Exploring OWASP Juice Shop with OWASP ZAP

And a quick introduction to OWASP DefectDojo

April 26, 2021

Agenda

- Introduction
- Exercise 0: Setting up OWASP Juice Shop
- Exercise 1: Proxying with OWASP ZAP
- Exercise 2: Exploring OWASP Juice Shop and capturing traffic
- Exercise 3: Sites and Context
- Exercise 4: Break and Request Editor
- Exercise 5: SQL injection
- Exercise 6: Parameter manipulation
- Exercise 7: Scoreboard
- Exercise 8: Active Scan
- Exercise 9: Export results
- Exercise 10: DefectDojo

Introduction

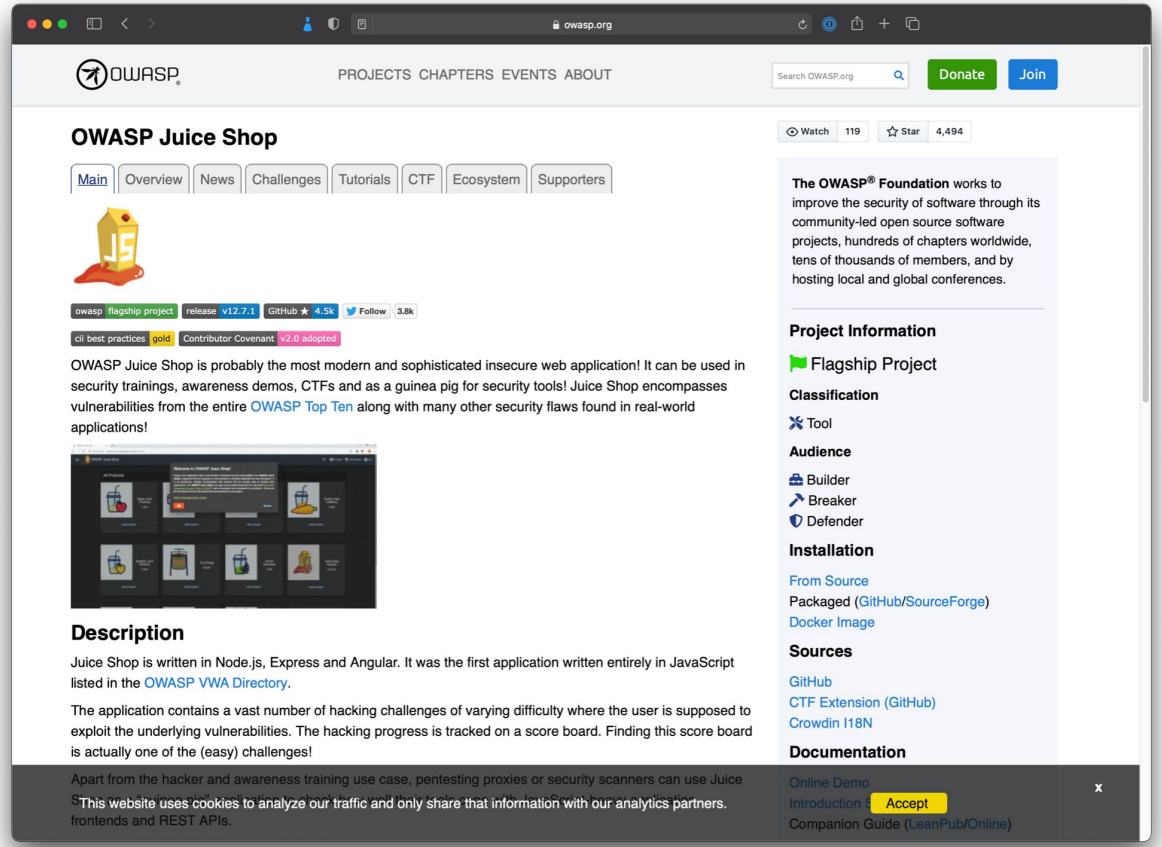
1. Our objective is to introduce you to learning AppSec testing through OWASP Juice Shop, a purposefully insecure web application, and OWASP ZAP.

2. This is an extension of Jack Ender's talk in January 2021 where he introduced OWASP ZAP.

3. This is not meant to be a session on the OWASP Top 10, application vulnerabilities, or a full class on web application penetration testing.

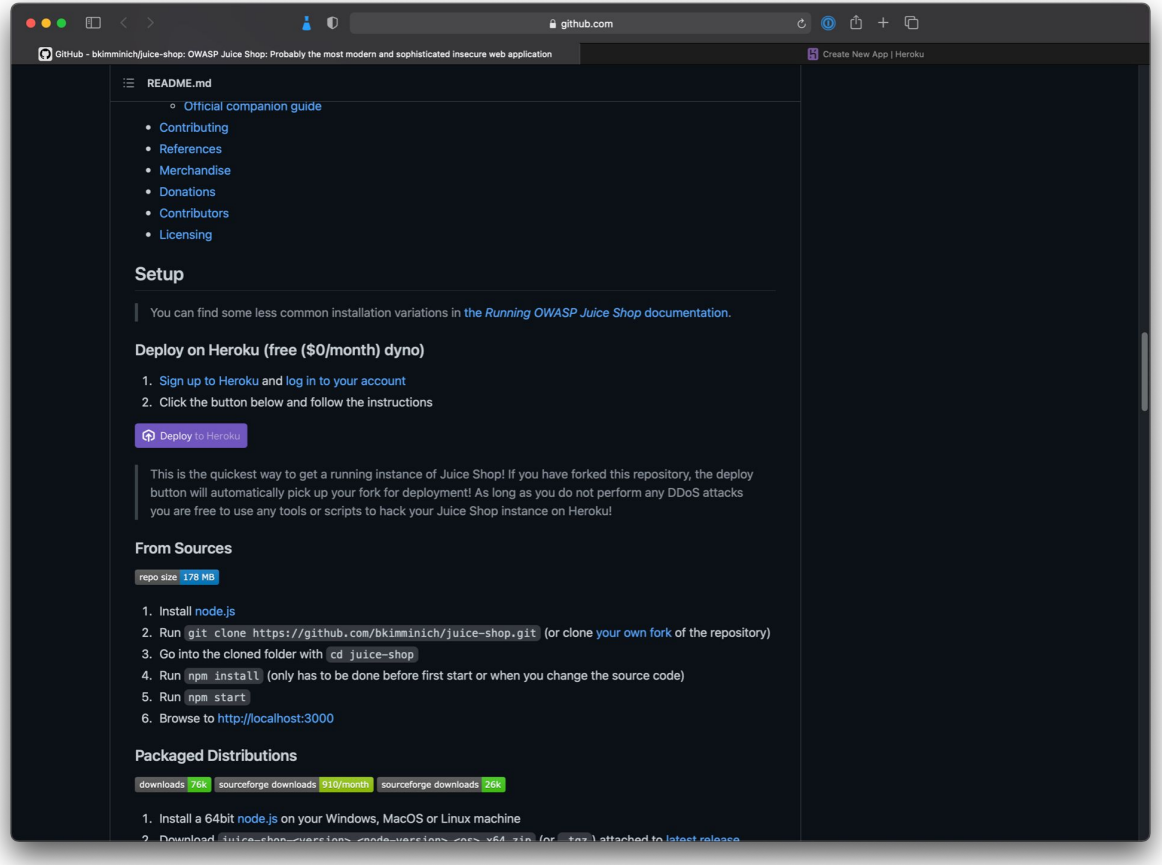
Exercise 0: Setting up OWASP Juice Shop

Exercise 0: Visiting the project main page



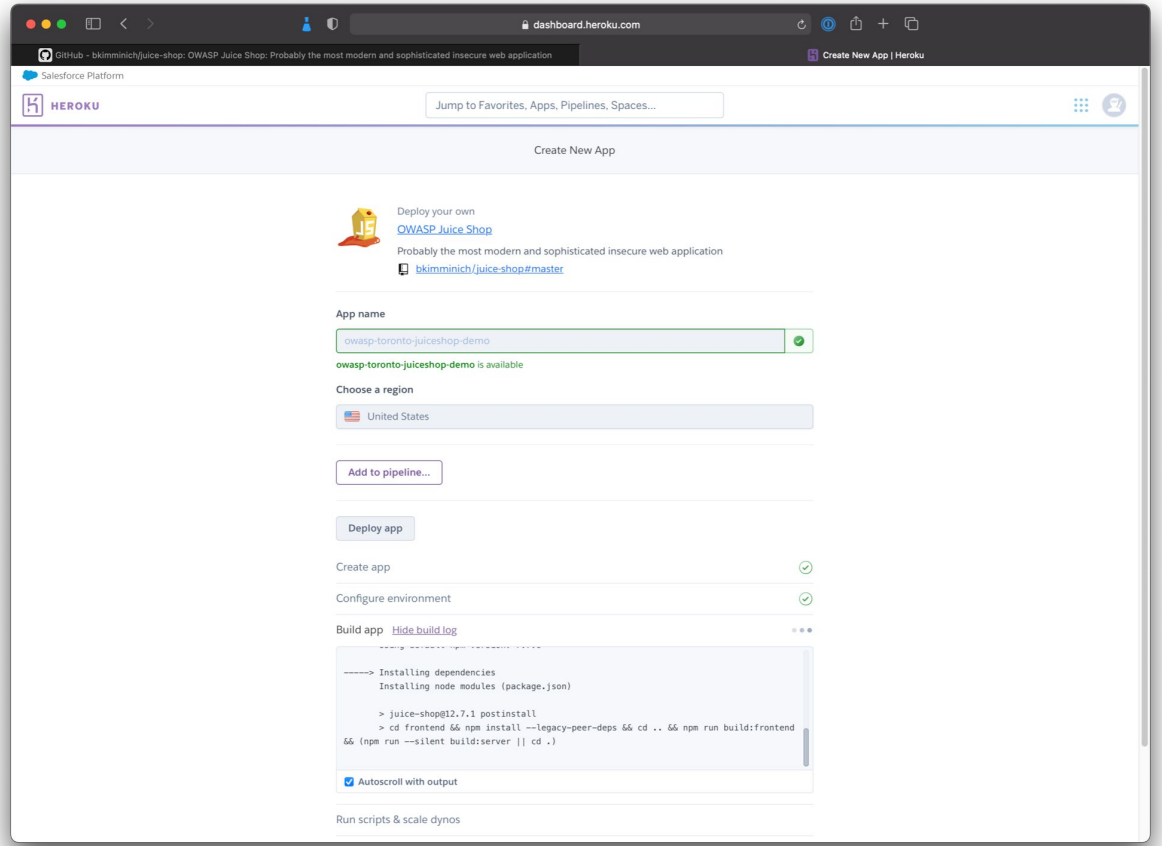
https://owasp.org/www-project-juice-shop/

Exercise 0: Visiting Github & deployment options

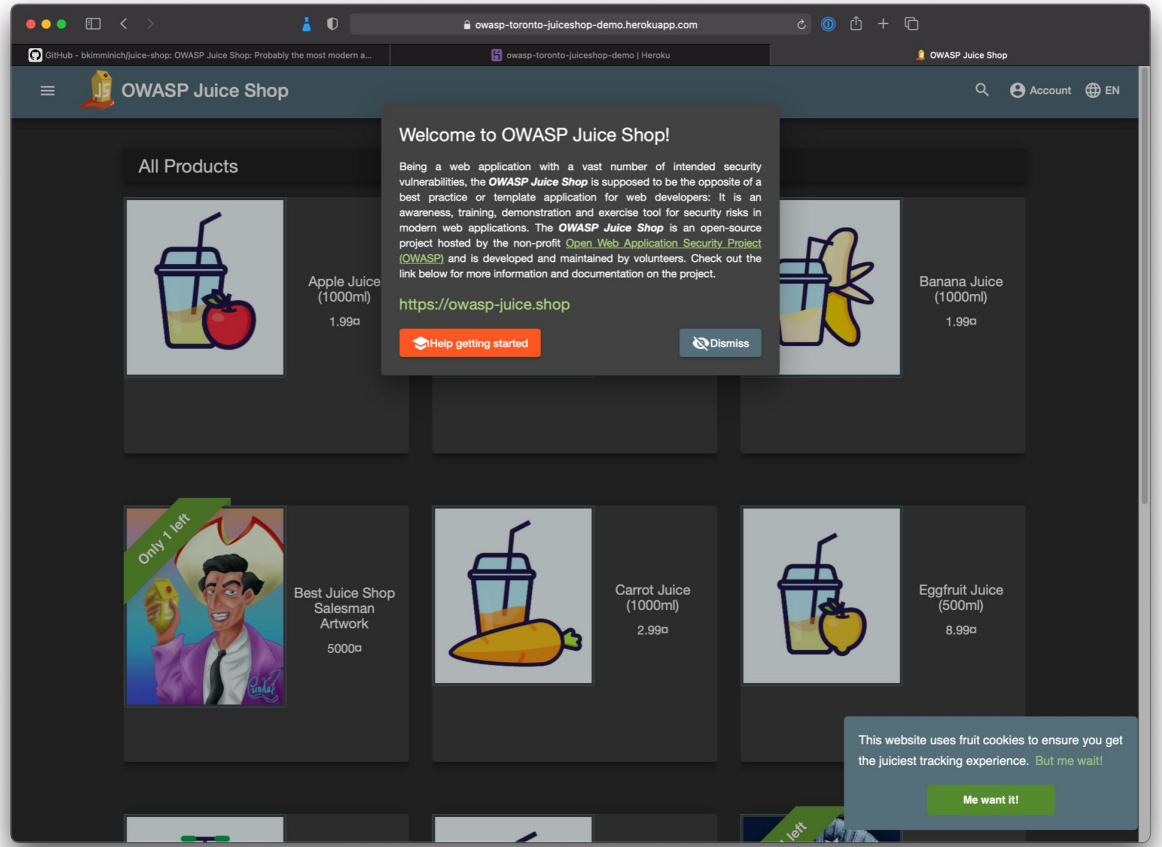


https://github.com/bkimminich/juice-shop

Exercise 0: Deploying to Heroku

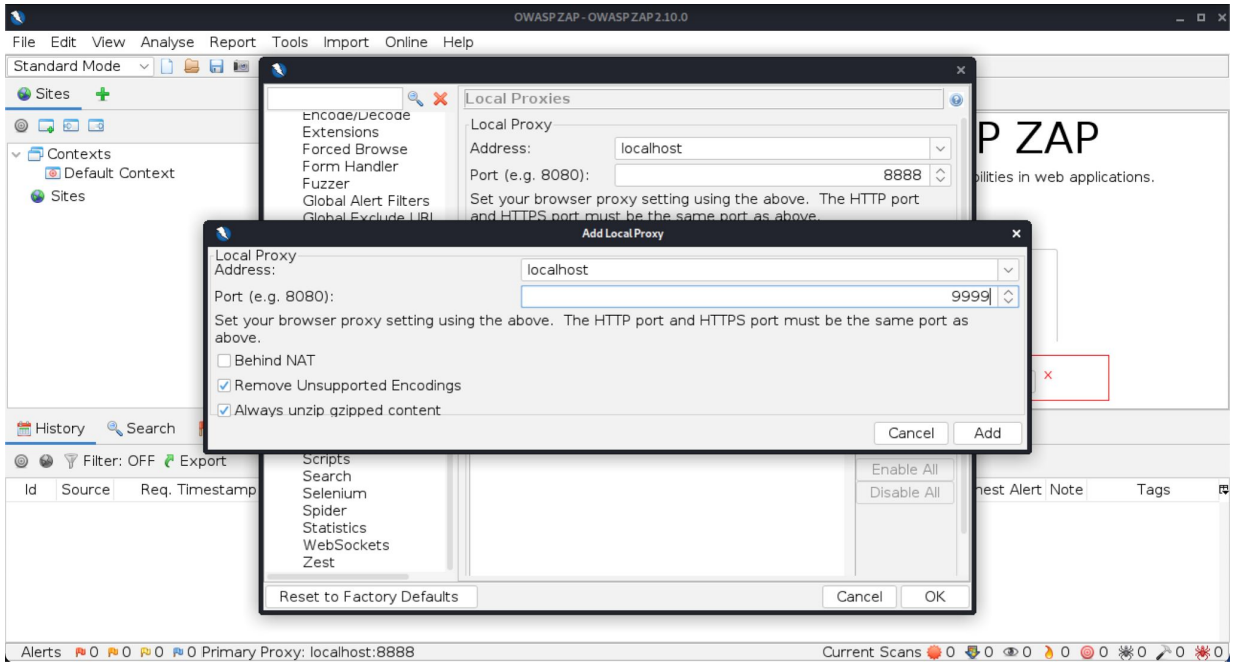


Exercise 0: App deployed!

