

Name:Chirantan Sawant  
Intern ID-286

Tool Name:  
BeEF (Browser Exploitation Framework) + msfvenom

Description:  
A penetration testing combo used to exploit browser vulnerabilities (via BeEF) and deliver custom payloads (via msfvenom) to gain access or execute commands on the target system.

What Is This Tool About?  
BeEF hooks a browser using XSS, then exploits the victim through browser-based modules. msfvenom is used to generate payloads (e.g., reverse shells) for post-exploitation access.

Key Characteristics / Features:  
Browser hooking via XSS

Full control over victim browser

Live session tracking

Supports social engineering modules

Custom payload delivery (via msfvenom)

Works on LAN and WAN

Meterpreter support

Command execution via browser

Payload obfuscation support

Multiplatform payloads (Windows/Linux/macOS)


Fake update delivery (Flash, PDF, etc.)

Automation via RESTful API

Works with Kali Linux, ParrotOS, etc.

Real-time command execution

Multi-browser support (Chrome, Firefox, Edge)

 Types / Modules Available:  
Fake Flash Update (Social Engineering)

Webcam Snapper

Keylogger Injection

Java Applet Attack

ClickJacking Module

Custom Script Injection

Browser Fingerprinting

Command Execution Shell

Payload Dropper

Clipboard Stealer

How Will This Tool Help?

Exploits browser-based sessions post-XSS

Drops and executes backdoors or reverse shells

Acts as a foothold into internal networks

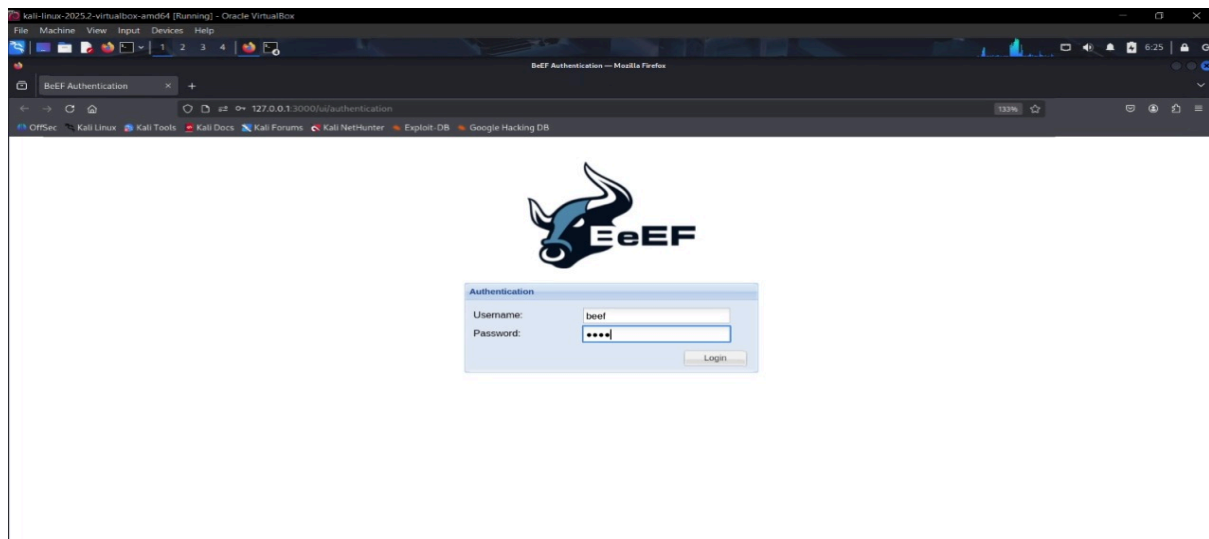
Helps simulate phishing/drive-by download attacks

