

Juice Shop Information Gathering

2025-07-06

Contents

Information gathering	6
1. nmap	6
Comando completo	6
Risultato della scansione	6
Analisi della scansione	7
2. ffuf	8
2.1 Comando completo (prima scansione)	8
Risultato della scansione	8
Analisi della scansione	9
2.2 Comando con filtro sulla lunghezza (seconda scansione)	9
Spiegazione	10
Scansione con wordlist più grande	10
Passi della seconda scansione	10
Risultato della scansione	11
Analisi della scansione	11
2.3 Scansione con un'altra wordlist (terza scansione)	11
Risultato della scansione	12
Analisi della scansione	12
3. Burp	13
Spiegazione	13
3. Ricerca manuale sul sito web	13
3.1 About	13
3.2 User enumeration	14
3.3 Architecture enumeration	15
3.4 Path enumeration	15
3.5 Input	16
3.6 File	17
4. Ricerca di informazioni dopo autenticazione	17
4.1 Informazioni di login	17
4.2 User token	18
4.3 Review	19
4.4 Pagina di feedback	19
4.5 Chatbot	19
4.6 Complaint	20
4.7 Basket	20
4.8 Login information	21
5. Analisi dei path trovati	22
Introduzione	22
5.1 Cartella FTP	22

File accessibili	23
5.2 Cartella metrics	24
5.3 Cartella api-docs	24
5.4 API e REST	25
5.5 Cartella .well-known	27
5.6 Cartella encryptionkey	27
5.7 Robots.txt	27
6. whois	28
Comando completo	28
Risultato della scansione	28
Analisi della scansione	29
7. dnsrecon	29
Comando completo	29
Risultato della scansione	30
Analisi della scansione	30
8. whatweb	30
Comando completo	30
Risultato della scansione	30
Analisi della scansione	31
8.1 Modalità verbosa	31
Comando completo	31
Spiegazione	31
Risultato	31

Contents

Information gathering

Information gathering completo per il progetto su Juice Shop.

1. nmap

Comando completo

```
nmap -sV 127.0.0.1 -p 3000
```

Lo scopo nell'usare `nmap -sV` è per identificare quale servizio (e versione) è attivo sulla porta 3000 del localhost. Il comando analizza la risposta del servizio confrontandola con il database di firme di Nmap quindi scoprire se c'è un'applicazione in ascolto (es. server web) e qual è la sua versione precisa.

Risultato della scansione

Il risultato della scansione eseguita usando nmap.

```
[kali㉿kali: ~] kali㉿kali: ~ [x]
└─(kali㉿kali)-[~]
$ nmap -sV 127.0.0.1 -p 3000
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-21 10:40 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000069s latency).

PORT      STATE SERVICE VERSION
3000/tcp    open  ppp?
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=7.95%I=7%D=6/21%Time=6856C47B%P=x86_64-pc-linux-gnu%R=Ge
SF:tRequest,10189,"HTTP/1.\.1\x20200\x200K\r\nAccess-Control-Allow-Origin:\r
SF:x20*\r\nContent-Type-Options:\x20nosniff\r\nX-FRame-Options:\x20SAME
SF:ORIGIN\r\nFeature-Policy:\x20payment\x20'self'\r\nX-Recruiting:\x20/#/j
SF:obs/r\nAccept-Ranges:\x20bytes\r\nCache-Control:\x20public,\x20max-age=
SF:0\r\nLast-Modified:\x20Sat,\x2021\x20Jun\x202025\x2014:22:26\x20GMT\r\n
SF:ETag:\x20W/"138f5-19792de8677"/\r\nContent-Type:\x20text/html;\r\nchar
SF:set=UTF-8\r\nContent-Length:\x2080117\r\nVary:\x20Accept-Encoding\r\nDa
SF:te:\x20Sat,\x2021\x20Jun\x202025\x2014:40:59\x20GMT\r\nConnection:\x20c
SF:lose\r\nr\nr\n!--\n\x20\x20~\x20Copyright\x20(c)\x202014-2025\x20Bjoer
SF:n\x20Kimmiminich\x206\x20the\x20WASP\x20Juice\x20Shop\x20contributors.\r
SF:n\x20\x20-\x20SPDX-License-Identifier:\x20MIT\n\x20\x20-->\n<!doctype
SF:\x20html>\n<html\x20lang="en"\x20data-beasties-container>\n<head>\n\x
SF:20\x20<meta\x20charset="utf-8"/>\n\x20\x20<title>OWASP\x20Juice\x20Sho
SF:p</title>\n\x20\x20<meta\x20name="description"\x20content="Probably\x
SF:x20the\x20most\x20modern\x20and\x20sophisticated\x20insecure\x20web\x20
SF:application"\x20>\n\x20\x20<meta\x20name="viewport"\x20content="width=d
SF:evice-width,\x20initial-scale=1"\x20>\n\x20\x20<link\x20id="favicon"\x20
SF:rel="icon"\x20>%r[Help,2F,"HTTP/1.\.1\x20400\x20Bad\x20Request\r\nCon
SF:nnection:\x20close\r\nr\nr\n"%r[NCP,2F,"HTTP/1.\.1\x20400\x20Bad\x20Reques
SF:t\r\nConnection:\x20close\r\nr\nr\n"%r[HTTPOptions,EA,"HTTP/1.\.1\x20204\
SF:x20No\x20Content\r\nAccess-Control-Allow-Origin:\x20*\r\nAccess-Contro
SF:l-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nVary:\x20Access-C
SF:ontrol-Request-Headers\r\nContent-Length:\x200\r\nDate:\x20Sat,\x2021\x
SF:20Jun\x202025\x2014:40:59\x20GMT\r\nConnection:\x20close\r\nr\nr\n"%r[RT
SF:SPRequest,EA,"HTTP/1.\.1\x20204\x20No\x20Content\r\nAccess-Control-Allow
SF:-Origin:\x20*\r\nAccess-Control-Allow-Methods:\x20GET,HEAD,PUT,PATCH,P
SF:OST,DELETE\r\nVary:\x20Access-Control-Request-Headers\r\nContent-Length
SF::\x200\r\nDate:\x20Sat,\x2021\x20Jun\x202025\x2014:40:59\x20GMT\r\nConn
SF:ection:\x20close\r\nr\nr\n";
```

Figure 1: Risultati della scansione Nmap

Analisi della scansione

nmap non è stato in grado di identificare correttamente il nome del servizio e la sua versione, probabilmente perchè il container nasconde l'infrastruttura che ci sta dietro.

2. ffuf

2.1 Comando completo (prima scansione)

```
ffuf -w /usr/share/wordlists/dirb/small.txt -u  
http://127.0.0.1:3000/FUZZ -t 5
```

Lo scopo nell'uso di ffuf è per trovare directory e file nascosti su un sito web (<http://127.0.0.1:3000>) tramite brute-forcing. Ogni parola nella wordlist (es. small.txt) sostituisce FUZZ nell'URL. ffuf invia richieste HTTP e analizza le risposte. Il flag -t 5 limita a 5 thread per evitare sovraccarichi o difese anti-bot.

Risultato della scansione

Il risultato della scansione eseguita usando ffuf.

```

kali@kali: ~
File Actions Edit View Help
kali@kali: ~
(kali㉿kali)-[~]
$ ffuf -w /usr/share/wordlists/dirb/small.txt -u http://127.0.0.1:3000/FUZZ -t 5
v2.1.0-dev

:: Method      : GET
:: URL         : http://127.0.0.1:3000/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/small.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 5
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500

02      [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 59ms]
03      [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 59ms]
0      [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 63ms]
01      [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 65ms]
00      [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 67ms]
1      [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 54ms]
10     [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 53ms]
100    [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 50ms]
1000   [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 28ms]
123    [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 50ms]
2      [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 50ms]
20     [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 49ms]
200    [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 50ms]
2000   [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 51ms]
2001   [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 41ms]
2003   [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 99ms]
2002   [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 100ms]
]
2004   [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 100ms]
]
3      [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 96ms]
2005   [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 99ms]
@
Administration [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 55ms]
Admin [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 57ms]
CYBERDOCS [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 43ms]
CVS [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 46ms]
CYBERDOCS31 [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 47ms]
CYBERDOCS25 [Status: 200, Size: 80117, Words: 3629, Lines: 34, Duration: 36ms]

```

Figure 2: Risultati della prima scansione Ffuf

Analisi della scansione

ffuf è stato in grado di mappare i path del sito web. A quanto pare il sito web gestisce qualsiasi path non presente con status 200 e payload di lunghezza 80117.