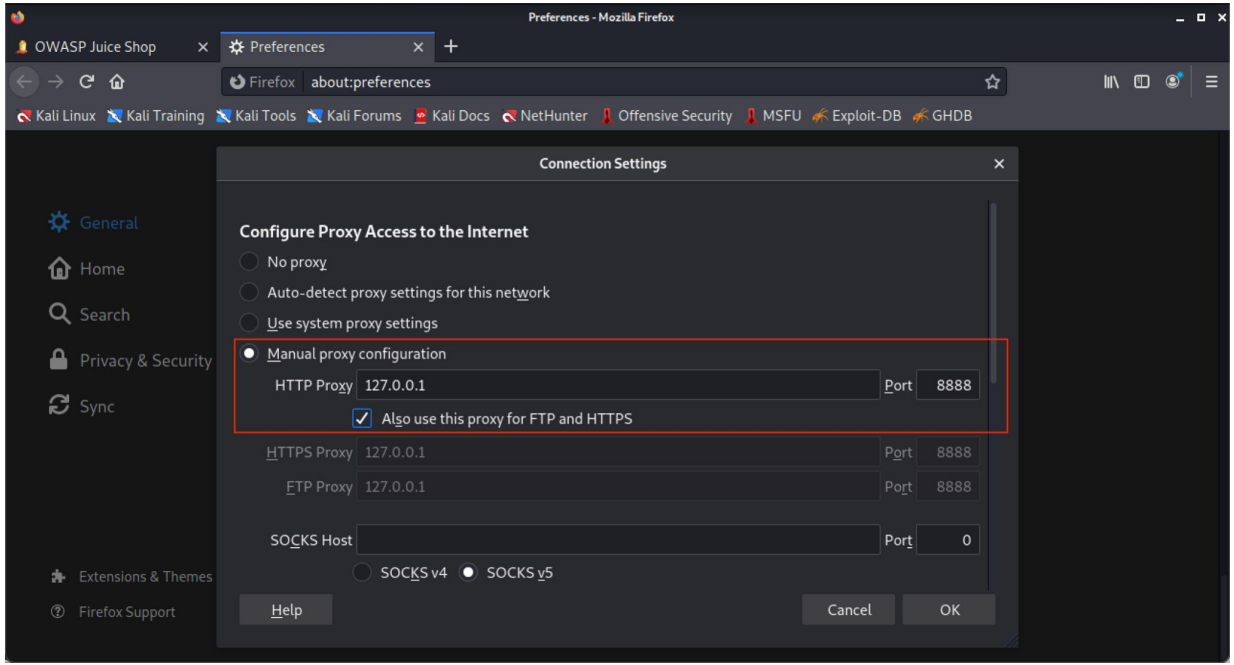


Exercise 1: Proxying with OWASP ZAP

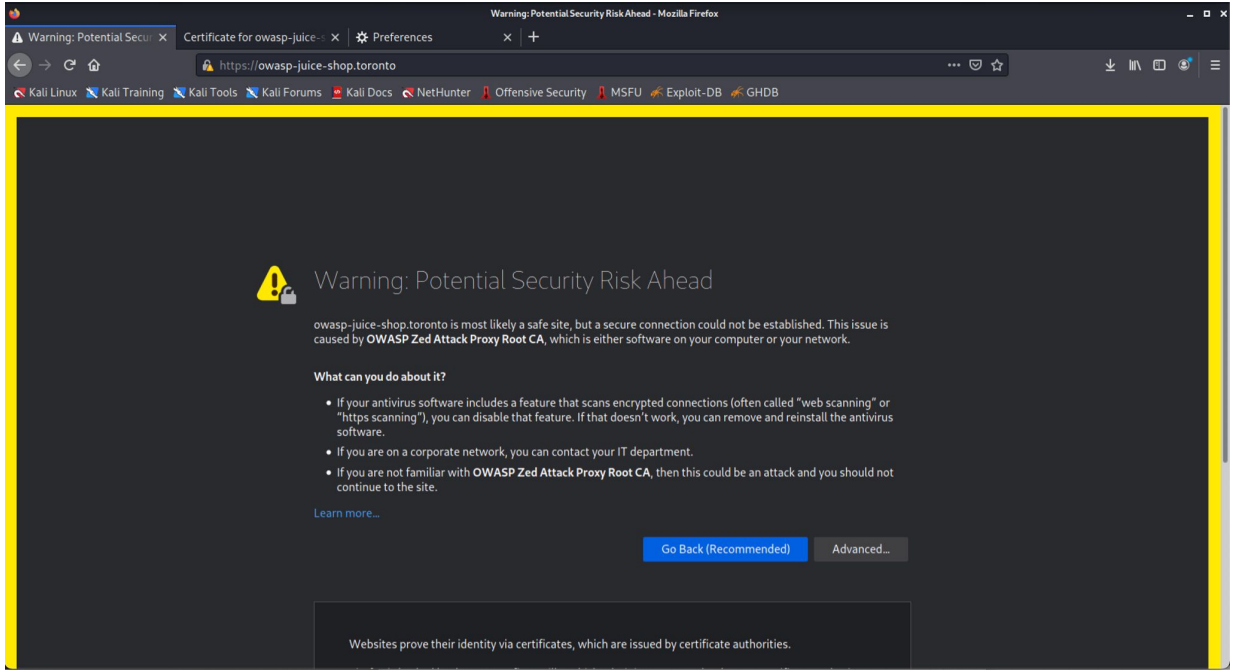
Exercise 1: Proxying traffic



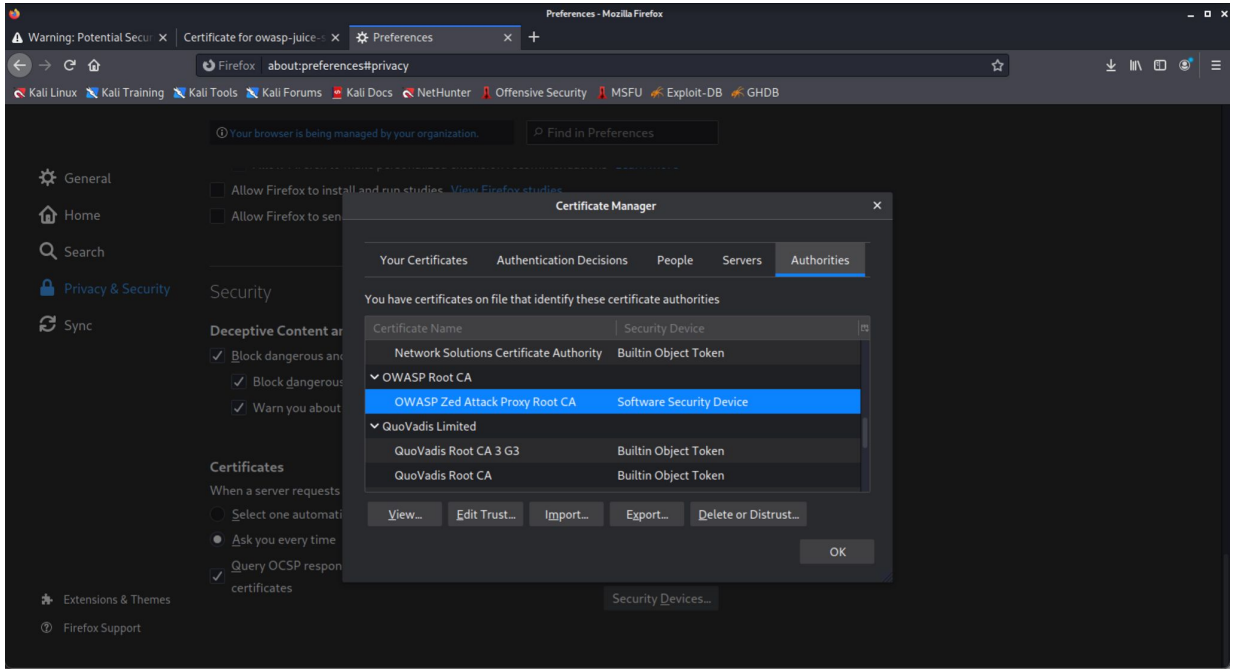
Exercise 1: Proxying traffic



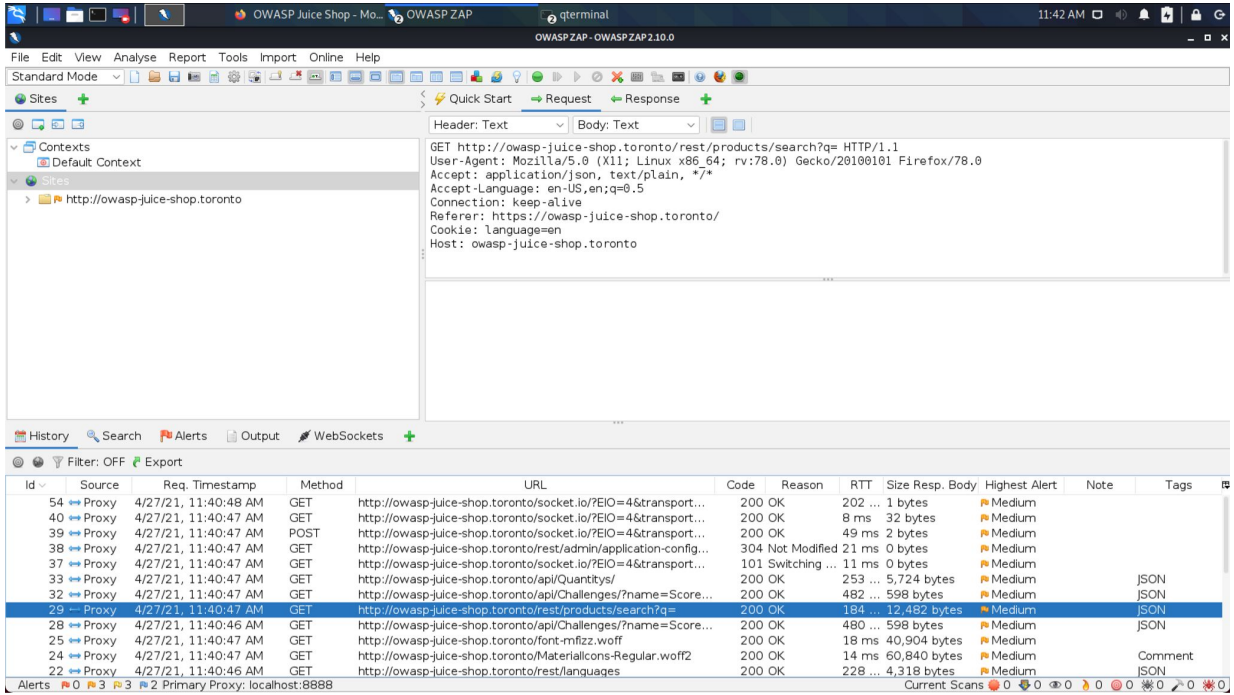
Exercise 1: Proxying traffic



Exercise 1: Proxying traffic



Exercise 1: Proxying traffic

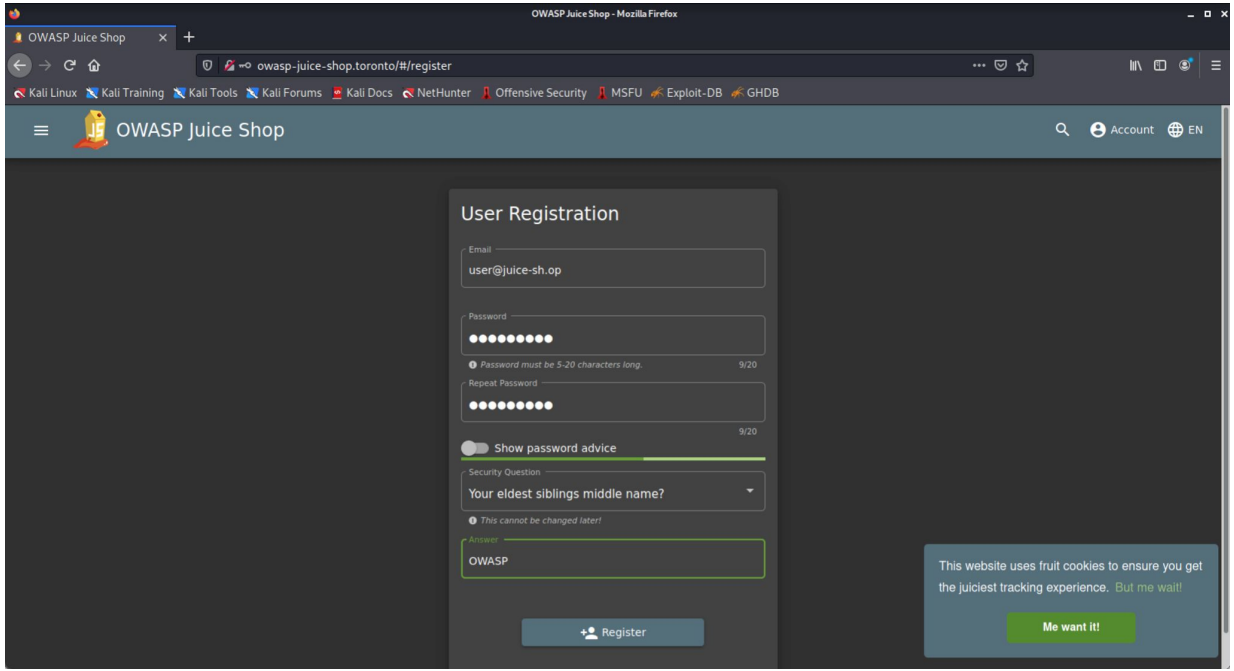


Exercise 2: Exploring OWASP Juice Shop and capturing traffic

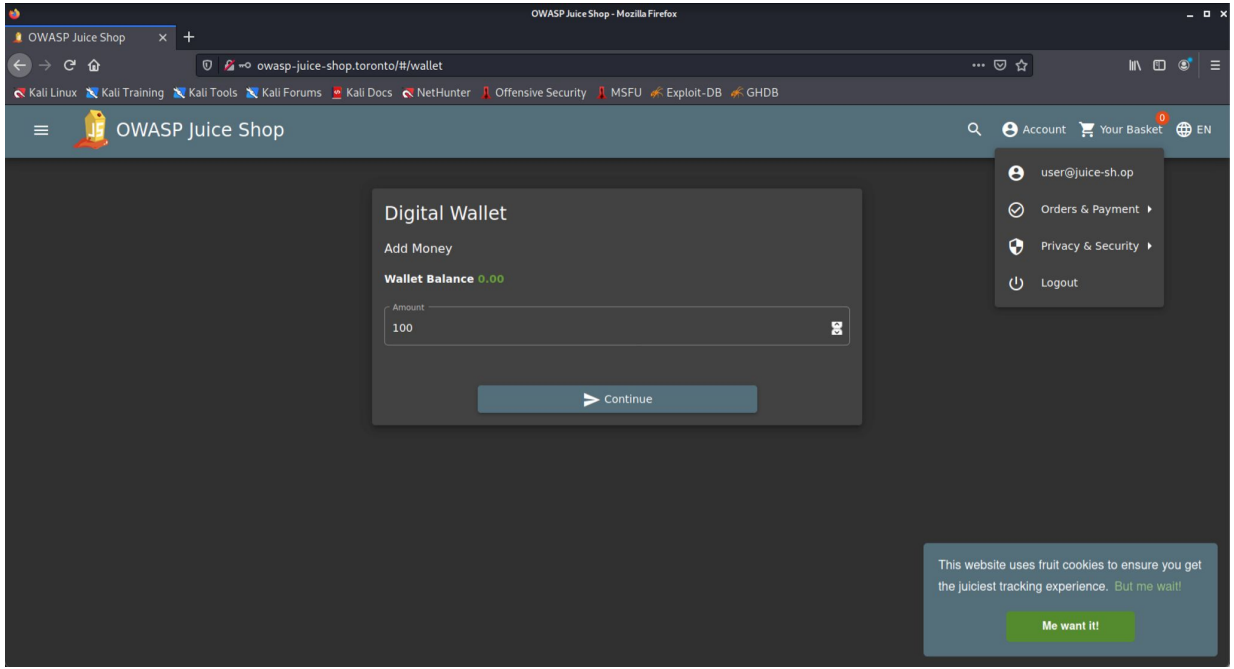
Exercise 2: Create an account and capture traffic with ZAP