Offers red teams realistic attack scenarios

**\*\*Proof of Concept (PoC) Images:**

1)Installing Beef-xss





### 3)Inititating apache server

```
(root@kali)-[~]
└─# sudo systemctl apache2
Unknown command verb 'apache2', did you mean 'cancel'?

(root@kali)-[~]
└─# sudo systemctl start apache2

(root@kali)-[~]
└─# sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-07-25 07:28:35 EDT; 1h 15min ago
     Invocation: 565f3221cf8d459a8e9b0ba0bbc856dc
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 50591 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 50595 (apache2)
      Tasks: 7 (limit: 2208)
     Memory: 4.2M (peak: 22.8M, swap: 9.9M, swap peak: 10.1M)
        CPU: 312ms
      CGroup: /system.slice/apache2.service
              └─50595 /usr/sbin/apache2 -k start
                └─50606 /usr/sbin/apache2 -k start
                  └─50607 /usr/sbin/apache2 -k start
                    └─50608 /usr/sbin/apache2 -k start
                      └─50609 /usr/sbin/apache2 -k start
                        └─50610 /usr/sbin/apache2 -k start
                          └─51537 /usr/sbin/apache2 -k start

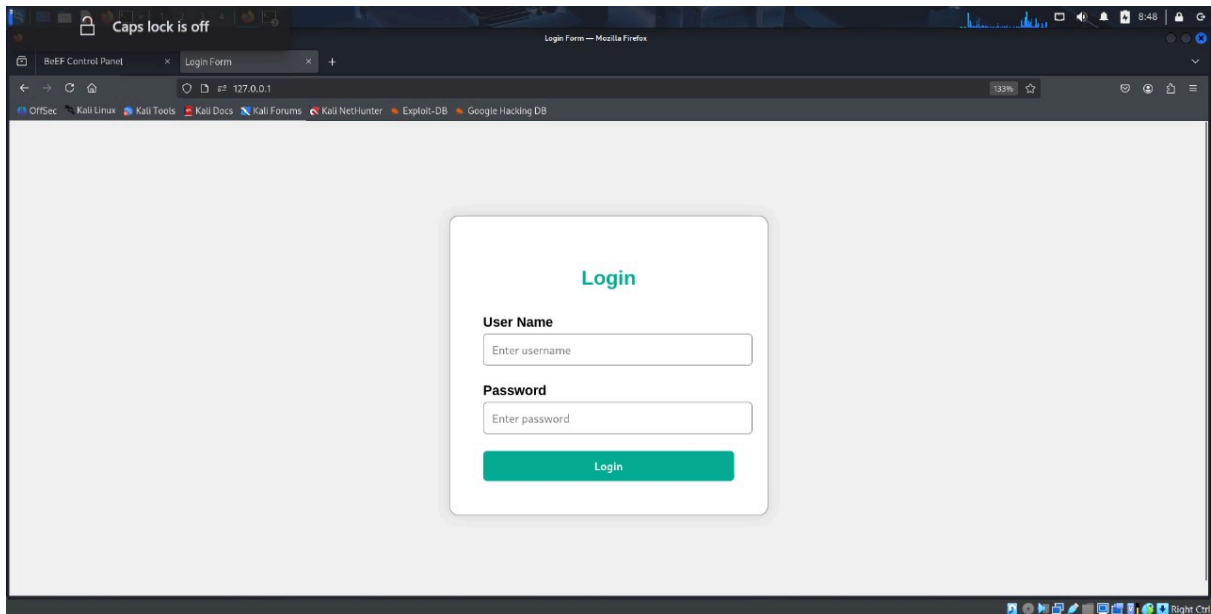
Jul 25 07:28:35 kali systemd[1]: Starting apache2.service - The Apache HTTP Server ...
Jul 25 07:28:35 kali apachectl[50593]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'Se
Jul 25 07:28:35 kali systemd[1]: Started apache2.service - The Apache HTTP Server.
```

