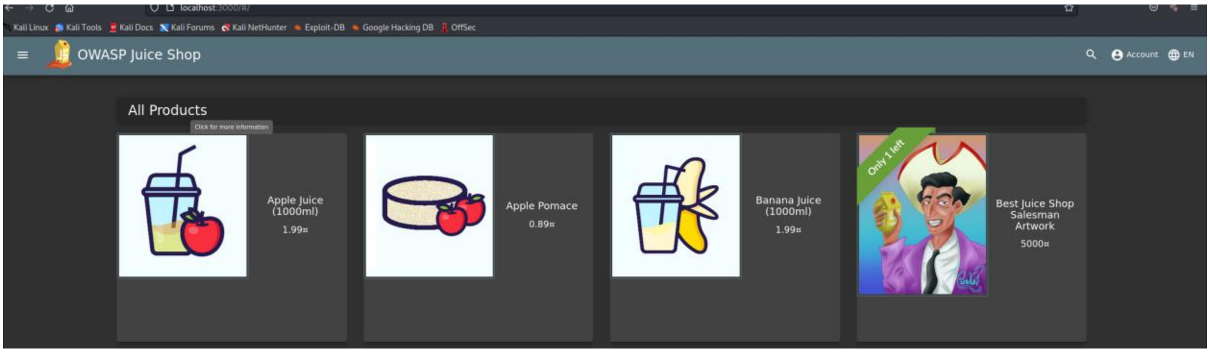
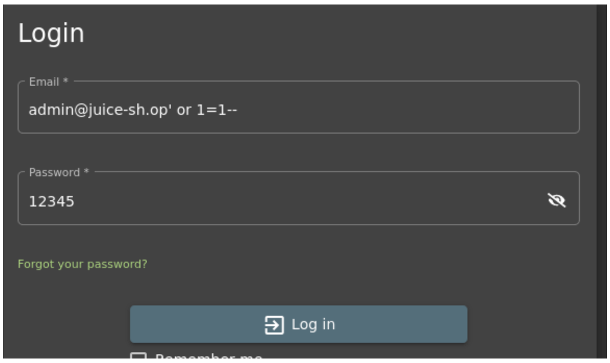
Penetration Testing (OWASP Juice Shop)

Target Site:



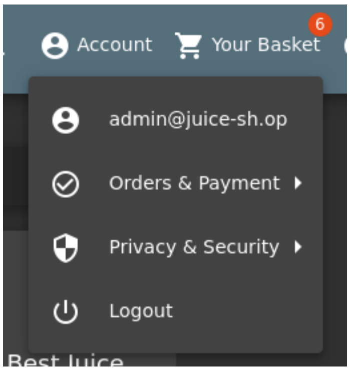
1.SQL Injection



Login

Email *
admin@juice-sh.op' or 1=1--

Password *
12345



Vulnerability: Unauthorized access/compromised the admin account by inserting SQL injection payload in the email field.

Impact: Ability to changre,delete, or add data this means an attacker could manipulate sensitive information within the database,potentially leading to data corruption, fraud, or other malicious activities by accessing admin account.

Solution: SQL injection attacks can be prevented by validating user input, using parameterized queries, and using a web application firewall.

Input validation

- Verify user input: Ensure that user-submitted data is properly inspected and formatted
- Sanitize user input: Remove invalid or unsafe characters and reformat it
- Use an allowlist: Define valid user inputs and reject incoming queries that appear abnormal

- Escape user-supplied input: Treat user-supplied input as input, rather than commands or conditionals.