- Create account:
  - user1@juice-sh.op
  - password1
- Add money to wallet
- Add any item to basket
- Checkout
- Payment

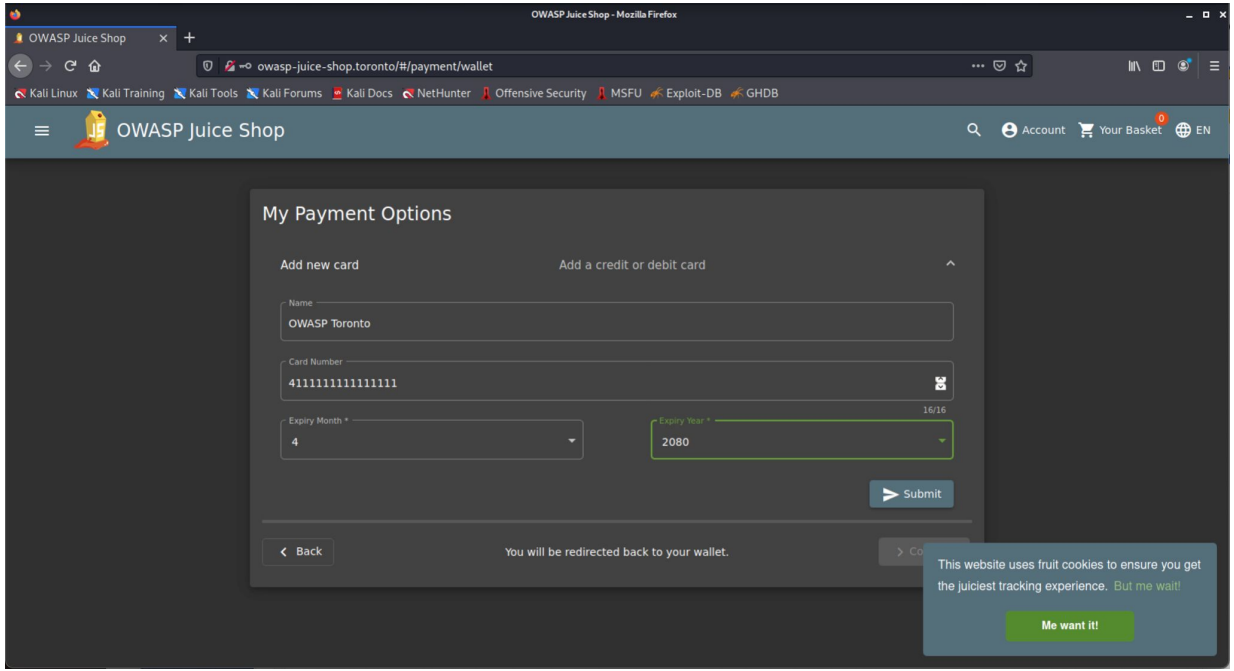
Exercise 2: Create account



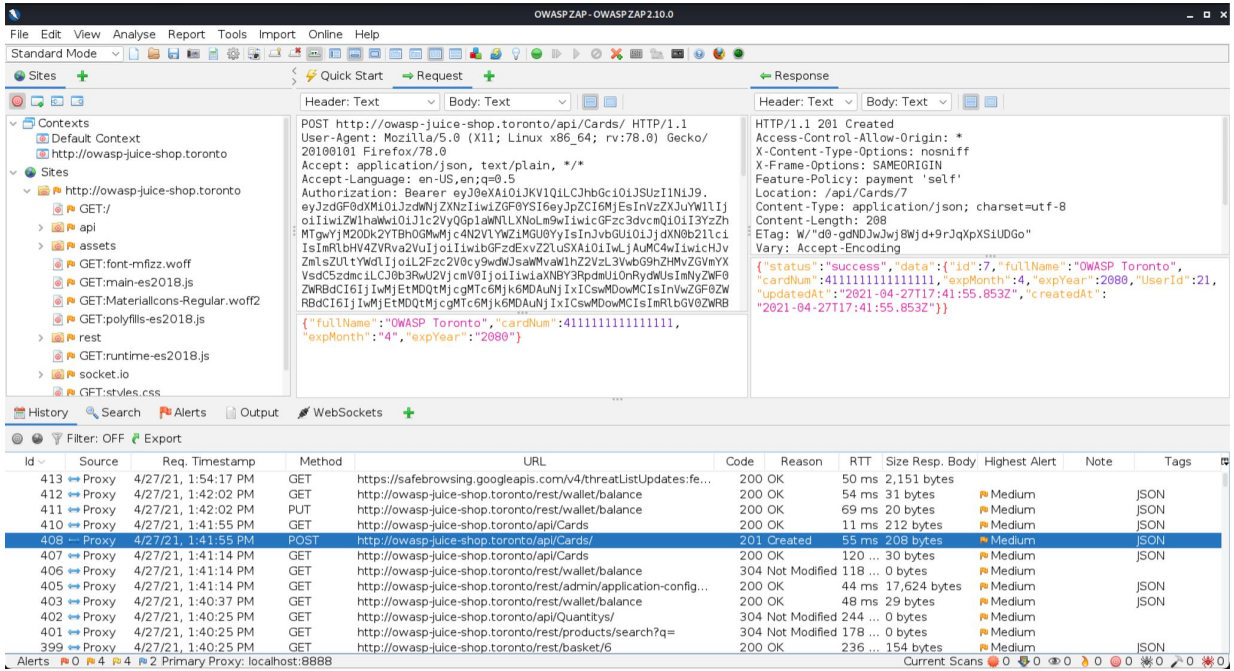
Exercise 2: Add money to wallet



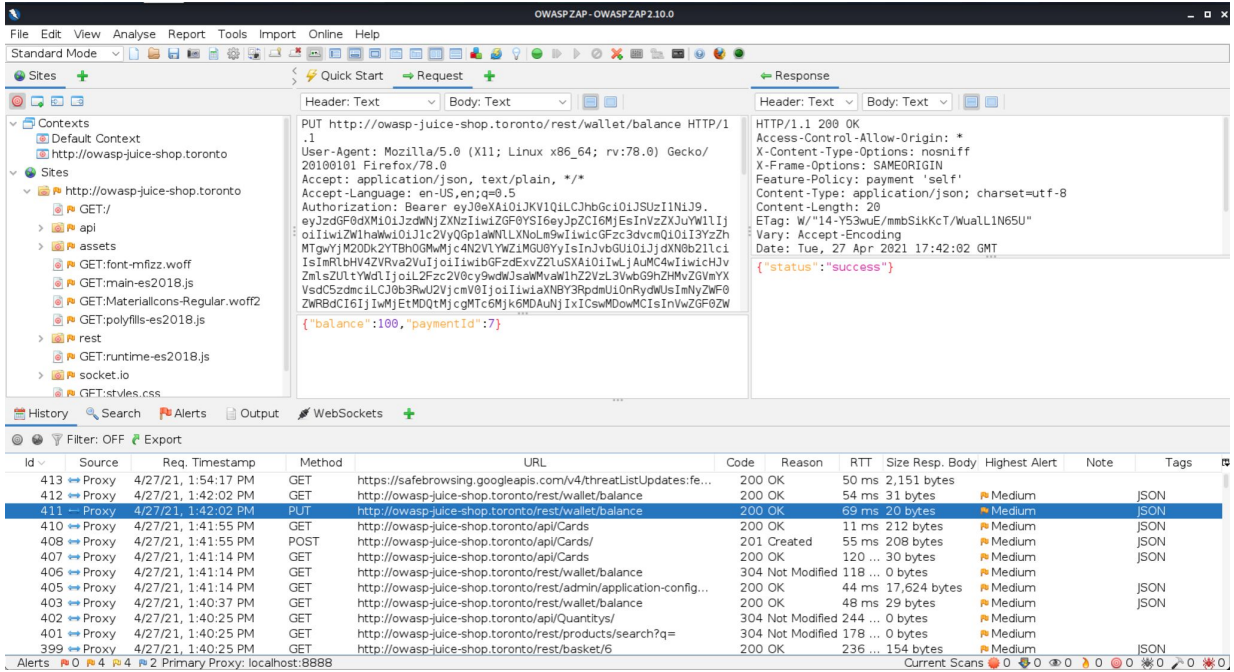
Exercise 2: Add money to wallet



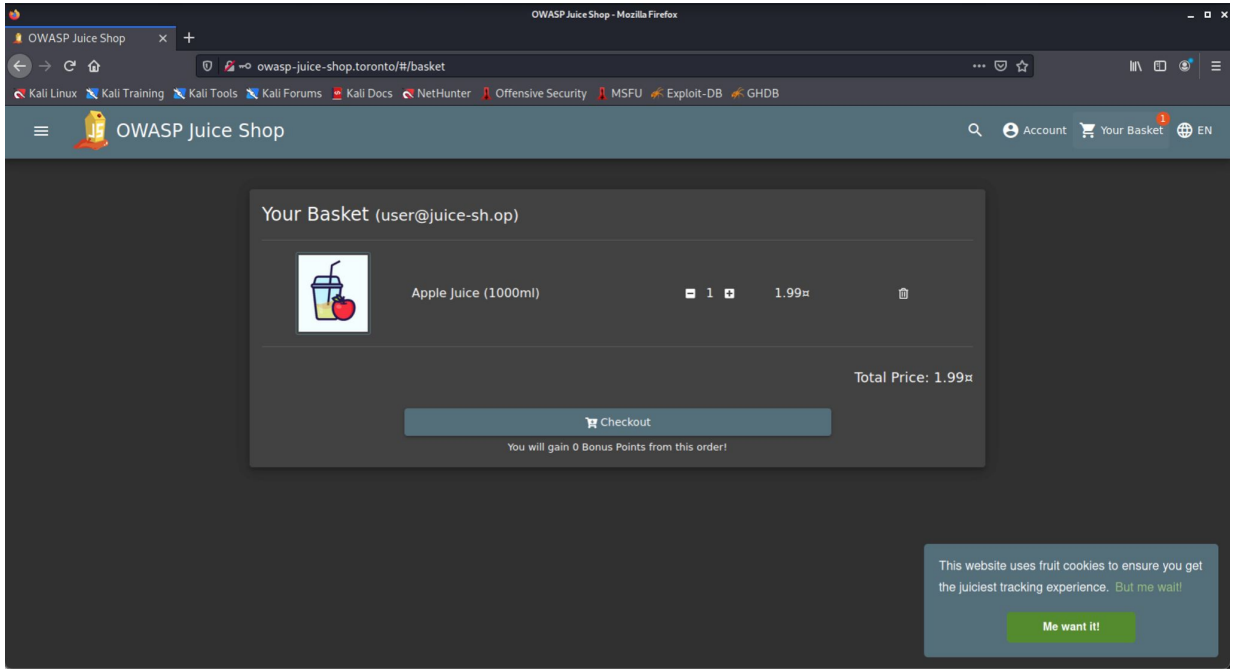
Exercise 2: Add money to wallet



