NA Security

2025/05/19 Lab13
Wireless 謝政洋

Outline

- Introduction
- Lab
- Submission

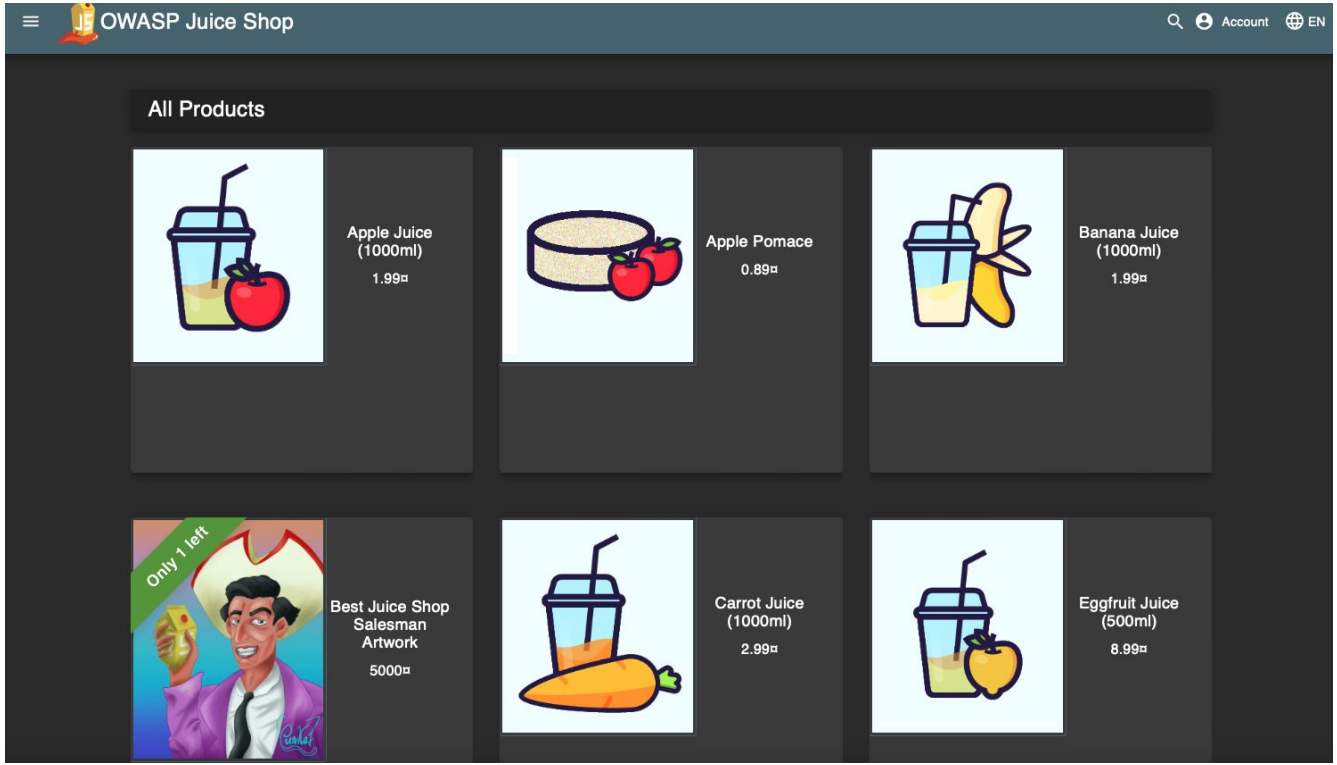
OWASP

The Open Web Application Security Project, or OWASP, is an international non-profit organization dedicated to web application security. The OWASP Top 10 is a regularly updated report outlining security concerns for web application security, focusing on the 10 most critical risks.