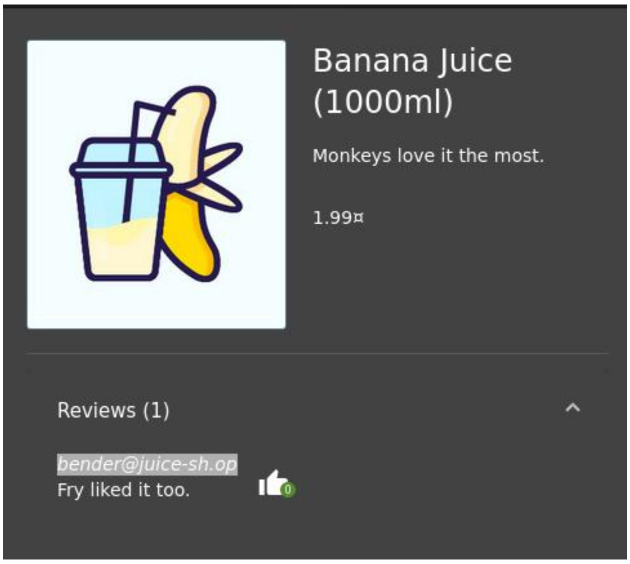
Parameterized queries

- Use prepared statements: Write the SQL command and the user-provided data separately
- Use parameterized stored procedures: Encapsulate SQL logic and use parameterized queries

Web application firewall

- Monitor network traffic at the application level
- Inspect and block incoming requests for potentially malicious signatures
- Filter out malware and suspicious traffic between the internet and a web application.

2. Sensitive Data Exposure



Banana Juice (1000ml)

Monkeys love it the most.

1.99¤

Reviews (1)

bender@juice-sh.op
Fry liked it too.

Vulnerability: This is a product page and its clearly showing email address to everyone.

Impact: Exposed email addresses can lead to a surge in spam, phishing attempts, and potential identity theft, as cybercriminals and spammers can use this information to target individuals and organizations.

He re's a more detailed explanation of the potential impacts:

1. Increased Spam and Unsolicited Emails:

- Exposed email addresses become attractive targets for spammers, who use software programs to gather information from websites, newsgroups, and other online services.
- This can lead to a cluttered inbox and wasted time trying to filter out unwanted emails.

2. Phishing and Identity Theft:

- Cybercriminals can use exposed email addresses to launch phishing attacks, attempting to trick individuals into revealing sensitive information like passwords, credit card details, or social security numbers.
- Phishing emails often mimic legitimate sources, creating a sense of urgency or authority to prompt users to act quickly and forget their usual caution.
- In severe cases, attackers might use your leaked email address to access your accounts, potentially taking control of them.

3. Malware and Cyberattacks:

- Spammers and cybercriminals can use email to spread malware, which can damage systems, steal data, or disrupt network security.
- Email viruses can infiltrate systems by embedding harmful code directly within messages or through deceptive links.

Solution: Show email address to only verified users with certain permissions. Instead of showing email address directly, apply encryption or hide contact information.