2.2 Comando con filtro sulla lunghezza (seconda scansione)

Per superare il problema precedente, è possibile rieseguire la scansione andando a filtrare gli eventi con questa lunghezza di payload.

```
ffuf -w /usr/share/wordlists/dirb/small.txt -u
http://127.0.0.1:3000/FUZZ \
-t 5 -fs 80117
```

Spiegazione

Il flag `-fs 80117` esclude dalla visualizzazione tutti i risultati con una lunghezza di contenuto di 80117 byte, mostrando solo i percorsi che generano una risposta di lunghezza diversa, che presumibilmente sono quelli validi.

Scansione con wordlist più grande

La prima scansione ha avuto l'obiettivo di determinare come venissero gestite le rotte. Questa seconda scansione è stata effettuata in più profondità, usando una wordslist di dimensioni maggiori.

Per non sovraccaricare il server, usando una wordlist più grande (`common.txt`), è stato deciso di dividerla in parti più piccole ed effettuando una scansione in loop con un'attesa di qualche secondo tra una scansione e l'altra.

Passi della seconda scansione

1. Suddivisione del file `common.txt`

```
split -l 500 /usr/share/wordlists/dirb/common.txt  
common_part_
```

Questo comando crea file più piccoli (`common_part_aa`, `common_part_ab`, ecc.), ognuno contenente 500 righe del file originale da 4000 righe.

2. Esecuzione del loop di scansione Si esegue un loop di scansione usando il comando:

```
for wordlist in common_part_*; do  
    echo "Testing with $wordlist"  
  
    ffuf -w "$wordlist" -u http://127.0.0.1:3000/FUZZ -t 5  
        -fs 80117 \  
        -o "risultati_${wordlist}.json" -of json  
  
    sleep 10  
done
```

- `for wordlist in ...:` Itera su tutti i file creati dallo `split`.
- `-t 5:` Riduce il numero di thread a 5 per non sovraccaricare il server.
- `-o ..." -of json:` Salva i risultati di ogni scansione in un file JSON separato.
- `sleep 10:` Introduce una pausa di 10 secondi tra una scansione e l'altra per evitare troppo scansioni di fila.

3. Riepilogo dei risultato Si usare jq per creare un report finale di tutti i singoli risultati:

```
jq -r '.results[] | "\(.input) -> \(.status) [\(.length)
    bytes]"'
risultati_*.json > riepilogo.txt
```

Risultato della scansione

Il risultato della scansione eseguita usando ffuf.

```
(kali㉿kali)-[~]
$ cat riepilogo.txt
[{"FUFUHASH": "a98581ac", "FUZZ": "api"} → 500 [3017 bytes]
[{"FUFUHASH": "a98581ad", "FUZZ": "apis"} → 500 [3019 bytes]
[{"FUFUHASH": "a98581f3", "FUZZ": "assets"} → 301 [156 bytes]
[{"FUFUHASH": "f962fd4", "FUZZ": "ftp"} → 200 [11317 bytes]
[{"FUFUHASH": "50884a0", "FUZZ": "profile"} → 500 [1043 bytes]
[{"FUFUHASH": "50884b1", "FUZZ": "promotion"} → 200 [6586 bytes]
[{"FUFUHASH": "50884143", "FUZZ": "redirect"} → 500 [3119 bytes]
[{"FUFUHASH": "50884198", "FUZZ": "rest"} → 500 [3019 bytes]
[{"FUFUHASH": "50884199", "FUZZ": "restaurants"} → 500 [3033 bytes]
[{"FUFUHASH": "5088419a", "FUZZ": "restore"} → 500 [3025 bytes]
[{"FUFUHASH": "5088419c", "FUZZ": "restricted"} → 500 [3031 bytes]
[{"FUFUHASH": "5088419b", "FUZZ": "restored"} → 500 [3027 bytes]
[{"FUFUHASH": "508841b4", "FUZZ": "robots.txt"} → 200 [28 bytes]
[{"FUFUHASH": "58142129", "FUZZ": "video"} → 200 [10075518 bytes]
[{"FUFUHASH": "5814212a", "FUZZ": "Video"} → 200 [10075518 bytes]
```

Figure 3: Risultati della scansione Ffuf avanzata

Analisi della scansione

La seconda analisi più approfondita ha permesso di determinare la presenza di path interessanti come ad esempio ftp.

2.3 Scansione con un'altra wordlist (terza scansione)

Si esegue una terza scansione, questa volta con una wordlist più ampia fornita da dirbuster seguendo le stesse operazioni precedenti.

```
split -l 500
    /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
    \
dirbuster_common_part_

for wordlist in dirbuster_common_part_*; do
    echo "Testing with $wordlist"
```

```

ffuf -w "$wordlist" -u http://127.0.0.1:3000/FUZZ -t 5
    -fs 80117 \
    -o "risultati_${wordlist}.json" -of json

sleep 5
done

jq -r '.results[] | "\(.input) -> \(.status) [\(.length)
    bytes]"' \
risultati_*.json > riepilogo.txt

```

Risultato della scansione

Il risultato della scansione eseguita usando ffuf.

```

File Edit Search View Document Help
File Edit Search View Document Help
1 {"FFFUHASH":"fa26356","FUZZ":"profile"} → 500 [1043 bytes]
2 {"FFFUHASH":"fa26385","FUZZ":"video"} → 200 [10075518 bytes]
3 {"FFFUHASH":"fa263123","FUZZ":"assets"} → 301 [156 bytes]
4 {"FFFUHASH":"fa2631bd","FUZZ":"redirect"} → 500 [3119 bytes]
5 {"FFFUHASH":"4d2889","FUZZ":"ftp"} → 200 [11318 bytes]
6 {"FFFUHASH":"33d071a","FUZZ":"api"} → 500 [3017 bytes]
7 {"FFFUHASH":"33adbia","FUZZ":"api-docs"} → 500 [5017 bytes]
8 {"FFFUHASH":"33d07bd","FUZZ":"video"} → 200 [10075518 bytes]
9 {"FFFUHASH":"21e10ee","FUZZ":"restaurants"} → 500 [3033 bytes]
10 {"FFFUHASH":"21e10193","FUZZ":"promotion"} → 200 [6586 bytes]
11 {"FFFUHASH":"9b2761a8","FUZZ":"Profile"} → 500 [1943 bytes]
12 {"FFFUHASH":"c141c1a3","FUZZ":"FTP"} → 200 [11318 bytes]
13 {"FFFUHASH":"a1a0d11d","FUZZ":"rest"} → 500 [3019 bytes]
14 {"FFFUHASH":"3d58541","FUZZ":"restricted"} → 500 [3031 bytes]
15 {"FFFUHASH":"f63e19d","FUZZ":"Redirect"} → 500 [3119 bytes]
16 {"FFFUHASH":"10f5f5f","FUZZ":"metrics"} → 200 [24305 bytes]
17 {"FFFUHASH":"db93ad7","FUZZ":"Restaurant"} → 500 [3031 bytes]
18 {"FFFUHASH":"ada5963","FUZZ":"apis"} → 500 [3019 bytes]
19 {"FFFUHASH":"04a511b","FUZZ":"Promotion"} → 200 [6586 bytes]
20 {"FFFUHASH":"0c76a116","FUZZ":"restore"} → 500 [3025 bytes]
21 {"FFFUHASH":"c4bf6f17c","FUZZ":"restoration"} → 500 [3033 bytes]
22 {"FFFUHASH":"02cc086","FUZZ":"apidocs"} → 500 [3025 bytes]
23 {"FFFUHASH":"1fa10101","FUZZ":"VIDEO"} → 200 [10075518 bytes]
24 {"FFFUHASH":"3454213a","FUZZ":"restrictions"} → 500 [3035 bytes]
25 {"FFFUHASH":"99a0f2b","FUZZ":"mini"} → 200 [0 bytes]
26 {"FFFUHASH":"1921f1ca","FUZZ":".well-known"} → 200 [1323 bytes]
27 {"FFFUHASH":"fff2cf2a","FUZZ":"encryptionkeys"} → 200 [3210 bytes]
28

```

Figure 4: Risultati della scansione ffuf con lista ampliata

Analisi della scansione

La seconda ricerca ha permesso di trovare ulteriori path che non erano stati scoperti prima, in particolare possono essere path di interesse: `api-docs`, `.well-known` ed `encryptionkeys`.

