

# Vulnerability Assessment Report: OWASP Juice Shop (Project 3)

**Project ID:** Project 3

**Assessed by:** Muhammad Talha

**Environment:** Kali Linux VM (VMware)

**Target:** OWASP Juice Shop (localhost)

**Date:** 23 June, 2025

---

## 1. Executive Summary

This report documents the results of a web application vulnerability assessment conducted on the OWASP Juice Shop project, a deliberately insecure web application. The testing was performed in a local environment using Kali Linux to simulate real-world attacks and identify critical vulnerabilities commonly found in modern web applications.

---

## 2. Tools Used

Tool	Purpose
Docker	Hosting OWASP Juice Shop
Nmap	Network reconnaissance
WhatWeb	Web technology fingerprinting
Nikto	Web server vulnerability scanning
Firefox Dev Tools	Manual inspection & network monitoring
Terminal/CLI	Payload delivery & testing

---

## 3. Reconnaissance

### WhatWeb

WhatWeb identified the underlying technologies of the OWASP Juice Shop application. The server stack included Node.js (JavaScript runtime), AngularJS (front-end framework), and Express (web framework). This stack helps assess relevant vulnerabilities like JavaScript-based client-side flaws or server-side Node exploits.

- Node.js
- AngularJS
- Express server

```
(kali㉿kali)-[~]
$ whatweb http://localhost:3000
http://localhost:3000 [200 OK] HTML5, IP[::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]
```

## Nmap

Nmap was used to scan localhost. The scan revealed that only port 3000 was open, which is the default port for the OWASP Juice Shop application. No other open ports or services were detected, indicating minimal network exposure. This limits attack vectors to the web application layer.

Figure: Nmap Scan - Output Continued

```
SF:te:\x20Mon,\x2023\x20Jun\x202025\x2010:25:22\x20GMT\r\nConnection:\x20c
SF:lose\r\n\r\n!—\n\x20\x20-\x20Copyright\x20(c.)\x202014-2025\x208joer
SF:\x20Kimmich\x20\x20the\x200WASP\x20Juice\x20Shop\x20contributors.\\
SF:\x20\x20\x20-\x20SPDX-License-Identifier:\x20MIT\x20\x20—\n\n<doctype
SF:\x20html>\n<html>\x20lang=\\"en\\">\n\x20\x20<title>OWASP\x20Juice\x20Shop
SF:</title>\n\x20\x20<meta>\x20name=\\"description\"\x20content=\\"Probably\
SF:\x20the\x20most\x20modern\x20and\x20sophisticated\x20insecure\x20web\x20
SF:application\"\>\n\x20\x20<meta>\x20name=\\"viewport\"\x20content=\\"width=d
SF:evice-width,\x20initial-scale=1"\>\n\x20\x20<link\x20id=\\"favicon\"\x20
```

Figure: Nmap Scan - Port Discovery

Performed a full port scan on localhost. Only port 3000 (Juice Shop) was open.

```
(kali㉿kali)-[~]
$ docker --version
Docker version 26.1.5+dfsg1, build a72d7cd

(kali㉿kali)-[~]
$ sudo docker run -d -p 3000:3000 bkimminich/juice-shop
[sudo] password for kali:
7d6cc37ba2d60361346642beac13e85e9bd3176063149c2078746283d79cf4e4

(kali㉿kali)-[~]
$ nmap -sV -p- localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 06:25 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000011s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
3000/tcp   open  ppp?
9050/tcp   open  tor-socks Tor SOCKS proxy
45031/tcp  open  http   Golang net/http server
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-TCPV=7.95%I=7%D=6/23%T=68592B92%P=x86_64-pc-linux-gnu%r(Ge
SF:TRequest,10189,"HTTP/1.1\x20200\x20KV\r\nAccess-Control-Allow-Origin:\\
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:\x20\r\nLast-Modified:\x20Mon,\x2023\x20Jun\x202025\x2010:21:47\x20GMT\r\n
SF:ETag:\x20W/\x20f5-1979c4eed8f"\r\nContent-Type:\x20text/html;\x20char
SF:set=UTF-8\r\nContent-Length:\x2080117\r\nVary:\x20Accept-Encoding\r\nDa
SF:te:\x20Mon,\x2023\x20Jun\x202025\x2010:25:22\x20GMT\r\nConnection:\x20c
```

```
SF:te:\x20Mon,\x2023\x20Jun\x202025\x2010:25:22\x20GMT\r\nConnection:\x20c
SF:lose\r\n\r\n!—\n\x20\x20-\x20Copyright\x20(c.)\x202014-2025\x208joer
SF:\x20Kimmich\x20\x20the\x200WASP\x20Juice\x20Shop\x20contributors.\\
SF:\x20\x20\x20-\x20SPDX-License-Identifier:\x20MIT\x20\x20—\n\n<doctype
SF:\x20html>\n<html>\x20lang=\\"en\\">\n\x20\x20<title>OWASP\x20Juice\x20Shop
SF:</title>\n\x20\x20<meta>\x20name=\\"description\"\x20content=\\"Probably\
SF:\x20the\x20most\x20modern\x20and\x20sophisticated\x20insecure\x20web\x20
SF:application\"\>\n\x20\x20<meta>\x20name=\\"viewport\"\x20content=\\"width=d
SF:evice-width,\x20initial-scale=1"\>\n\x20\x20<link\x20id=\\"favicon\"\x20
```

```

SF:evice-width,\x20initial-scale=1\>">\n\x20\x20<link\x20id=\\"favicon\\">
SF:rel=\\"icon\"\x20")%r(Helper,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nCon
SF:nnection:\x20close\r\n\r\n")%r(NCP,2F,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:\r\nConnection:\x20close\r\n\r\n")%r(HTTPOptions,EA,"HTTP/1\.1\x20204\
SF:\x20No\x20Content\r\nAccess-Control-Allow-Origin:\x20*\r\nAccess-Contro
SF:-Allow-Methods:\x20GET,HEAD,PUT,PATCH,POST,DELETE\r\nVary:\x20Access-C
SF:ontral-Request-Headers\r\nContent-Length:\x200\r\nDate:\x20Mon,\x2023\x
SF:20Jun\x202025\x2010:25:22\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RT
SF:SPPRequest,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:\x20Mon,\x2023\x20Jun\x202025\x2010:25:22\x20GMT\r\nConn
SF:ection:\x20close\r\n\r\n");