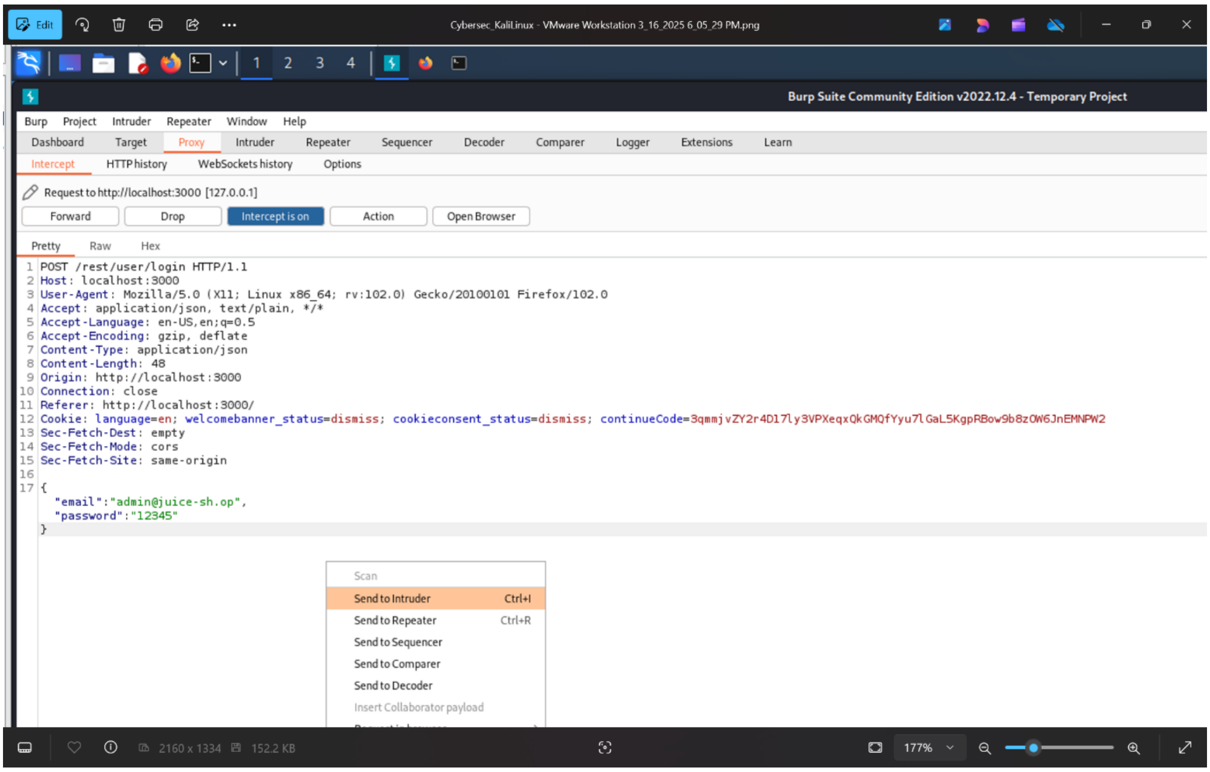
3. Brute Force Attack

In this section **Brute Force Attack** is used to access Administration account with passwords list using **Burpsuite.**

- The attack used **Burp suite's Intruder** module.
- A password list(passwords.txt) using the **SecLists** library was loaded as payload.

- Different passwords must be tried to access the administrator account. An intruder can quickly test a large number of possible passwords(payload)

First, I intercepted the login request using Burp Suite. Instead of forwarding the request directly to the server. I sent it to Intruder to execute a brute-force attack.



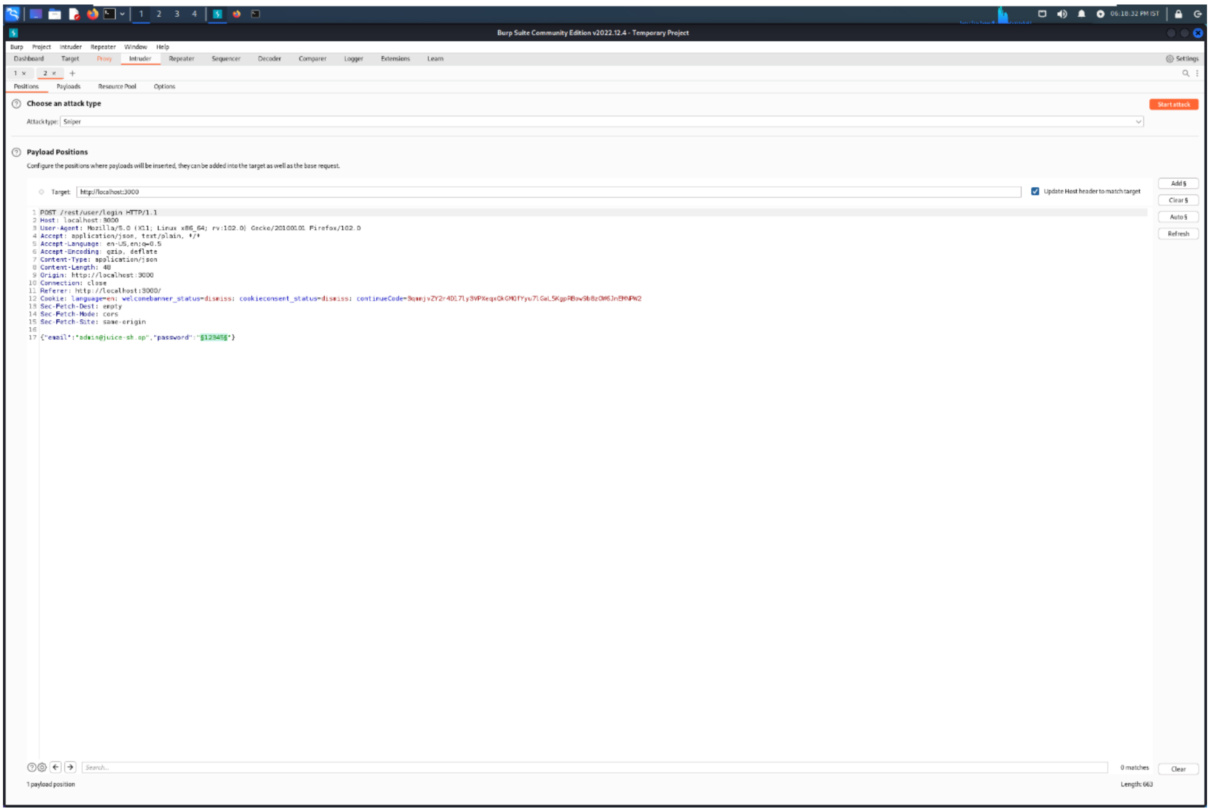
Cybersec_Kali.linux - VMware Workstation 3_16_2025 6_05_29 PM.png
Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Insert Collaborator payload
2160 x 1334 152.2 KB
177%