3. Burp

Spiegazione

Lo scopo di Burp è per analizzare il traffico tra browser e server e identificare vulnerabilità nel sito web. Intercetta le richieste HTTP/HTTPS, mappa automaticamente la struttura del sito e permette modifiche in tempo reale alle richieste, con l'obiettivo finale di: scoprire risorse, endpoint, parametri e testare difese contro attacchi come SQL injection e XSS in un ambiente sicuro e controllato.

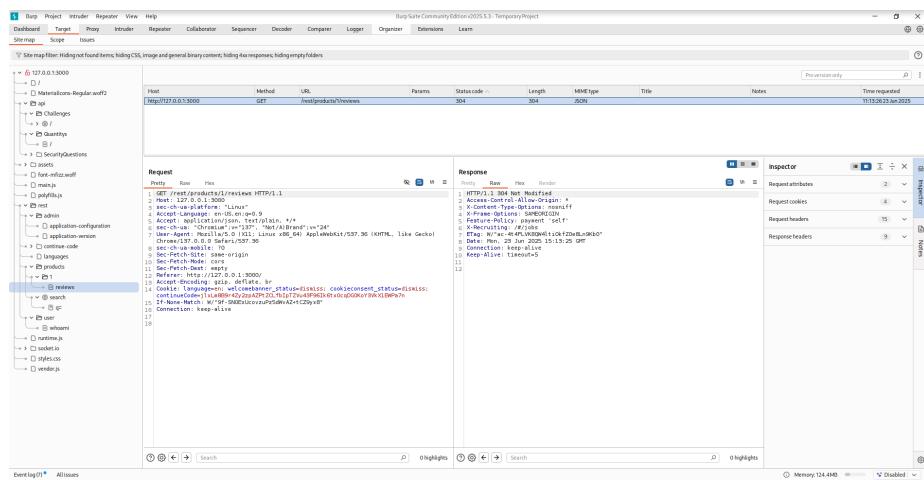


Figure 5: Mappatura del sito web

3. Ricerca manuale sul sito web

3.1 About

Dentro about c'è un link che rimanda alla pagina `legal.md` che si trova dentro la cartella `ftp`. Questo è un altro modo per raggiungere `ftp`.

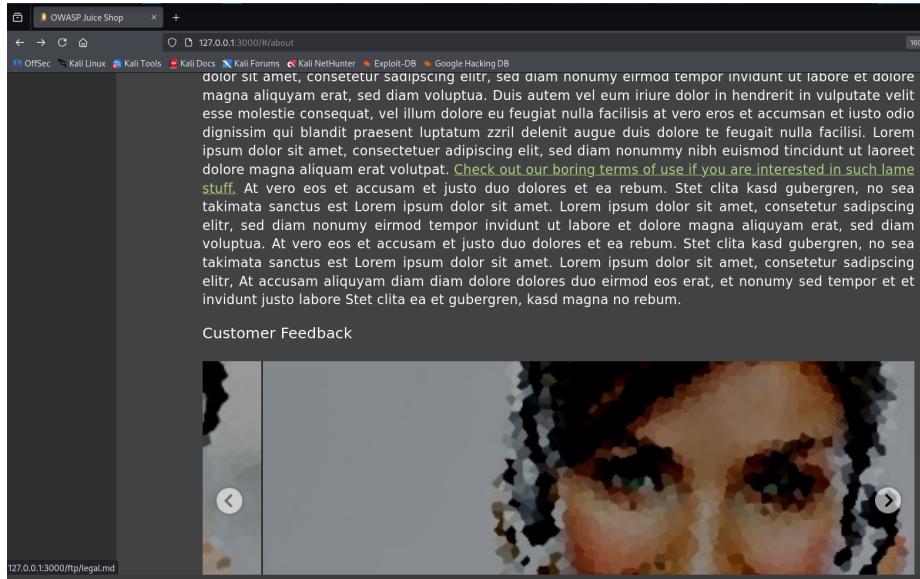


Figure 6: Pagina about

3.2 User enumeration

Cercando tra i prodotti è stato possibile capire quali sono gli utenti, possibilmente i ruoli collegati per poter effettuare successivamente attacchi mirati.

In questo caso questo utente con admin nella sua email potrebbe essere un admin del sito.

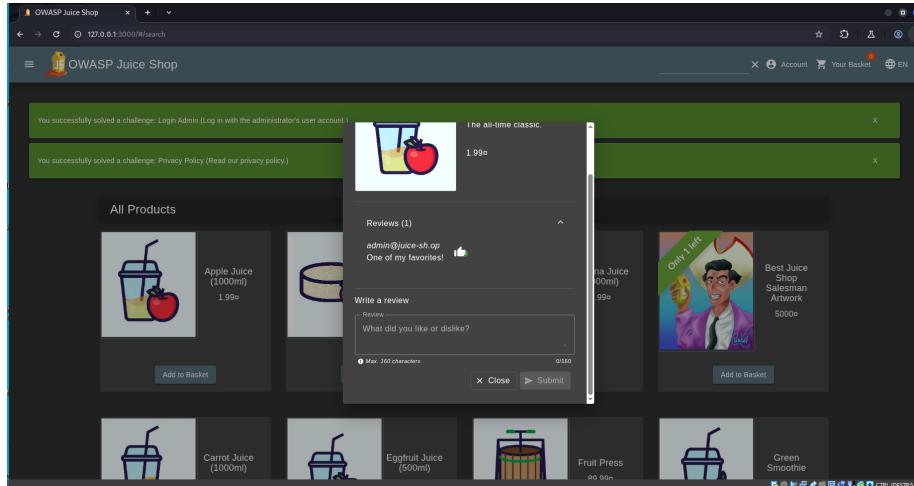


Figure 7: Probabile account dell'asdmin del sito

3.3 Architecture enumeration

Dal menu a tendina, è possibile conoscere gli stack tecnologici usati dal sito web tra cui troviamo:

- Angular
- HTML5
- SASS
- CSS3
- Javascript
- Node.js
- DB SQL
- Mongo DB



Figure 8: Tecnologie disponibili

3.4 Path enumeration

Andando a leggere il file javascript `main.js` è possibile scoprire eventuali nuove rotte non scoperte prima.

The screenshot shows the Chrome DevTools debugger interface. The title bar says "OWASP Juice Shop" and the address bar shows "127.0.0.1:3000/sitemap.xml#". The main area displays the Angular component tree for the "sitemap.xml" route. The tree starts with "main" and branches into "administration", "accounting", "addressbook", "addressselect", "addressview", "addresscreate", and "addressedit/addressId". Each node is expanded to show its child components and their properties. The right side of the screen has a sidebar with tabs for "Breakpoints", "Watch expressions", "Event Listener Breakpoints", and "DOM Mutation Breakpoints".

Figure 9: Path di angular

3.5 Input

Il sito web presenta diverse punti nel quale è possibile inserire degli input utente.

Search: esempio di search con la possibilità di eseguire una ricerca.

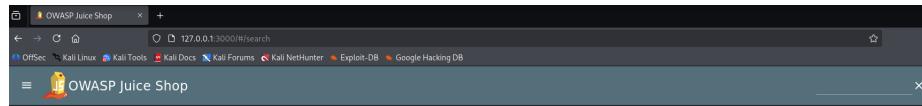


Figure 10: Search input

Login: esempio di login/registration con la possibilità di mandare sicuramente dati al server.

