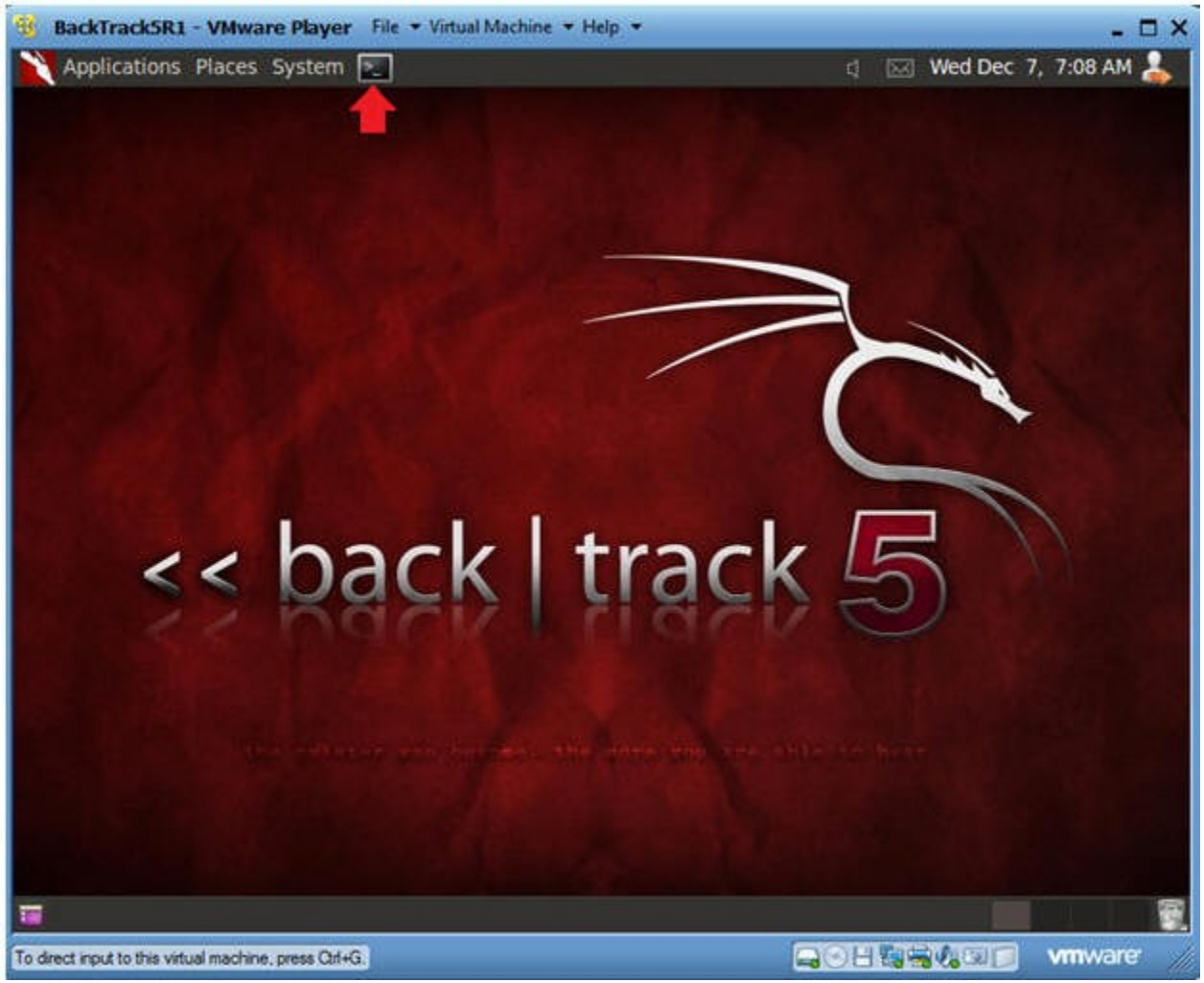


2. Bring up the GNOME
    - **Instructions:**
        1. Type startx



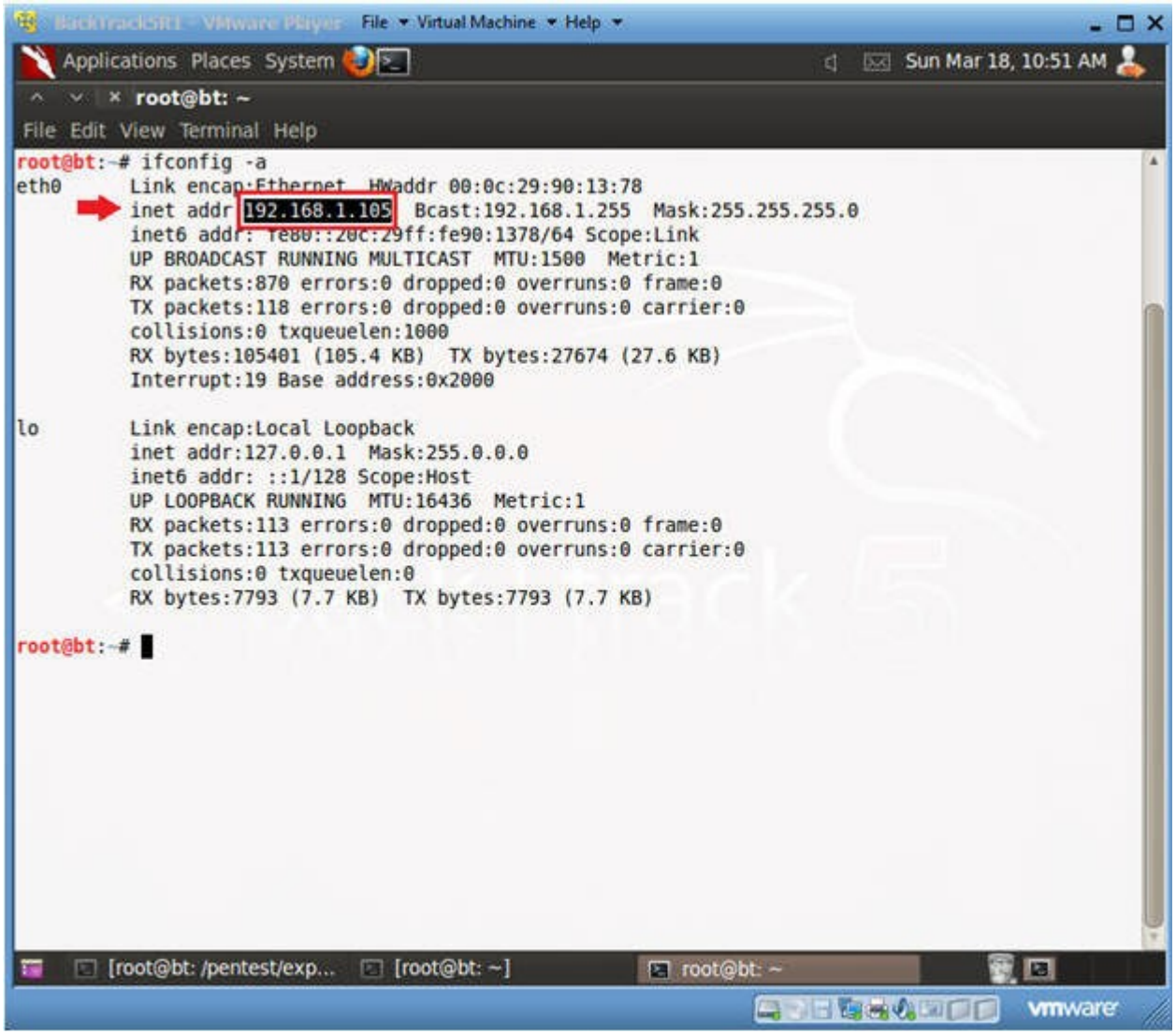
Section 7. Open Console Terminal and Retrieve IP Address

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.



