*Web Application Pen-Testing*

*AY 2022/2023*

*Week 6.1 Practical*

*OWASP Top 10 - 2021*

*A03:2021-Injection*

*Part 3*

*XSS Post Exploitation using BeEF*

*Table of Contents*

[*1.* *Setup* 3](#_Toc120007233)

[*1.1.* *Start and Login to Kali Linux VM with NAT enabled* 3](#_Toc120007234)

[*1.2.* *Install BeEF* 4](#_Toc120007235)

[*1.3.* *Start OWASP Broken Web Apps (owaspbwa) VM in Host-only* 5](#_Toc120007236)

[*1.4.* *Set Kali Linux VM to Host-only enabled* 6](#_Toc120007237)

[*2.* *XSS Post Exploitation using BeEF* 7](#_Toc120007238)

[*2.1.* *Start BeEF* 7](#_Toc120007240)

[*2.2.* *Stored / Persistent XSS Exploitation* 8](#_Toc120007241)

[*2.3.* *XSS Post Exploitation* 11](#_Toc120007242)

# *Setup*

## *Start and Login* *to Kali Linux VM with NAT enabled*

This practical requires Kali Linux VM to be connected to the Internet. Therefore, make sure the Virtual Machine Settings 🡪 Network Adapter 🡪 NAT

|  |  |
| --- | --- |
| *Graphical user interface, application  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*

## *Install BeEF*

BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser. It is commonly deployed via Cross Site Scripting (XSS) Attack.

Amid growing concerns about web-born attacks against clients, including mobile clients, BeEF allows the professional penetration tester to assess the actual security posture of a target environment by using client-side attack vectors. Unlike other security frameworks, BeEF looks past the hardened network perimeter and client system and examines exploitability within the context of the one open door: the web browser. BeEF will hook one or more web browsers and use them as beachheads for launching directed command modules and further attacks against the system from within the browser context. [Source: https://www.kali.org/tools/beef-xss/]

Type the following command into the Kali Linux’s Terminal Emulator and press Enter:

sudo apt-get update

[The apt-get update is responsible for updating the package information using the URLs defined in the sources list.]

A screenshot of a computer

Description automatically generated

sudo apt install beef-xss

A picture containing graphical user interface

Description automatically generated

## *Start OWASP Broken Web Apps (owaspbwa) VM in Host-only*

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

Graphical user interface, text

Description automatically generated

1. Type in the owaspbwa VM IP Address below: OWASPBWA\_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

## *Set Kali Linux VM to 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* |

# *XSS Post Exploitation using BeEF*



## *Start BeEF*

Under Kali Linux Applications Icon, type beef and click beef start

A screenshot of a computer

Description automatically generated with medium confidence

Type any new password, such as kalibeef

Text

Description automatically generated

BeEF would be auto launched on your Kali Linux Web Browser. Enter Username: beef, and Password: kalibeef and press Login.

|  |  |
| --- | --- |
| Graphical user interface, text, website  Description automatically generated | A screenshot of a computer  Description automatically generated |

You will notice on the left pane that there are neither any hooked Online Browsers nor Offline Browsers, this is because we haven’t carried out Cross Site Scripting (XSS) attack on any victim.

## *Stored / Persistent XSS Exploitation*

Before being able to fully explore the BeEF framework you will have to 'hook' a browser.

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

http://OWASPBWA\_IP

We see a list of several websites. However, in this practical exercise we will **focus on “**OWASP Mutillidae II**” website**. Click on the link “OWASP Mutillidae II”.

Graphical user interface, text, application

Description automatically generated

On the left menu, click OWASP 2013 and follow the navigation shown below until you reach “Add to your blog” page. You had already learnt in your SSD module that this page is vulnerable to Stored / Persistent Cross Site Scripting Attack.

