

## OUR TEAM

OMAR ATEF MAHMOUD	2305099
-------------------	---------

OSAMA MAHMOUD MOHAMED	2305572
-----------------------	---------

HOPE YOU LIKE IT

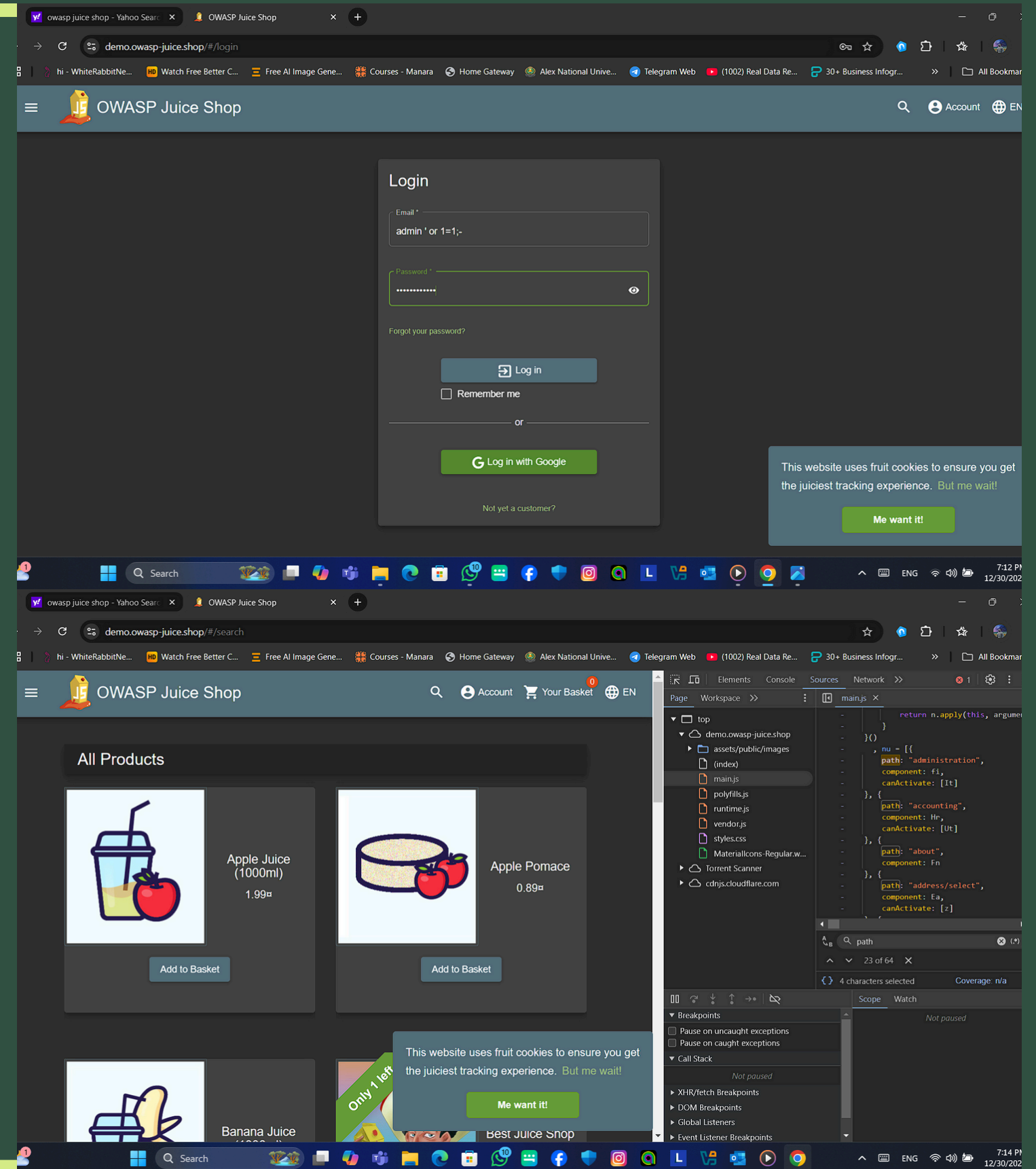
# SQL INJECTION

1– used user input field to insert malicious SQL payload "admin' or 1=1;-"

2– became able to Gain an administrative privileges  
“Authentication Bypass”

3– Unauthorized access to sensitive information

4– gained access to the admin website.