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

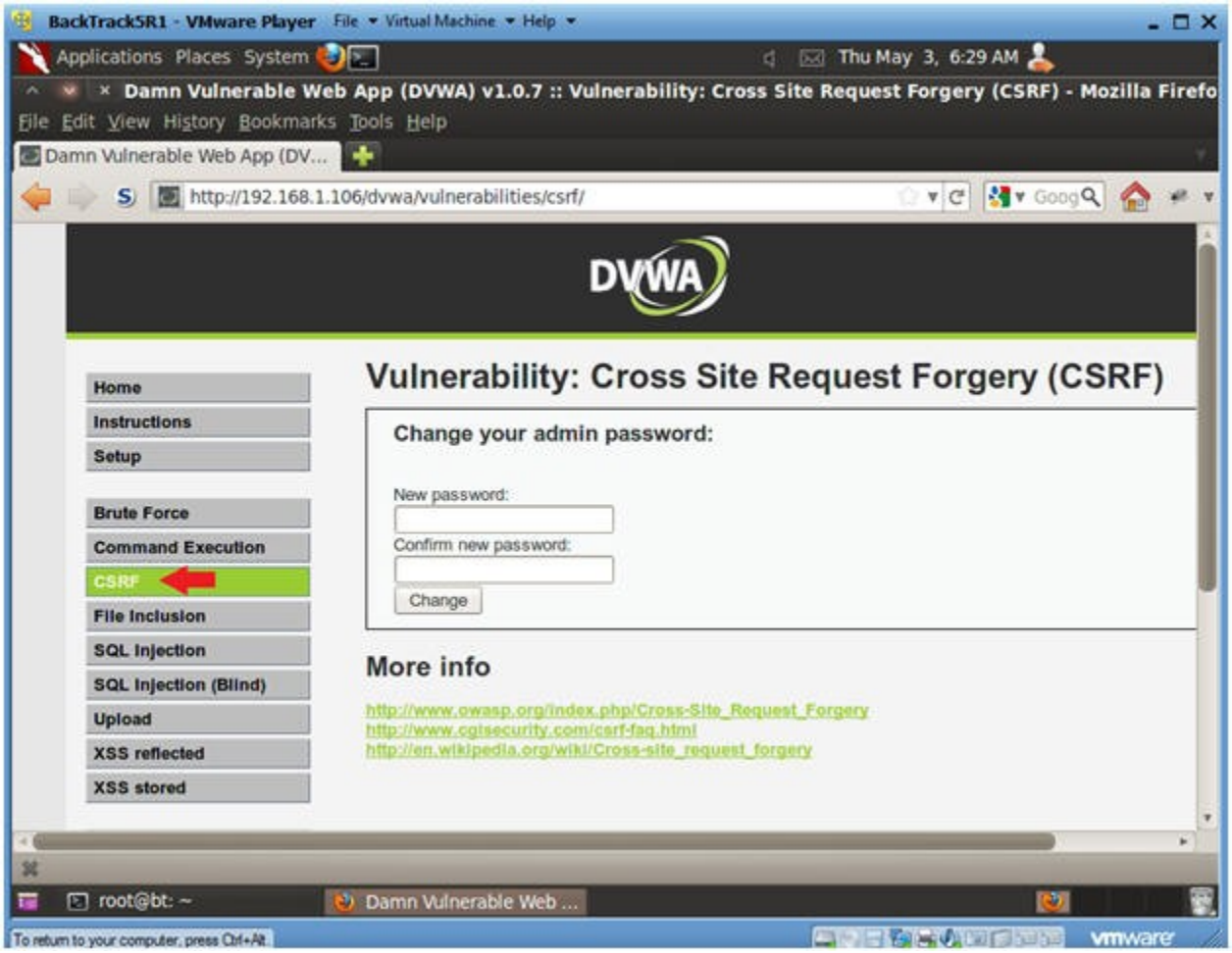
Section 9. Set Security Level

1. Set DVWA Security Level

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

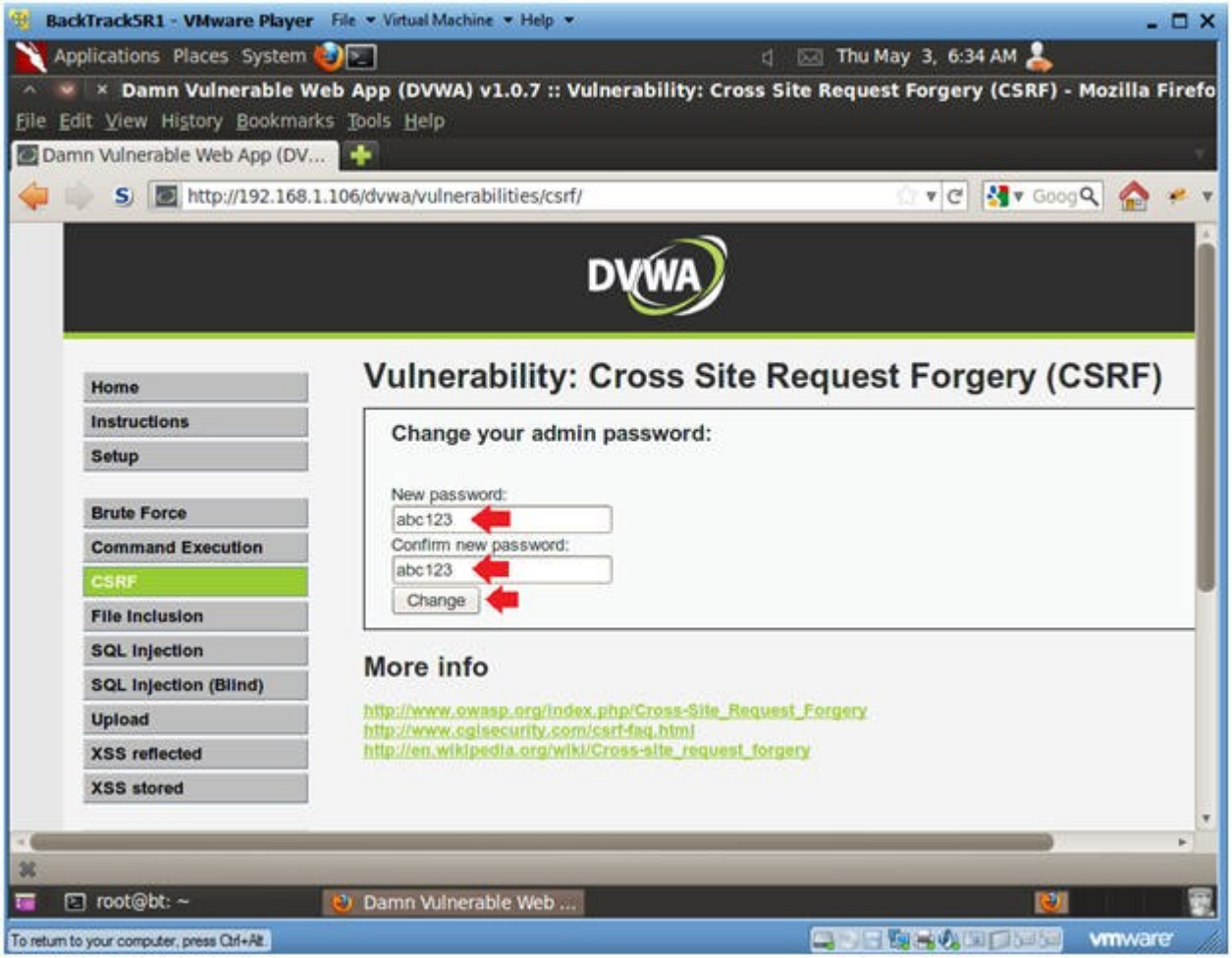
Cross Site Request Forgery

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



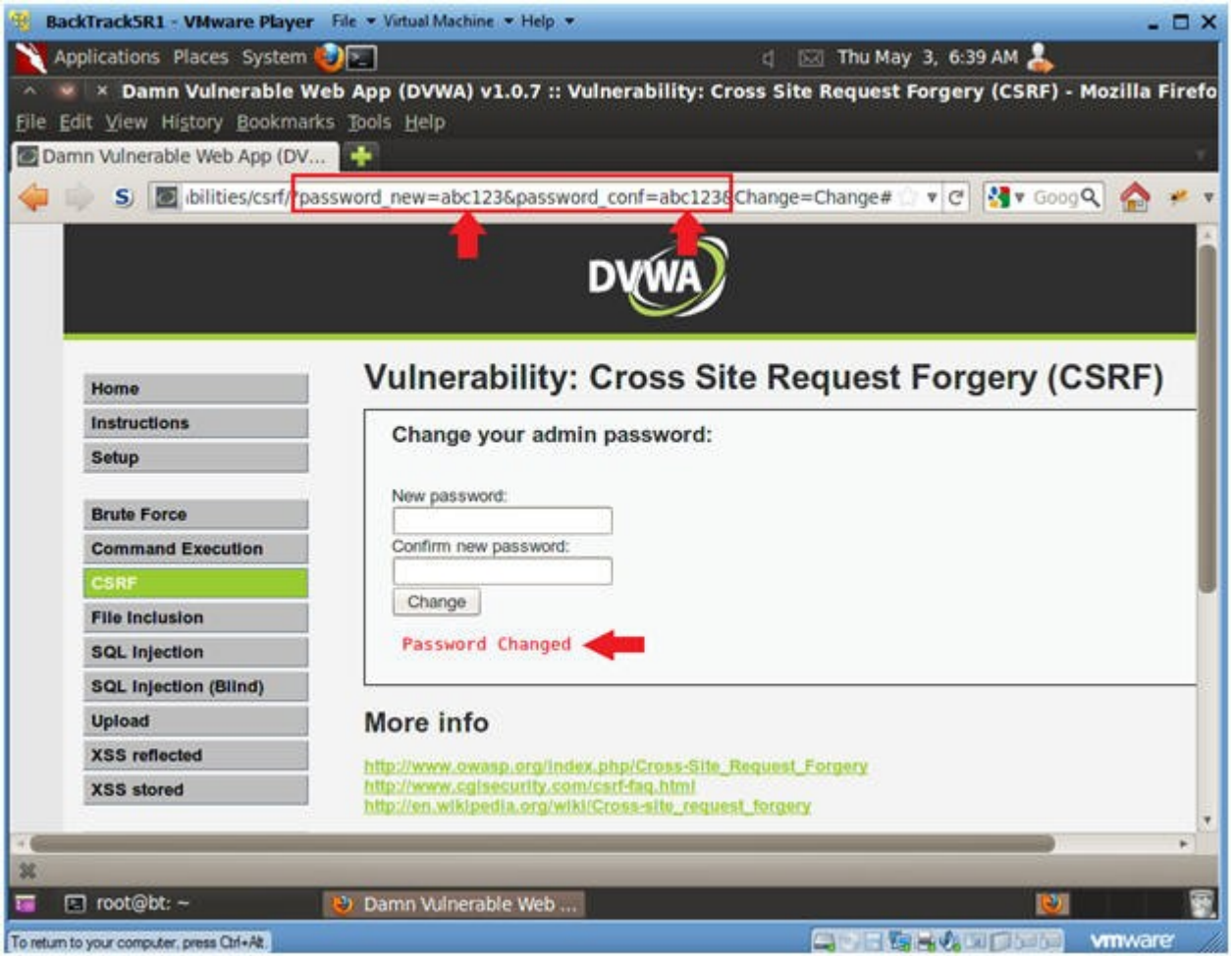
2. Basic CSRF Test
    - **Instructions:**
        1. New password: abc123
        2. Confirm new password: abc123

3. Click Change



3. View Password Change Results
   - **Notes:**
     1. Below the change button you will notice the message that says "Password Changed."

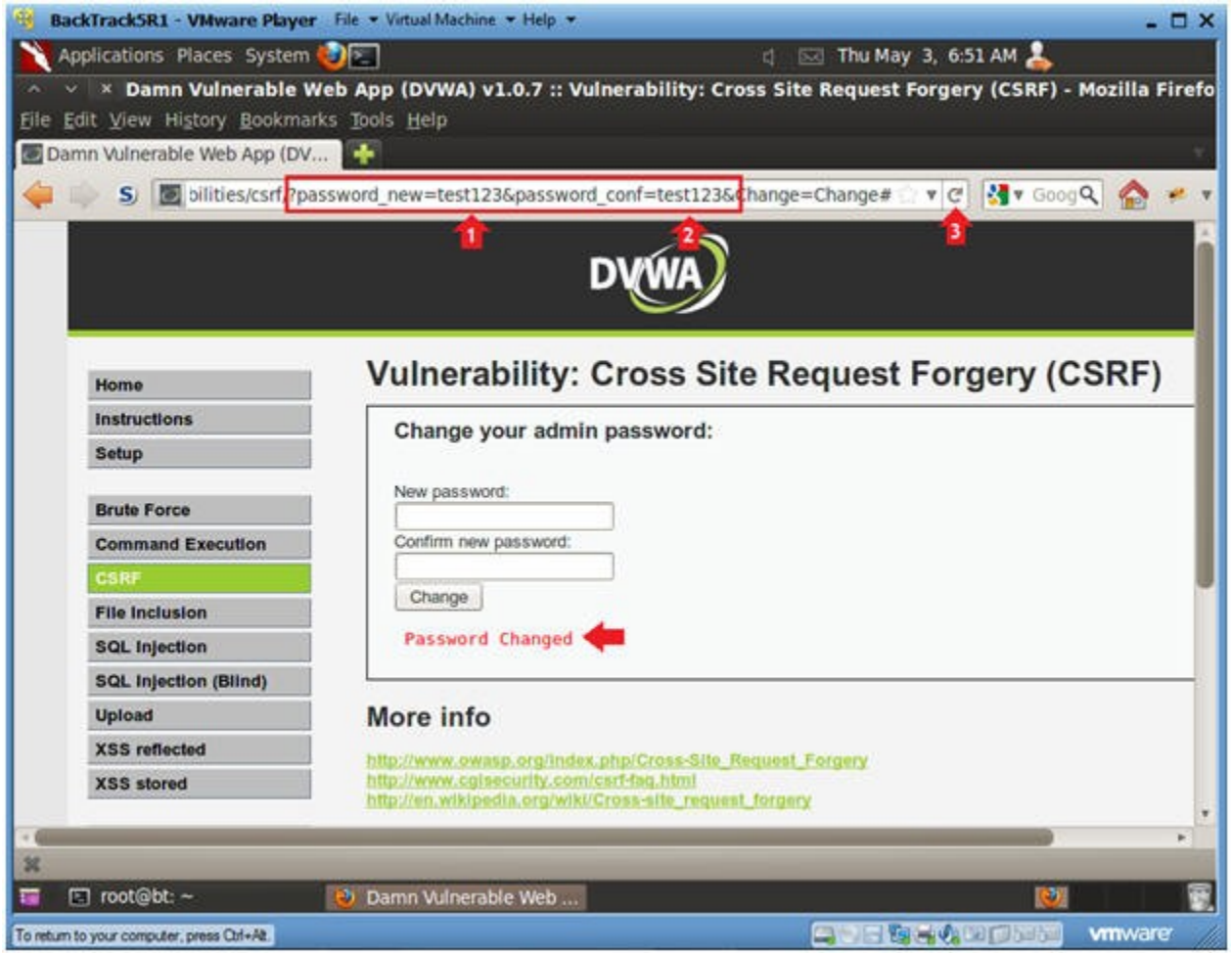
2. What I really want you to notice is the URL string.
3. See how the URL string has the below two parameters separated by a "&".
    a. password_new=abc123
    b. password_conf=abc123
4. This is DVWA's example of bad implementation of how to change a password on a web application for the following reasons:
    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.