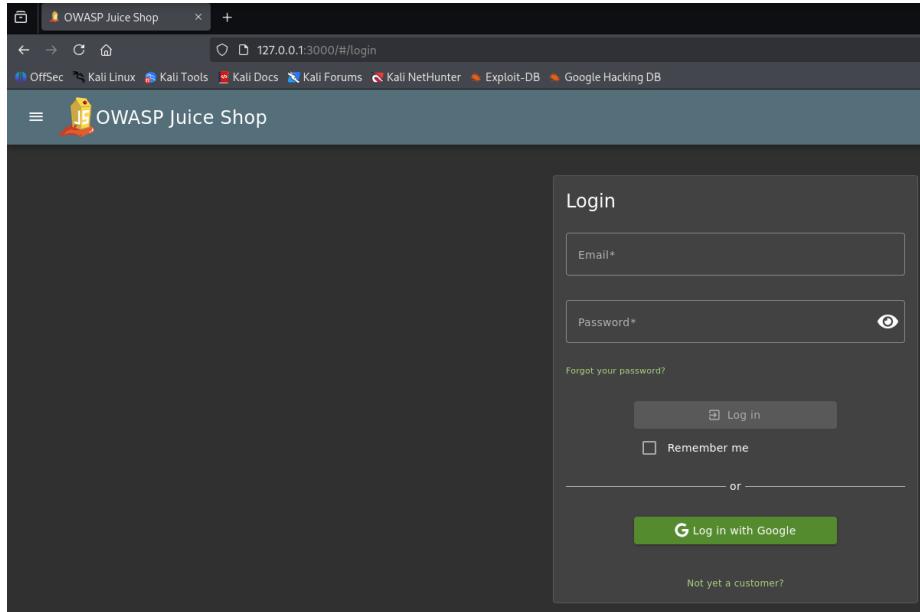


Figure 11: Login/Registration

3.6 File

Nel file main.js sono state trovate delle credenziali hard-coded.



```
POST /api/auth/login net::ERR_CERT_AUTHORITY_INVALID
```

Request URL	Request Method	Status Code	Response Headers	Request Headers	Preview
https://127.0.0.1:3000/api/auth/login	POST	200	Content-Type: application/json; charset=UTF-8 Date: Mon, 10 Jul 2023 10:30:40 GMT Server: Apache/2.4.41 (Ubuntu) Set-Cookie: token=eyJhbGciOiJIUzI1NiJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.vDwvLcXWzqkPQHdC9hRqMqgkqoqLsBzJ; expires=Mon Jul 10 10:30:40 2023; Max-Age=3600; path=/; secure; HttpOnly; SameSite=None; Strict-Transport-Security: max-age=31536000, includeSubDomains, preload	Content-Type: application/json	{<redacted>}

Figure 12: Hardcoded account

4. Ricerca di informazioni dopo autenticazione

4.1 Informazioni di login

Si può ottenere informazioni di login, soprattutto dati riguardanti i dati contenuti dentro il DB.

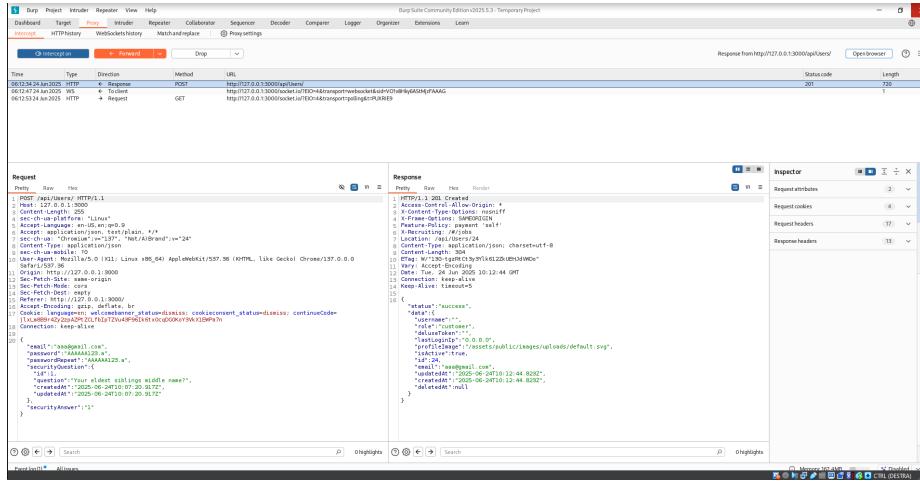


Figure 13: Registration response

4.2 User token

Quando viene effettuato il login, il server si occupa di creare un token JWT firmato per inviarlo al client. Questo token rappresenta la modalità di identificazione dell'utente per il server senza la necessità di richiedere al client ogni volta le informazioni di login.

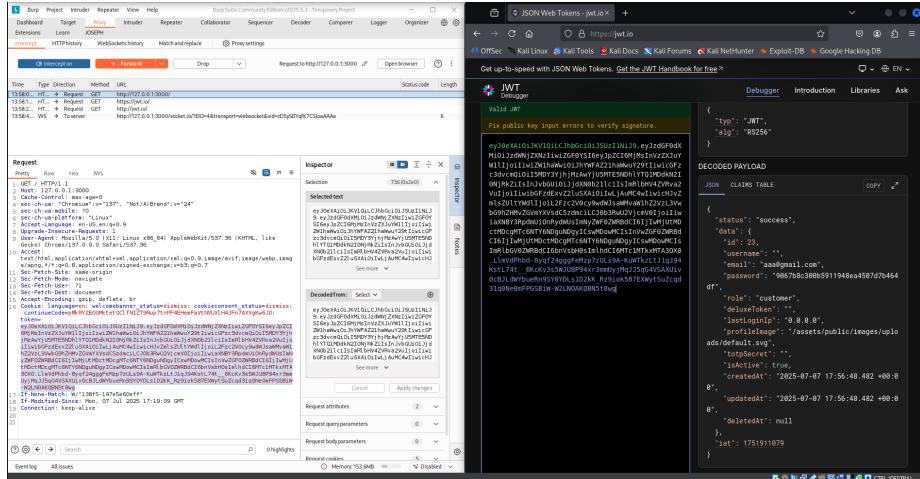


Figure 14: Use token

4.3 Review

La pagina di review contiene un input che potrebbe essere manipolato.

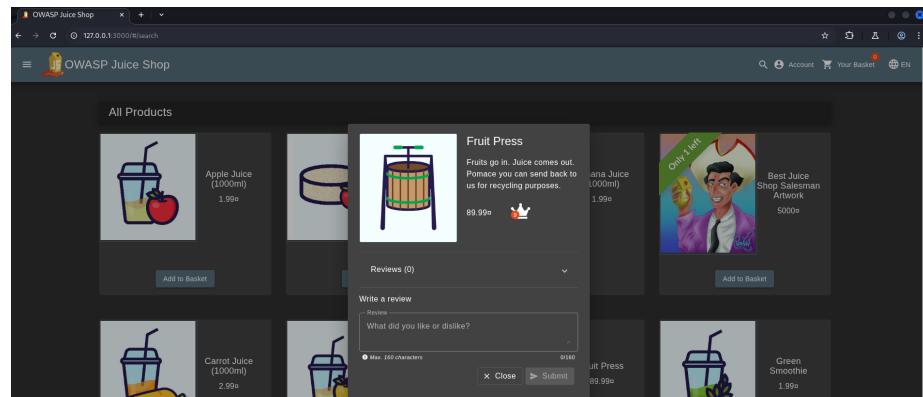


Figure 15: Review page

4.4 Pagina di feedback

Anche la pagina di feedback contiene un input che potrebbe essere manipolabile.

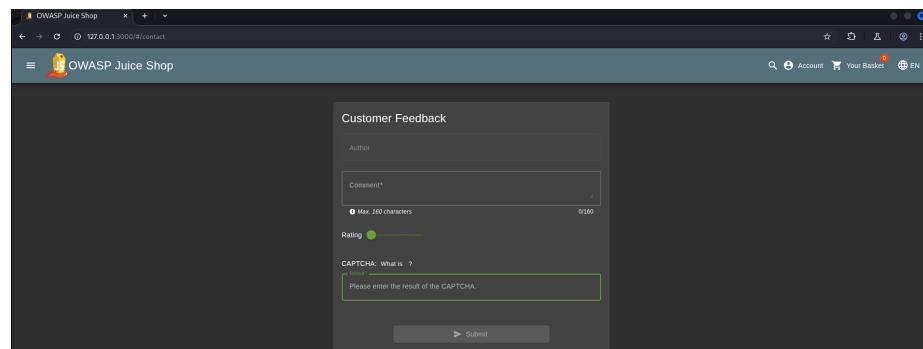


Figure 16: Feedback page

4.5 Chatbot

Molti similmente, anche la pagina del chatbot contiene un input utente che potrebbe essere manipolato.