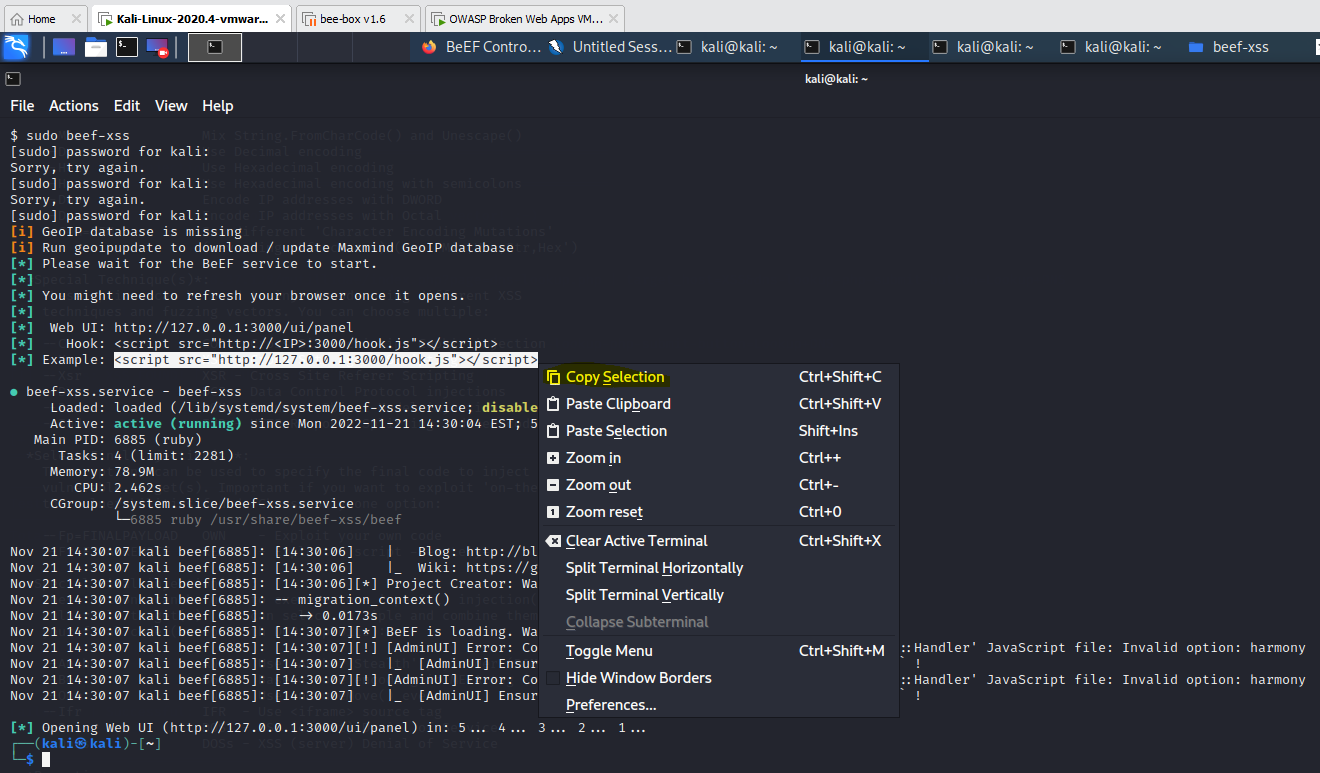
Graphical user interface, text

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Let us now copy the hook script from the terminal that got launched when you click beef start



Paste this hook script into the text box under the “Add blog for anonymous” but change only the IP address in the hook script to that of your own KALI\_IP address (do not delete the port :3000) and click “Save Blog Entry”. The moment you clicked “Save Blog Entry” this hook script is saved into Mutillidae’s database. By doing all this, we are exploiting the characteristic of this Stored / Persistent Cross Site Scripting Attack whereby this hook script will run on any victim’s browser visiting this “Add to your blog” page.

Graphical user interface, text, application

Description automatically generated

The moment you click “Save Blog Entry” you will notice on the BeEF webpage that your own Kali Linux Web Browser has been hooked and is shown below the Online Browsers group.

A screenshot of a computer

Description automatically generated

You can now close the Mutillidae Kali Linux Web Browser Tab. The moment you close this tab, inside the BeEF webpage, your Kali Linux Web Browser will be moved to Offline Browsers group. Give BeEF webpage a few seconds to affect this change.

Graphical user interface, text, application, website

Description automatically generated

However, we would really want to hook a victim’s web browser to show a client the dangers of XSS post exploitation as a proof of concept. This would encourage the client to immediately take necessary actions to secure the code.

Open a web browser on your host machine Windows 10 or Window 11. Type the following into the address bar of your host machine’s web browser. Here, type your own OWASPBWA\_IP address