```

NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)

```

SF:Port45031-TCP:V=7.95%T=6/23%Time=6859288D%P=x86_64-pc-linux-gnu%r(G
SF:enericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\x400\x20Bad\
SF:\x20Request")%r(GetRequest,8F,"HTTP/1\.0.\x20404\x20Not\x20Found\r\nDate:
SF:\x20Mon,\x2023\x20Jun\x202025\x2010:25:17\x20GMT\r\nContent-Length:\x20
SF:\x9\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\n\r\n\x404:\x20Page
SF:\x20Not\x20Found")%r(HTTPOptions,8F,"HTTP/1\.0.\x20404\x20Not\x20Found\r
SF:\x20Date:\x20Mon,\x2023\x20Jun\x202025\x2010:25:17\x20GMT\r\nContent-Leng
SF:\x20:\x2019\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\n\r\n\x404:\x
SF:20Page\x20Not\x20Found")%r(RTSPRequest,67,"HTTP/1\.1\x20400\x20Bad\x20
SF:Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:
SF:\x20close\r\n\r\n\x400\x20Bad\x20Request")%r(Helper,67,"HTTP/1\.1\x20400\x2
SF:0Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConn
SF:ection:\x20close\r\n\r\n\x400\x20Bad\x20Request")%r(SSLSessionReq,67,"HT
SF:TP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20cha
SF:rset=utf-8\r\nConnection:\x20close\r\n\r\n\x400\x20Bad\x20Request")%r(Fou
SF:rOhFourRequest,8F,"HTTP/1\.0.\x20404\x20Not\x20Found\r\nDate:\x20Mon,\x2

```

```

SF:rOhFourRequest,8F,"HTTP/1\.0.\x20404\x20Not\x20Found\r\nDate:\x20Mon,\x2
SF:023\x20Jun\x202025\x2010:25:32\x20GMT\r\nContent-Length:\x2019\r\nConte
SF:n-Type:\x20text/plain;\x20charset=utf-8\r\n\r\n\x404:\x20Page\x20Not\x20
SF:Found")%r(LPDString,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-T
SF:type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n\x400
SF:\x20Bad\x20Request")%r(SIPOptions,67,"HTTP/1\.1\x20400\x20Bad\x20Reques
SF:\r\nContent-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20cl
SF:ose\r\n\r\n\x400\x20Bad\x20Request")%r(Sock5,67,"HTTP/1\.1\x20400\x20Bad
SF:\x20Request\r\nContent-type:\x20text/plain;\x20charset=utf-8\r\nConnect
SF:ion:\x20close\r\n\r\n\x400\x20Bad\x20Request")%r(OfficeScan,A3,"HTTP/1\.1
SF:\x20400\x20Request\x20missing\x20required\x20Host\x20Header\r\n\r\n\x400
SF:Content-Type:\x20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r
SF:\n\r\n\x400\x20Bad\x20Request\x20missing\x20required\x20Host\x20Header");

```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.  
Nmap done: 1 IP address (1 host up) scanned in 28.50 seconds

## Nikto

Nikto scanned the Juice Shop web server hosted on port 3000. It returned multiple warnings including missing security headers, potential directory listing issues, and use of outdated libraries. These findings indicate possible exposure to basic misconfigurations and outdated server-side components.

Figure: Nikto scan - Additional findings

```

kalilocal ~
$ nikto -h http://localhost:3000
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    3000
+ Start Time:    2025-06-23 06:39:58 (GMT-4)

+ Server: No banner retrieved
+ /: Retrieved access-control-allow-origin header: *.
+ /: Uncommon header 'x-recruiting' found, with contents: #!/jobs.
+ NCG Directories found (use '-C all' to force check all possible dirs)
+ 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
+ assets/public/favicon_js.ico: 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.cer: 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
+ /localhost.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.egg: 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
+ /dump.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.alz: 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
+ /backup.alz: 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
+ /archive.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html

```

## Scanned for known web server vulnerabilities on port 3000.

```
kali㉿kali:~
File Actions Edit View Help
└$ nikto -h http://localhost:3000
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    3000
+ Start Time:    2025-06-23 06:39:58 (GMT-4)

+ 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)
+ /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
+ assets/public/favicon.ico: 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.netspark.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /site.cer: 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
+ /localhost.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.egg: 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
+ /dump.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.alz: 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
+ /backup.alz: 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
+ /archive.tar: 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
+ /site.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.cer: 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
+ /127.0.0.1.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.war: 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
+ /localhost.tar.bz2: 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
+ /127.0.0.1.tar: 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.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.war: 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
+ /site.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tar: 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
+ /database.cer: 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
+ /backup.cer: 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
+ /127.0.0.1.tar.lzma: 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
+ /localhost.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.egg: 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
```

```
+ /dump.tar: 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
+ /127.0.0.1.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tar: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.tgz: 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
+ /database.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.tgz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /127.0.0.1.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.jks: 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
+ /database.alz: 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
+ /127.0.0.1.cer: 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
+ /127.0.0.1.tgz: 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
+ /localhost.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /localhost.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /dump.jks: 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
+ /database.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.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
+ /archive.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /ftp/: This might be interesting.
+ /public/: This might be interesting.
+ /wp-content/plugins/nextgen-gallery/products/photocrati_nextgen/modules/nextgen_addgallery_page/static/jquery.filetree/connectors/jqueryFil
eTree.php: NextGEN Gallery LFI. See: https://seclists.org/fulldisclosure/2014/Feb/171
```