2024 OWASP TOP 10

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF)

OWASP JUICE SHOP



Setup

1. Docker

   $ docker pull bkimminich/juice-shop

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

2. node.js

   https://github.com/juice-shop/juice-shop

Difficulty

Difficulty	Number of Challenges
⭐ (1 star)	12
⭐⭐ (2 stars)	22
⭐⭐⭐ (3 stars)	24
⭐⭐⭐⭐ (4 stars)	24
⭐⭐⭐⭐⭐ (5 stars)	12
⭐⭐⭐⭐⭐⭐ (6 stars)	15
Total	**109**

Sql

- Structured Query Language
- Managing data stored in relational database management systems
- Example:

```
SELECT * FROM customers WHERE country = 'USA';
```

SQL Injection

1. Authorization Bypass

SELECT * FROM users WHERE username =' -name- ' AND password = ' -password-'

admin' OR 1=1 --

"SELECT * FROM customers WHERE name ='admin' OR 1=1 -- 'AND password = ' -password-'

SQL Injection

2. Injecting SQL Sub-Statements into SQL Queries

SELECT * FROM users WHERE username =' -name- ' AND password = ' -password-'

' ; DROP TABLE users; --

SELECT * FROM customers WHERE name ='' ; DROP TABLE users; -- AND password = ' -password-'

SQL Injection

3. Exploiting Stored Procedures:

SELECT * FROM users WHERE username =' -name- ' AND password = ' -password-'

'; EXEC xp_cmdshell('net user attacker password /add'); --

SELECT * FROM customers WHERE name ='; EXEC xp_cmdshell('net user attacker password /add'); --
AND password = ' -password-'