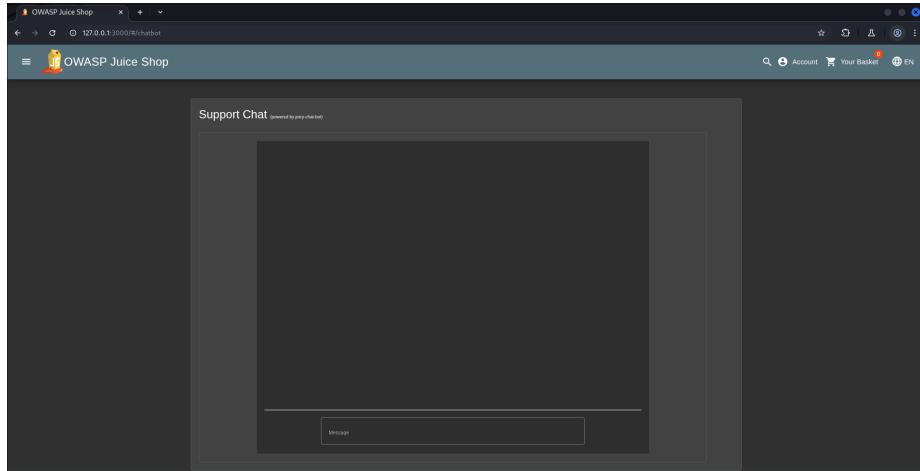


Figure 17: Chatbot page

4.6 Complaint

Similmente, anche la pagina di complaint rappresenta un altro possibile vettore d'attacco.

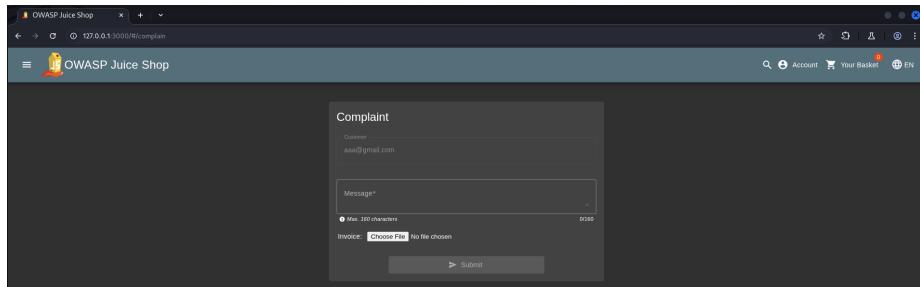


Figure 18: Complaint page

4.7 Basket

Quando si richiede i prodotti inseriti nel carrello, il server invia una richiesta GET usando il basket id dell'utente.

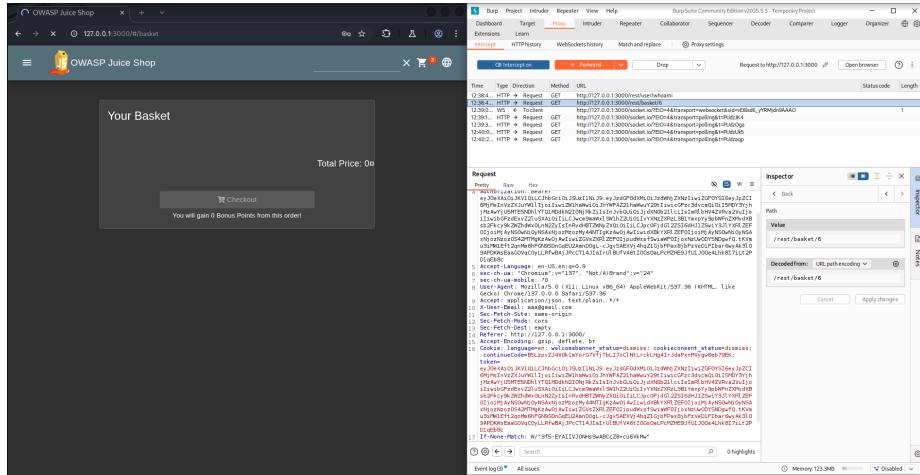


Figure 19: Basket

4.8 Login information

Dopo il logout, il server invia questi dati personali dell'utente riguardante l'autenticazione al server, tra cui la password hashata.

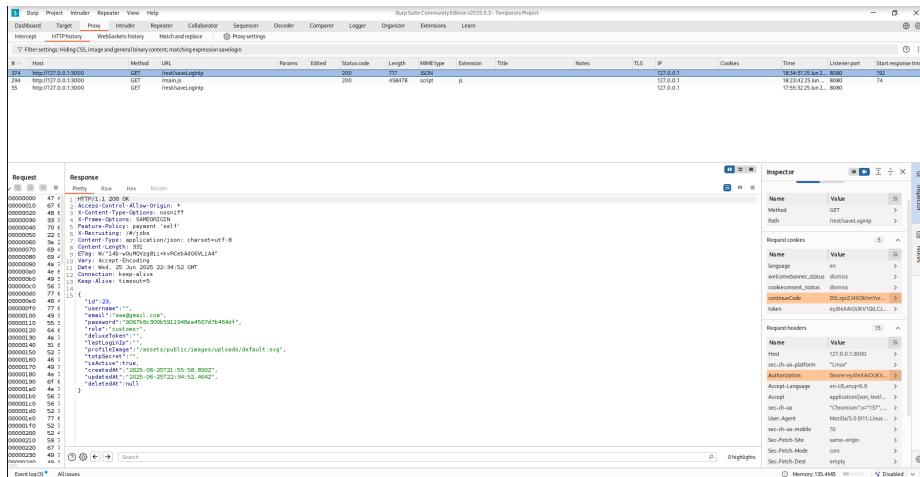


Figure 20: Login information

5. Analisi dei path trovati

Introduzione

Le pagine trovate precedentemente sono di 3 tipi 500, 200 e 301. Essi rappresentano:

1. **200**: pagine visitabili
2. **301**: pagine che reindirizzano ad altre pagine
3. **500**: pagine non visitabili direttamente come la api che probabilmente richiede dei parametri aggiuntivi.

5.1 Cartella FTP

La **cartella ftp** contiene una serie di file sensibili o che dovrebbero essere protetti da accessi indesiderati.