Request to http://localhost:3000 [127.0.0.1]

```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 48
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=3qmmjvZY2r4D17ly3VPXeqxQkGMQfYyu7lGaL5KgpRBow9b8zOW6JnEMNPW2
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
  "email":"admin@juice-sh.op",
  "password":"12345"
}
```

Now, I navigated this to the Positions tab in Intruder and clicked the Clear § button to remove all predefined attack positions. Then, I placed two § symbols around the password field, marking it as the insertion point for passwords from the passwordslist. This setup guided Burp Suite to replace the marked area with each password during the brute-force attempt.



Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
1 × 2 × +
Positions Payloads Resource Pool Options
Start attack
Add §
Clear §
Auto §
Refresh
Search...
0 matches
Clear

Choose an attack type

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: http://localhost:3000

☑ Update Host header to match target

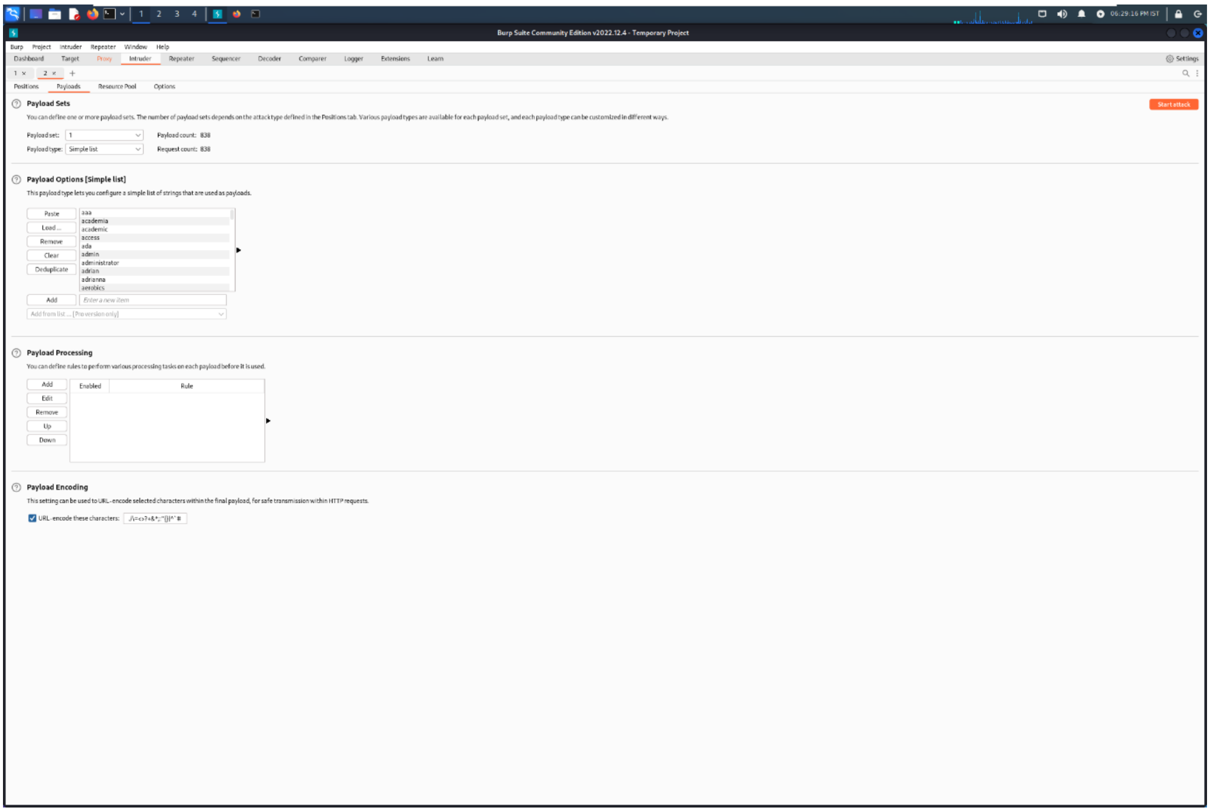
```
POST /rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json
Content-Length: 48
Origin: http://localhost:3000
Connection: close
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=3qmmjvZY2r4D17ly3VPXeqxQkGMQfYyu7lGaL5KgpRBow9b8zOW6JnEMNPW2
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{"email":"admin@juice-sh.op","password":"§12345§"}
```