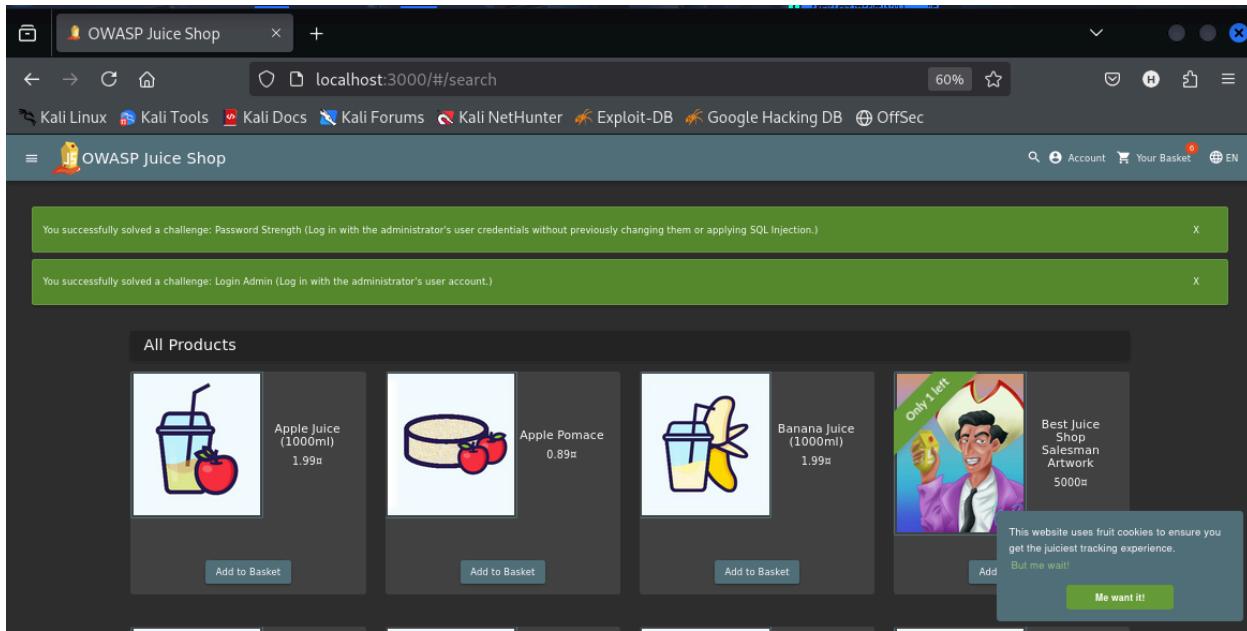
```
eTree.php: NextGEN Gallery LFI. See: https://seclists.org/fulldisclosure/2014/Feb/171
+ /wordpress/wp-content/plugins/nextgen-gallery/products/photocrati_nextgen/modules/nextgen_addgallery_page/static/jquery.filetree/connectors
/jQueryFileTree.php: NextGEN Gallery LFI. See: https://seclists.org/fulldisclosure/2014/Feb/171
+ 7789 requests: 2 error(s) and 79 item(s) reported on remote host
+ End Time: 2025-06-23 06:43:59 (GMT-4) (241 seconds)
+ 1 host(s) tested
```

---

## 4. Vulnerabilities Identified

### 1. Broken Authentication via Default Credentials

- Gained admin access using weak default credentials:  
Username: admin@juice-sh.op  
Password: admin123
- Accessed the administrative dashboard without brute force.



## 2. SQL Injection – Login Bypass

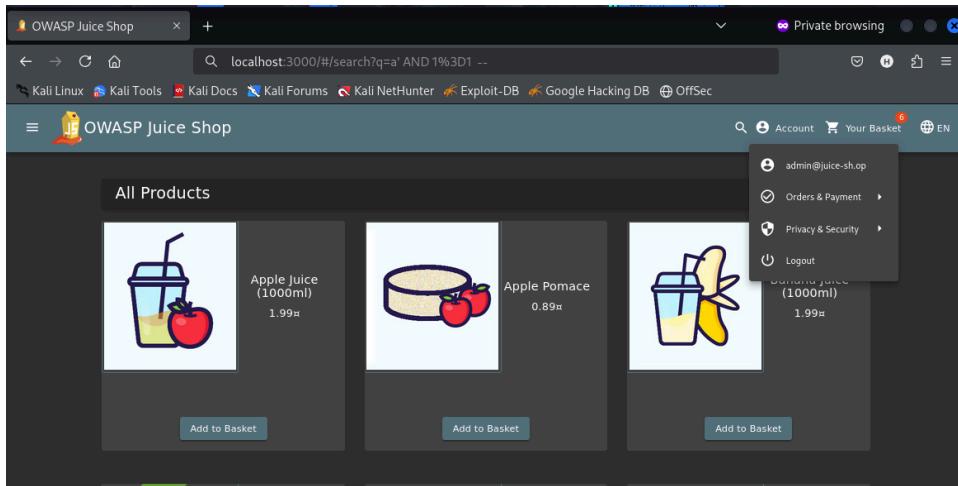


Figure: Proof of login via SQL Injection

- Successfully bypassed authentication using:  
Username: ' OR 1=1 --  
Password: any
- Logged in directly as administrator without valid credentials.

OWASP Juice Shop

localhost:3000/#/search?q=a' AND 1%3D1 --

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OWASP Juice Shop Account EN

Login

Email\*  
' OR 1=1 --

Password\* password

Forgot your password?

Log in

Remember me

or

[Log in with Google](#)

The screenshot shows the OWASP Juice Shop login page. The user has entered "' OR 1=1 --" into the email field, which is a classic SQL injection attack. The password field contains "password". Below the fields, there is a link for "Forgot your password?". A "Log in" button is present, along with a "Remember me" checkbox. Below the login form, there is a "or" link followed by a "Log in with Google" button. The browser's address bar shows the URL "localhost:3000/#/search?q=a' AND 1%3D1 --". The page title is "OWASP Juice Shop".

OWASP Juice Shop

localhost:3000/#/search?q=a' AND 1%3D1 --

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

OWASP Juice Shop

All Products

Apple Juice (1000ml) 1.99€

Apple Pomace 0.89€

Banana Juice (1000ml) 1.99€

Add to Basket Add to Basket Add to Basket

admin@juice-sh.op

Orders & Payment

Privacy & Security

Logout

The screenshot shows the OWASP Juice Shop products page. It displays three items: "Apple Juice (1000ml)" at 1.99€, "Apple Pomace" at 0.89€, and "Banana Juice (1000ml)" at 1.99€. Each item has an "Add to Basket" button below it. On the right side, there is a user menu for "admin@juice-sh.op" which includes "Orders & Payment", "Privacy & Security", and "Logout". The browser's address bar shows the URL "localhost:3000/#/search?q=a' AND 1%3D1 --". The page title is "OWASP Juice Shop".

### 3. Stored XSS (Attempted)

The screenshot shows the 'Administration' section of the OWASP Juice Shop application. On the left, there's a list of registered users. On the right, there are two tables of customer feedback. The top table has 8 rows, and the bottom table has 8 rows. Both tables show reviews from users like 'marty@juice-sh.op' and 'mc.safesearch@juice-sh.op'. The reviews contain various payloads, such as 'Can't even upload photo of broken purchase!', 'Support Team: Sorry, only order confirmation PDFs can be attached to complaints!', and 'This is the store for awesome stuff of all kinds! (anonymous)'. The payloads are reflected in the review text.