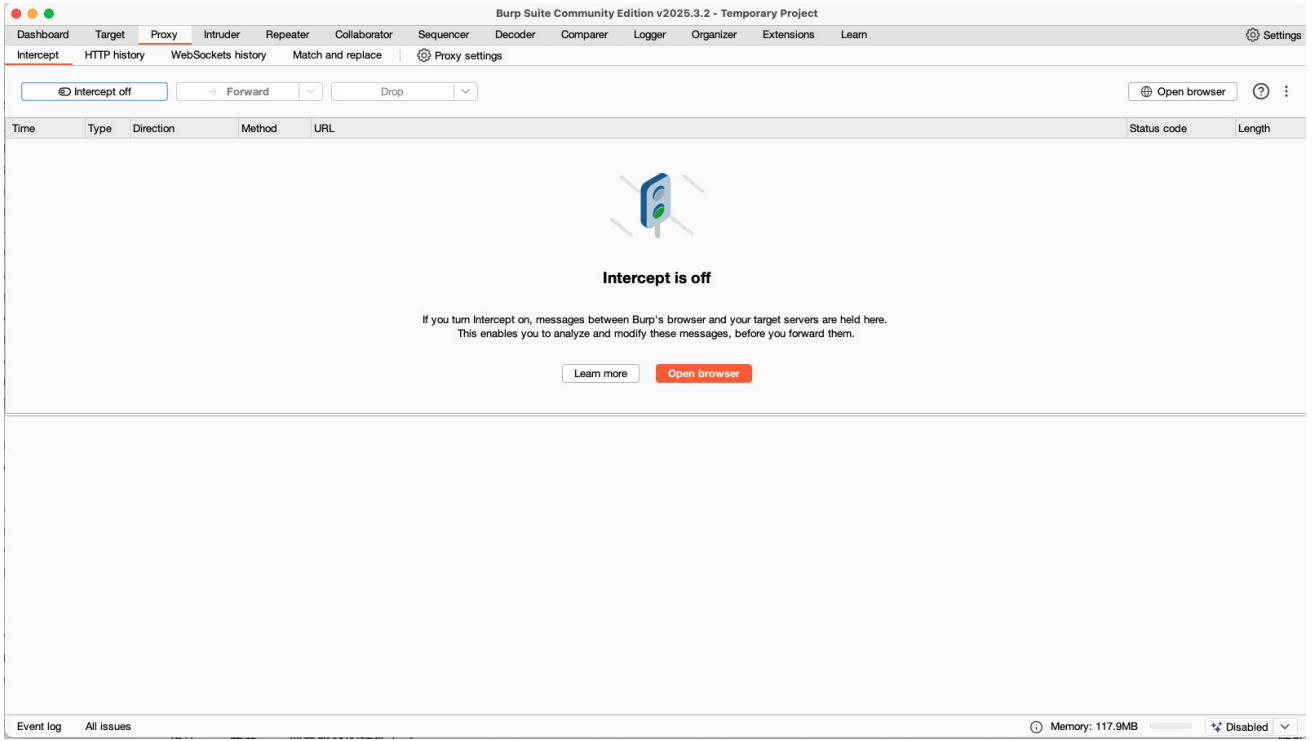
Burp Suite

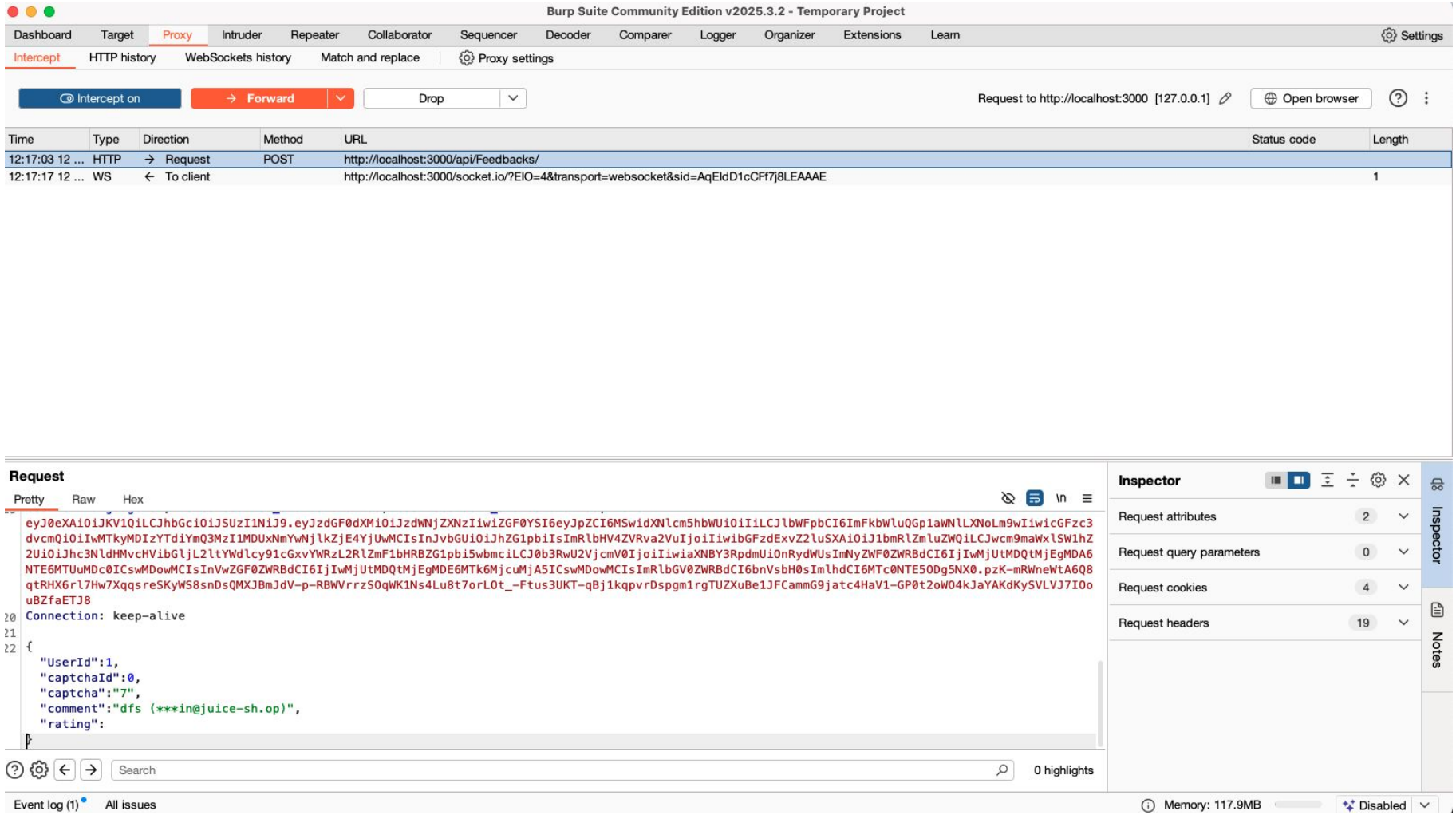
https://portswigger.net/burp/releases/professional-community-2025-3-2?requestededition=community&requestedplatform=