1 payload position

Length: 663

Attack was activated after mentioned list(passwords.txt) was loaded, then click start attack.



Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Settings
1 × 2 × +
Positions Payloads Resource Pool Options
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1
Payload count: 838
Payload type: Simple list
Request count: 838

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

aaa
academia
academic
access
ada
admin
administrator
adrian
adrianna
aerobics

Enter a new item

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

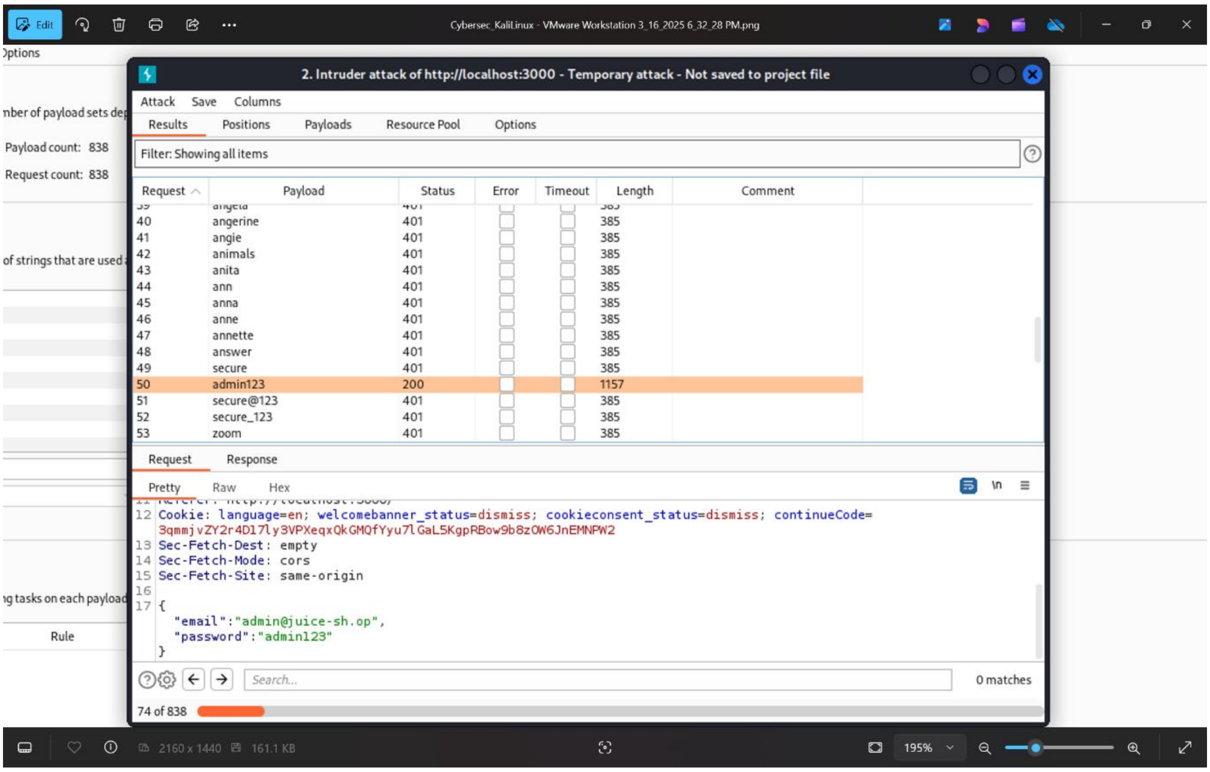
Enabled	Rule

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☑ URL-encode these characters: ./\=<>?+&*;:"{}|^`#

When “200” or noticeable differences are found between the responses, this is an indication of a successful attack. The “400” status code means invalid password. The final successful result was achieved.