Figure: Admin panel reflecting payloads

This screenshot is similar to the previous one but shows a different view of the customer feedback. It has two main sections: 'Registered Users' on the left and 'Customer Feedback' on the right. The 'Customer Feedback' section contains two tables with 8 rows each. The reviews reflect the same payloads seen in the previous screenshot, such as 'Can't even upload photo of broken purchase!' and 'Support Team: Sorry, only order confirmation PDFs can be attached to complaints!'. The payloads are clearly visible in the review text.

Figure: Payload reflected in feedback view

This screenshot shows a 'Customer Feedback' form. In the 'Comment' field, there is a reflected payload: '<svg/onload=alert('HackerSVG')>'. Below the comment field, there is a CAPTCHA input with the value '-10'. The rest of the form includes fields for 'Author' (set to 'mc.safesearch@juice-sh.op'), 'Rating' (set to 1), and a 'Submit' button.

Figure: SVG onload injection payload

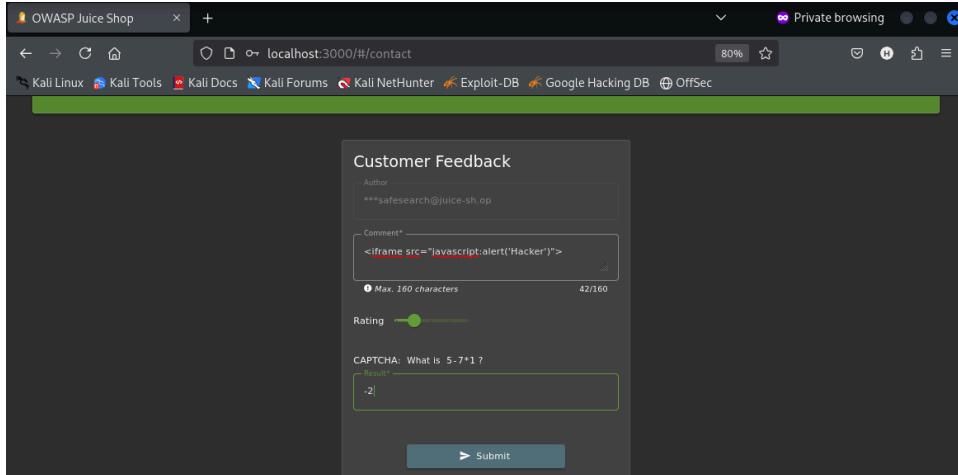


Figure: IFrame-based payload injection

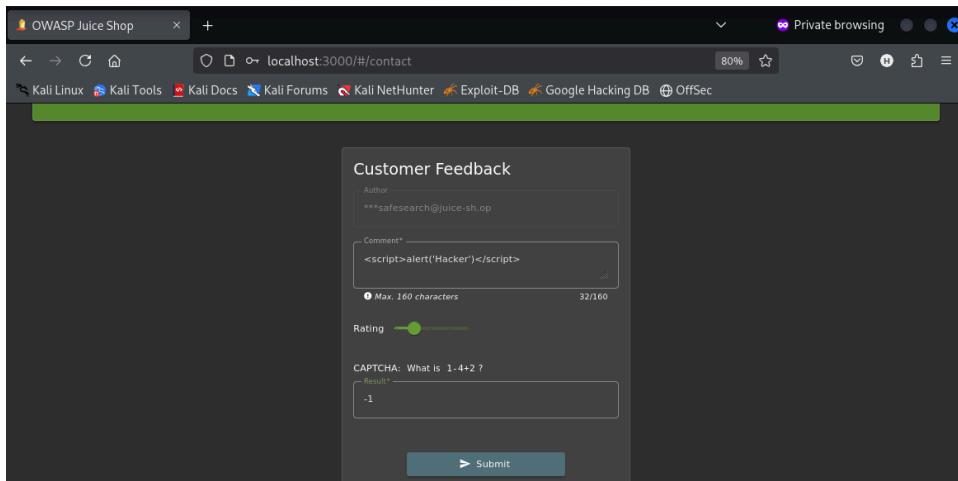


Figure: Script Payload - <script>alert('Hacker')</script>

- Payloads submitted:

```
<img src=x onerror=alert('XSS')>
<svg/onload=alert('HackerSVG')>
<iframe src="javascript:alert('Hacker')">
<script>alert('Hacker')</script>

<img src=x onerror=alert('XSS')>
<svg/onload=alert('HackerSVG')>
<iframe src="javascript:alert('Hacker')">
```

- Feedback was stored (user email visible in admin panel), but the message body was not rendered.

- This indicates a potential execution vector under certain rendering contexts.

The screenshot shows a web browser window for the OWASP Juice Shop application. The URL is `localhost:3000/#/contact`. The page title is "Customer Feedback". There is a form with fields for "Author" (set to `***safesearch@juice-sh.op`), "Comment" (containing the payload `<img src=x onerror=alert('Hacked')>`), "Rating" (set to 5), and a CAPTCHA field (set to `-17`). A "Submit" button is at the bottom. The browser interface includes a toolbar with various icons and a status bar indicating "Private browsing" and "80%".

This screenshot shows the same "Customer Feedback" page from the OWASP Juice Shop. The "Comment" field now contains the payload `<svg/onload=alert('HackerSVG')>`. The rest of the form (Author, Rating, CAPTCHA) and the browser interface remain the same.

OWASP Juice Shop

localhost:3000/#/contact

Private browsing

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

### Customer Feedback

Author: \*\*\*@juice-sh.op

Comment\*: <iframe src="lavascript:alert('Hacker')">

Max. 160 characters 42/160

Rating: ██████████

CAPTCHA: What is 5-7\*1 ?

Result: -2

Submit

This screenshot shows a user attempting to submit a comment containing a reflected XSS payload. The payload is <iframe src="lavascript:alert('Hacker')">. The browser's developer tools highlight the entire payload in red, indicating it was not properly sanitized before being rendered.

OWASP Juice Shop

localhost:3000/#/contact

Private browsing

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

### Customer Feedback

Author: \*\*\*@juice-sh.op

Comment\*: <script>alert('Hacker')</script>

Max. 160 characters 32/160

Rating: ██████████

CAPTCHA: What is 1-4+2 ?

Result: -1

Submit

This screenshot shows a user attempting to submit a comment containing a reflected XSS payload. The payload is <script>alert('Hacker')</script>. The browser's developer tools highlight the entire payload in red, indicating it was not properly sanitized before being rendered.

The screenshot shows a web browser window for the OWASP Juice Shop application. The URL is `localhost:3000/#/administration`. The page displays a list of reviews and a detailed view of a specific review.