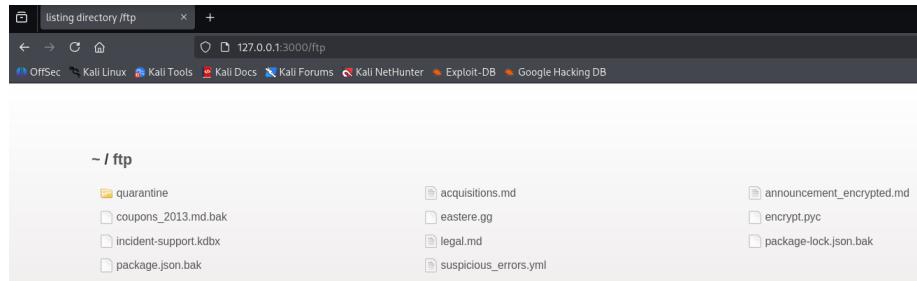
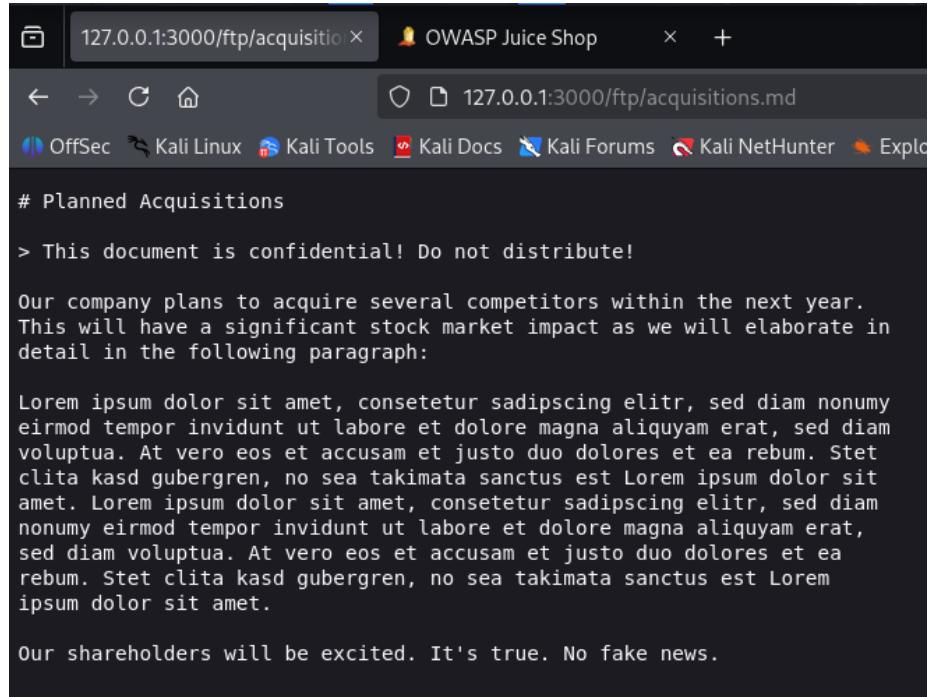


Figure 21: Cartella FTP

Un esempio di file è **acquisition.md** che come è stato dichiarato nel file stesso, contiene informazioni confidenziali.



The screenshot shows a web browser window with the URL `127.0.0.1:3000/ftp/acquisitions.md`. The page title is "OWASP Juice Shop". The content of the page is as follows:

```
# Planned Acquisitions

> This document is confidential! Do not distribute!

Our company plans to acquire several competitors within the next year. This will have a significant stock market impact as we will elaborate in detail in the following paragraph:

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Our shareholders will be excited. It's true. No fake news.
```

Figure 22: File acquisition

File accessibili

Sembra che tutti i file siano accessibili pubblicamente ma solo i file `.md` e `.pdf` vengono restituiti dal server. Forse è possibile aggirare in qualche modo, magari modificando la richiesta verso il server.

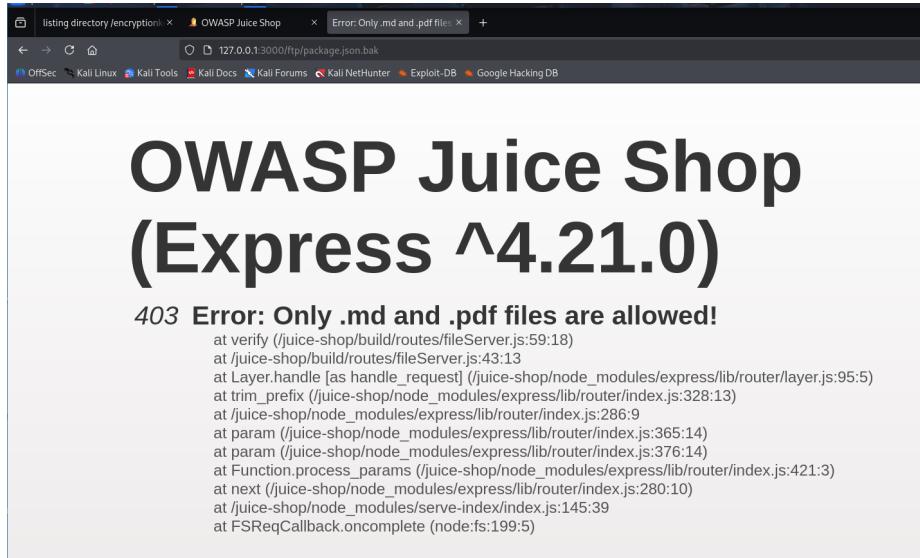


Figure 23: File accessibili di tipo .md e .pdf

5.2 Cartella metrics

La cartella metrics sembra contenere delle informazioni riguardanti le metriche che vengono raccolte dal sito. Sono probabilmente informazioni che dovrebbero rimanere protette.

```

listing directory /encryption/ x OWASP Juice Shop x 127.0.0.1:3000/metrics + 
← → ⌂ 127.0.0.1:3000/metrics + 
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

# HELP file_uploads_count Total number of successful file uploads grouped by file type.
# TYPE file_uploads_count counter

# HELP file_upload_errors Total number of failed file uploads grouped by file type.
# TYPE file_upload_errors counter

# HELP juiceshop_startup duration seconds Duration juiceshop required to perform a certain task during startup
# TYPE juiceshop_startup duration_seconds gauge
juiceshop_startup_duration_seconds{task="validateConfig",app="juiceshop"} 0.046985198
juiceshop_startup_duration_seconds{task="cleanupFtpFolder",app="juiceshop"} 0.109478174
juiceshop_startup_duration_seconds{task="validatePreconditions",app="juiceshop"} 0.14790947
juiceshop_startup_duration_seconds{task="datacreator",app="juiceshop"} 9.894952561
juiceshop_startup_duration_seconds{task="customizeApplication",app="juiceshop"} 0.066267375
juiceshop_startup_duration_seconds{task="customizeEasterEgg",app="juiceshop"} 0.042427518
juiceshop_startup_duration_seconds{task="ready",app="juiceshop"} 10.053

```

Figure 24: Cartella metrics

5.3 Cartella api-docs

Sembra che sia una pagina di documentazione di una API usata, in particolare per gestire gli ordini.

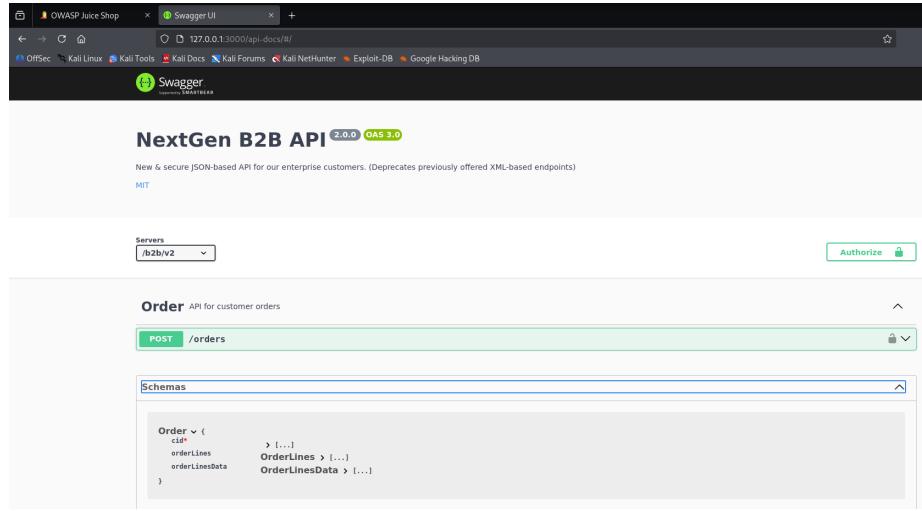


Figure 25: Cartella API-docs

5.4 API e REST

Sia API sia REST sono usati per chiamate API al server.

