



Cybersecurity 701

Directory Traversal
Lab



Directory Traversal Materials

- Materials needed
 - Kali Linux Virtual Machine
 - Windows 7 Virtual Machine
- Software Tools used
 - DVWA
 - Vulnerable Web Application



Objectives Covered

- Security+ Objectives (SY0-701)
 - Objective 2.4 – Given a scenario, analyze indicators of malicious activity.
 - Application attacks
 - Directory traversal



What is a Directory Traversal Attack?

- When an image is called, it will look like this:
 - filename = images/panda.jpg
 - Could be pulling image from server location: /var/www/html/images/panda.jpg
- What happens if a malicious actor does this?
 - filename=../../penguin.jpg
 - This would be looking for a penguin.jpg image two folders back
- What happens if the malicious person knows the location of a password file?
 - They could gain access to all sorts of 'secure' files
 - ...if the web server allows directory traversal



Directory Traversal Lab Overview

1. Set up Environments
2. Find Linux IP Address
3. Start DVWA Web Services
4. Log in to DVWA & Lower Security
5. Directory Traversal
6. Place Confidential File
7. Directory Traversal (Again)



Set up Environments

- Log into your range
- Open the Kali Linux and Windows 7 Environments
 - You should be on your Kali Linux Desktop
 - You should also be on your Windows 7 Desktop



Locate Linux IP Address

- You will need the IP address of the Kali machine
- Open the Terminal
- In the Linux VM, open the Terminal and type the following command:
 - `hostname -I`
- This will display the IP Address
 - Write down the Kali VM IP address

```
(kali@10.15.3.44) - [~]  
$ hostname -I  
10.15.3.44
```

The IP Address

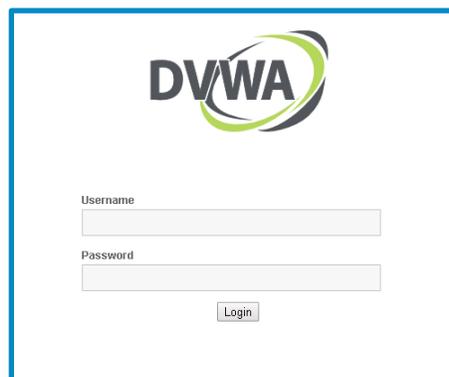
Start the DVWA Web Services

- Start up the web server (on the Kali machine)
 - Use the following command to start XAMPP which will start the services needed to run DVWA

```
sudo /opt/lampp/xampp start
```

```
(kali@10.15.69.200)-[~]  
$ sudo /opt/lampp/xampp start  
Starting XAMPP for Linux 8.2.4-0...  
XAMPP: Starting Apache...ok.  
XAMPP: Starting MySQL...ok.  
XAMPP: Starting ProFTPD...ok.
```

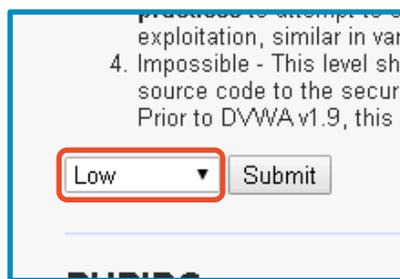
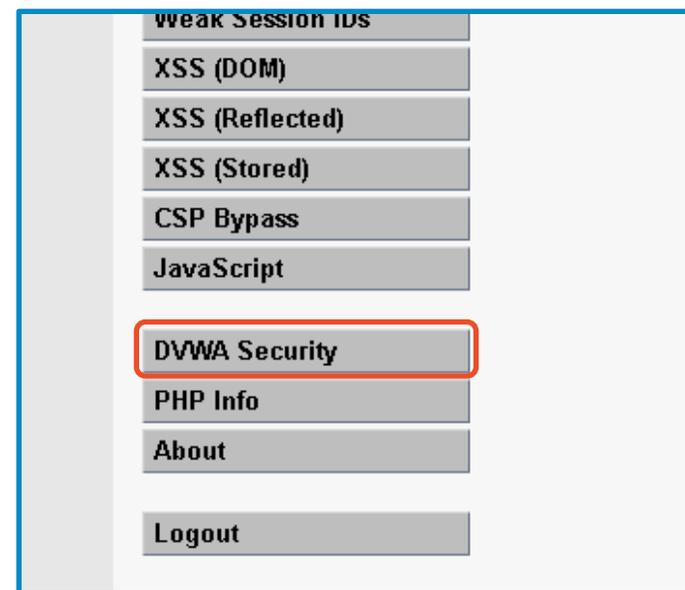
- On the Windows Machine, go to the DVWA webpage
<http://<Kali-IP-Address>/dvwa>



The screenshot shows the DVWA login page. At the top center is the DVWA logo, which consists of the letters 'DVWA' in a bold, sans-serif font, with a stylized green and blue swoosh underneath. Below the logo are two input fields: the first is labeled 'Username' and the second is labeled 'Password'. Both fields are empty. Below the password field is a 'Login' button.