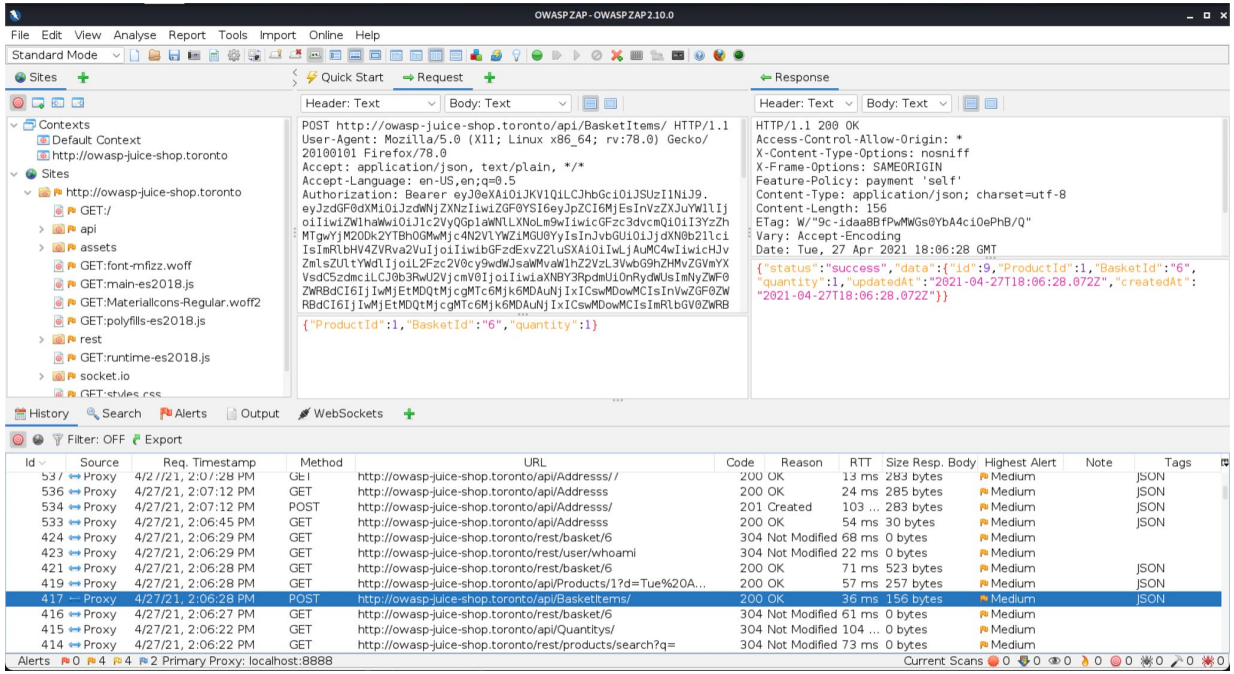
Exercise 2: Add money to wallet



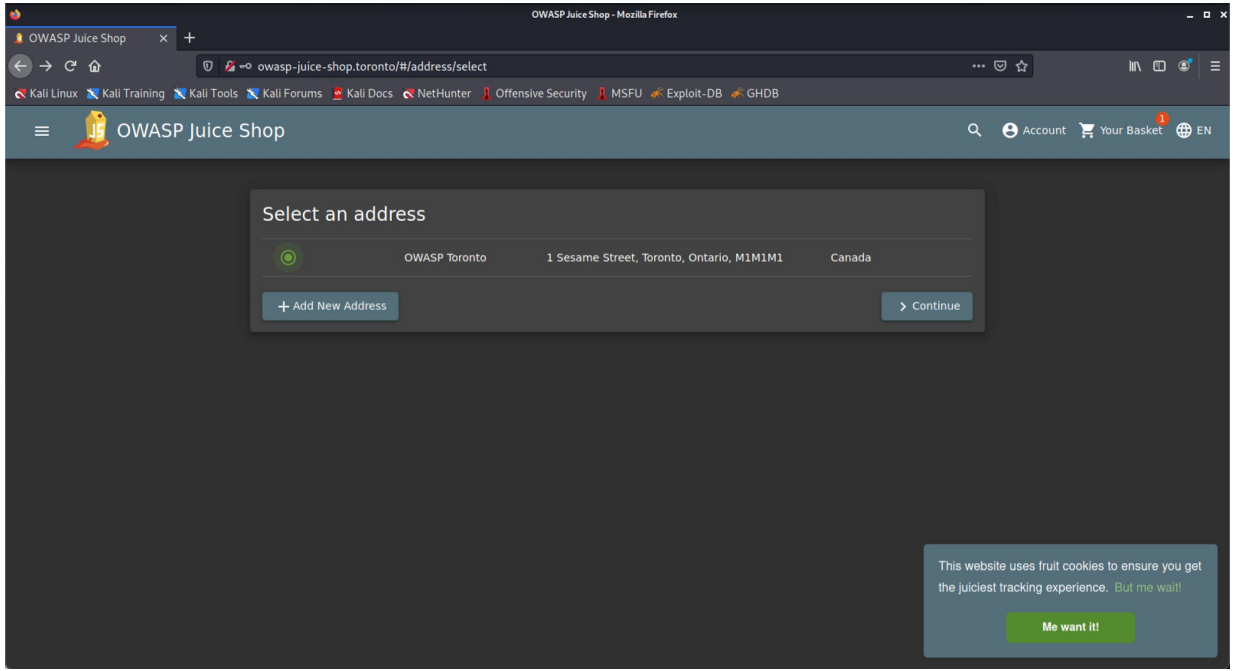
Exercise 2: Add item to basket



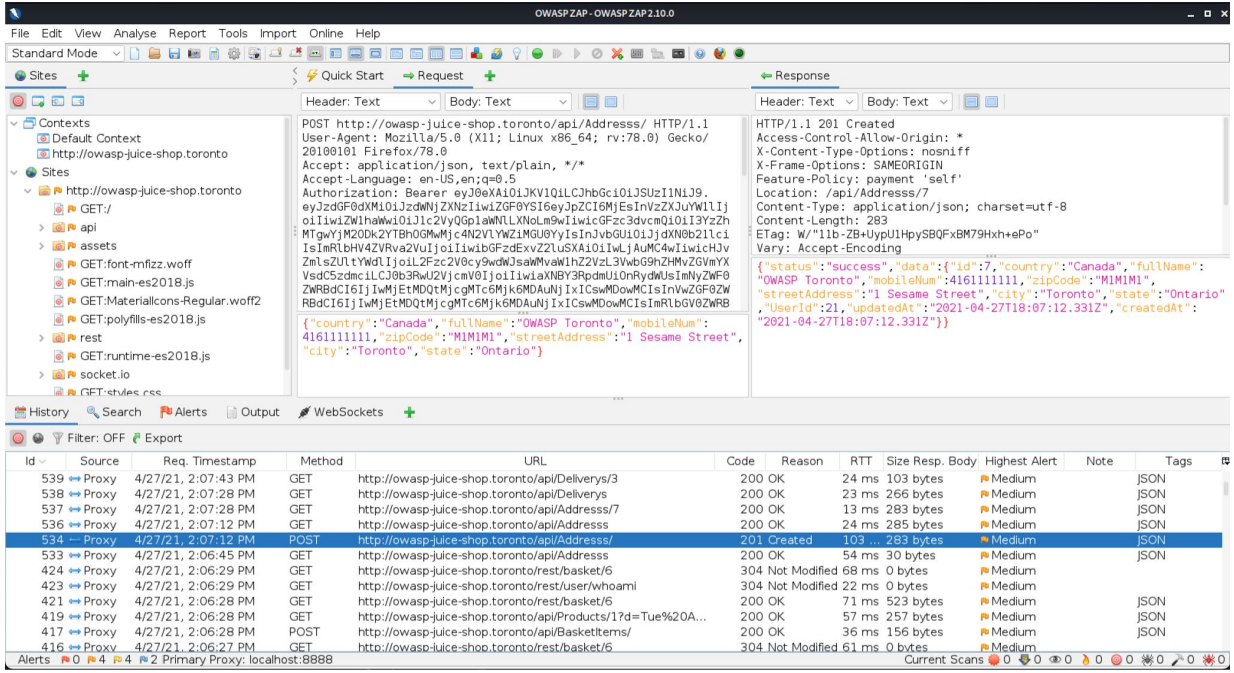
Exercise 2: Add item to basket



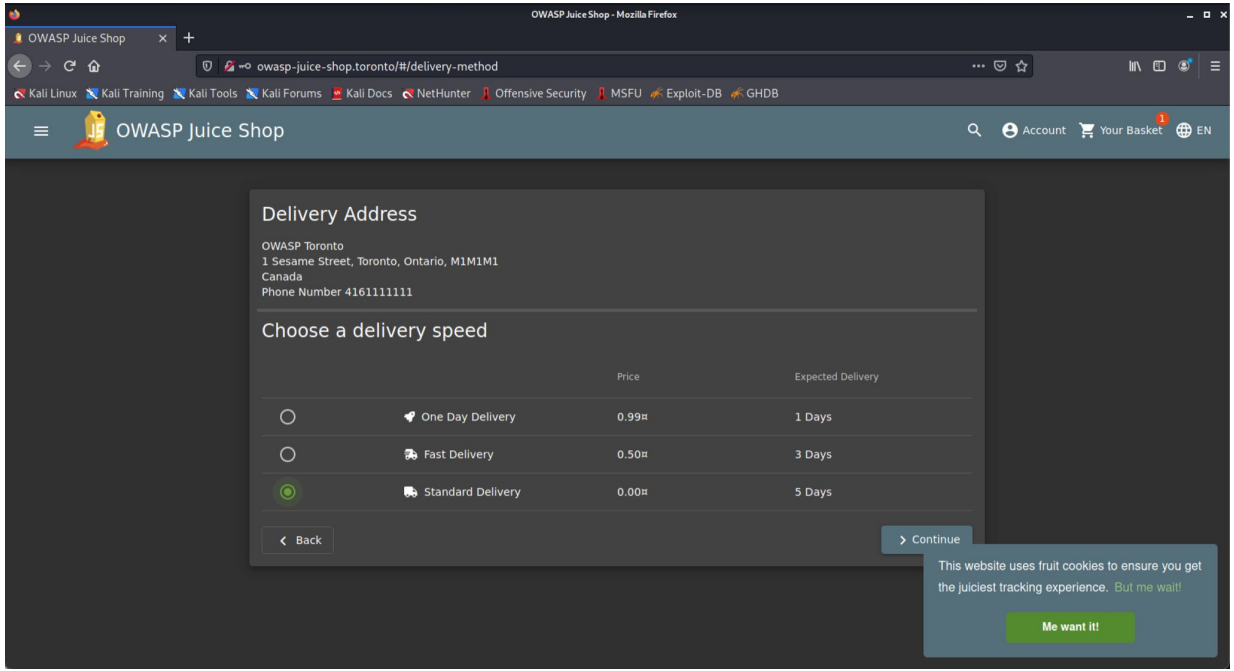
Exercise 2: Checkout



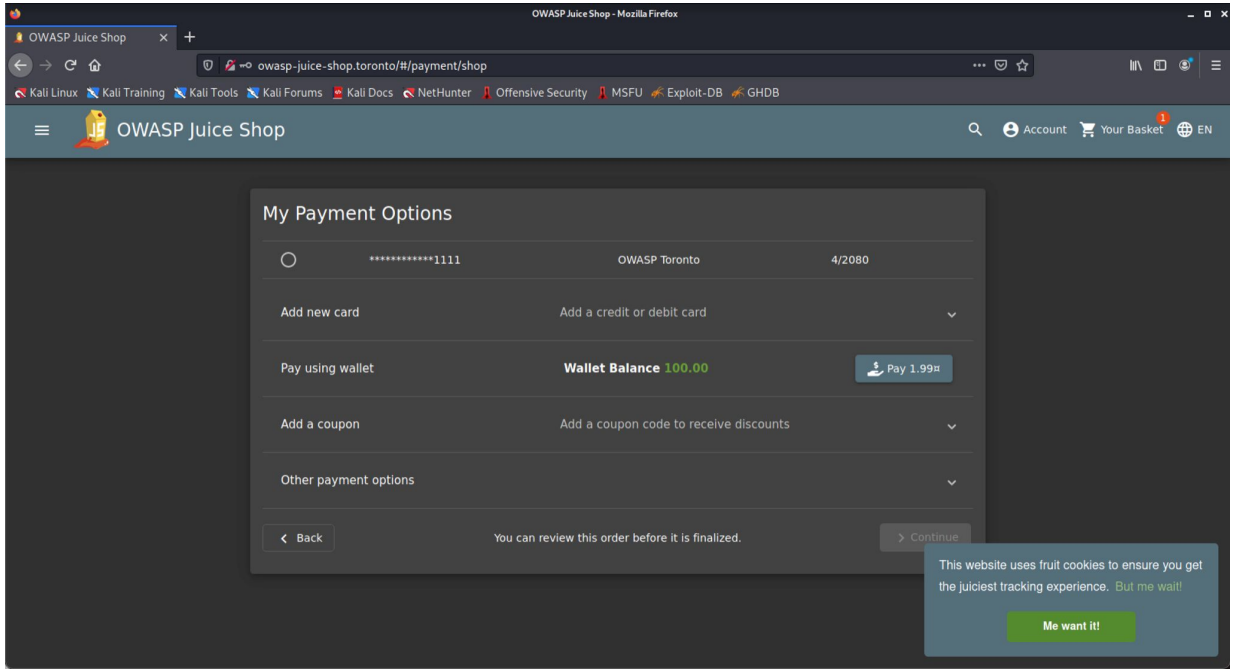
Exercise 2: Checkout



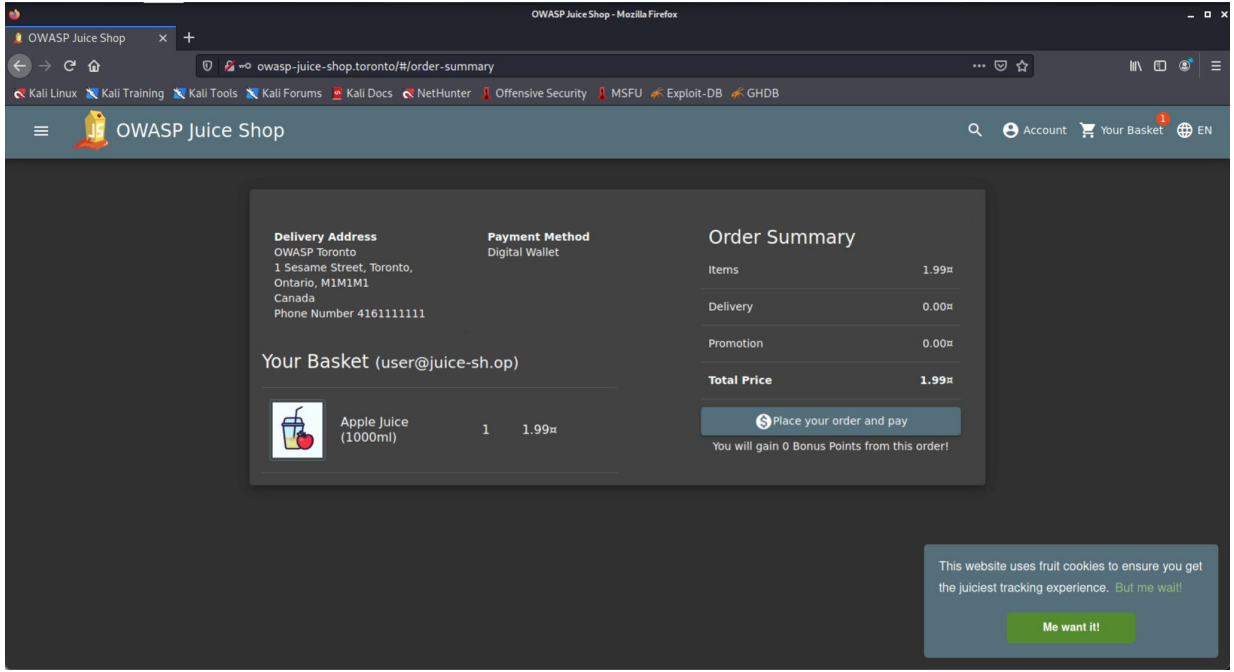
Exercise 2: Checkout



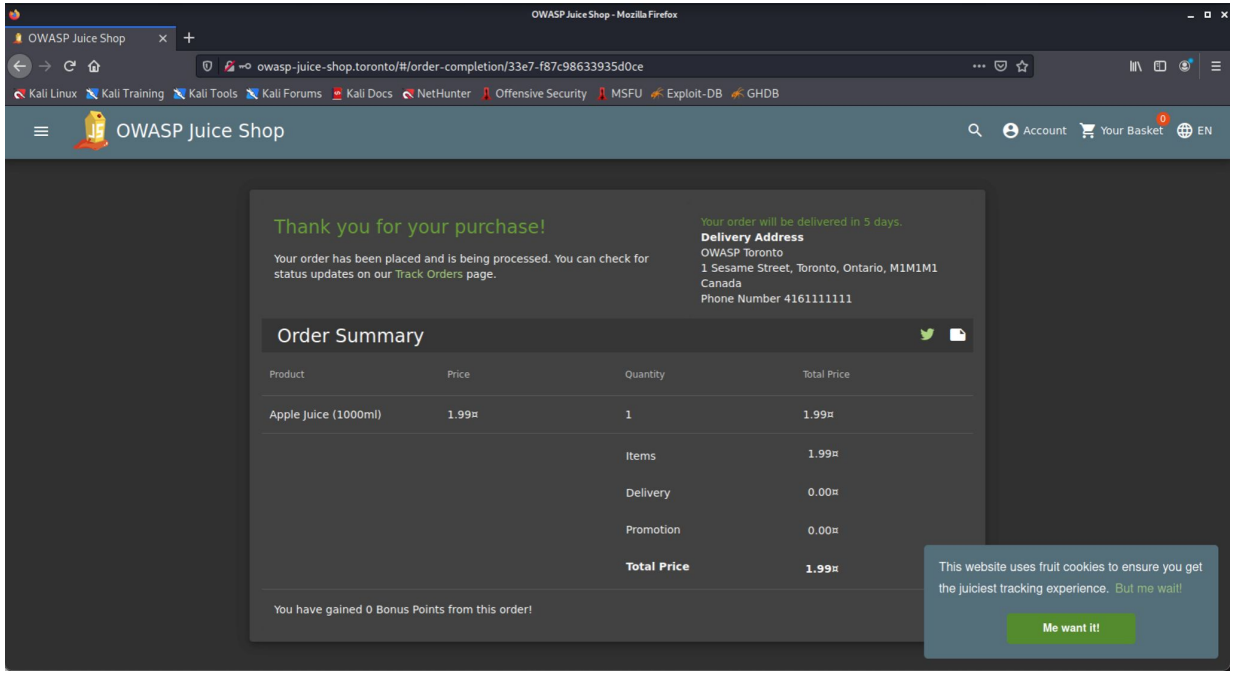