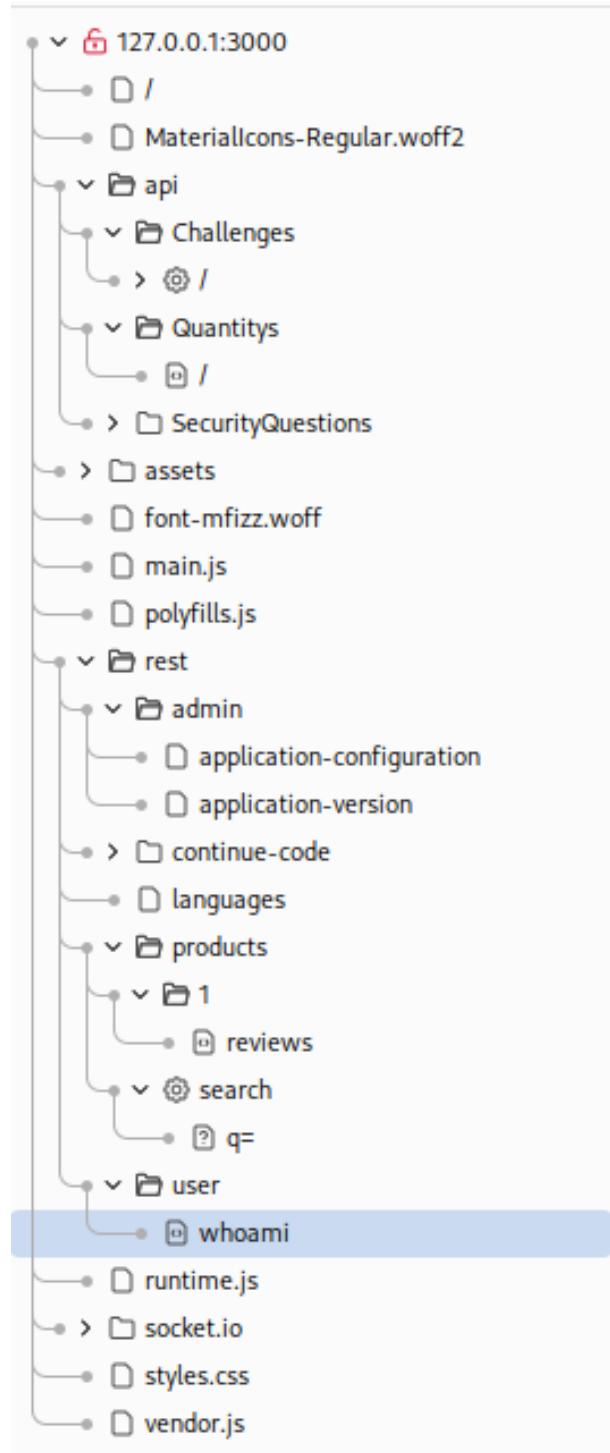
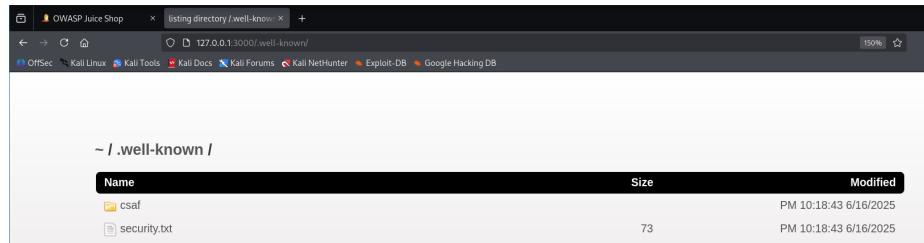


Figure 26: API e REST
26

5.5 Cartella .well-known

Sembra contenere informazioni di contatto in fatto di sicurezza e vulnerabilità passate trovate nel sito web.



The screenshot shows a file listing for the directory `.well-known`. The browser title bar says "listing directory /well-known". The address bar shows "127.0.0.1:3000/.well-known". The page content displays the following table:

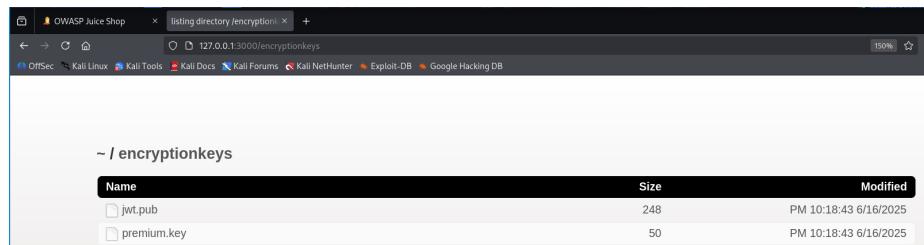
Name	Size	Modified
csaf		PM 10:18:43 6/16/2025
security.txt	73	PM 10:18:43 6/16/2025

Figure 27: Cartella .well-known

5.6 Cartella encryptionkey

Questa cartella sembra contenere 2 tipi di chiave:

- jwt.pub: potrebbe essere collegato a jwt usando per creare, leggere, modificare i token d'accesso.
- premium.key: una qualche chiave per accedere a servizi premium di qualche tipo.



The screenshot shows a file listing for the directory `encryptionkeys`. The browser title bar says "listing directory /encryptionkeys". The address bar shows "127.0.0.1:3000/encryptionkeys". The page content displays the following table:

Name	Size	Modified
jwt.pub	248	PM 10:18:43 6/16/2025
premium.key	50	PM 10:18:43 6/16/2025

Figure 28: Cartella encryption-key

5.7 Robots.txt

Il file robots.txt rappresenta un file usato dai siti web per regolare i crawler ovvero script automatici di scansione delle pagine web. Può essere utile per conoscere path nascosti.

In questo caso l'unica informazione data è la presenza della cartllea ftp di cui si conosceva già la presenza.

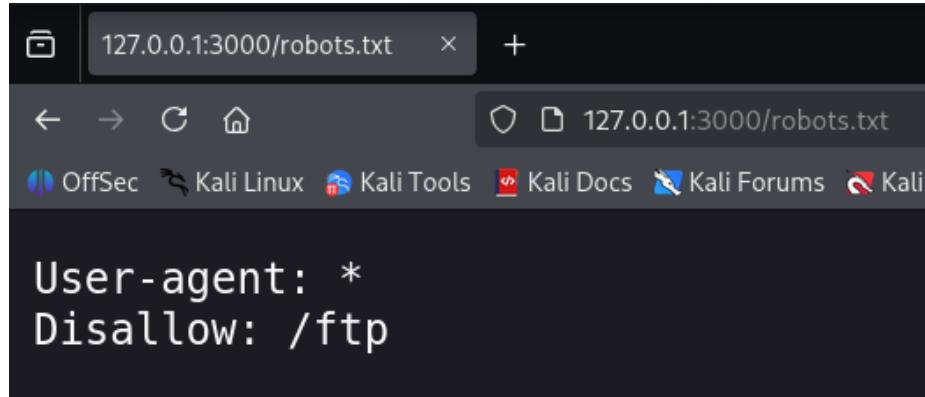


Figure 29: File robots

6. whois

Comando completo

```
whois owasp-juice.shop
```

Lo scopo di usare whois è per raccogliere informazioni di registrazione su un dominio web. Interroga i database WHOIS pubblici per ottenere dati come registrar, date di creazione/scadenza, nameserver e contatti amministrativi con l'obiettivo finale di ottenere una panoramica iniziale dell'infrastruttura del dominio.

Risultato della scansione

Il risultato della scansione eseguita usando whois.

```

sky@Dev:~$ whois owasp-juice.shop
Domain Name: OWASP-JUICE.SHOP
Registry Domain ID: D02909101-GMO
Registrar WHOIS Server:
Registrar URL: http://www.strato.de
Updated Date: 2025-02-13T04:02:15.0Z
Creation Date: 2017-11-20T10:26:02.0Z
Registry Expiry Date: 2025-11-20T23:59:59.0Z
Registrar: CRONON GmbH
Registrar IANA ID: 141
Registrar Abuse Contact Email: abuse-domains@cronon.net
Registrar Abuse Contact Phone: +49.30398020
Domain Status: ok https://icann.org/epp#ok
Registrant Country: DE
Registrant Email:
Admin Email:
Tech Email:
Name Server: DOCKS10.RZONE.DE
Name Server: SHADES01.RZONE.DE
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2025-06-28T17:17:07.0Z <<<

```

Figure 30: Risultati della scansione Whois

Analisi della scansione

Il dominio `owasp-juice.shop` è regolarmente registrato dal 2017 e ha una data di scadenza nel novembre 2025, il che conferma che si tratta di un progetto attivamente mantenuto. Il dominio è stato registrato presso il registrar **CRONON GmbH** (IANA ID 141), con sede in Germania. I server DNS associati sono `docks10.rzone.de` e `shades01.rzone.de`. Non sono presenti informazioni pubbliche su email o dettagli amministrativi (i campi sono omessi o oscurati), il che è normale per motivi di privacy o per il tipo di dominio. Il dominio ha uno stato “ok”, il che indica che non ci sono restrizioni particolari (es. blocchi, sospensioni, trasferimenti in corso).