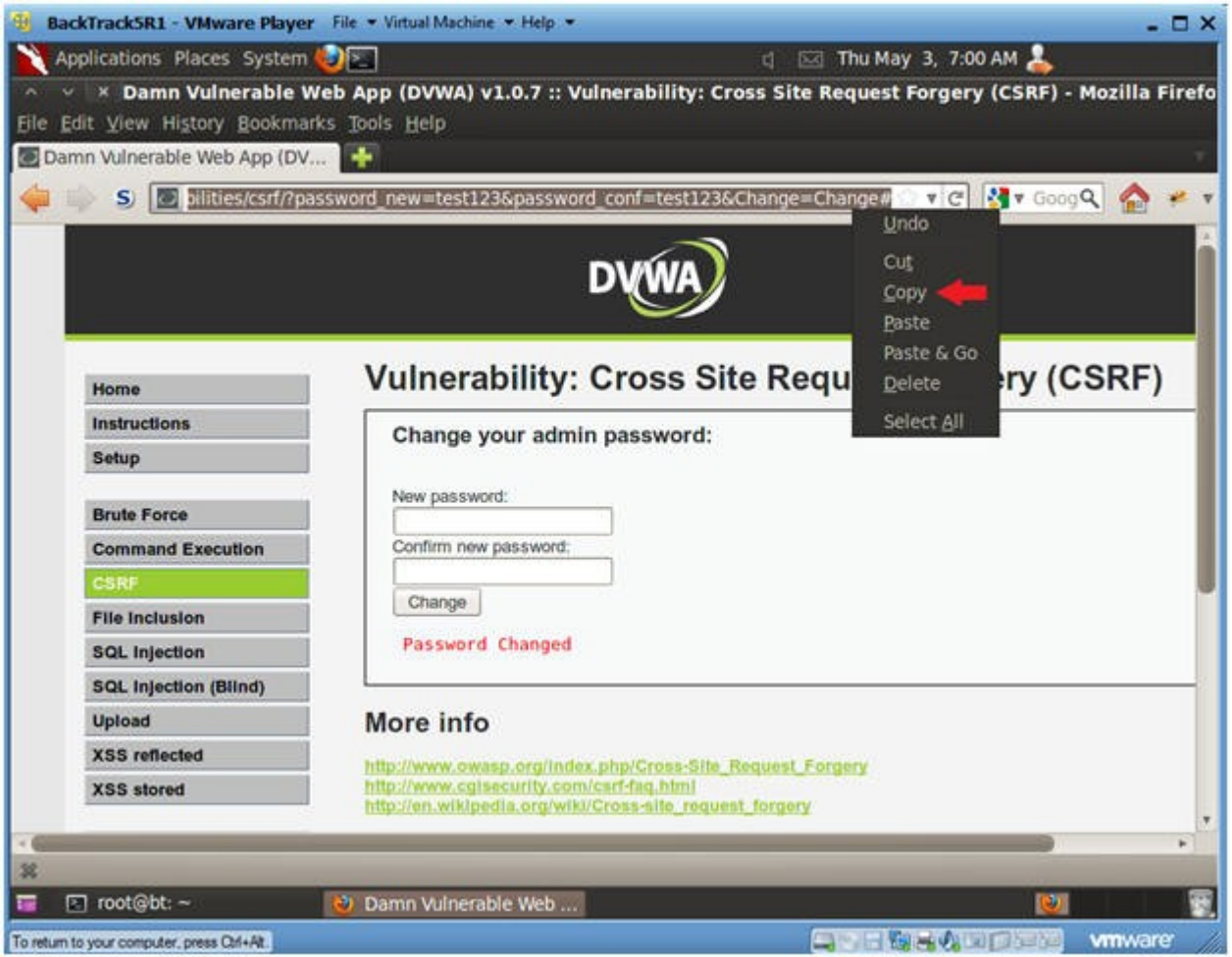
3. Click the Reload Current Page Arrow

- **Notes:**
  1. Notice the Password is changed

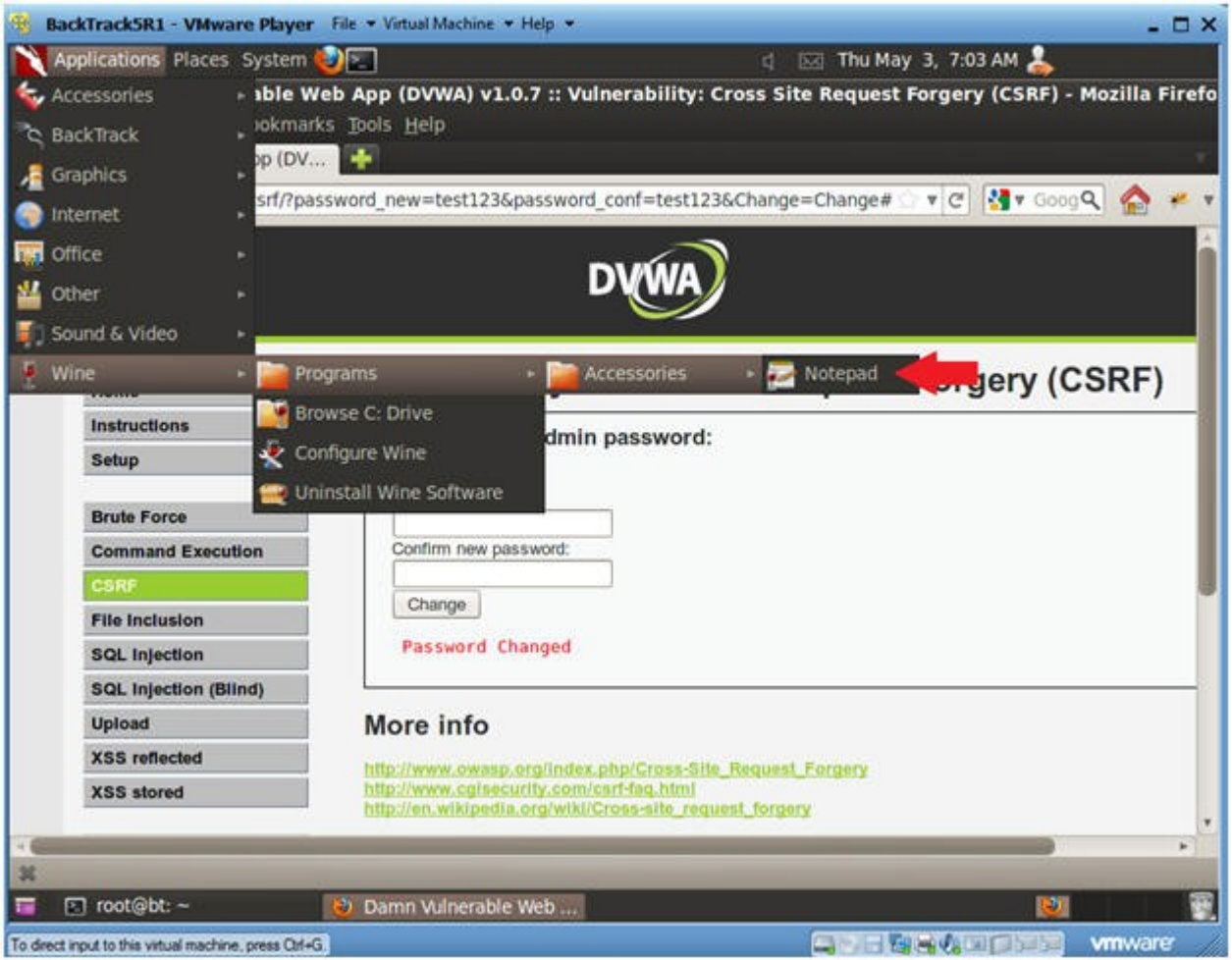


5. Copy CSRF URL

- **Instructions:**
  1. Highlight the URL
  2. Right Click
  3. Copy

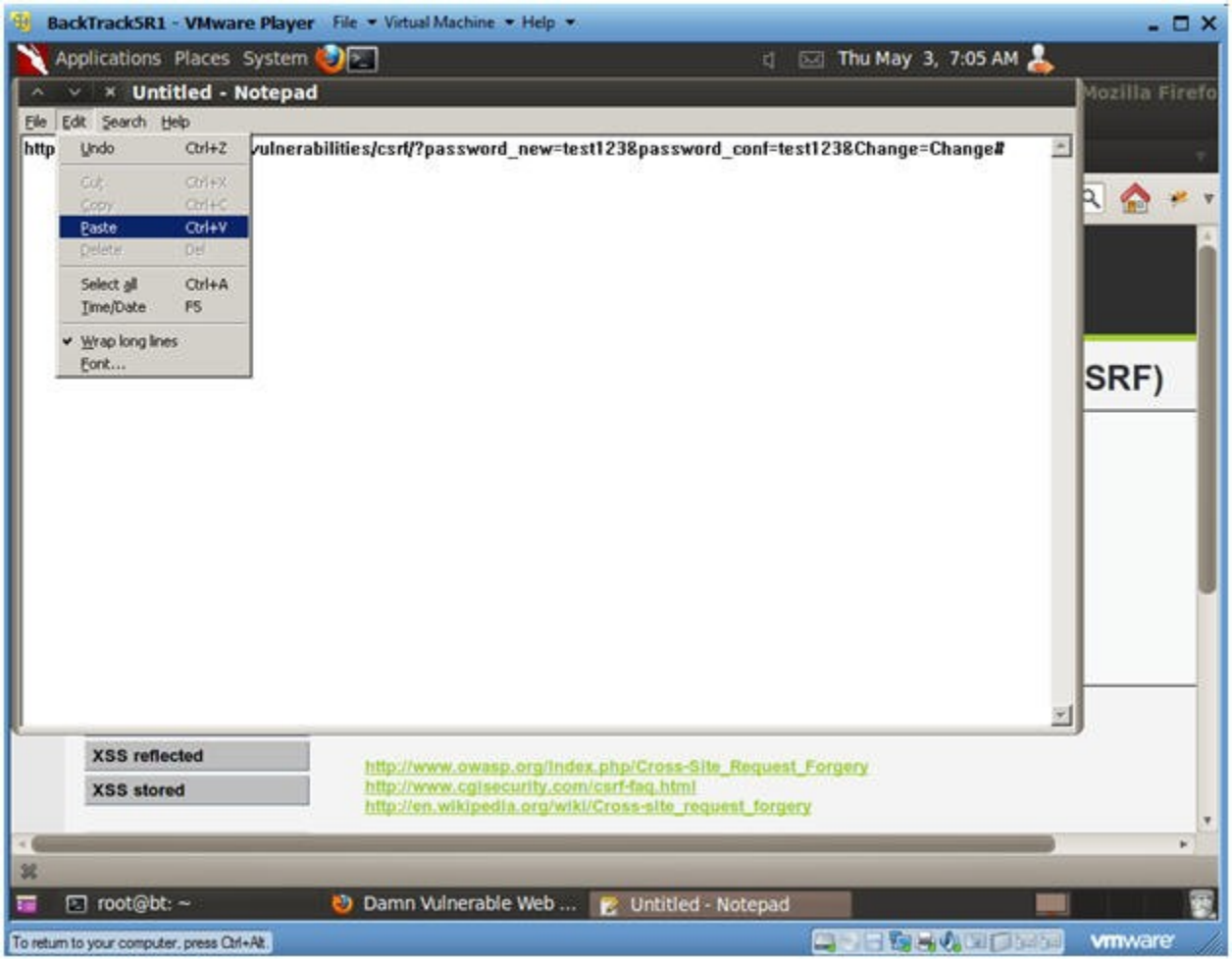


6. Start Notepad
    - **Instructions:**
        1. Applications --> Wine --> Programs --> Notepad