**Reviews List:**

Review	Rating	Action
morty@juice-sh.op	★ ★	edit
mc.safesearch@juice-sh.op	★	edit
j12934@juice-sh.op	★ ★ ★	edit
wurstbrot@juice-sh.op	★ ★ ★	edit

**Review Detail View:**

Review	Rating	Action
Incompetent customer support! Can't even upload photo of broken purchase! Support Team: Sorry, only order confirmation PDFs can be attached to complaints!	★ ★	edit
This is the store for awesome stuff of all kinds!	★ ★ ★	edit
Never gonna buy anywhere else from now on! Thanks for the great service!	★ ★ ★	edit
Keep up the good work!	★ ★ ★	edit

Items per page: 10    1 - 10 of 21    < >

Items per page: 10    1 - 10 of 12    < >

## 4. Broken Access Control – Tested and Secure

The screenshot shows a web browser window for the OWASP Juice Shop application. The URL is `localhost:3000/#/order-history`. The page displays the "Order History" section.

**Order History:**

No results found  
You have not placed any orders yet.

Figure: Order history route accessed

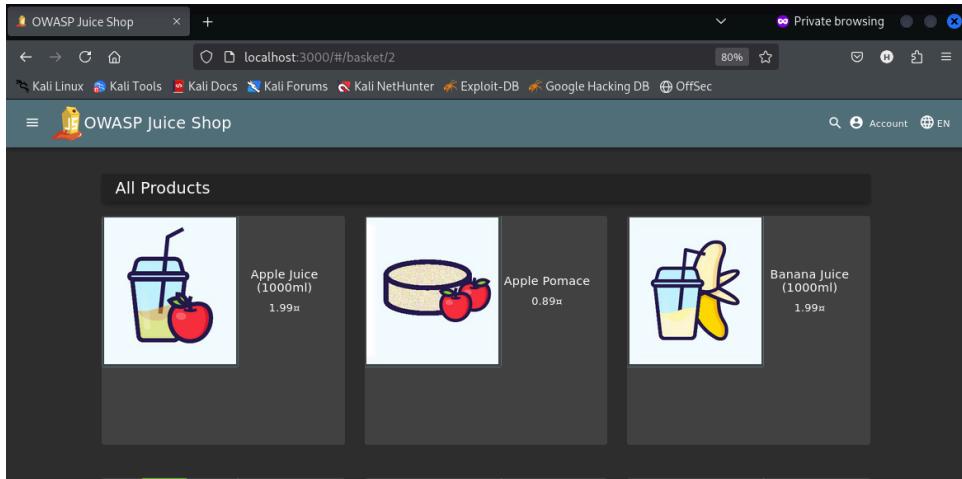


Figure: Accessing basket #2

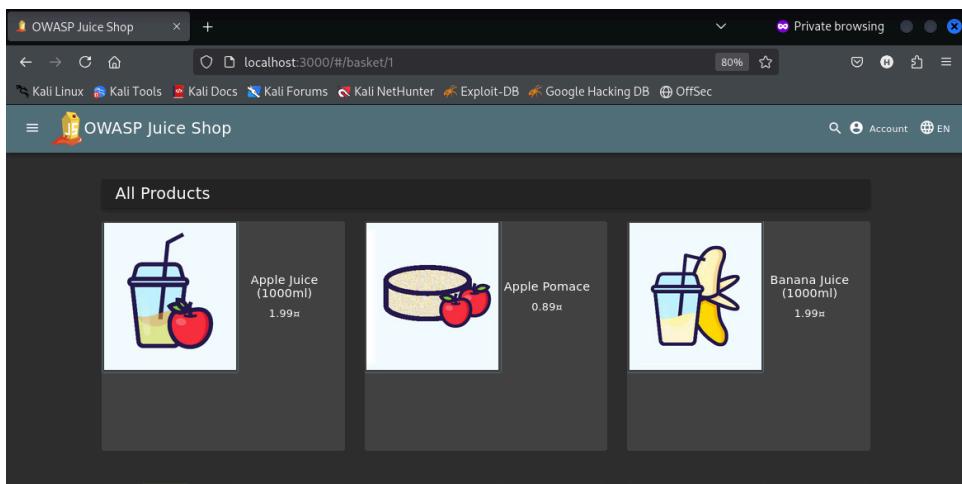
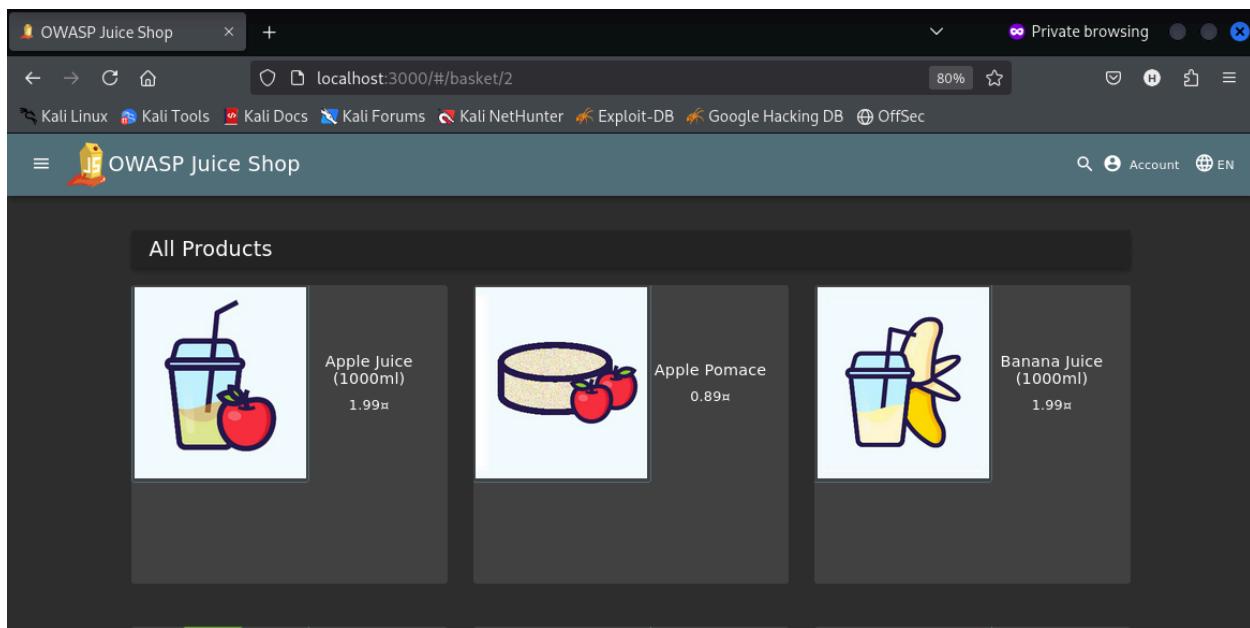
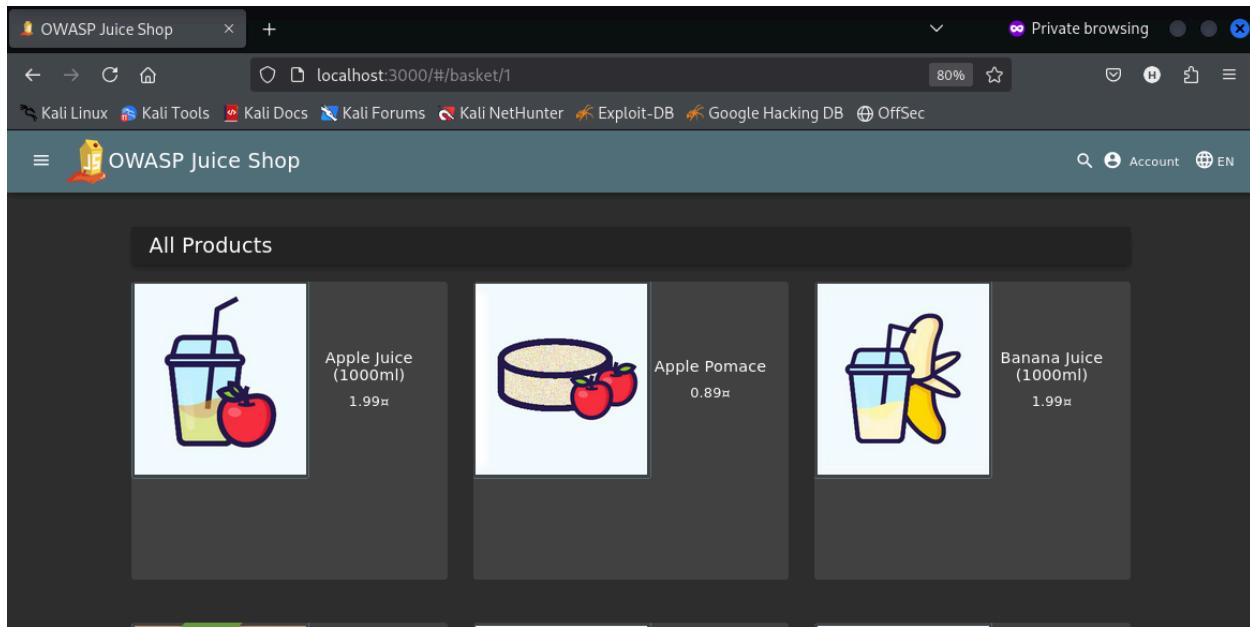
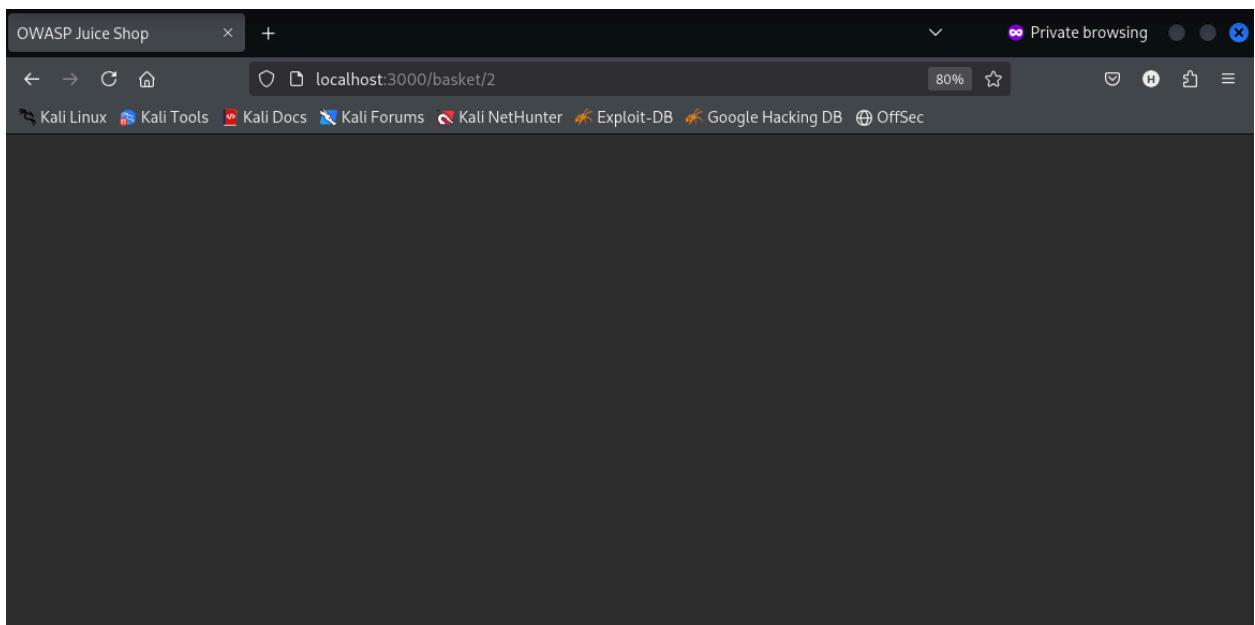
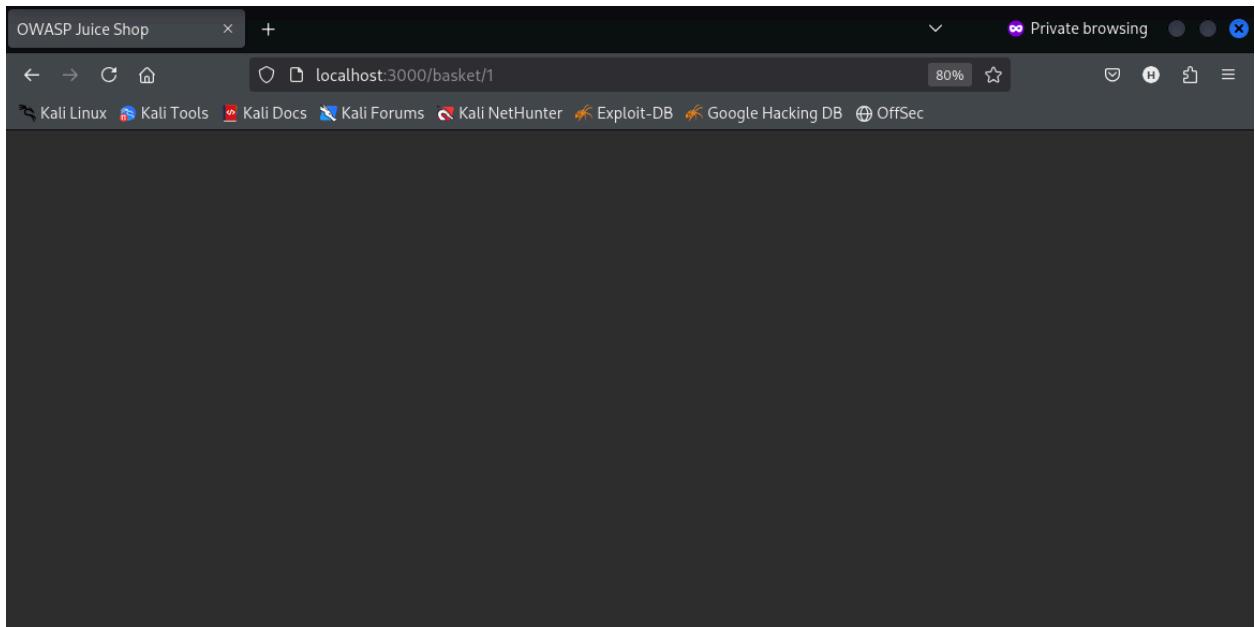
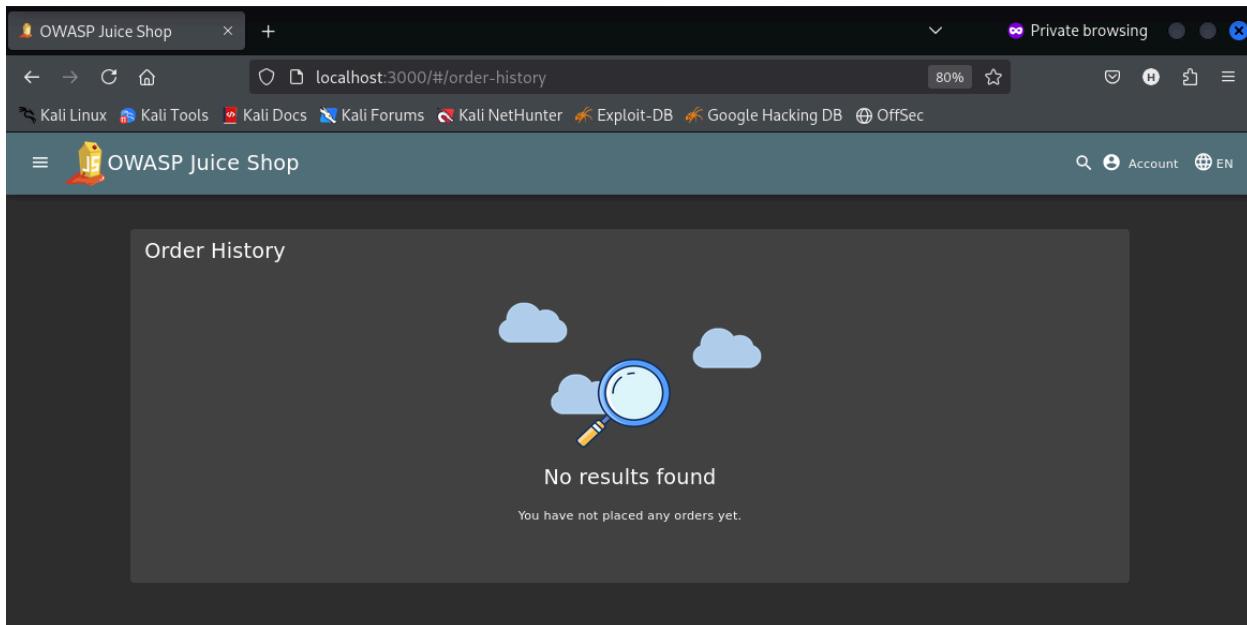