Exercise 2: Checkout



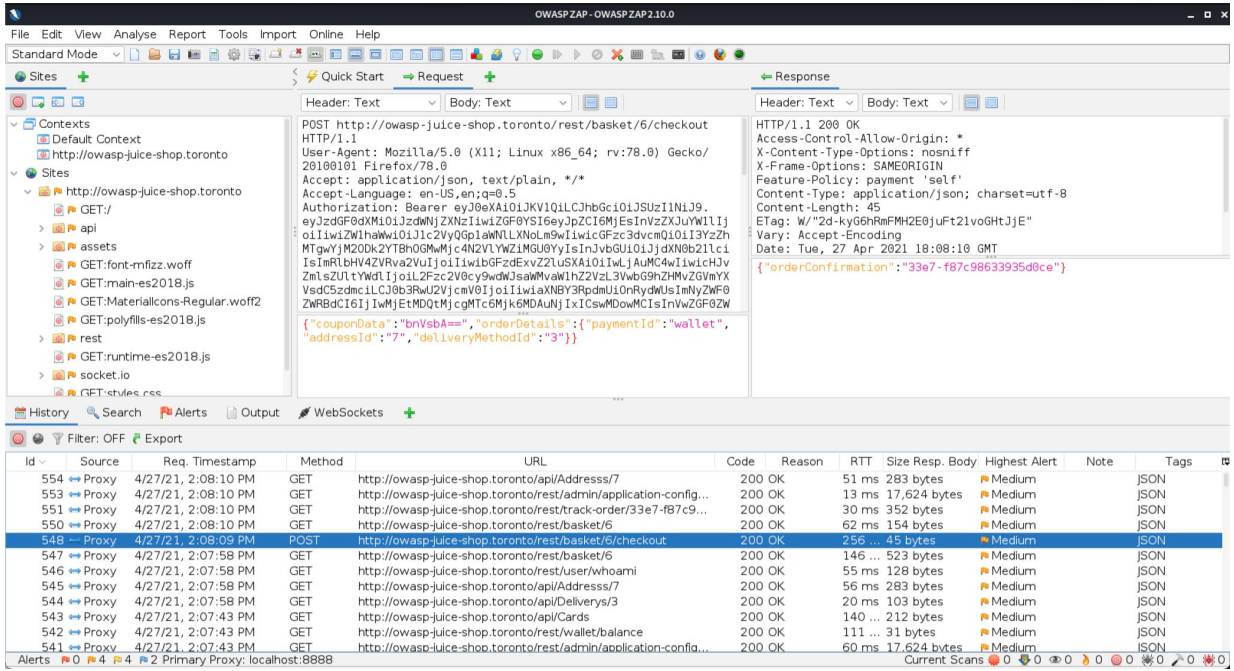
Exercise 2: Checkout



Exercise 2: Checkout

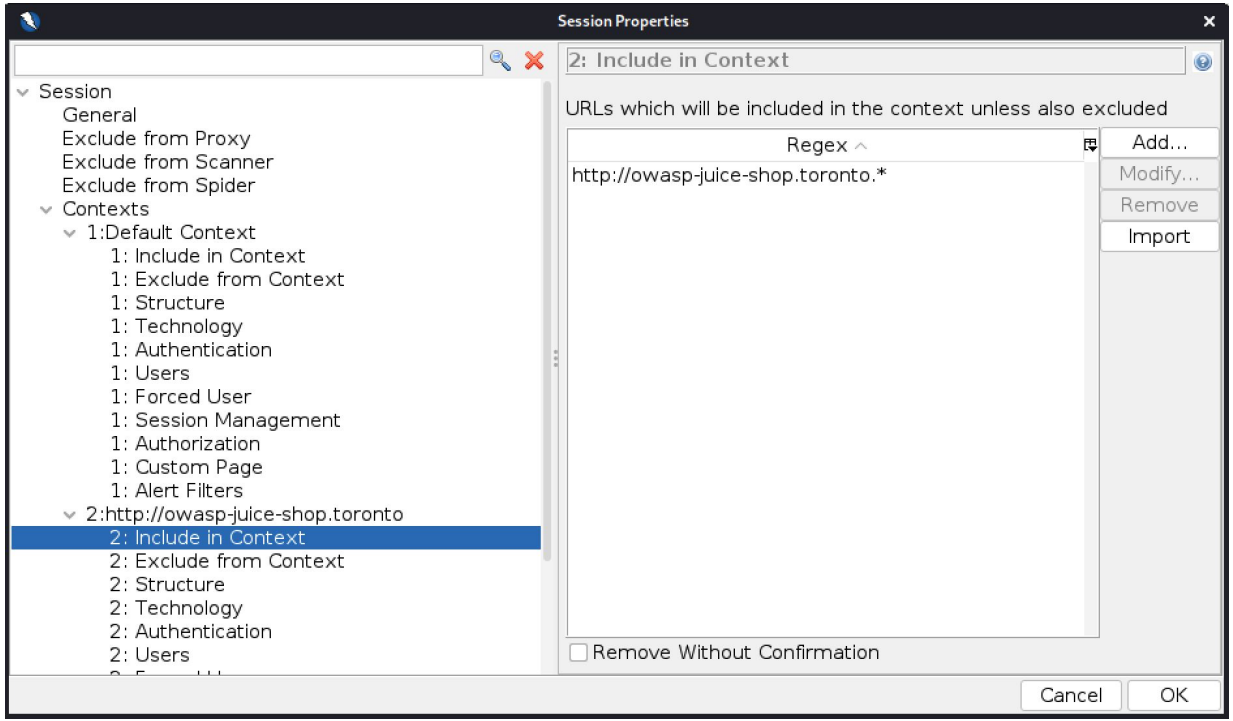


Exercise 2: Checkout

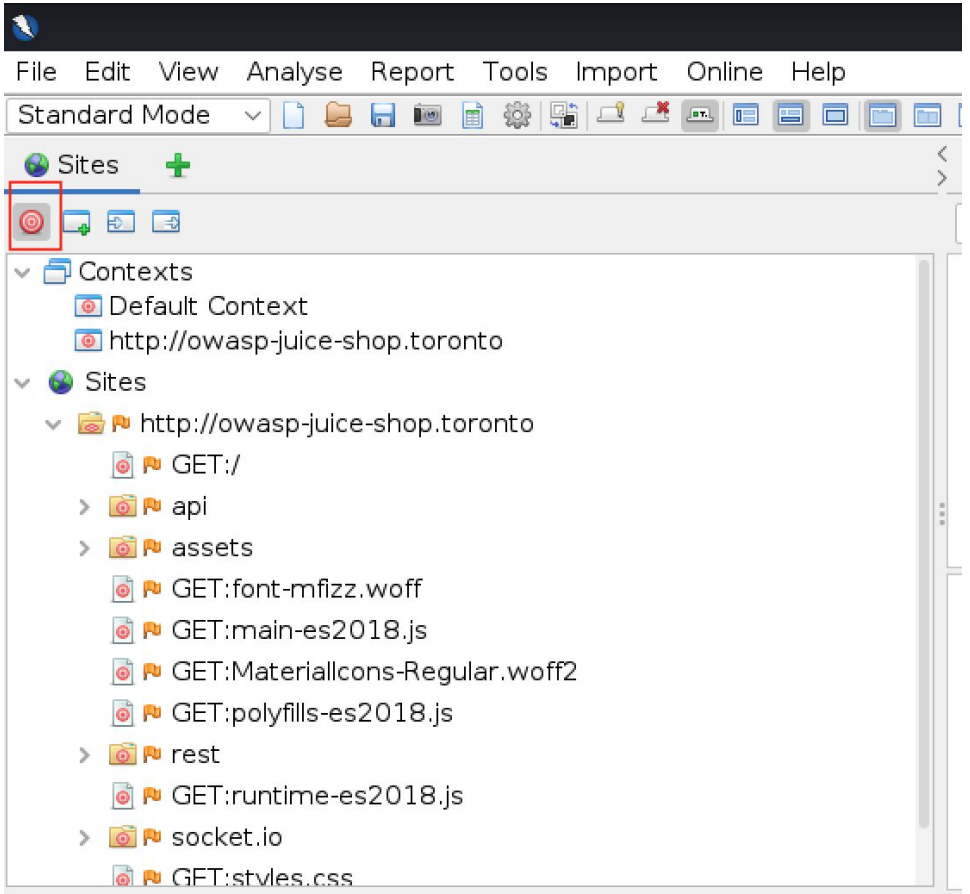


Exercise 3: Sites and Context

Exercise 3: Using Context

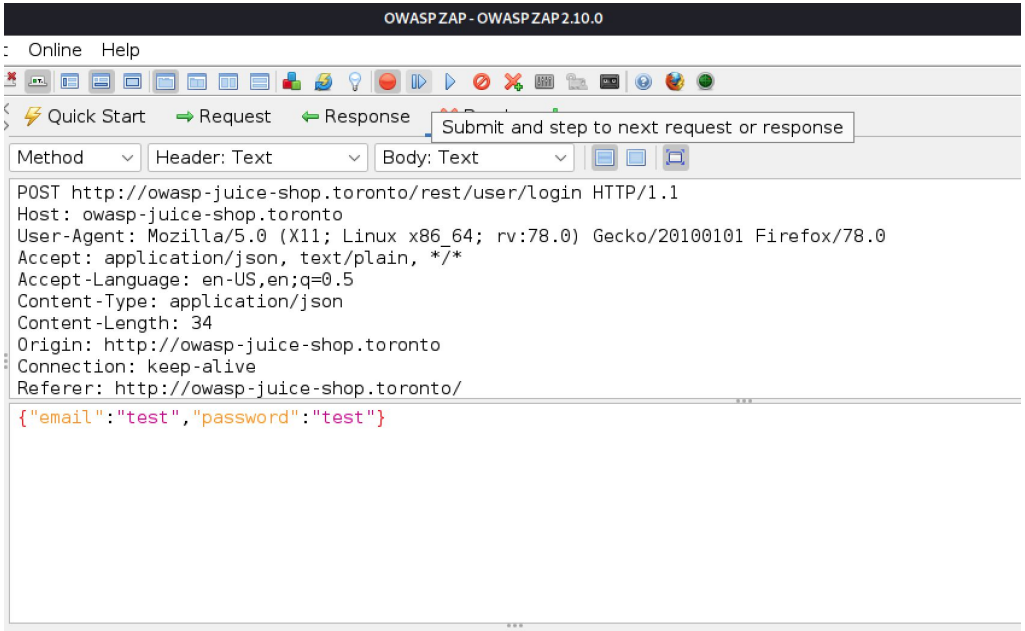


Exercise 3: Using Context

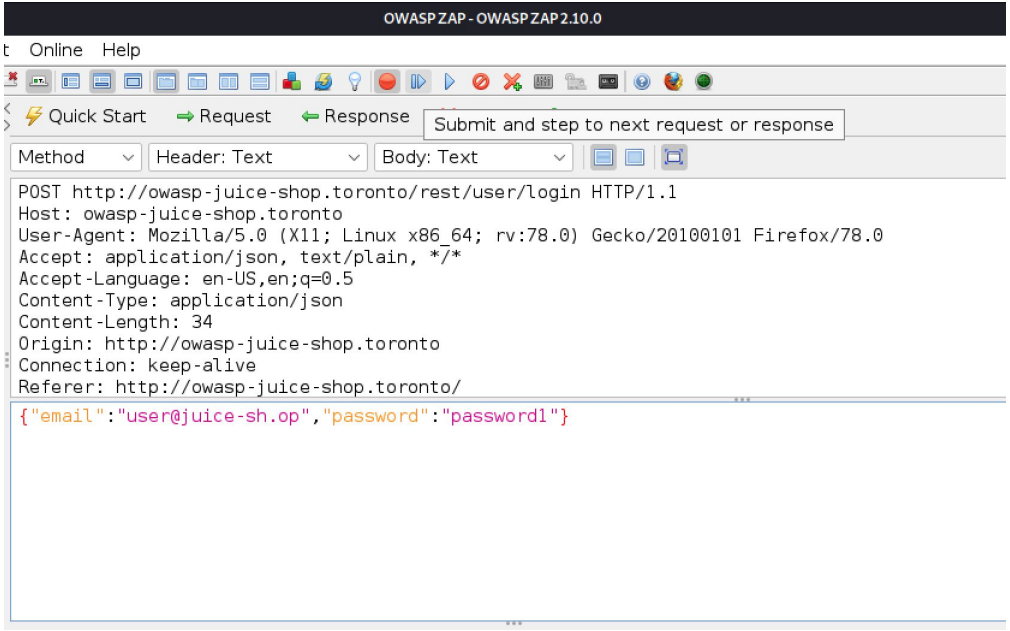


Exercise 4: Break and Request Editor