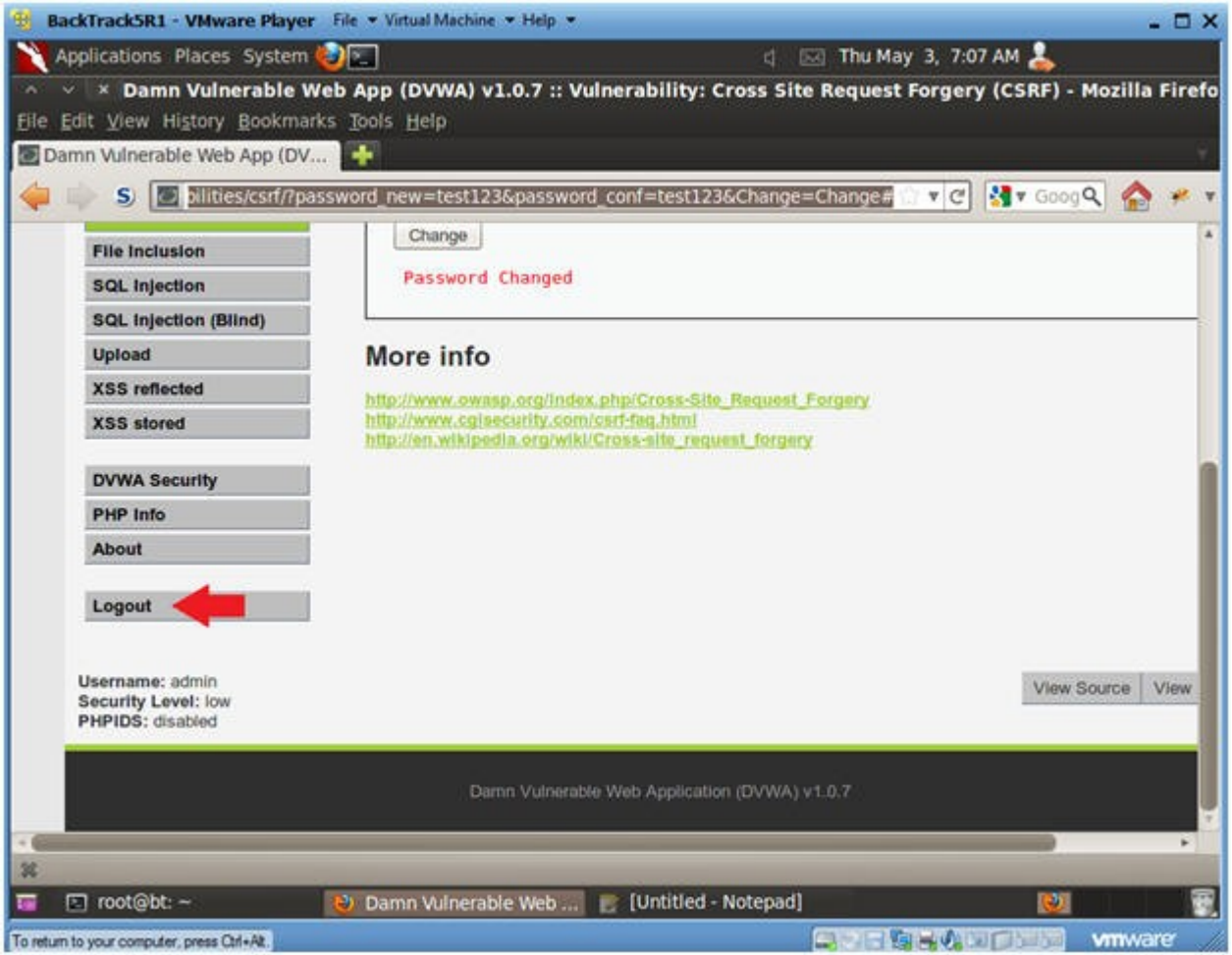
7. Paste URL into Notepad

- **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

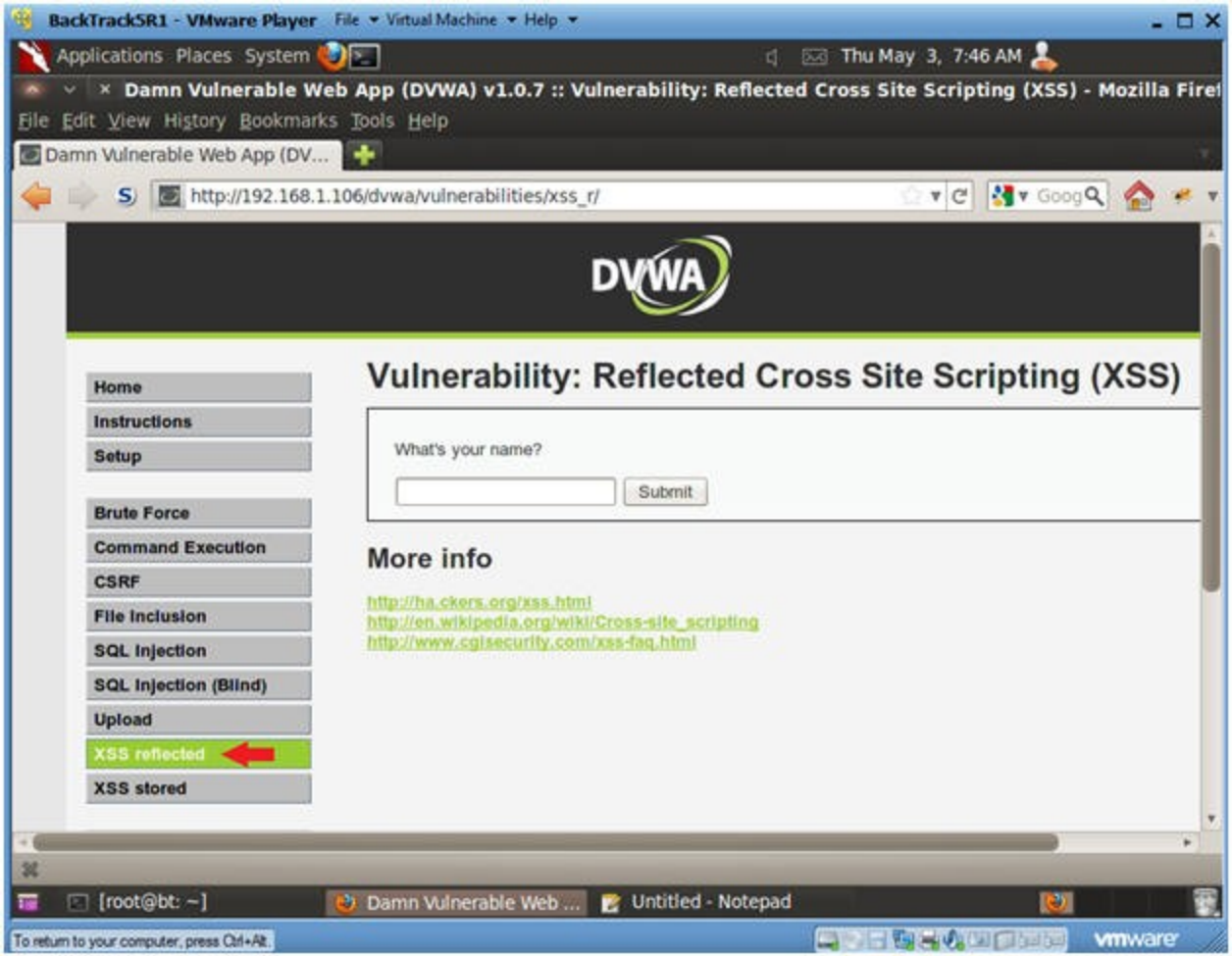
- **Instructions:**
  1. Username: admin
  2. Password: test123

3. Set DVWA Security Level

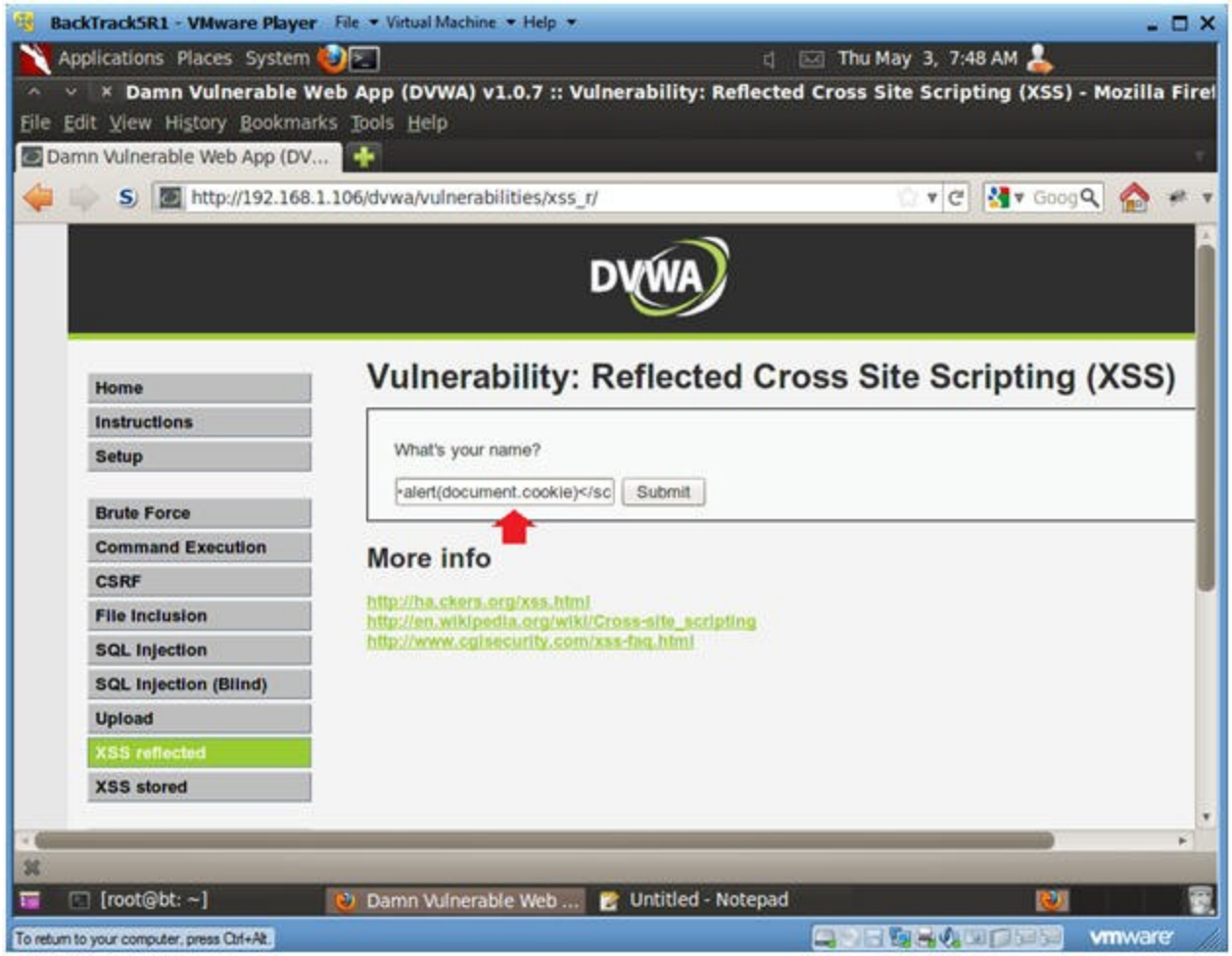
- **Instructions:**
  1. Click on DVWA Security, in the left hand menu.
  2. Select "low"
  3. Click Submit