The screenshot shows a web browser with the address bar displaying `demo.owasp-juice.shop/#/administration`. The browser tabs include "hi - WhiteRabbitNe...", "Watch Free Better C...", "Free AI Image Gene...", "Courses - Manara", "Home Gateway", "Alex National Unive...", "Telegram Web", "(1002) Real Data Re...", "30+ Business Infor...", and "All Bookmarks".

The web application displays an "Administration" page with two main sections: "Registered Users" and "Customer Feedback".

**Registered Users:**

Email	Avatar	Feedback	Stars	Actions
admin@juice-sh.op		1 I love this shop! Best products in town! Highly recommende...	★★★★	
jim@juice-sh.op		2 Great shop! Awesome service! (**@juice-sh.op)	★★★★	
bender@juice-sh.op		3 Nothing useful available here! (**der@juice-sh.op)	★	
bjoern.kimminich@g mail.com		21 Please send me the juicy chat-bot NFT in my wallet at /juic...	★	
ciso@juice-sh.op		Incompetent customer support! Can't even upload phot...	★★★★	
support@juice-sh.op		This is the store for awesome stuff of all kinds! (anonymous)	★★★★	
morty@juice-sh.op		Never gonna buy anywhere else from now on! Thanks fo...	★★★★	
mc.safesearch@juic e-sh.op		Keep up the good work! (anonymous)	★★★★	
J12934@juice-sh.op		this is a test comment	★★★★	