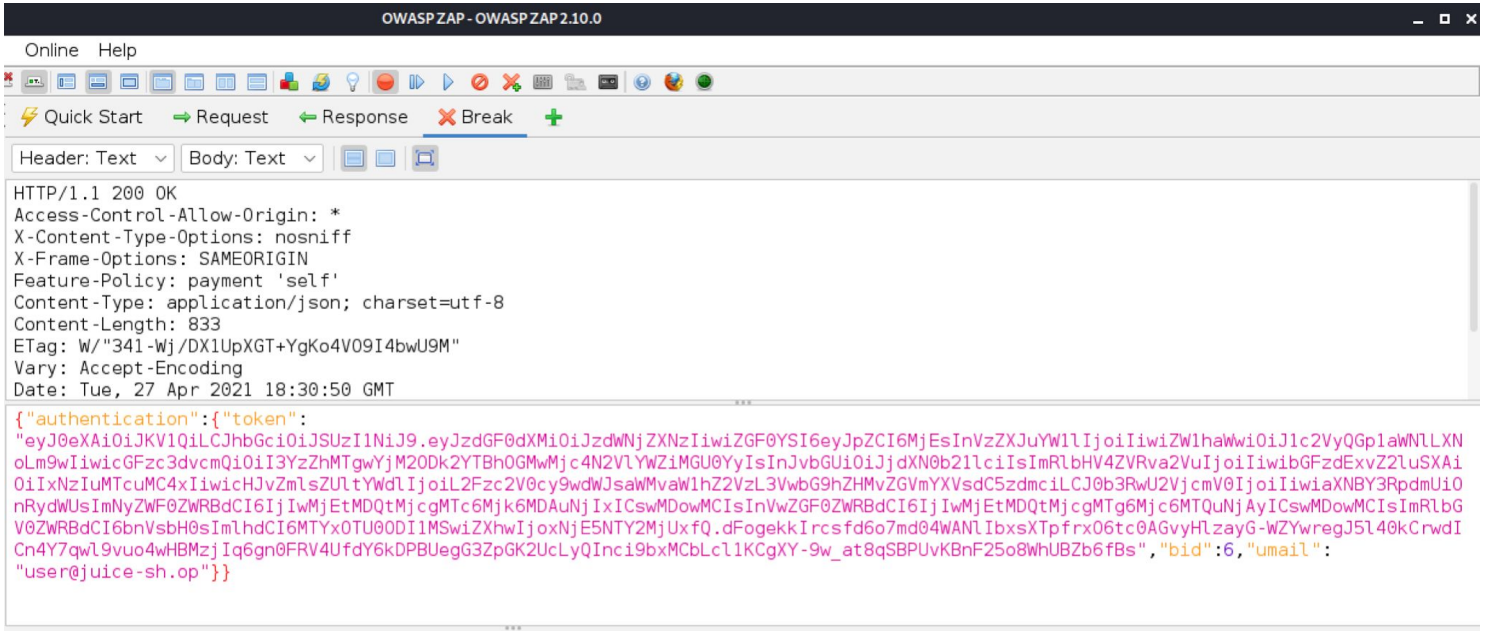
Exercise 4: Break



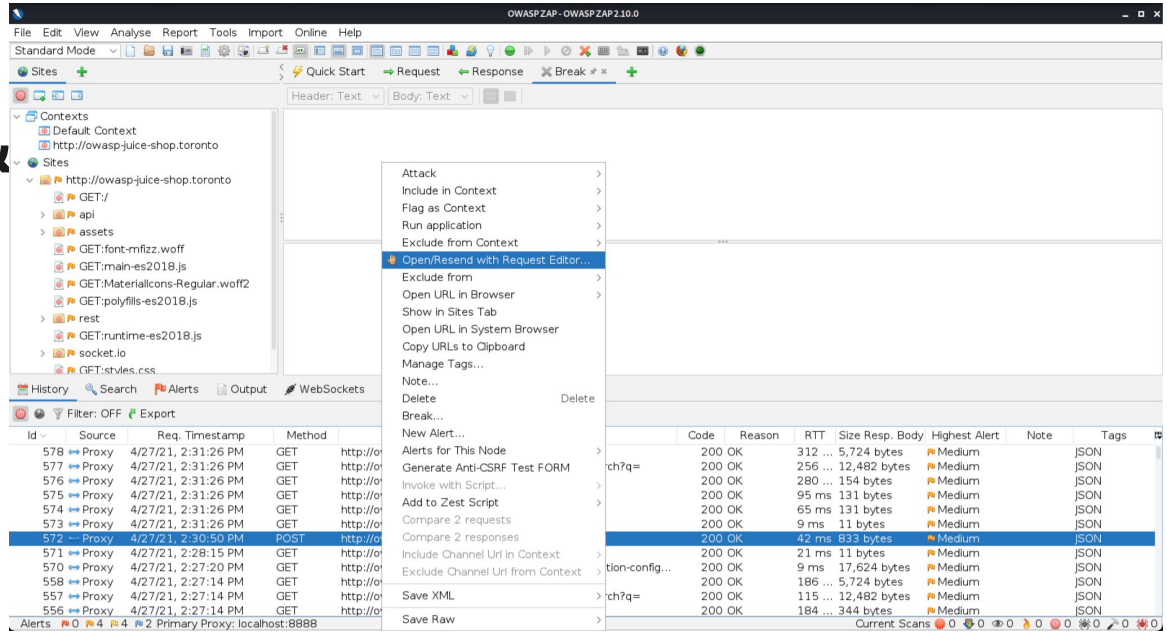
Exercise 4: Break



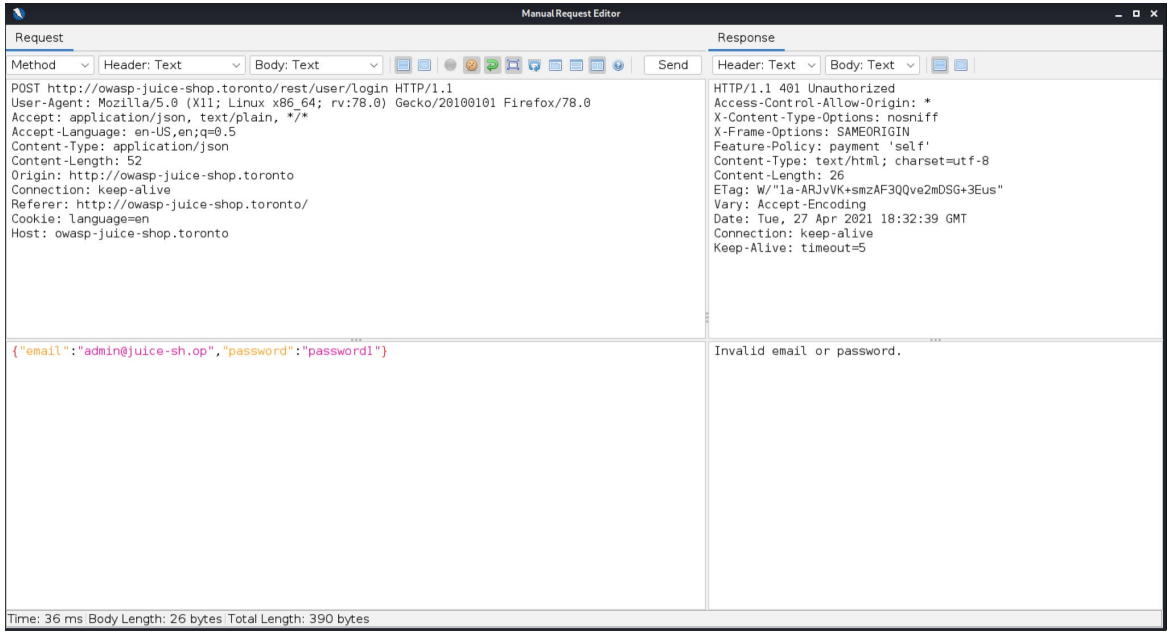
Exercise 4: Break



Exercise 4: Request Editor & Resend



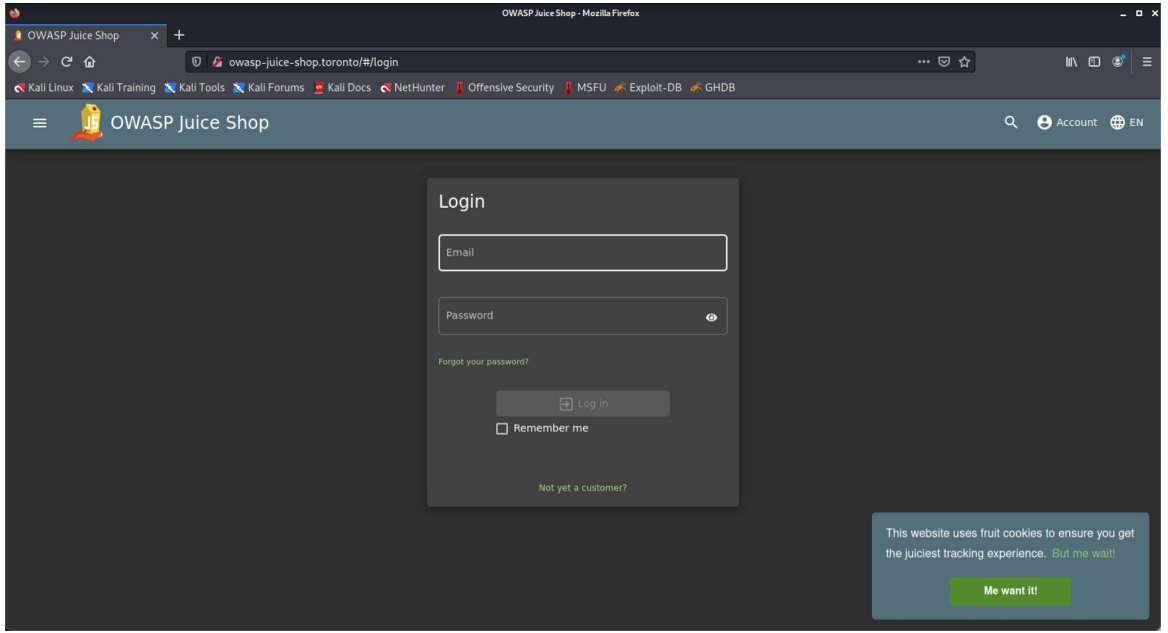
Exercise 4: Request Editor & Resend



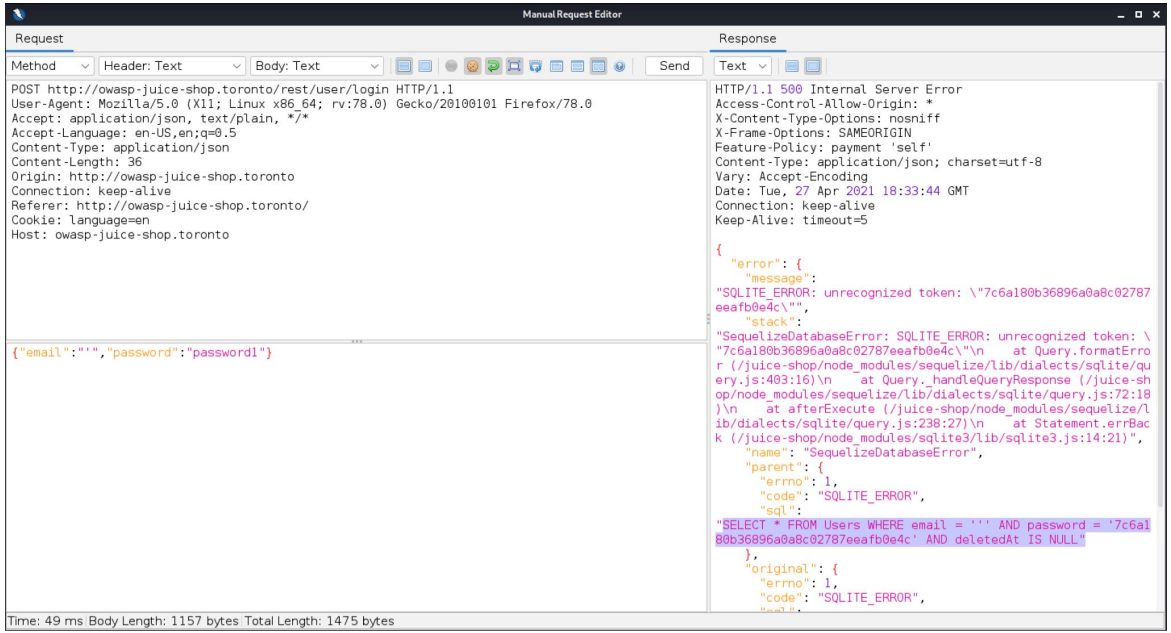
Exercise 5: SQL injection

How do I use SQL injection with ZAP to bypass login in Juice Shop?