Section 12. XSS reflected

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

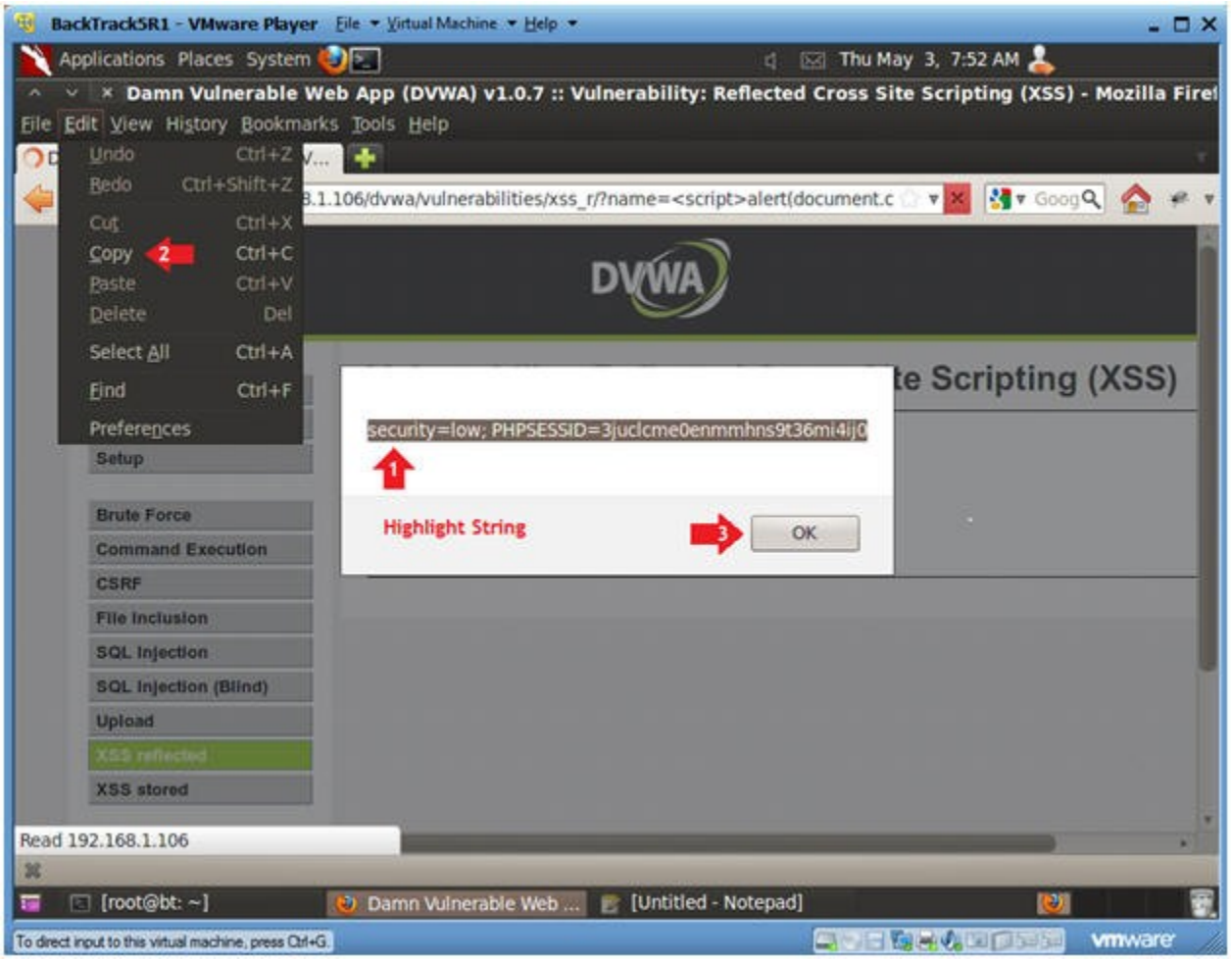


2. Submit cookie XSS attack
    - **Instructions:**
        1. What's your Name? <script>alert(document.cookie)</script>
        2. Click Submit



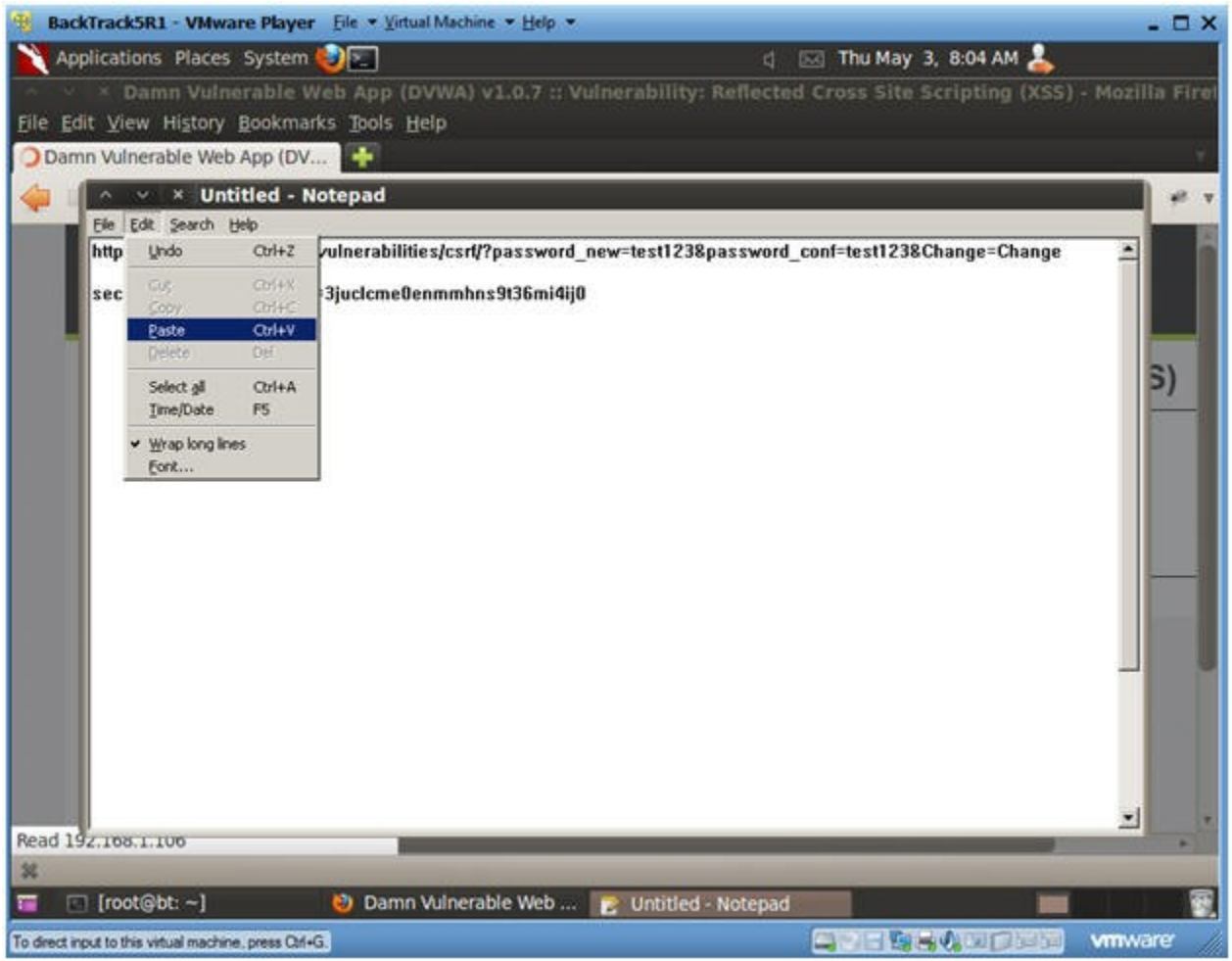
3. Copy Cookie String
    - **Instructions:**
        1. Highlight The Cookie String
        2. Edit --> Copy