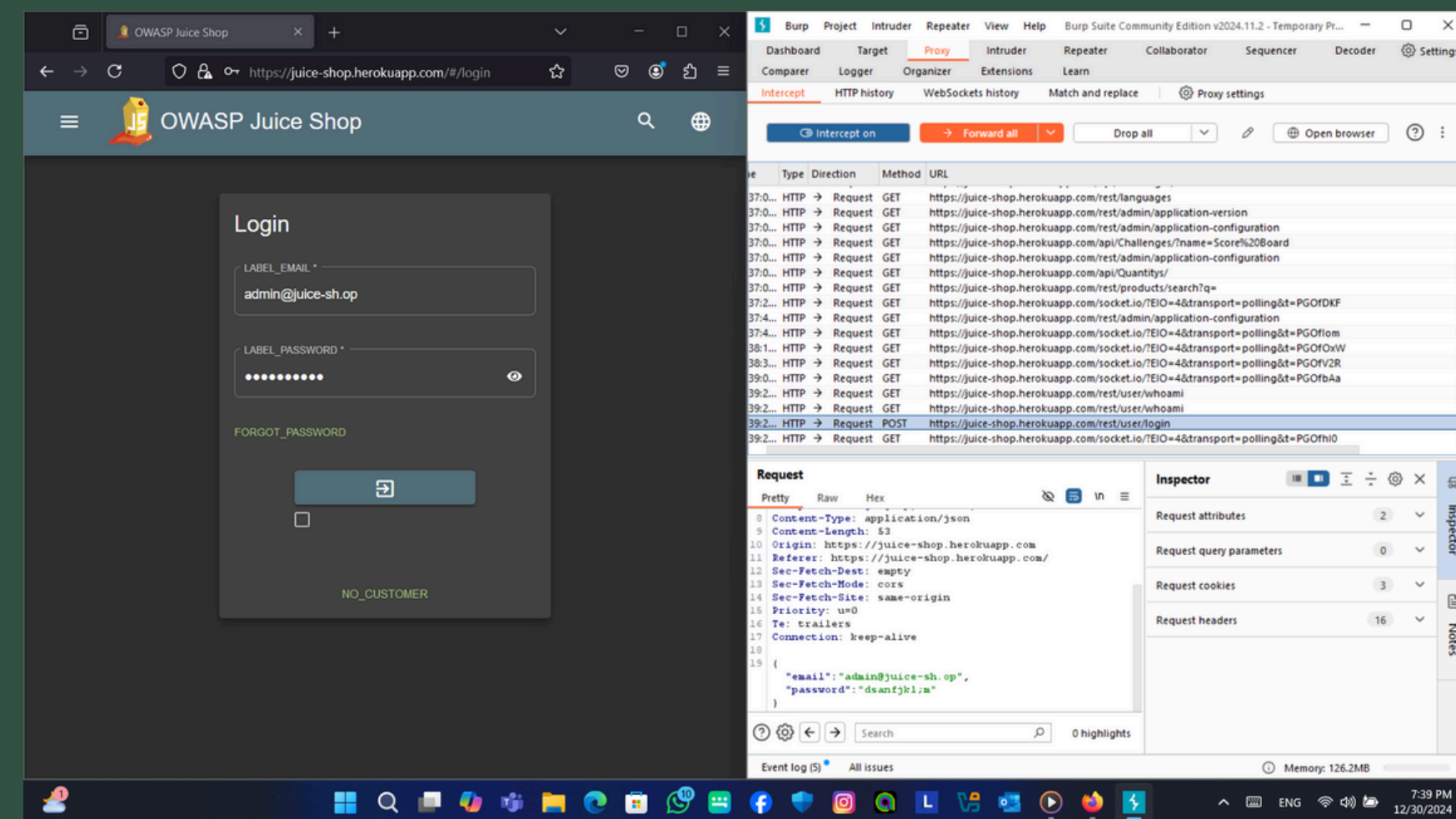
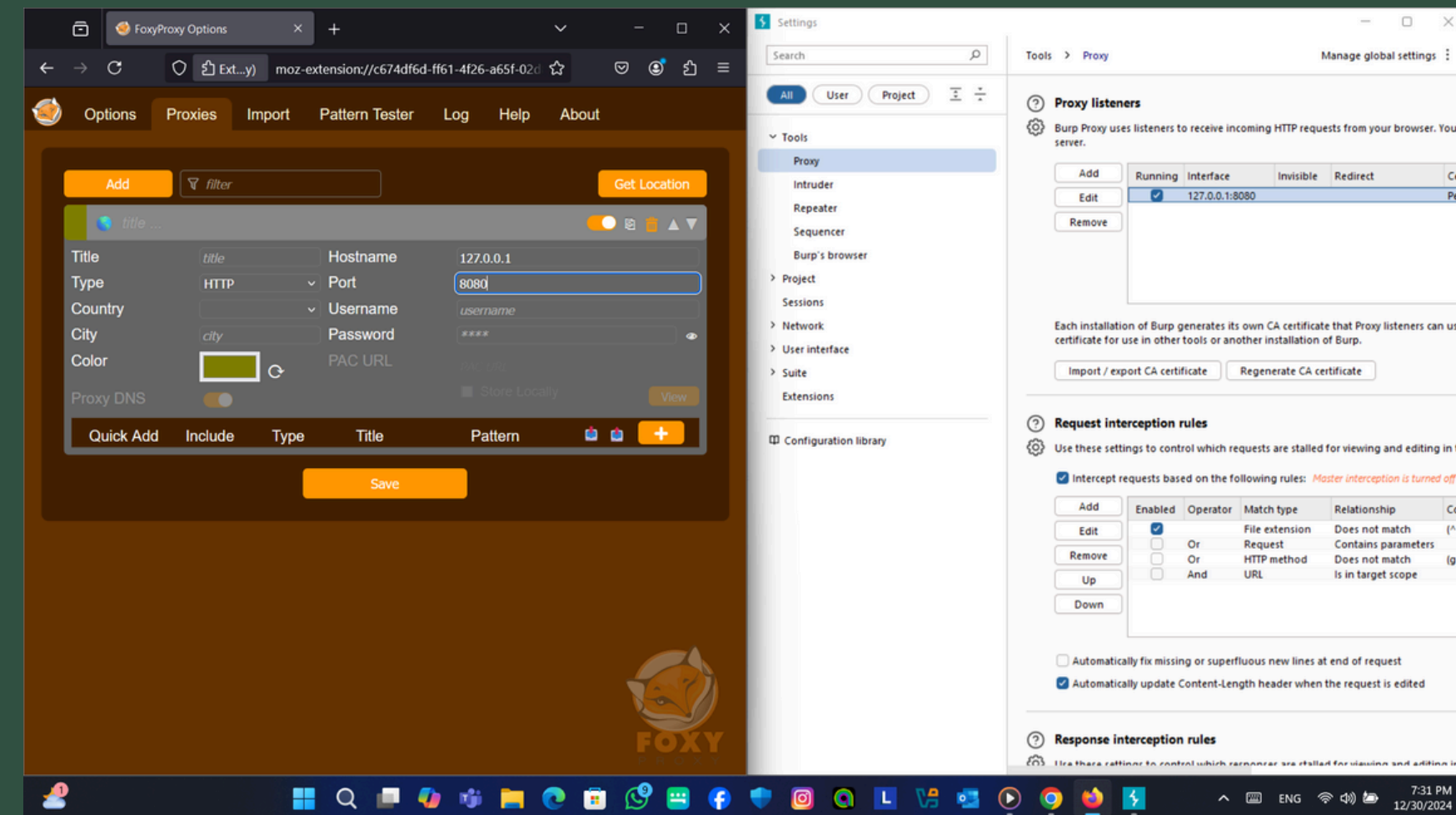
**Customer Feedback:**