http://OWASPBWA\_IP and click on OWASP Mutillidae II

Graphical user interface, application

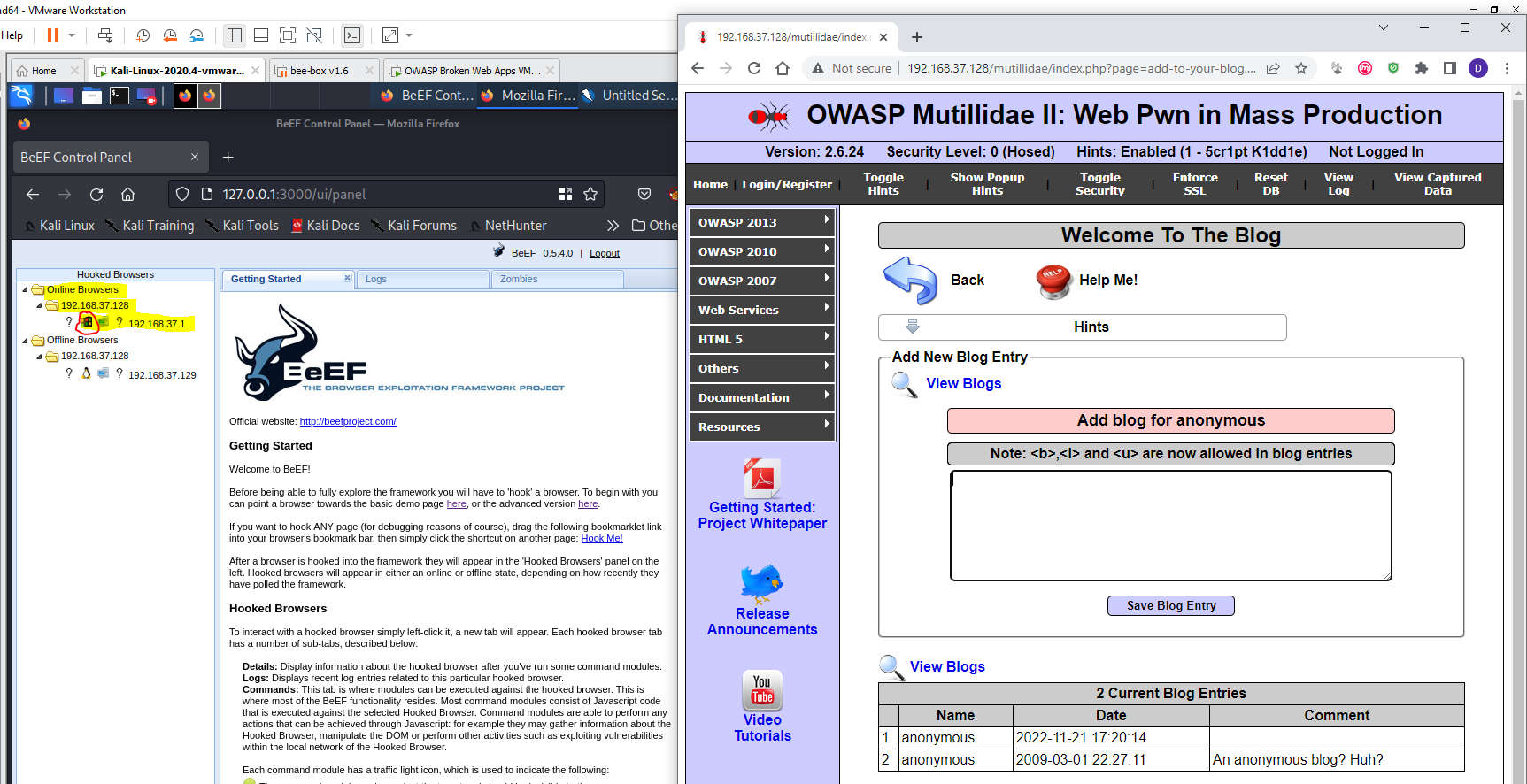
Description automatically generated

On the left menu, click OWASP 2013 and follow the navigation shown below until you reach “Add to your blog” page.

Graphical user interface, text

Description automatically generated

The moment you visit the “Add to your blog” page the stored hook script will run on your Windows Web Browser. Go back to your BeEF webpage and you will notice that your Windows Web Browser has been hooked and displayed under the Online Browsers group.



## *XSS Post Exploitation*

In the BeEF webpage, on the left menu, click on your host (Windows) machine’s IP address. The “Details” tab displays the information about the hooked browser. Click on the “Commands” tab.

Graphical user interface, text, website

Description automatically generated

Commands: This tab is where modules can be executed against the hooked browser. This is where most of the BeEF functionality resides. Most command modules consist of Javascript code that is executed against the selected Hooked Browser. Command modules are able to perform any actions that can be achieved through Javascript: for example they may gather information about the Hooked Browser, manipulate the DOM or perform other activities such as exploiting vulnerabilities within the local network of the Hooked Browser.

Text

Description automatically generated

Expand and explore the Commands inside the different Folder categories. In the “Commands” tab search for the following Commands and Execute them to see interesting Post Exploitation outcomes on the hooked browser (your host (Windows) machine’s web browser). Try other Commands too.

|  |  |
| --- | --- |
| Alert Dialog | Pretty Theft (Under Social Engineering) |
| Prompt screen | Spyder eye |
| Google phishing | Detect social media |
| Redirect browser (note: once redirected the hook with the BeEF will be disconnected) | |

Graphical user interface, application

Description automatically generated