3. Click the OK button



4. Paste Cookie into Notepad
   - **Instructions:**
     1. Go back to your notepad

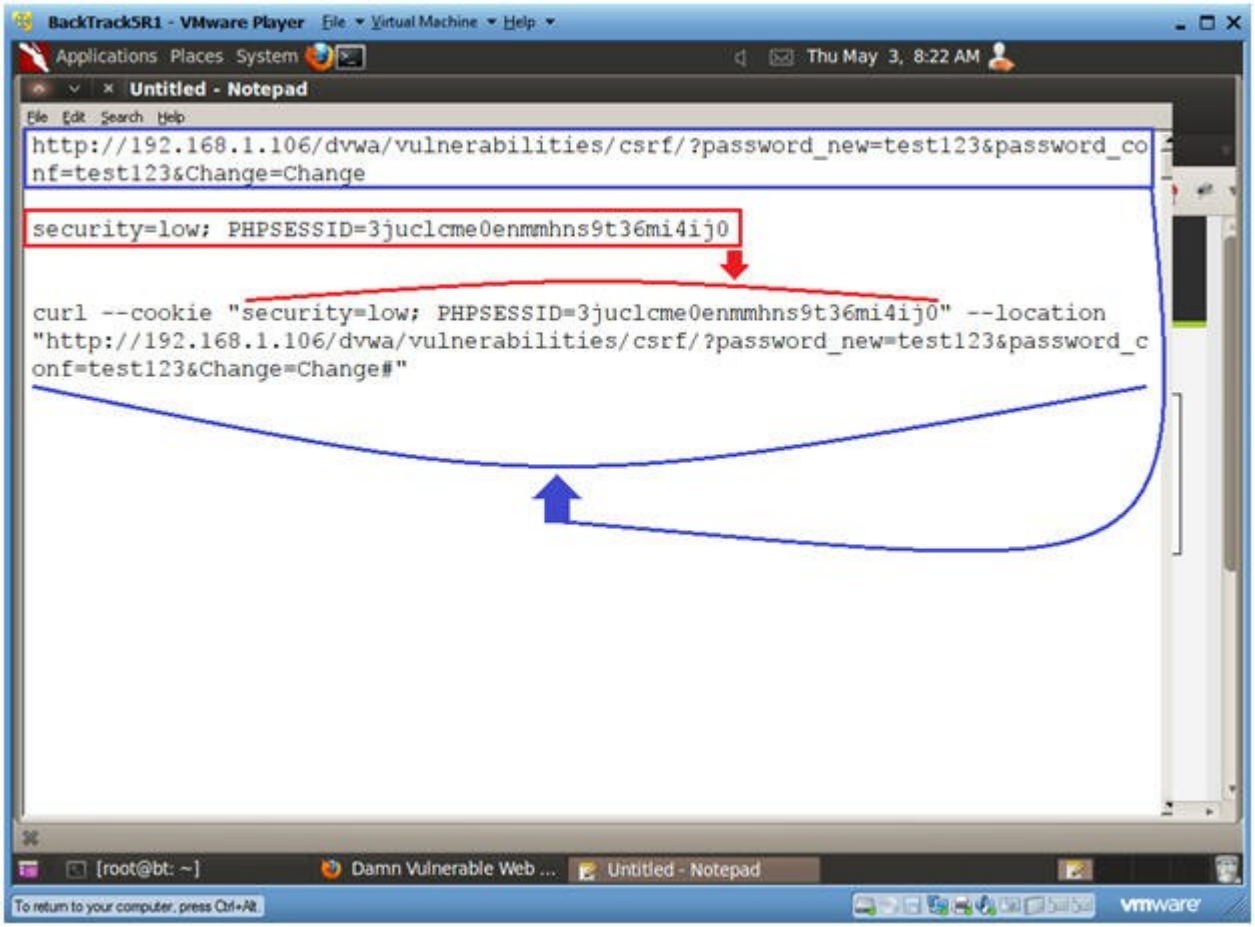
2. Edit --> Paste



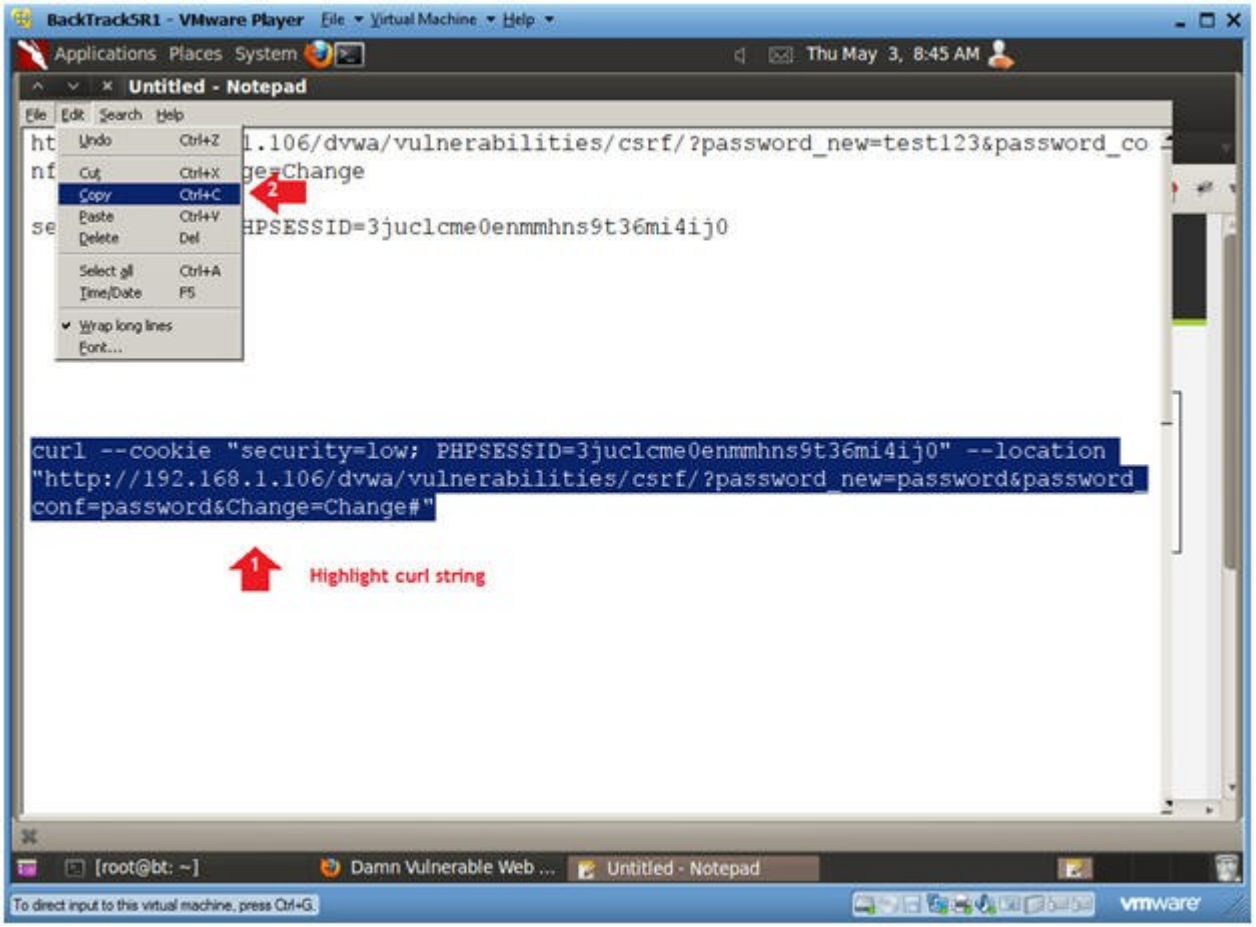
Section 13. Build Curl String

1. Open a console terminal

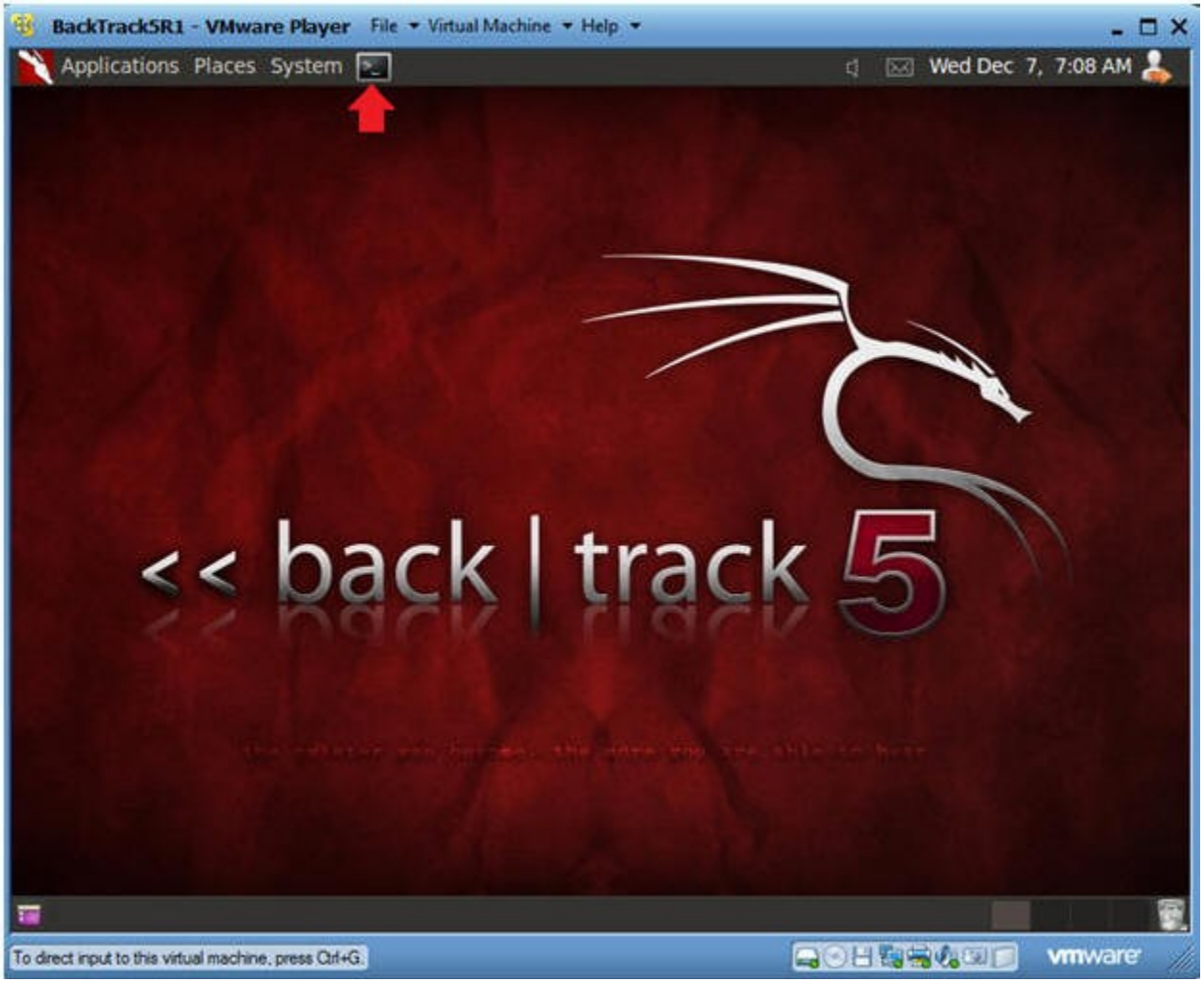
- **Instructions:**
  1. **Go to notepad**
  2. **In notepad type the following**
     a. curl --cookie "" --location ""
     b. Place the cookie string between the quotes after the --cookie tag.
     c. Place the html string between the quotes after the --location tag.
  3. **Your string should now look like the below line and picture**
     a. curl --cookie "security=low; PHPSESSID=3juclcme0enmmhns9t36mi4ij0" --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=3juclcme0enmmhns9t36mi4ij0" --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