### 4)Creating HTML file in HTTP server

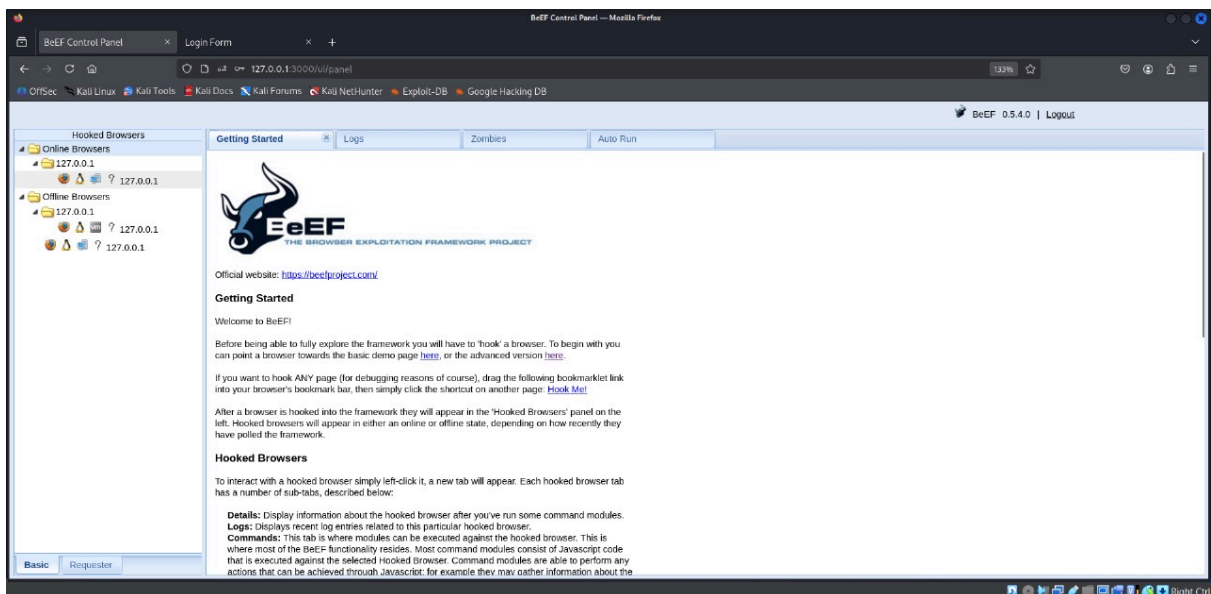
```
(root@kali)-[~]
└─# cd /var/www/html/
└─# ls
index.html
└─# sudo nano index.html
About CentOS
Enterprise Operating System (CentOS) is an Enterprise-class Linux Distribution derived from sources freely provided to the public by a prominent North
American Enterprise Linux vendor. CentOS conforms fully with the upstream vendors redistribution policy and aims to be 100% binary compatible. (CentOS mainly changes
vendor branding and artwork.) The CentOS Project is the organization that builds CentOS.
For information on CentOS please visit the CentOS website.
```

### 5)Creating html web page and inserting a hook javascript as a malicious code

### 6)Open http server by using inet id through firefox



7) After victim visits webpage their inet address is visible on beef-xss, which means the victim is hooked



8) By visiting the command section you can perform metasploit browser\_autopwn attack for that initiate msf console

9) Configure metasploit parameters by providing SRHOST id and LHOST id

10) Restarting beef-xss and metasploit after configuration

11) Now we are able to observe victims activities through session attacks which we are able to execute with help of metasploit

15-Liner Summary:  
Hook browsers via XSS

Control hooked clients

Execute JS in victim browser

Deliver payload with msfvenom

Use CLI/GUI for modules

Exploit across OS (Win/Linux/Mac)

Gain Meterpreter shell

Integrate with Metasploit

Use Fake Update to trick victims

Create custom payloads

Track live browser sessions

Post-exploitation browser attacks

Simulate real-world threats

Useful for training labs

Scriptable and modular

🕒 Time to Use / Best Case Scenarios:  
After identifying XSS vulnerability

During red team simulation

To test user awareness and SE defenses

For phishing campaign simulation

During penetration test PoC phase

👤 When to Use During Investigation:  
Web-based attack vector testing

Internal security assessment

Simulated phishing & drive-by attacks

Post-XSS exploitation path

Recon and payload delivery via browsers



Best Person to Use This Tool & Required Skills:

Best User: Red Team Operator / Ethical Hacker / Exploit Developer

Required Skills:

Strong knowledge of XSS and client-side scripting

Familiarity with Metasploit and msfvenom

Basic reverse shell and payload techniques

Command-line proficiency (Linux)

Understanding of social engineering vectors



Flaws / Suggestions to Improve:

No HTTPS support out of the box (manual config needed)

Real-time payload detection by AVs

Browser-based limitations (sandboxing)

Needs more encrypted payload options

Improve UI stability and client refresh rate



Good About the Tool:

Easy to set up on Kali Linux

Real-world attack simulation

Powerful with msfvenom integration

Works with wide range of browsers

Excellent for PoC and training