Figure: Accessing basket #1

- Accessed routes like:
  - /#/basket/1
  - /#/basket/2
  - /#/order-history
- While the front-end components loaded, no sensitive data was returned.
- Network tab confirmed no /rest/basket/:id or related data leaks.



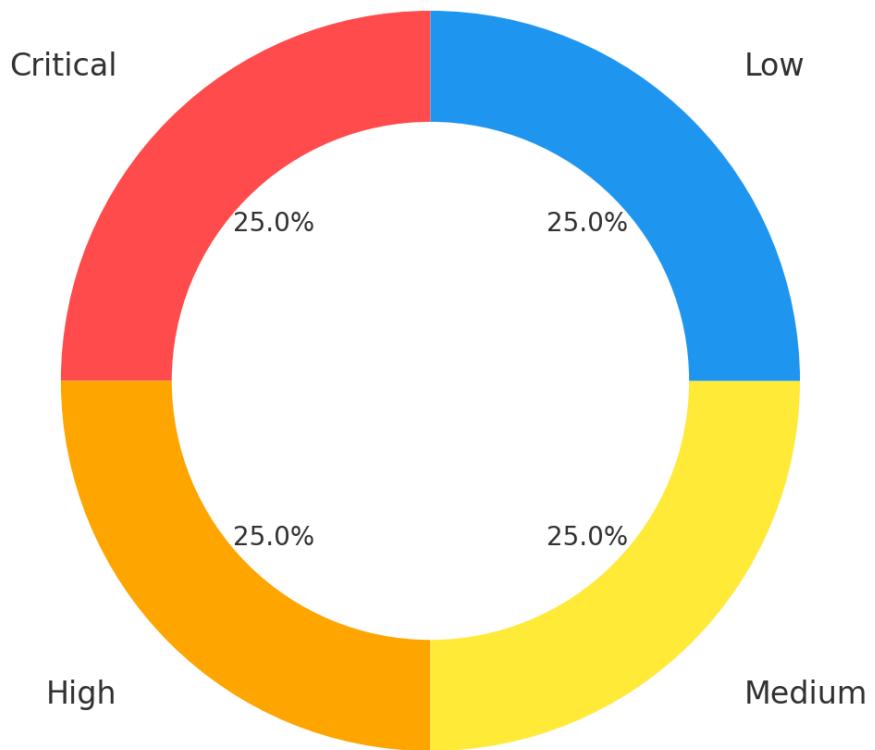




## 5. Risk Summary

Vulnerability	Severity	Status
Admin Login via Weak Creds	High	Confirmed
SQL Injection (Auth Bypass)	Critical	Confirmed
Stored XSS	Medium	Payload stored (not rendered)
Broken Access / IDOR	Low	Not exploitable