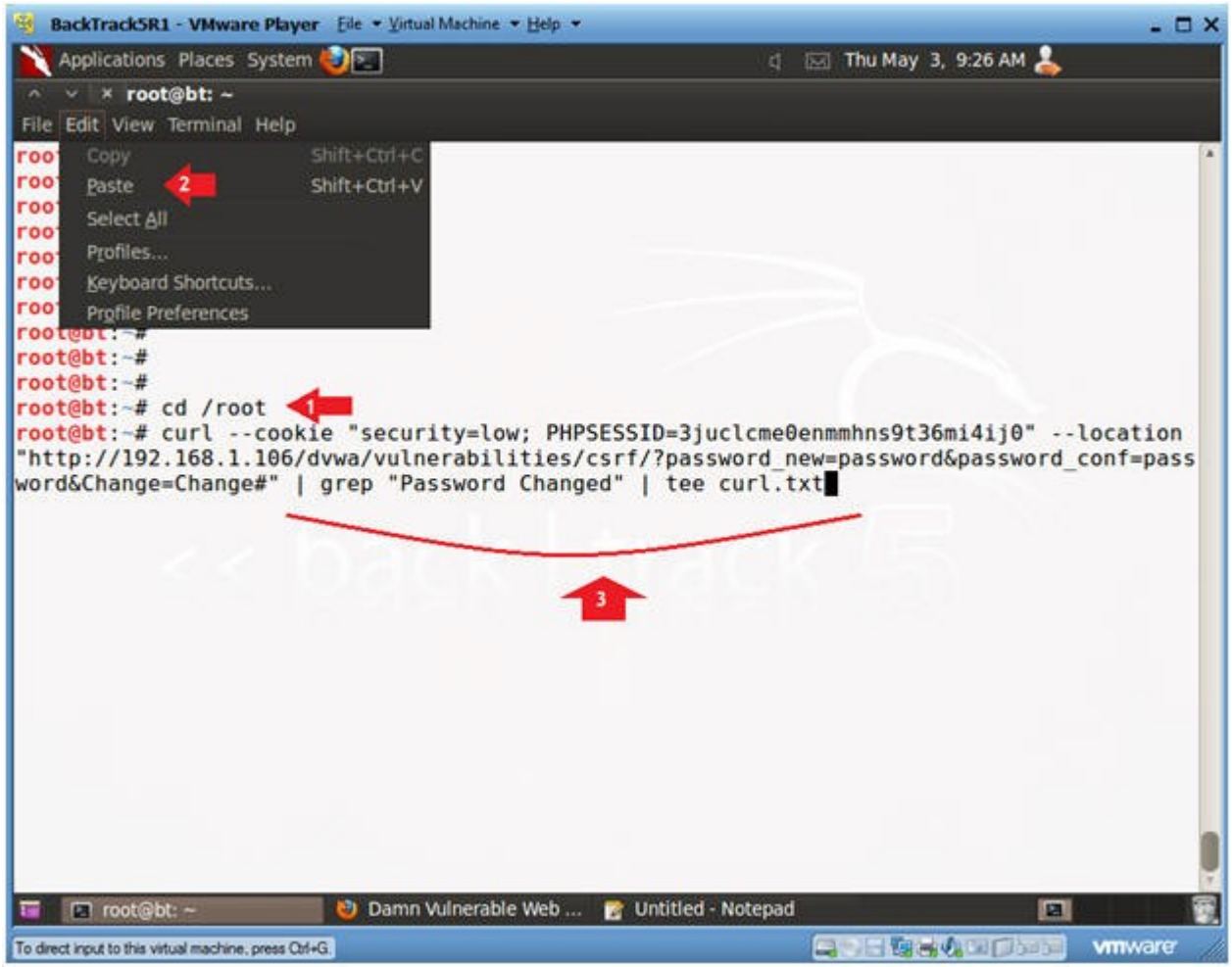


3. Open a console terminal
    - **Instructions:**
        1. Click on the console terminal

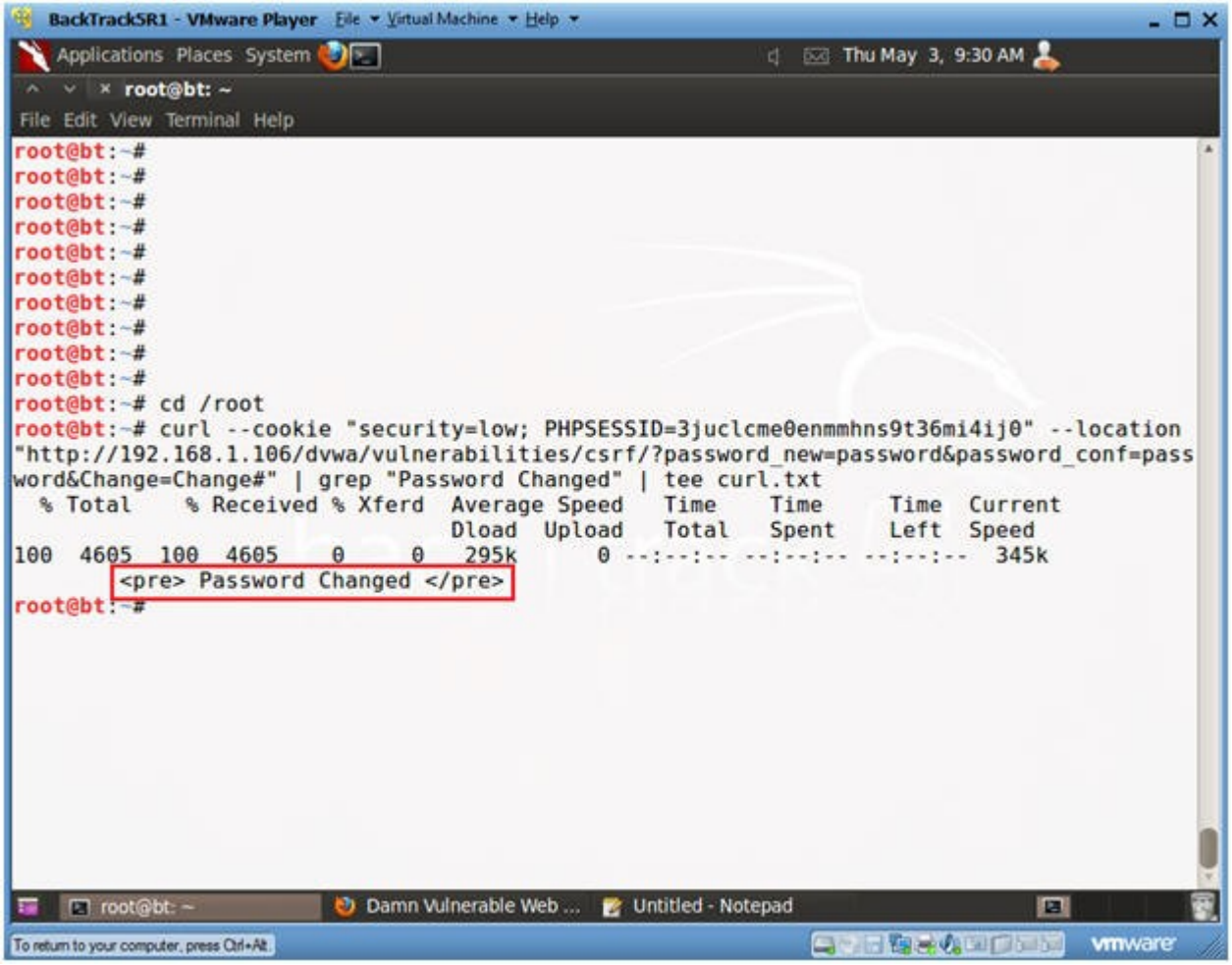


4. Execute Curl String
    - **Instructions:**
        1. cd /root

2. Edit --> Paste
3. Append the following to your curl string
    a. | grep "Password Changed" | tee curl.txt
2. Press <Enter>



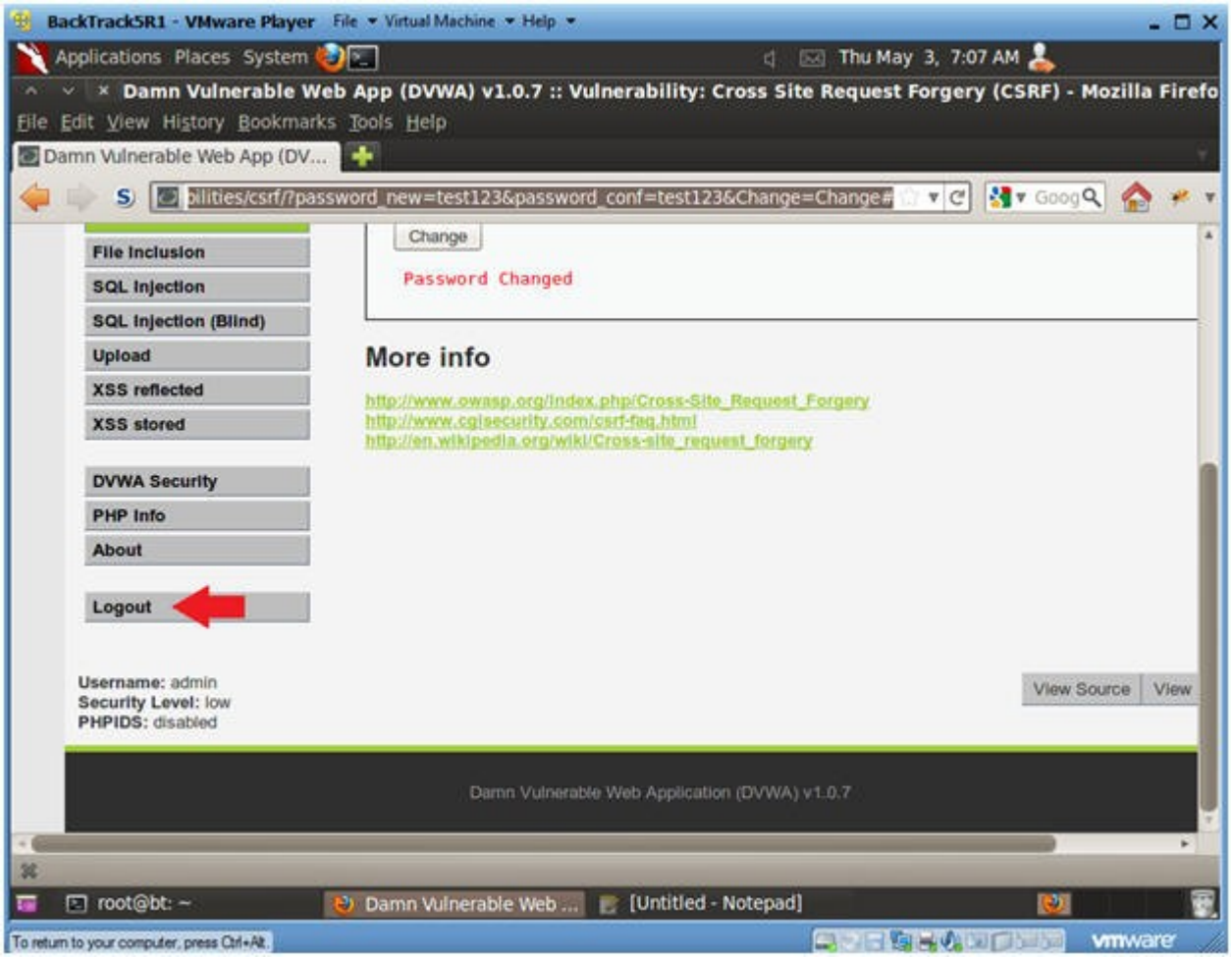
2. Verify Curl Results
   - **Notes:**
     1. Your should see the Password Changed message you saw earlier, when you changed your password using the CSRF menu.



