**1. Installation steps**

**1.** Opened Visual Studio Code and terminal.  
**2.** Ran the command:  
git clone https://github.com/juice-shop/juice-shop.git  
**3.** Installed dependencies using:  
npm install  
**4.** Started the server using:  
npm start  
**5.** Opened browser and accessed: http://localhost:3000  
**6.** Verified the application is running successfully.

*(Add 2–3 screenshots here: terminal, running site, DevTools window.)*

**2. Attack Surface Table**

| **Code** | **Attack Surface** | **Description** | **URL / Element** |
| --- | --- | --- | --- |
| AS-01 | Login Form | Email/password input fields | /#/login |
| AS-02 | Search Bar | Input field for product search | /#/search |
| AS-03 | Feedback Form | Sends user data via POST request | /#/contact |
| AS-04 | Basket API | Manages user cart operations | /rest/basket |
| AS-05 | Product API | Returns product list in JSON | /rest/products |

**3. Threat Analysis Table**

| **Code** | **Potential Threat** | **STRIDE Category** | **CIA Impact** | **Description** |
| --- | --- | --- | --- | --- |
| AS-01 | SQL Injection | Injection | Confidentiality | Attackers can bypass login validation |
| AS-02 | XSS | Tampering | Integrity | Malicious JS can execute in browser |
| AS-03 | Spam / Phishing | Social Engineering | Availability | Misuse of feedback form |
| AS-04 | API Data Exposure | Information Disclosure | Confidentiality | Unauthorized data access |
| AS-05 | Price Manipulation | Elevation of Privilege | Integrity | Change product prices in cart |

Screenshots:Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

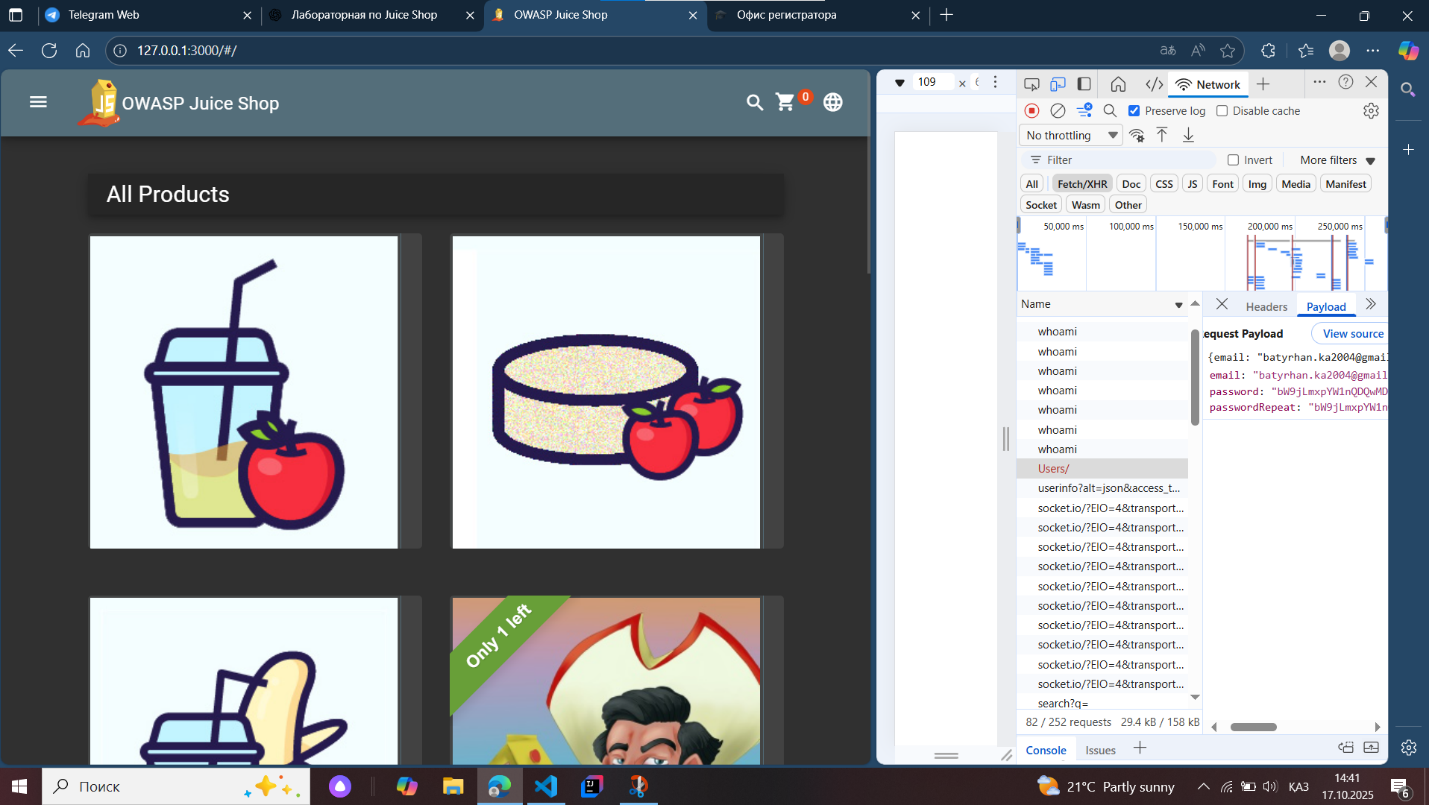
Содержимое, созданное искусственным интеллектом, может быть неверным.