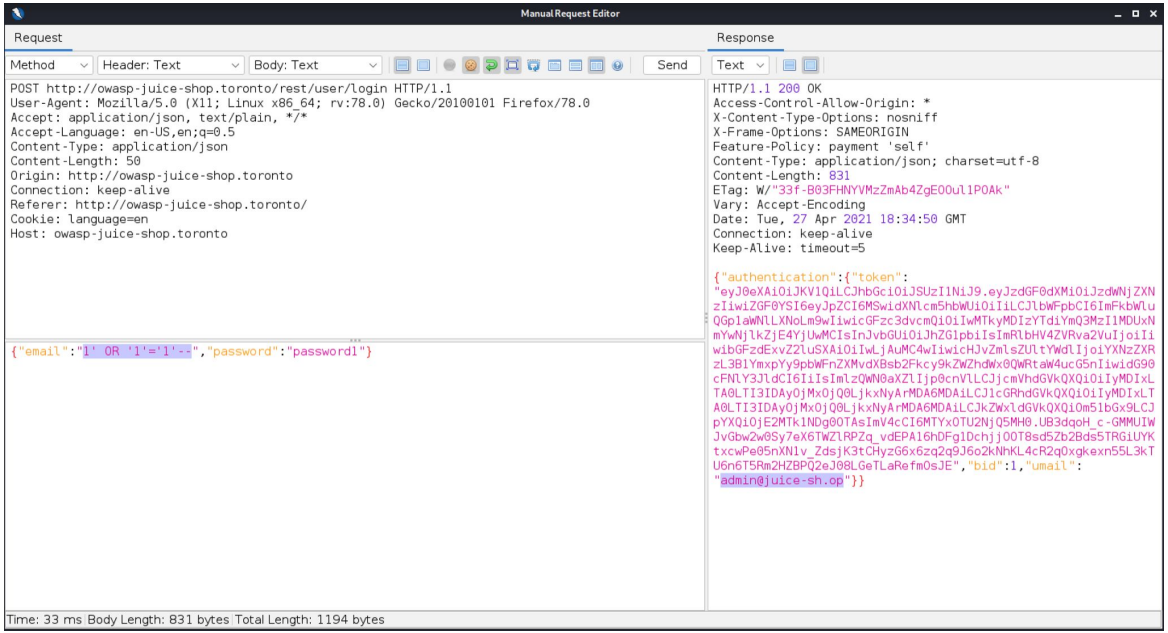
Exercise 5: SQLi



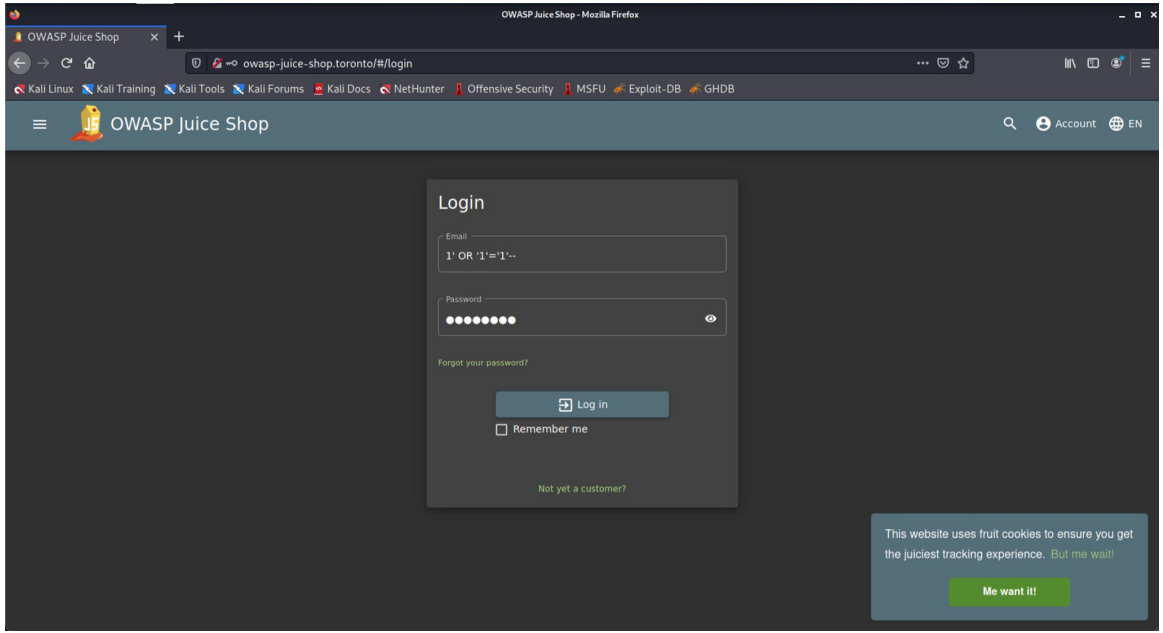
Exercise 5: SQLi



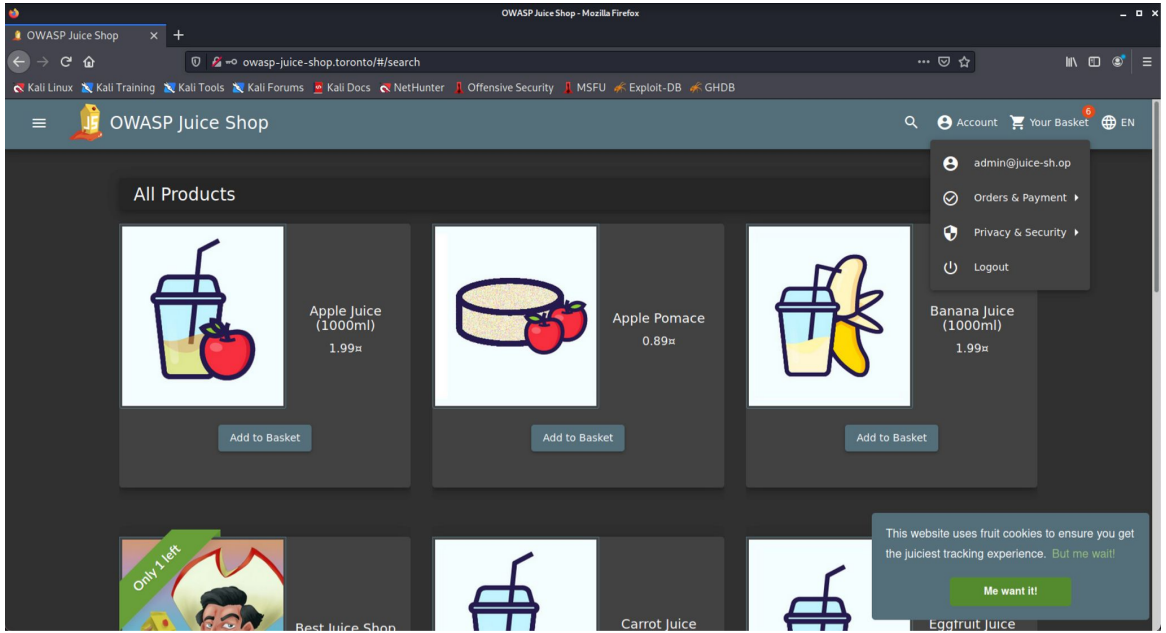
Exercise 5: SQLi



Exercise 5: SQLi

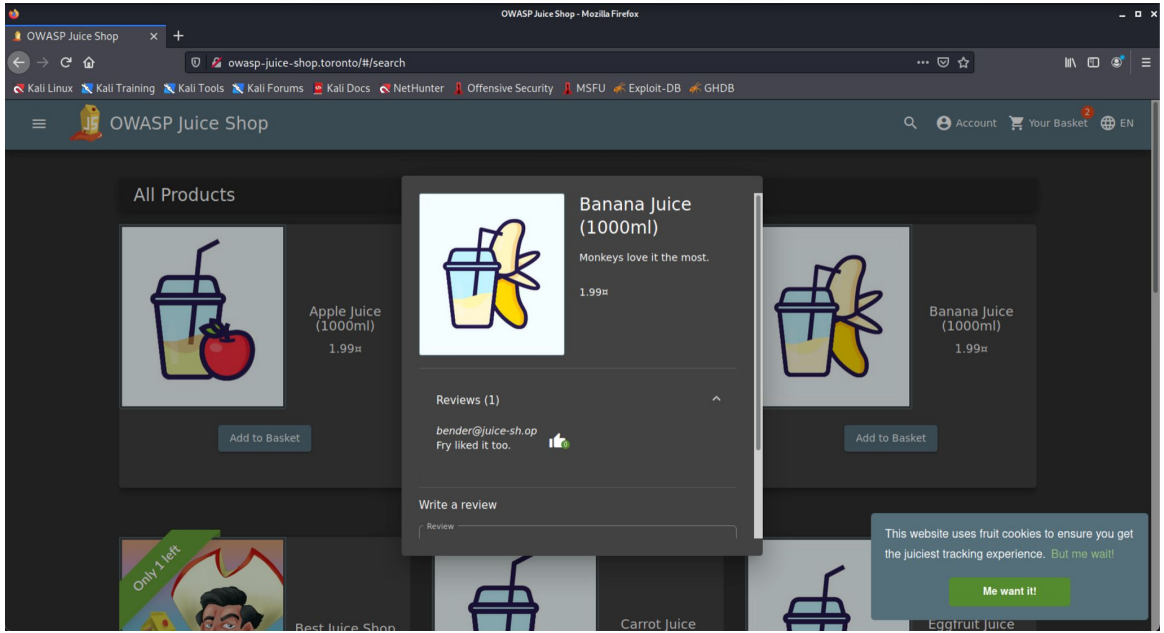


Exercise 5: SQLi

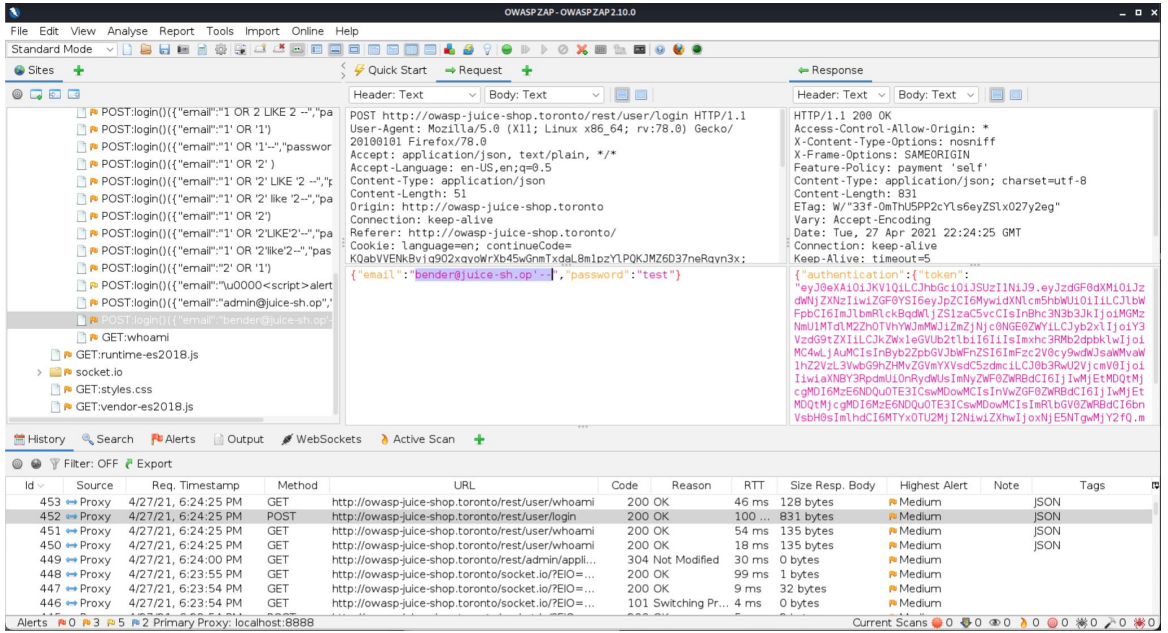


How do I use SQL injection with ZAP to log in as user “Bender”?

Exercise 5b: SQLi



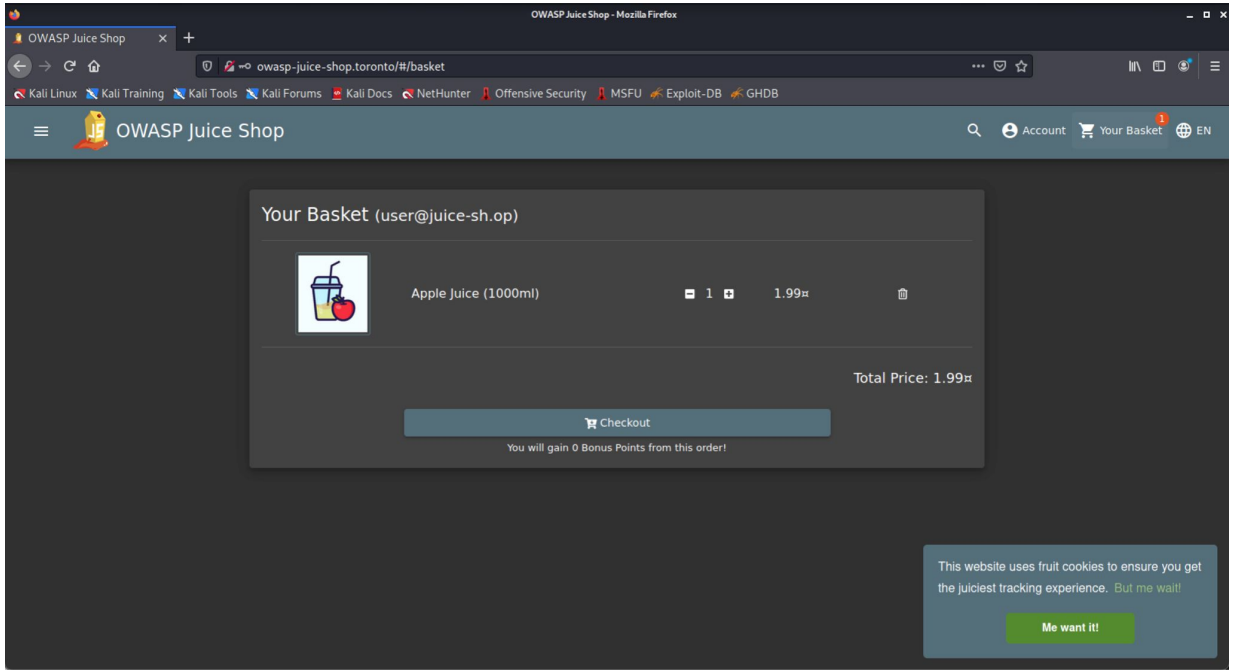
Exercise 5b: SQLi



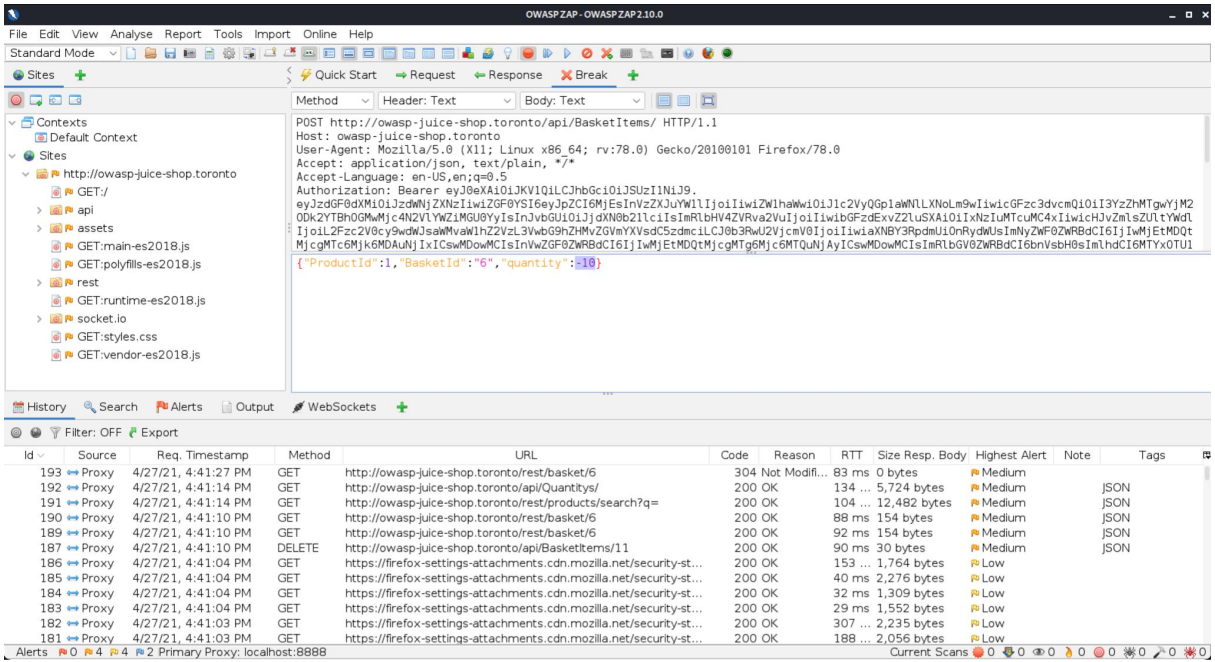
Exercise 6: Parameter manipulation

How do I “fraudulently” increase my wallet balance by $19.90 without funding with a credit card?