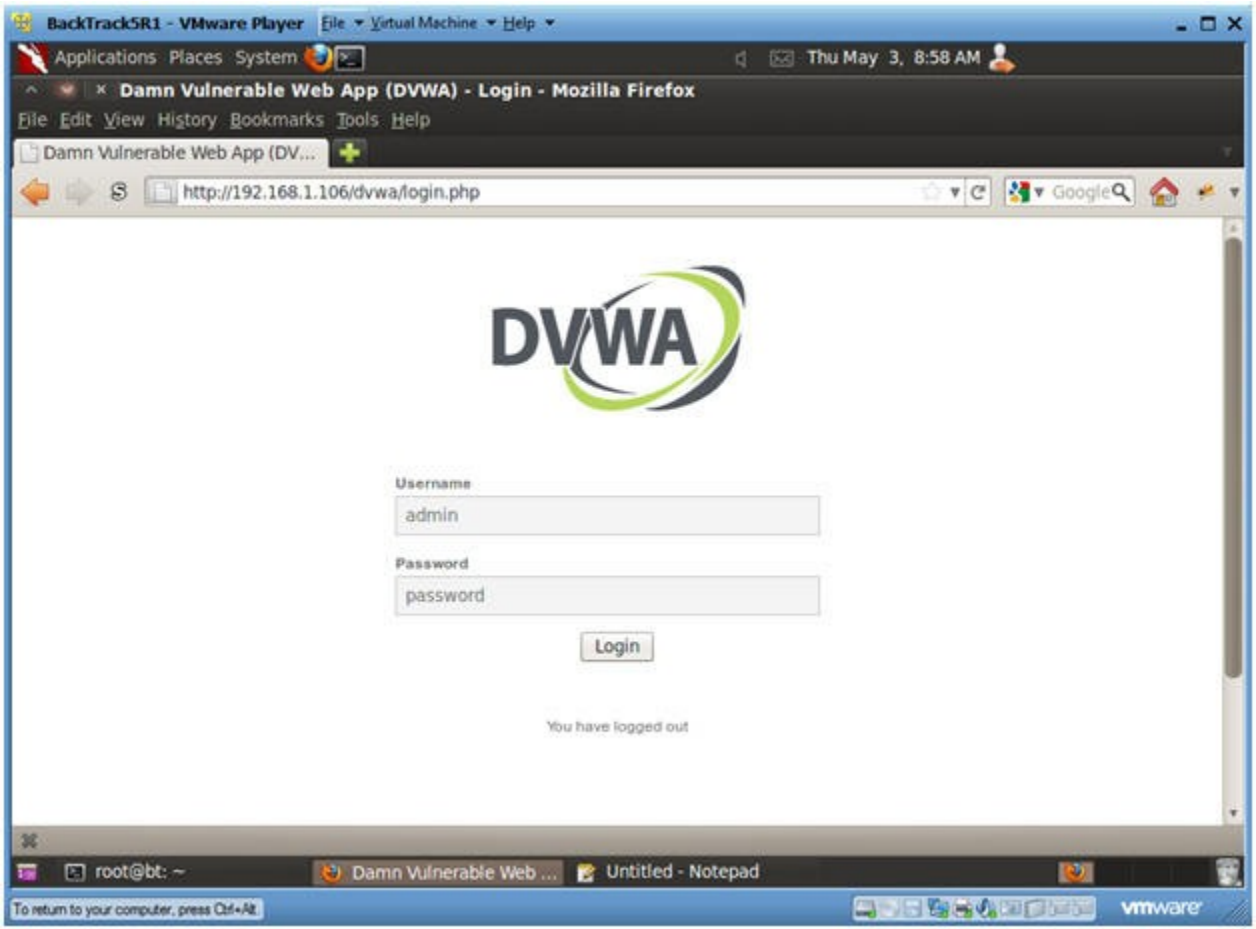
   -

Section 14. Test Curl String Password Change

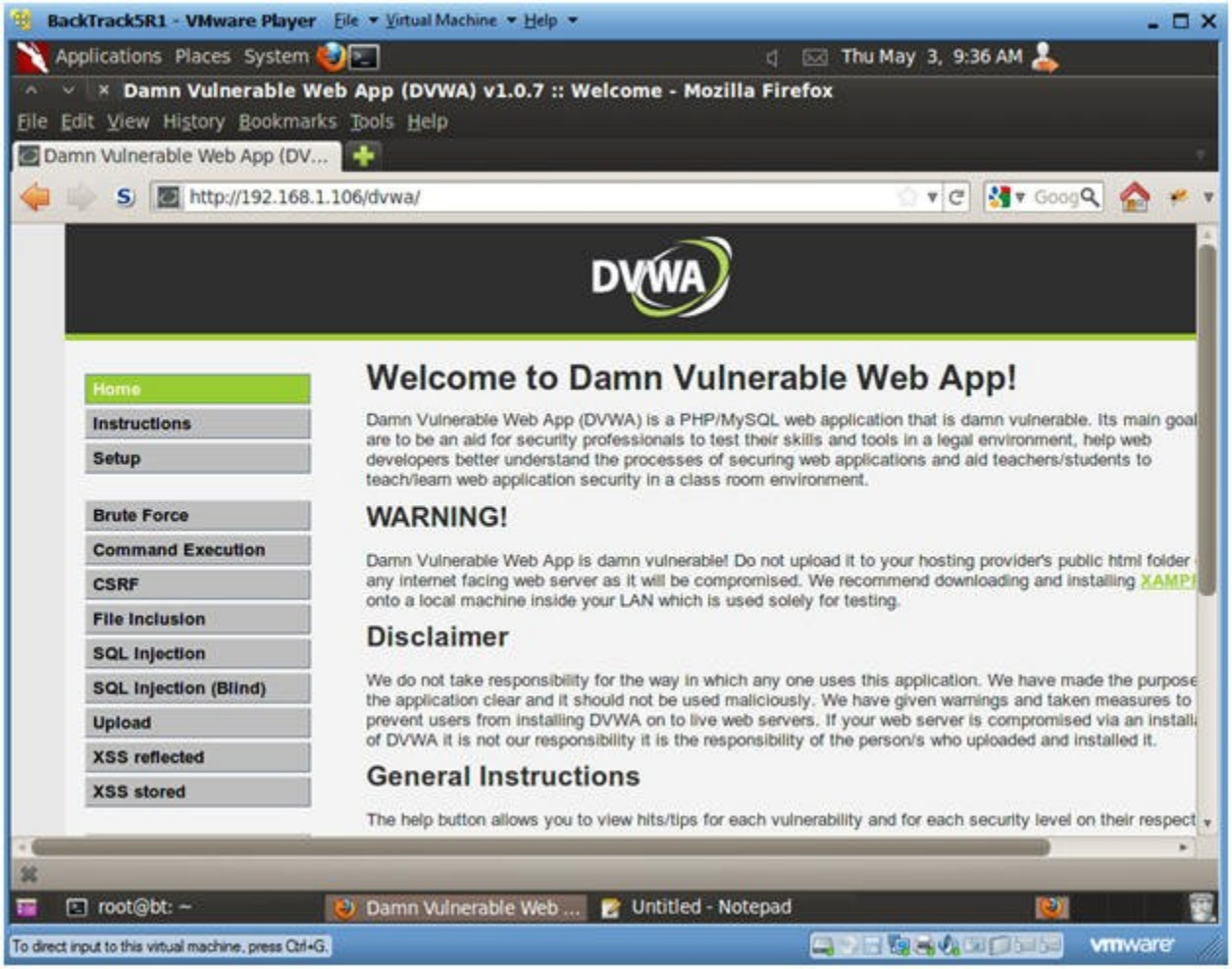
1. Logout of DVWA
    - **Instructions:**
        1. In the Left Navigation Menu, Click Logout



2. Login to DVWA
    - **Instructions:**
        1. Username: admin
        2. Password: password

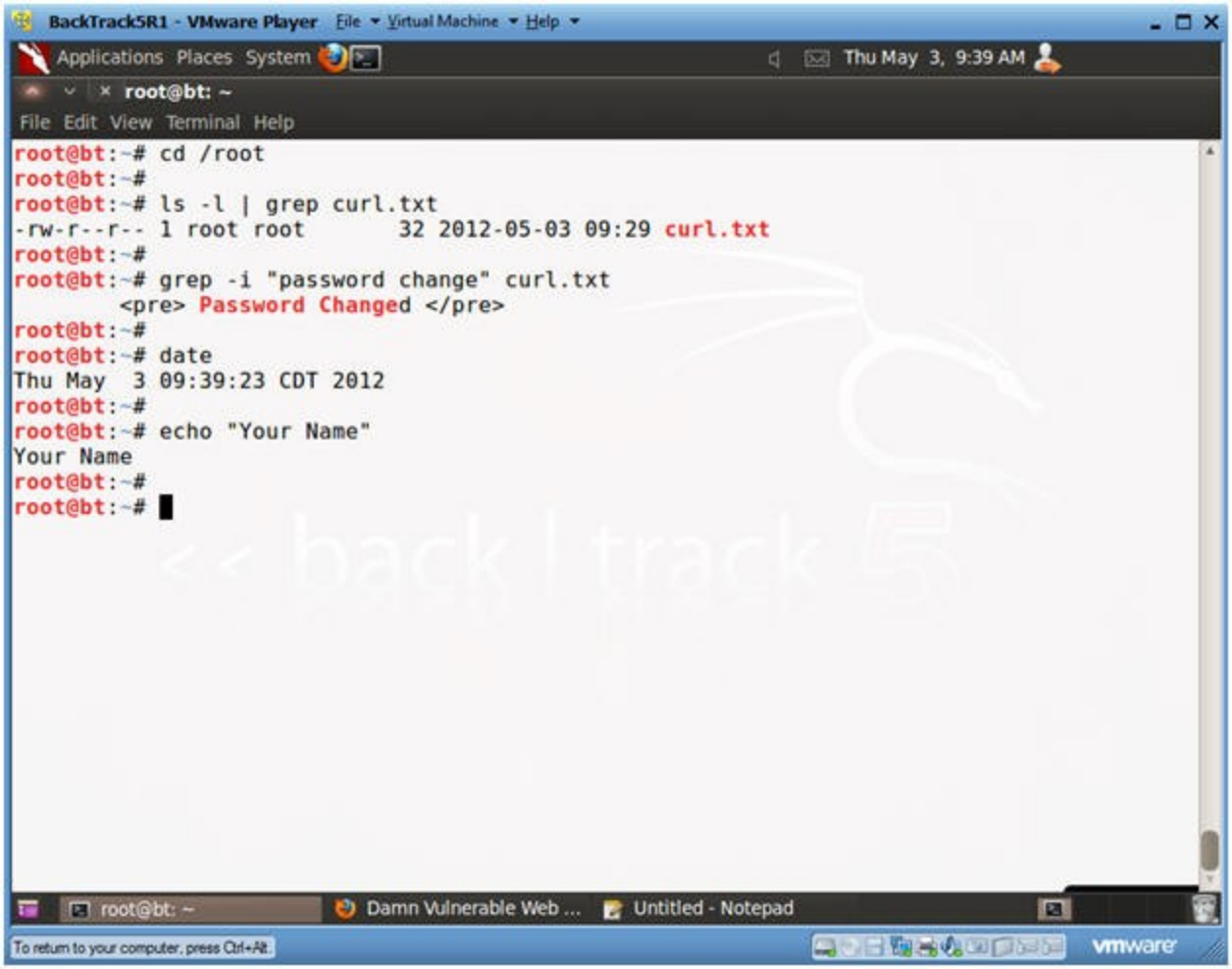


3. Welcome to DVWA
    - **Notes:**
        1. If you see the Welcome Screen, then you have successful use curl to change the password remotely without a browser.



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
Thu May 3, 9:39 AM
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
<pre> Password Changed </pre>
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:~#
root@bt: ~
Damn Vulnerable Web ...
Untitled - Notepad
To return to your computer, press Ctrl+Alt.
vmware