Log in to DVWA & Lower Security

- Login using the following credentials
 - Username: “admin”
 - Password: “password”
- Click on the **DVWA Security** option
- Change the Security Level to **Low**
- Click **Submit**
 - This lowers the DVWA security to the lowest setting



Directory Traversal Setup

- Open a file to view where it is called
 - Click on **File Inclusion**
 - Click on **file2.php**

Click on File Inclusion, and then select file2.php

Not secure | 10.1.58.193/dvwa/vulnerabilities/fi/?page=file2.php

DVWA

Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection

Vulnerability: File Inclusion

File 2

"I needed a password eight characters long so I picked Snow White and the Seven Dwarves." ~ Nick Helm

[\[back\]](#)

More Information

- [Wikipedia - File inclusion vulnerability](#)
- [WSTG - Local File Inclusion](#)
- [WSTG - Remote File Inclusion](#)

Here is where the website is calling the file



Directory Traversal Example

- Attempt to read the passwd file
 - In the URL, replace `file2.php` with the following:
`../../../../../../../../etc/passwd`

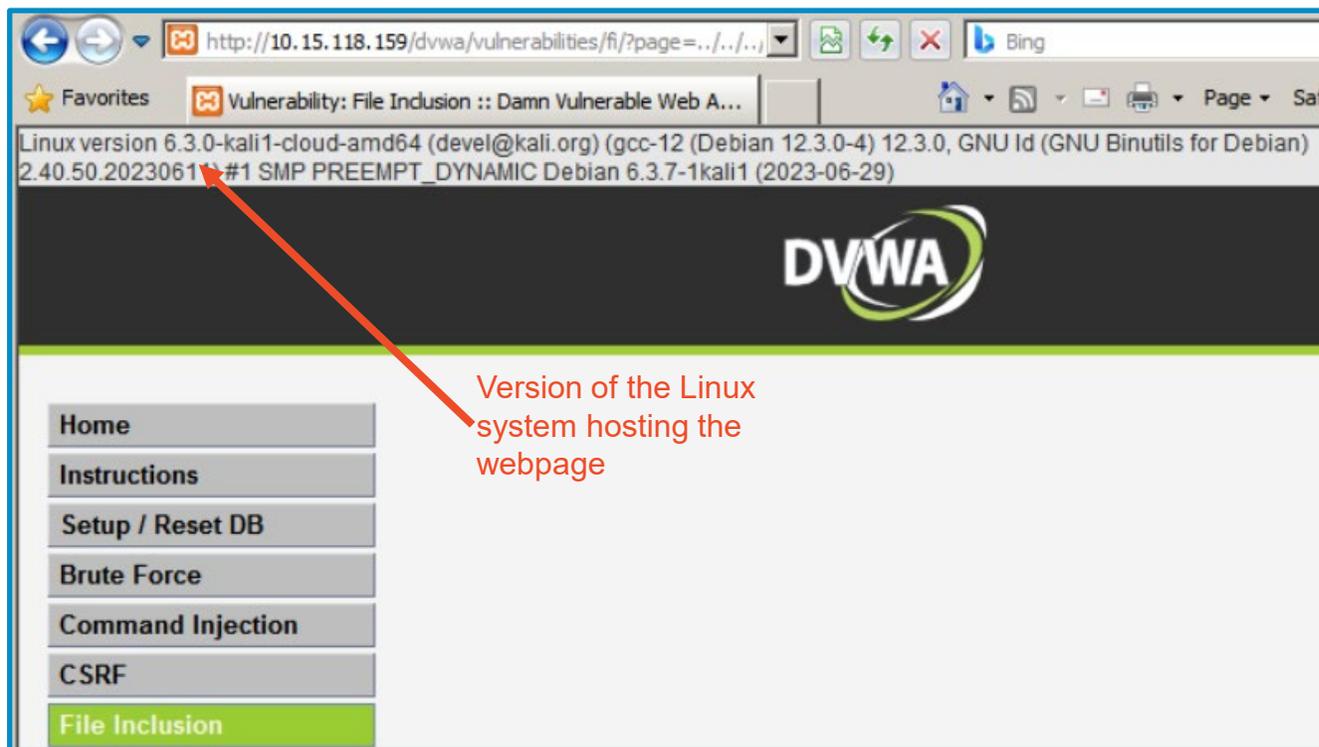
```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 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 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:101:systemd Time
Synchronization,,/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,/run/systemd:/usr/sbin/nologin
messagebus:x:104:105:/nonexistent:/usr/sbin/nologin _chrony:x:105:112:Chrony daemon,,/var/lib/chrony:/usr/sbin/nologin sshd:x:106:65534:/run/ssh:/usr/sbin/nologin systemd-coredump:x:999:999:systemd Core
Dumper:/usr/sbin/nologin student:x:1000:1001:Cyber Range Student:/home/student:/bin/bash mysql:x:107:113:MySQL Server,,/nonexistent:/bin/false tss:x:108:114:TPM software stack,,/var/lib/tpm:/bin/false
rtkit:x:109:115:RealtimeKit,,/proc:/usr/sbin/nologin dnsmasq:x:110:65534:dnsmasq,,/var/lib/misc:/usr/sbin/nologin strongswan:x:111:65534:/var/lib/strongswan:/usr/sbin/nologin ntp:x:112:117:/nonexistent:/usr/sbin/nologin
redsocks:x:113:118:/var/run/redsocks:/usr/sbin/nologin rwhod:x:114:65534:/var/spool/who:/usr/sbin/nologin lodine:x:115:65534:/var/run/lodine:/usr/sbin/nologin tcpdump:x:116:121:/nonexistent:/usr/sbin/nologin
xrdp:x:117:122:/run/xrdp:/usr/sbin/nologin miredo:x:118:65534:/var/run/miredo:/usr/sbin/nologin _rpc:x:119:65534:/run/rpcbind:/usr/sbin/nologin usbmux:x:120:46:usbmux daemon,,/var/lib/usbmux:/usr/sbin/nologin Debian-
snmp:x:121:125:/var/lib/snmp:/bin/false statd:x:122:65534:/var/lib/ifs:/usr/sbin/nologin postgres:123:126:PostgreSQL administrator,,/var/lib/postgresql:/bin/bash avahi:124:128:Avahi mDNS daemon,,/run/avahi-
daemon:/usr/sbin/nologin stunnel4:x:125:129:/var/run/stunnel4:/usr/sbin/nologin sslh:x:126:130:/nonexistent:/usr/sbin/nologin nm-openvpn:x:127:131:NetworkManager OpenVPN,,/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:128:132:NetworkManager OpenConnect plugin,,/var/lib/NetworkManager:/usr/sbin/nologin inetsim:x:129:134:/var/lib/inetsim:/usr/sbin/nologin geoclue:x:130:135:/var/lib/geoclue:/usr/sbin/nologin
lightdm:x:131:136:Light Display Manager:/var/lib/lightdm:/bin/false pulse:x:132:138:PulseAudio daemon,,/var/run/pulse:/usr/sbin/nologin saned:x:133:140:/var/lib/saned:/usr/sbin/nologin colord:x:134:141:colord colour
management daemon,,/var/lib/colord:/usr/sbin/nologin king-phisher:x:135:142:/var/lib/king-phisher:/usr/sbin/nologin
```