Edit
Cybersec_Kali.linux - VMware Workstation 3_16_2025 6_32_28 PM.png
Options
Rule
Attack Save Columns
Results Positions Payloads Resource Pool Options
Request Response
Pretty Raw Hex
Search...
0 matches
2160 x 1440
161.1 KB
195%

2. Intruder attack of http://localhost:3000 - Temporary attack - Not saved to project file

nber of payload sets dep

Payload count: 838

Request count: 838

of strings that are used

ng tasks on each payload

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
39	angela	401	□	□	385	
40	angerine	401	□	□	385	
41	angie	401	□	□	385	
42	animals	401	□	□	385	
43	anita	401	□	□	385	
44	ann	401	□	□	385	
45	anna	401	□	□	385	
46	anne	401	□	□	385	
47	annette	401	□	□	385	
48	answer	401	□	□	385	
49	secure	401	□	□	385	
50	admin123	200	□	□	1157	
51	secure@123	401	□	□	385	
52	secure_123	401	□	□	385	
53	zoom	401	□	□	385	

```
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
3qmmjvZY2r4D17ly3VPXeqxQkGMQfYyu7lGaL5KgpRBow9b8zOW6JnEMNPW2
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{
  "email":"admin@juice-sh.op",
  "password":"admin123"
}
```

74 of 838

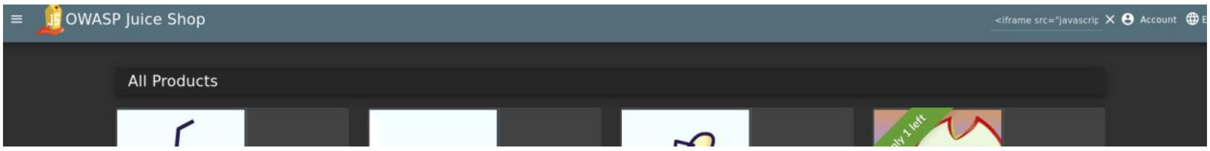
Vulnerability: It allows attackers to gain access to user accounts due to the system's weak login authentication mechanisms. The attacker can test hundreds or thousands of possible passwords.

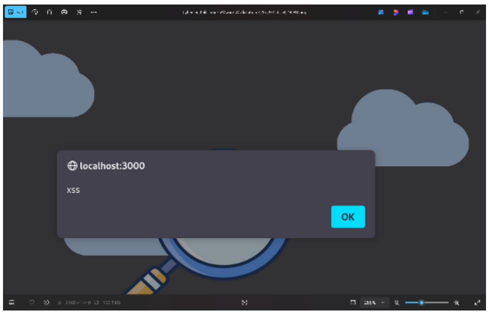
Impact: Attackers can gain access to the admin or other user account, which can lead to the theft of sensitive information and the seizure of system administration rights.

Solution: Limit the number of login attempts. Allow only a limited number of login attempts from the same IP address or user account within a certain time frame. Temporarily lock the account after 3-5 failed attempts. Use strong encryption algorithms, such as **Bcrypt, PBKDF2,** or **Argon2.**

4. XSS

The attacker injects malicious JavaScript code (<iframe src="javascript:alert('xss')">)can steal user data or modify the logic of the application by executing. In this task, the "Search Bar" field is vulnerable to a DOM XSS vulnerability. The attacker was able to trigger a JavaScript "alert" message by inserting the following malicious code.





Vulnerability: The search bar inserts user input directly into the DOM, which allows malicious JavaScript code to be executed.

Impact: The attacker can steal the user's session information, cookies, or sensitive data. The attacker can redirect the user to fake pages.

Solution: Validate all user input and only accept data that is in a secure format. Do not, accept special characters. Ensure that characters such as <, >, ", ', & are converted to HTML entities.