The "Customer Feedback" section is currently empty.

The browser's developer tools are open, showing the "Sources" panel. The file tree on the left lists the application's assets, including `demo.owasp-juice.shop/assets/public/images/index`, `main.js`, `polyfills.js`, `runtime.js`, `vendor.js`, `styles.css`, `MaterialIcons-Regular.w...`, `Torrent Scanner`, and `cdnjs.cloudflare.com`. The right pane shows the JavaScript code for `main.js`, which includes a `return n.apply(this, arguments)` statement. The "Scope" and "Watch" panels are also visible at the bottom.

# BRUTE FORCE ON ADMIN CREDENTIALS

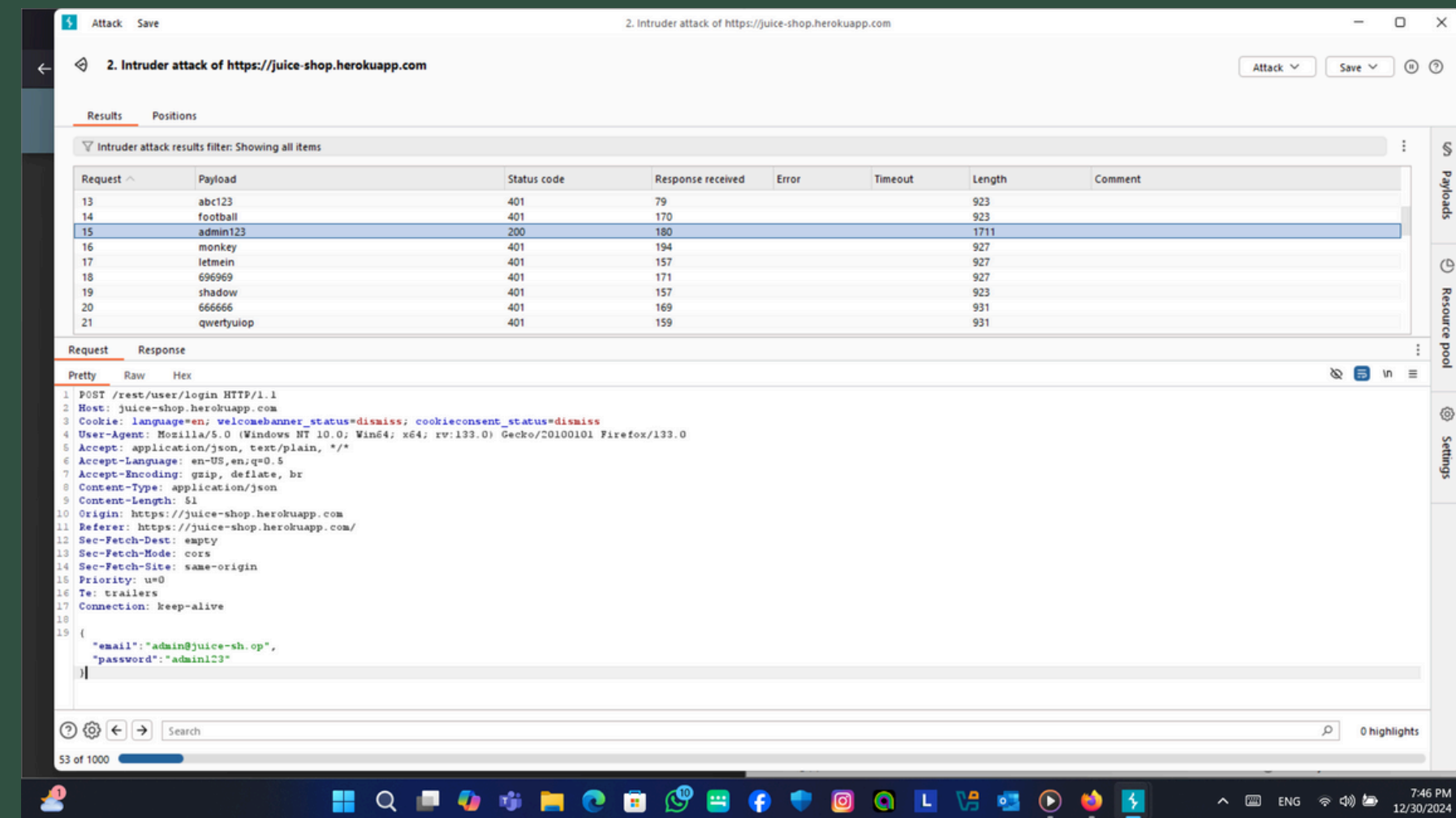
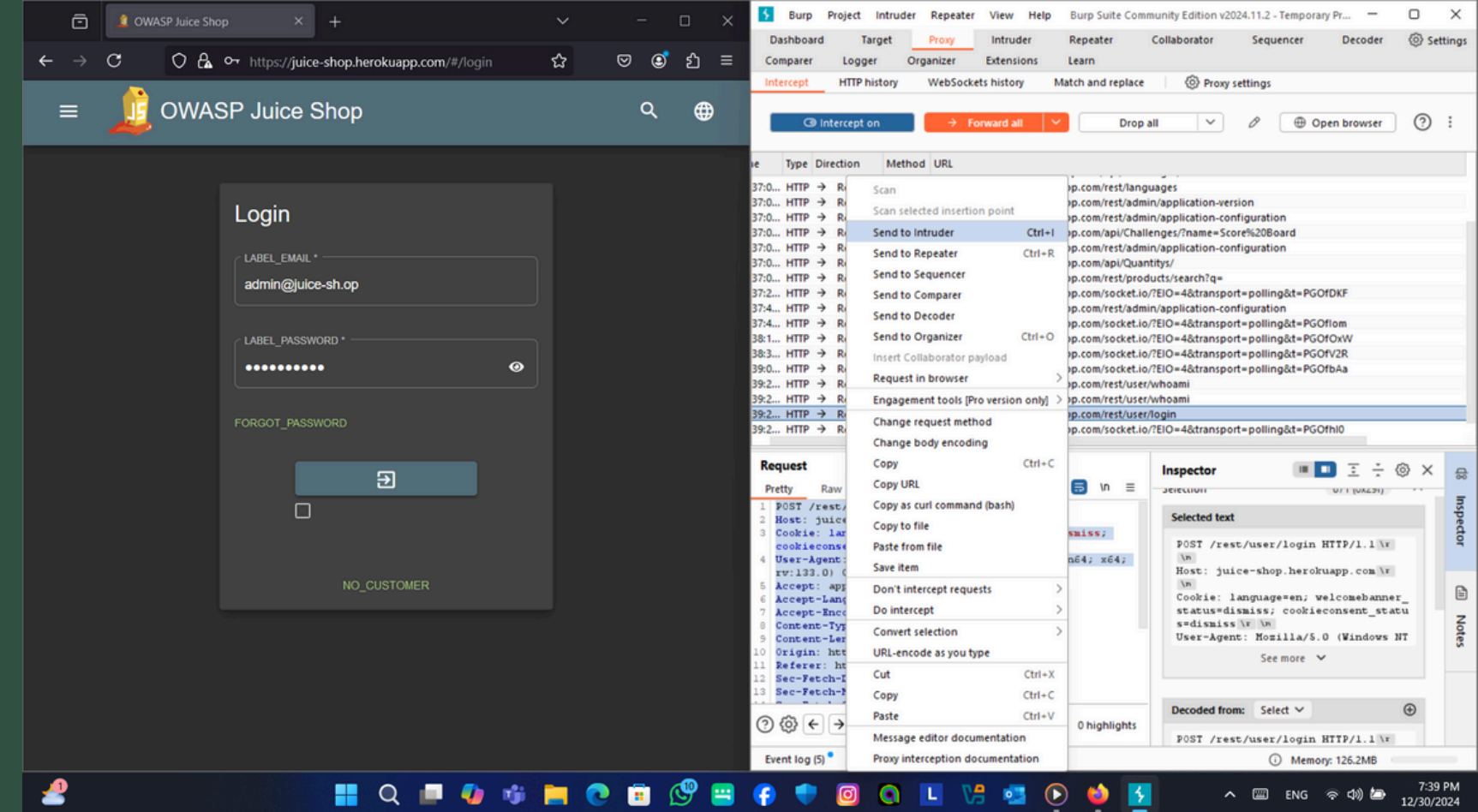
1. sets up a proxy on Firefox using the FoxyProxy extension.
2. They intercept a login request using Burp Suite.
3. The POST request containing the login credentials is sent to Hydra, a password-cracking tool.