7. dnsrecon

Comando completo

```
dnsrecon -d owasp-juice.shop -t std
```

Si usa il comando `dnsrecon -t std` per effettuare una ricognizione DNS completa sul dominio target. Interroga i DNS per raccogliere record chiave come A, AAAA, NS, MX, SRV, DMARC e DKIM. L’obiettivo finale è ottenere una mappa dell’infrastruttura DNS e dei servizi associati al dominio.

Risultato della scansione

Il risultato della scansione eseguita usando dnsrecon.

```
sky@Dev1:~$ dnsrecon -d owasp-juice.shop -t std
[*] std: Performing General Enumeration against: owasp-juice.shop...
[-] DNSSEC is not configured for owasp-juice.shop
[*] SOA docks10.rzone.de 217.160.80.137
[*] SOA docks10.rzone.de 2001:8d8:fe:53:5747:2a74:d:10
[*] NS docks10.rzone.de 217.160.80.137
[*] Bind Version for 217.160.80.137 https://www.powerdns.com/
[*] NS docks10.rzone.de 2001:8d8:fe:53:5747:2a74:d:10
[*] NS shades01.rzone.de 185.132.34.128
[*] Bind Version for 185.132.34.128 https://www.powerdns.com/
[*] NS shades01.rzone.de 2607:f1c0:fe:53:185:132:34:128
[*] MX smtpin.rzone.de 81.169.145.97
[*] MX smtpin.rzone.de 2a01:238:20a:202:50f0::1097
[*] A owasp-juice.shop 81.169.145.156
[*] AAAA owasp-juice.shop 2a01:238:20a:202:1156::
[*] TXT owasp-juice.shop keybase-site-verification=jvXPtfuHPkgsuHIZh9tLROyKLFxiyuRjNyIzLts6dIY
[*] TXT owasp-juice.shop 2024092302550343gqiwh2hpgqdk50zq2rf2ptuor3hqr2irx6mit7bswjt53r
[*] TXT _dmarc.owasp-juice.shop v=DMARC1;p=reject;
[*] TXT _domainkey.owasp-juice.shop o=~; t=y; r=dkim@rzone.de
[*] Enumerating SRV Records
[+] SRV _autodiscover._tcp.owasp-juice.shop autoconfigure.strato.de 81.169.145.141 443
[+] SRV _autodiscover._tcp.owasp-juice.shop autoconfigure.strato.de 2a01:238:20a:202:5800::1141 443
[+] 2 Records Found
```

Figure 31: Risultati della scansione Dnsrecon

Analisi della scansione

DNSSEC non configurato, potenziale vulnerabilità se l'integrità dei record DNS è importante. *SOA/NS/MX*, rivela provider DNS e di posta, utili per ricostruire l'infrastruttura. *Record A e AAAA*, forniscono IP pubblici. *Record TXT (DMARC/DKIM)*, utili per valutare la protezione da spoofing (manca SPF e DKIM è solo parzialmente attivo). *Record SRV*, indica un endpoint autodiscover che può essere testato per vulnerabilità, ad esempio in contesti Exchange o Outlook autodiscover leaks.

8. whatweb

Comando completo

```
whatweb http://127.0.0.1:3000
```

Si usa whatweb per identificare tecnologie web e configurazioni attive su un sito target. Analizza la risposta HTTP di un sito per rilevare framework, CMS, librerie JS, versioni software e intestazioni particolari. Viene quindi usato per scoprire potenziali vulnerabilità note o debolezze di configurazione attraverso il fingerprinting delle tecnologie usate.

Risultato della scansione

Il risultato della scansione eseguita usando whatweb.

```
sky@Dev:~$ whatweb http://127.0.0.1:3000
http://127.0.0.1:3000 [200 OK] Country[RESERVED][ZZ], HTML5, IP[127.0.0.1]
, JQuery[2.2.4], Script[module], Title[OWASP Juice Shop], UncommonHeaders[
access-control-allow-origin,x-content-type-options,feature-policy,x-recruiting], X-Frame-Options[SAMEORIGIN]
```

Figure 32: Risultati della scansione Whatweb

Analisi della scansione

Tecnologie rilevate: HTML5, JQuery 2.2.4 (libreria JS ampiamente diffusa ma in versione obsoleta), Script[module] (suggerisce l'uso di JavaScript moderno con moduli ES6). *Header HTTP rilevanti:* access-control-allow-origin: *: consente richieste cross-origin da qualsiasi dominio. Potrebbe indicare una potenziale debolezza di sicurezza (CORS misconfiguration) se associata a endpoint sensibili; x-content-type-options: nosniff, x-frame-options: SAMEORIGIN: header utili per la protezione contro alcuni attacchi (es. MIME sniffing, clickjacking); feature-policy, x-recruiting: headers non standard o personalizzati, probabilmente legati al deployment dell'app.

8.1 Modalità verbosa

Comando completo

```
whatweb -v http://127.0.0.1:3000
```

Spiegazione

- **Informazioni aggiuntive:** *Feature-Policy: payment ‘self’* → restrizione funzioni browser; *X-Recruiting: #/jobs* → potenziale endpoint interno/-nascosto; *Cache-Control, ETag, Content-Encoding, Content-Type* → info di caching e compressione.
- **Considerazioni:** L'header **X-Recruiting** suggerisce un collegamento a un endpoint *#/jobs* non immediatamente visibile dalla homepage. Potrebbe essere utile nella fase Exploit, ad esempio per ottenere accesso a funzionalità amministrative, backdoor o account interni di test. L'uso di **Access-Control-Allow-Origin: *** mostra una configurazione CORS permissiva, potenzialmente sfruttabile in scenari di attacco CSRF o di esfiltrazione da domini non autorizzati.

Risultato

Il risultato della scansione eseguita usando whatweb.

```
ky@Dev:~$ whatweb -v http://127.0.0.1:3000
WhatWeb report for http://127.0.0.1:3000
Status   : 200 OK
Title    : OWASP Juice Shop
IP       : 127.0.0.1
Country  : RESERVED, ZZ

Summary  : HTML5, JQuery[2.2.4], Script[module], UncommonHeaders[access-control-allow-origin,x-content-type-options,feature-policy,x-recruiting], X-Frame-Options[SAMEORIGIN]

Detected Plugins:
[ HTML5 ]
    HTML version 5, detected by the doctype declaration

[ JQuery ]
    A fast, concise, JavaScript that simplifies how to traverse
    HTML documents, handle events, perform animations, and add
    AJAX.

    Version     : 2.2.4
    Website    : http://jquery.com/

[ Script ]
    This plugin detects instances of script HTML elements and
    returns the script language/type.

    String      : module

[ UncommonHeaders ]
    Uncommon HTTP server headers. The blacklist includes all
    the standard headers and many non standard but common ones.
    Interesting but fairly common headers should have their own
    plugins, eg. x-powered-by, server and x-aspmx-version.
    Info about headers can be found at www.http-stats.com

    String      : access-control-allow-origin,x-content-type-options,feature-policy
    x-recruiting (from headers)
```

Figure 33: Risultati della scansione Whatweb_verbose_1

```
[ X-Frame-Options ]
  This plugin retrieves the X-Frame-Options value from the
  HTTP header. - More Info:
  http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
  aspx

  String      : SAMEORIGIN

HTTP Headers:
  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: Sat, 28 Jun 2025 17:04:23 GMT
  ETag: W/"138f5-197b77f4f8f"
  Content-Type: text/html; charset=UTF-8
  Vary: Accept-Encoding
  Content-Encoding: gzip
  Date: Sat, 28 Jun 2025 18:43:07 GMT
  Connection: close
  Transfer-Encoding: chunked
```

Figure 34: Risultati della scansione Whatweb_verbose_2