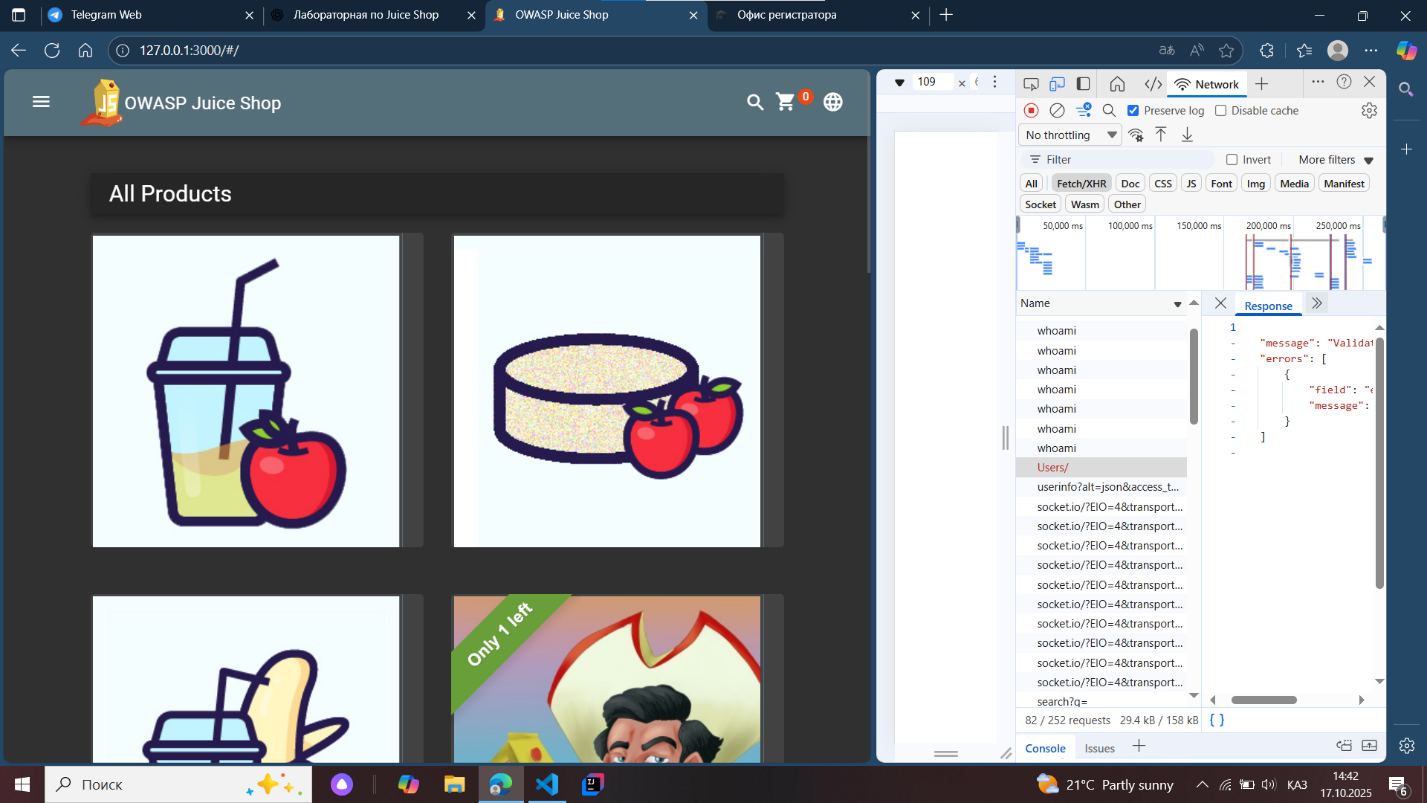
Изображение выглядит как текст, Мультимедийное программное обеспечение, программное обеспечение, Значок на компьютере

Содержимое, созданное искусственным интеллектом, может быть неверным.Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.Изображение выглядит как текст, программное обеспечение, снимок экрана, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Содержимое, созданное искусственным интеллектом, может быть неверным.Изображение выглядит как текст, снимок экрана, программное обеспечение, компьютер

Содержимое, созданное искусственным интеллектом, может быть неверным.

**4. Conclusion**

During the analysis of OWASP Juice Shop, several common attack surfaces were found such as input forms, APIs, and URLs.  
By using browser DevTools, these potential threats were identified, including injection, XSS, and privilege escalation.  
This demonstrates how developers should properly validate inputs and secure API endpoints.