Notice the passwd file is being displayed

This is an example of directory traversal

Another Directory Traversal Example

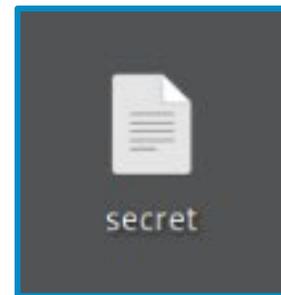
- Attempt to figure out the version of the system
 - In the URL, replace the traversal after “page=” with the following:
`../../../../../../../../proc/version`



Create Confidential File

- Go to the Kali Machine
- Open a Terminal
- Navigate to the Desktop
`cd Desktop`
- Place a secret file
`touch secret`

```
(kali@10.15.92.122) - [~]  
$ cd Desktop  
  
(kali@10.15.92.122) - [~/Desktop]  
$ touch secret
```



Verify a file named
"secret" appears on the
Desktop

Edit Confidential File

- Edit the file
`nano secret`
- Write fake credentials
- Save and Exit
CTRL+X
Y
ENTER

```
(kali@10.15.92.122) - [~/Desktop]  
$ nano secret
```

Fake credentials →

```
GNU nano 7.2  
US Bank Login Info  
Username: MLowery19  
Password: UncMike4L
```

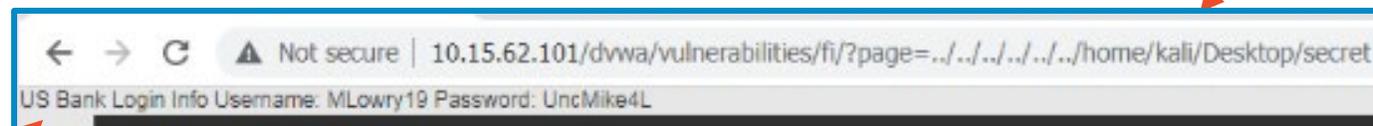


Directory Traversal to Read Secret File

- Go to the Windows system
- Attempt to read the secret file

`../../../../../../../../home/USERNAME/Desktop/secret`

- The **USERNAME** is likely `kali` for hosts on the CYBER.ORG range



Directory Traversal

The secret file displayed



How to Defend Against a Directory Traversal Attack?

- Validate inputs!
 - Don't allow directory traversal on the web server
 - Don't allow any “../..//”
- Validate the base directory
 - All files should come from a certain location
 - Verify the location of the file
- What are some other ways of defending against directory traversal?