# BRUTE FORCE ON ADMIN CREDENTIALS

1. Hydra uses a wordlist to guess the correct password for the admin account.
2. Once the password is found, the attacker logs in as the admin.



# FINALLY HOW TO DEFENCE AGAINST THESE ATTACKS

Validate All User Inputs: Always check and sanitize anything users type into forms, search bars, or URLs.

Use Prepared Statements: Prevent SQL injection by using prepared or parameterized queries instead of directly inserting user input into database commands.

Escape Output and Sanitize Content: For XSS, encode user-provided content before displaying it to prevent harmful scripts from running.

Add CAPTCHA and Rate Limits: Use these on login forms to prevent automated attacks like Hydra.

Implement HTTPS Everywhere: Encrypt all data exchanges between users and the website to prevent interception by tools like Burp Suite.

Monitor and Block Malicious Activity: Regularly review logs, detect suspicious patterns, and block problematic IPs.

Enforce Strong Password Policies: Require complex passwords, use account lockouts, and encourage users to update their passwords regularly.

Secure Your APIs: Protect APIs with authentication and authorization mechanisms to prevent unauthorized access.

Install Security Tools: Use Web Application Firewalls (WAFs) and regular vulnerability scanning tools to keep your website safe.

Educate Developers and Users: Ensure developers know secure coding practices and teach users about strong passwords and phishing awareness.