## Overall Vulnerability Severity

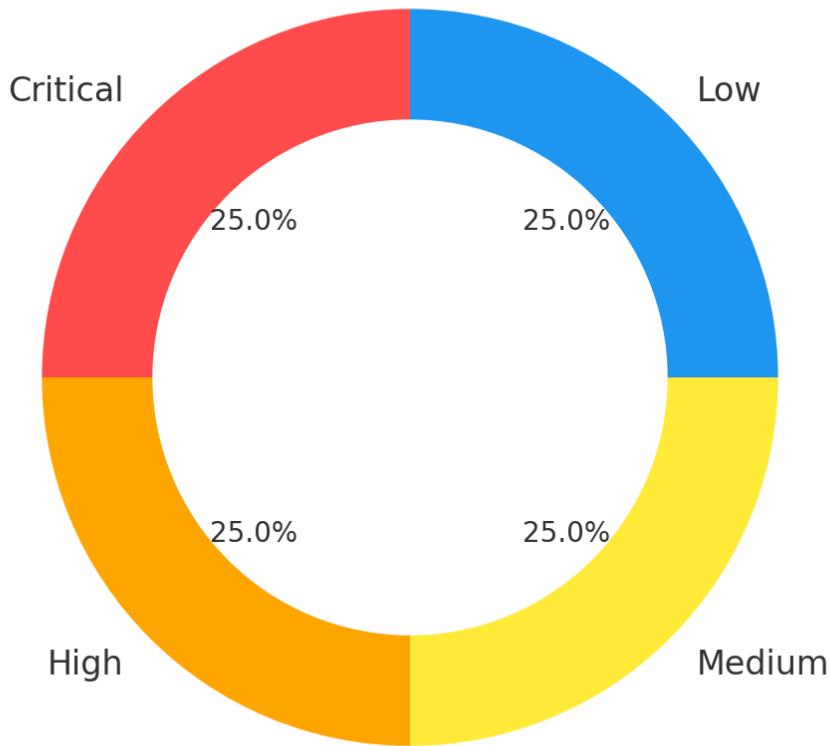


---

## 6. Recommendations

Issue	Recommendation
SQLi & Login Bypass	Use parameterized queries, enforce strong password policies
Stored XSS	Sanitize input/output and escape HTML/JS characters
Admin Account	Remove default creds, enforce MFA
SPA Route Exposure	Hide protected components without sessions

## Overall Vulnerability Severity



---

## 7. Conclusion

This project successfully simulated multiple real-world attack vectors against a modern web application in a controlled local environment. Two critical vulnerabilities were discovered and exploited (SQLi and default creds). While stored XSS was not executed, injection was successful. Access control appears secure for user-specific endpoints.

---

## 8. Appendix

- WhatWeb Output
- Nmap Output
- Nikto Scan Result
- Admin Login Screenshot

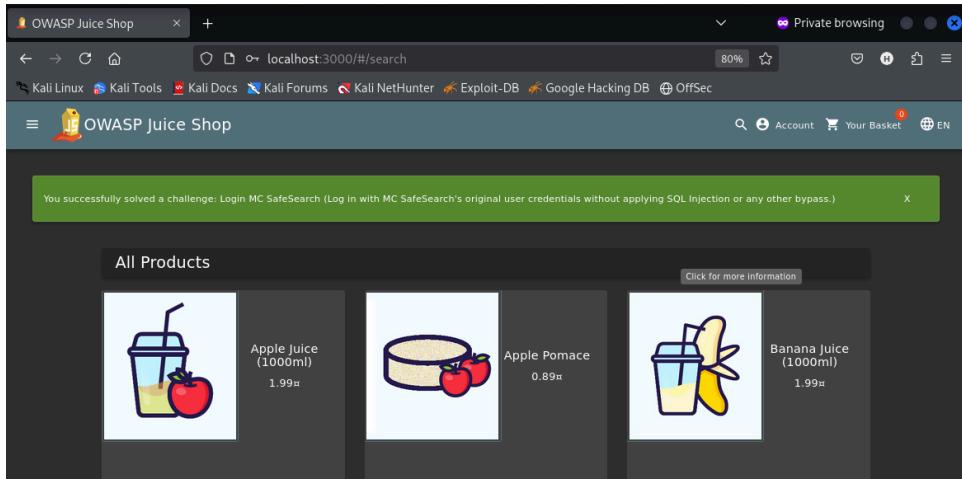


Figure: Logged-in admin dashboard

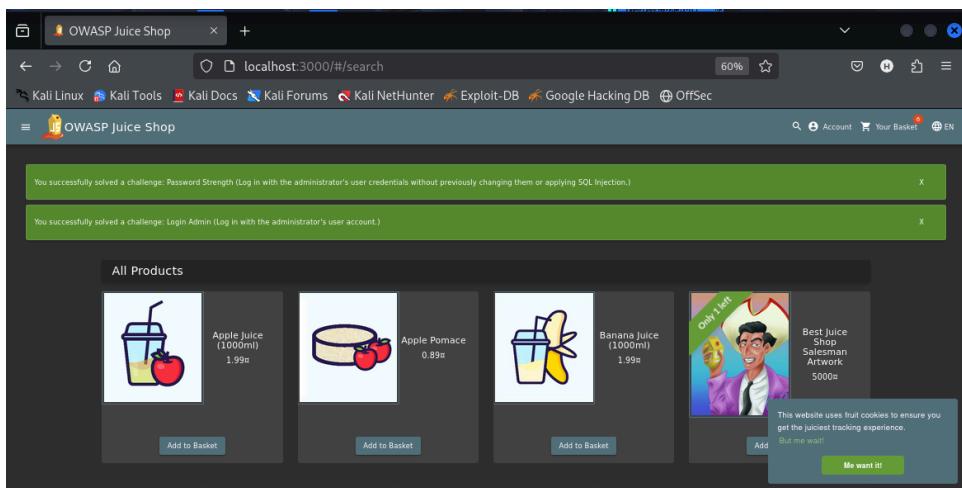


Figure: Admin access using default credentials

- SQLi Login Screenshot
- Feedback Submission Screenshot
- Admin Panel Feedback View Screenshot
- Network Tab (Basket) Screenshot

---

## End of Report