Burp是一款專門設計於做Web安全測試的工具，主要就是針對HTTP/HTTPS協定的通訊進行測試。

- Proxy: 使Burp作為Web proxy運行，並且位於瀏覽器和目標 Web server之間。
- Scanner: 執行 Web 應用程式的自動漏洞掃描。
- Intruder: 可以利用Intruder進行暴力破解或是FUZZING攻擊。
- Spider: 網站爬蟲，協助建立SiteMap。
- Repeater: 來手動測試HTTP Request的簡單功能，可以修改Request內容的請求，重新發送並觀察結果。
- Decoder: 將數據進行編碼/解碼工具。
- Comparer: 在任意兩個Requset/Response之間進行比較的工具。
- Extender: 使用安全測試人員自己的或第三方的（BAppStore）擴展功能
- Sequencer: 分析數據隨機性的工具。它可以用於測試應用程式的token或其他重要的數據。

Burp Suite Demo




Burp Suite Community Edition v2025.3.2 - Temporary Project
Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Organizer
Extensions
Learn
Settings
Intercept
HTTP history
WebSockets history
Match and replace
Proxy settings
Intercept on
Forward
Drop
Request to http://localhost:3000 [127.0.0.1]
Open browser
Time
Type
Direction
Method
URL
Status code
Length
12:17:03 12 ...
HTTP
Request
POST
http://localhost:3000/api/Feedbacks/
12:17:17 12 ...
WS
To client
http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=AqEldD1cCFf7j8LEAAAE
1
Request
Pretty
Raw
Hex
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiJ1bmRlZmluZWQiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjUtMDQtMjEgMDA6NTE6MTUuMDc0ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjUtMDQtMjEgMDE6MTk6MjcuMjA5ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTc0NTE5ODg5NX0.pzK-mRWneWtA6Q8qtRHX6rl7Hw7XqqsreSKyWS8snDsQMXJBmJdV-p-RBWVrrzSOqWK1Ns4Lu8t7orLOt_-Ftus3UKT-qBj1kqpvrDspgm1rgTUZXuBe1JFCammG9jatc4HaV1-GP0t2oWO4kJaYAKdKySVLVJ7IOouBZfaETJ8
Connection: keep-alive
{
"UserId":1,
"captchaId":0,
"captcha":"7",
"comment":"dfs (***in@juice-sh.op)",
"rating":
Search
0 highlights
Inspector
Request attributes
2
Request query parameters
0
Request cookies
4
Request headers
19
Inspector
Notes
Event log (1)
All issues
Memory: 117.9MB
Disabled

Submission

- 請將 lab 結果寫成 report 並以 pdf 格式上傳至 NTU Cool 作業區，report 內容須包含
  - 你寫哪些題目
  - 解題過程
  - 截圖score-board
- 題目數量：總計25顆星（black list除外）
- 檔案名稱格式：{student id}_lab13.pdf，e.g. *b13902999_lab13.pdf*
- Deadline: 2025/05/25 21:59
- 如果有遇到任何問題，請寄信到 vegetable@csie.ntu.edu.tw
  - 請在主旨前加上 [Lab13]

Blacklist

1. DOM XSS
2. Confidential Document
3. Login MC SafeSearch
4. Five-Star FeedBack
5. View Basket
6. Password Strength
7. Meta Geo Stalking
8. Missing Encoding
9. Repetitive Registration
10. Exposed Credentials
11. Zero Stars
12. Login Admin