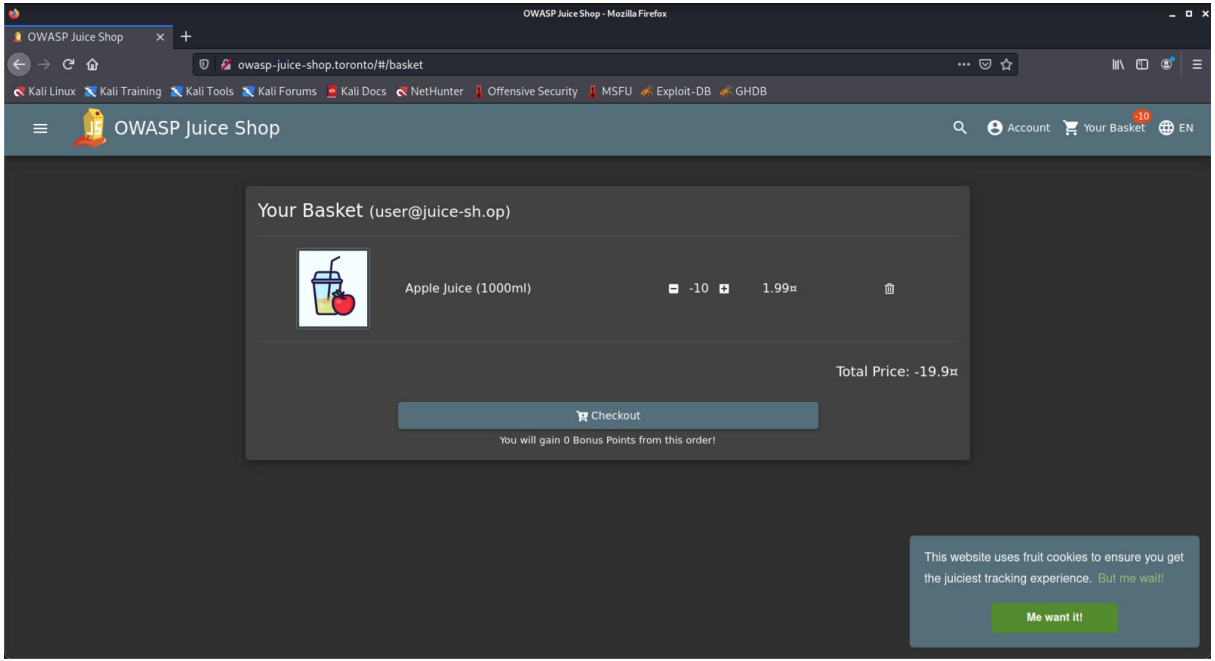
Exercise 6: RECALL: Add item to basket



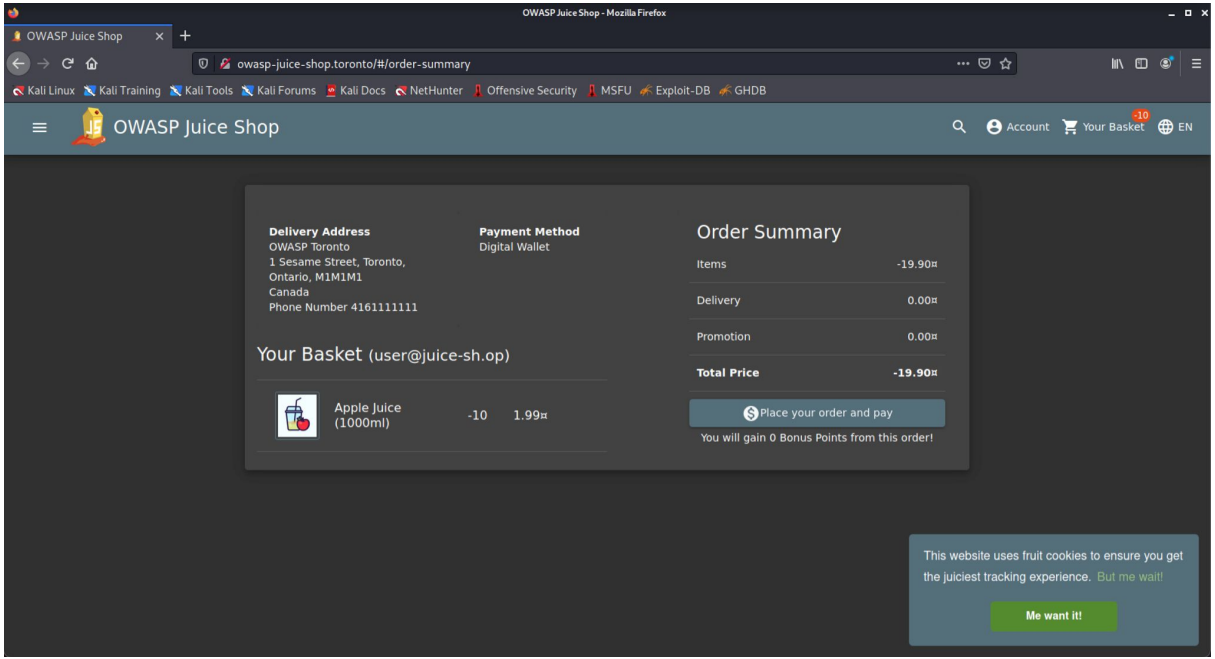
Exercise 6: Parameter manipulation



Exercise 6: Parameter manipulation

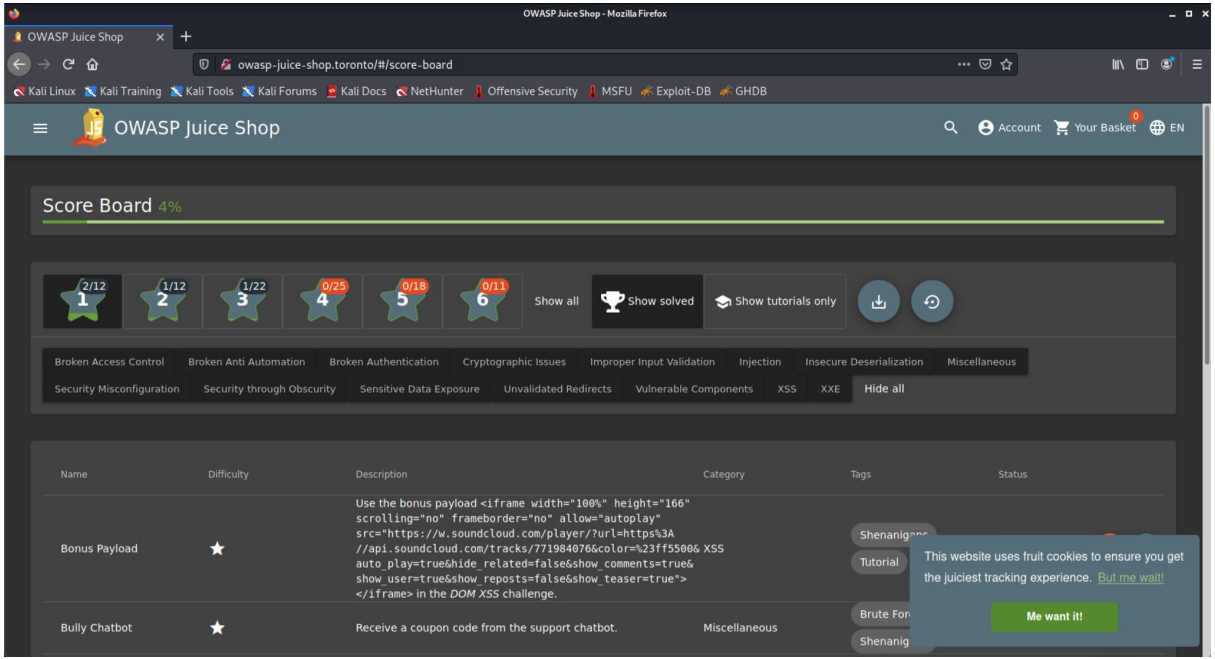


Exercise 6: Parameter manipulation



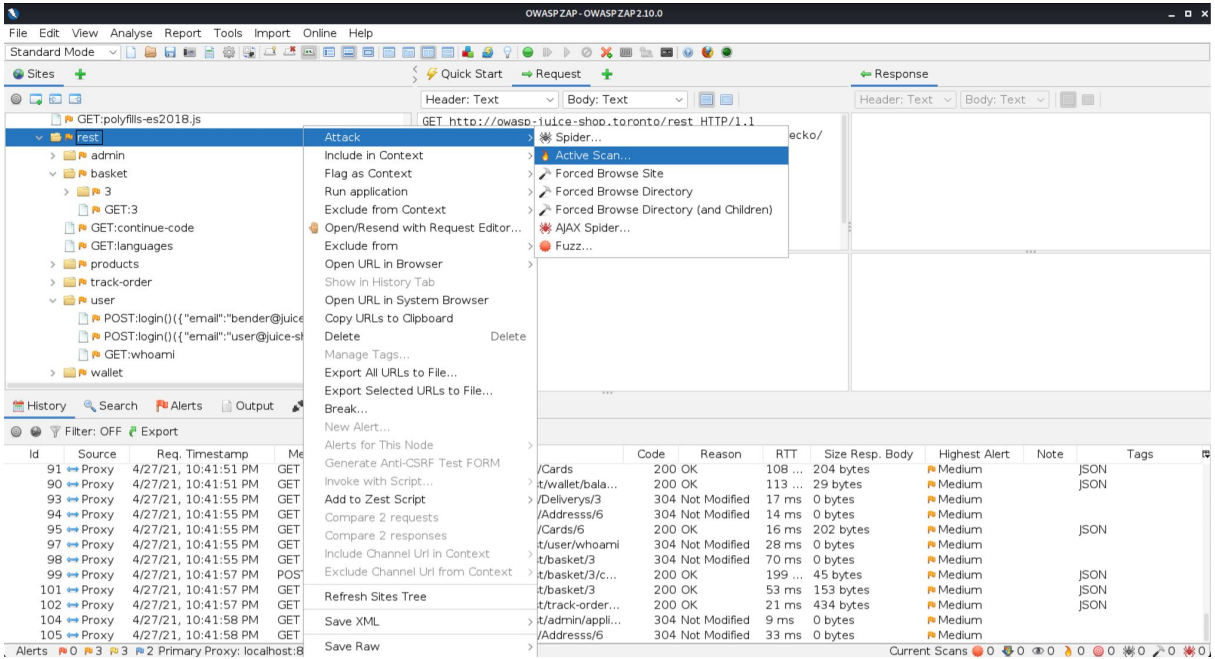
Exercise 7: Scoreboard

Exercise 7: Scoreboard

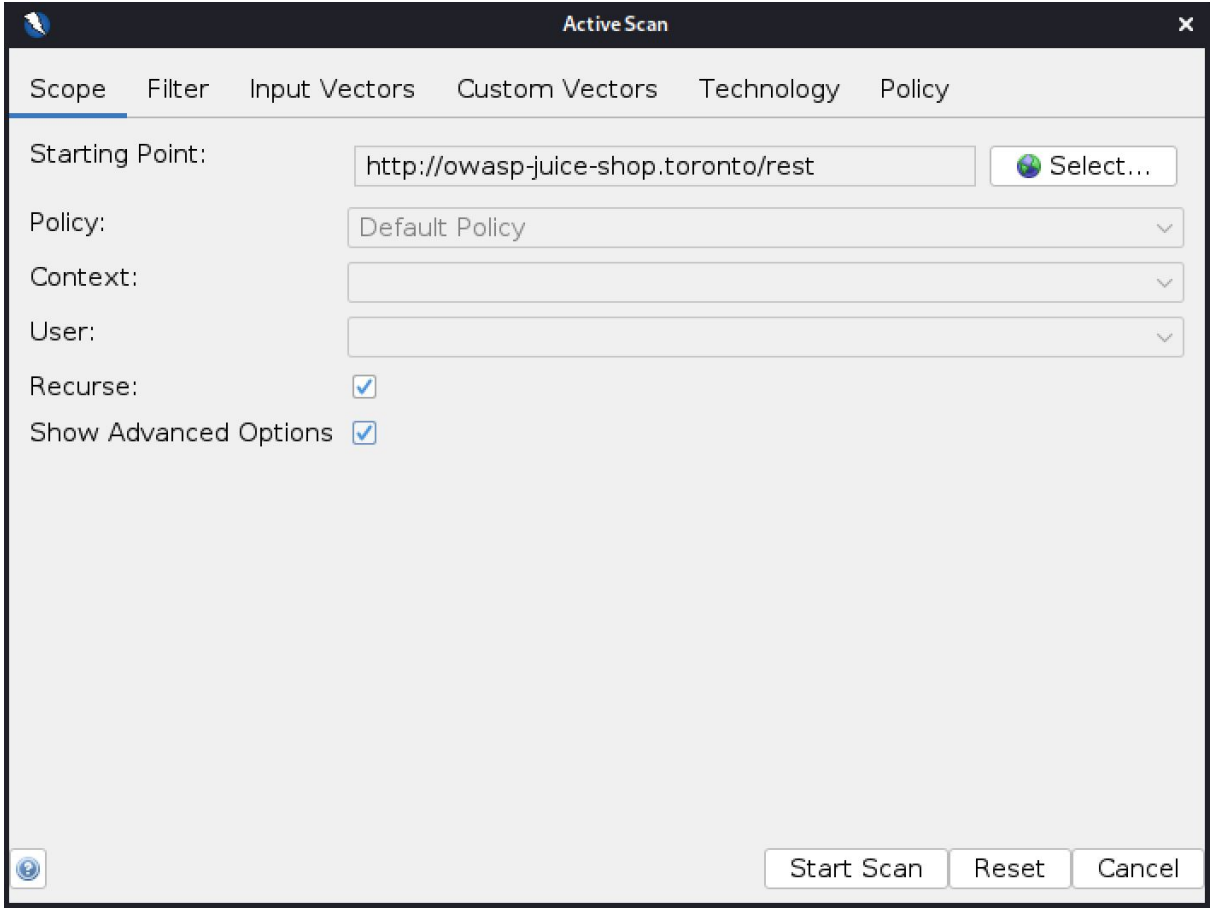


Exercise 8: Active Scan

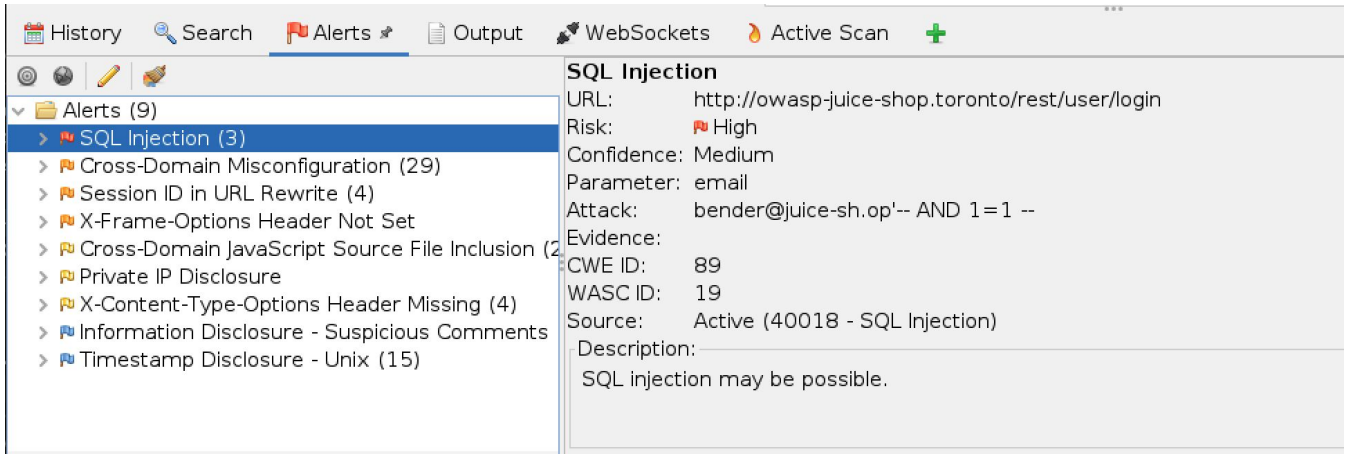
Exercise 8: Active Scan



Exercise 8: Active Scan

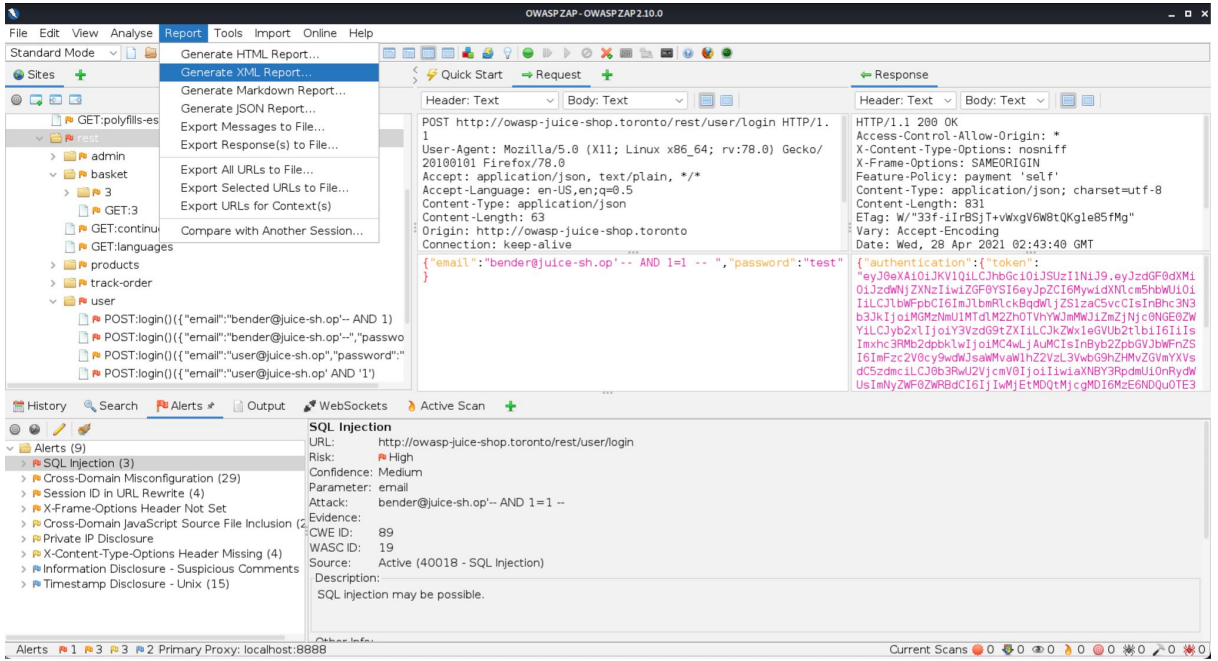


Exercise 8: Active Scan



Exercise 9: Export results

Exercise 9: Export results

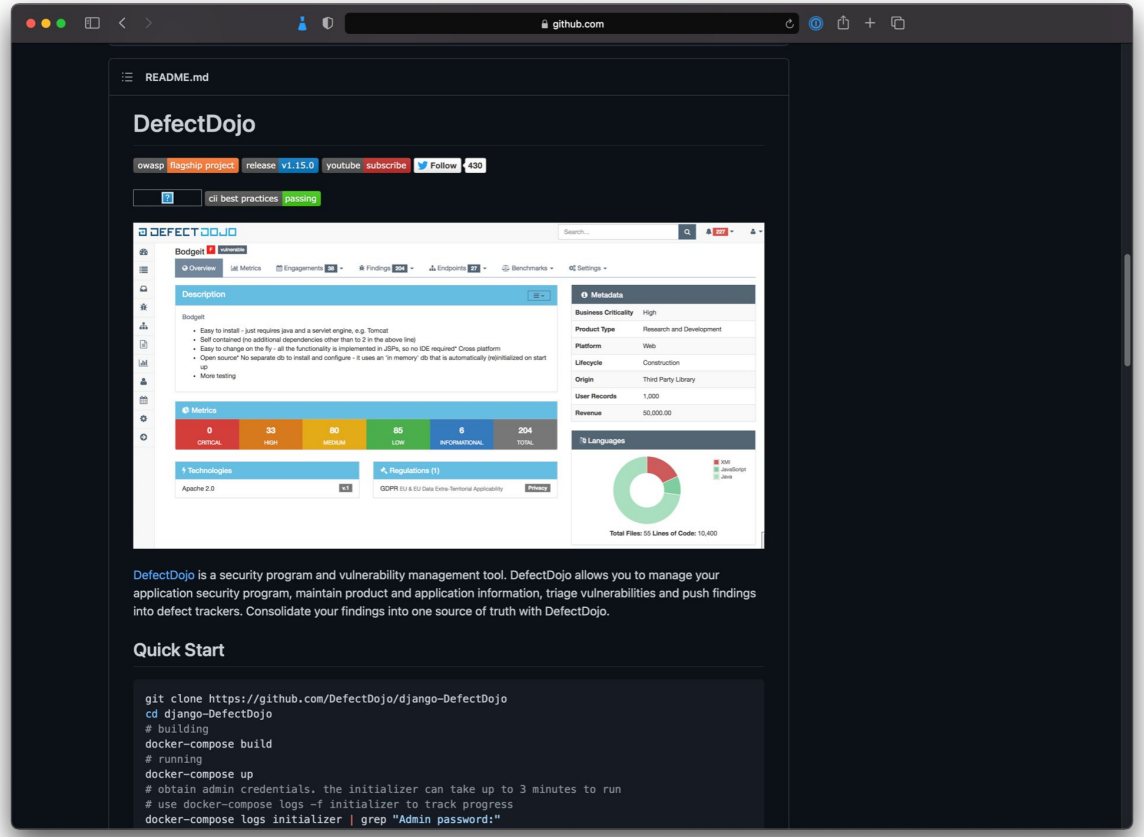


Exercise 10: OWASP DefectDojo

OWASP DefectDojo

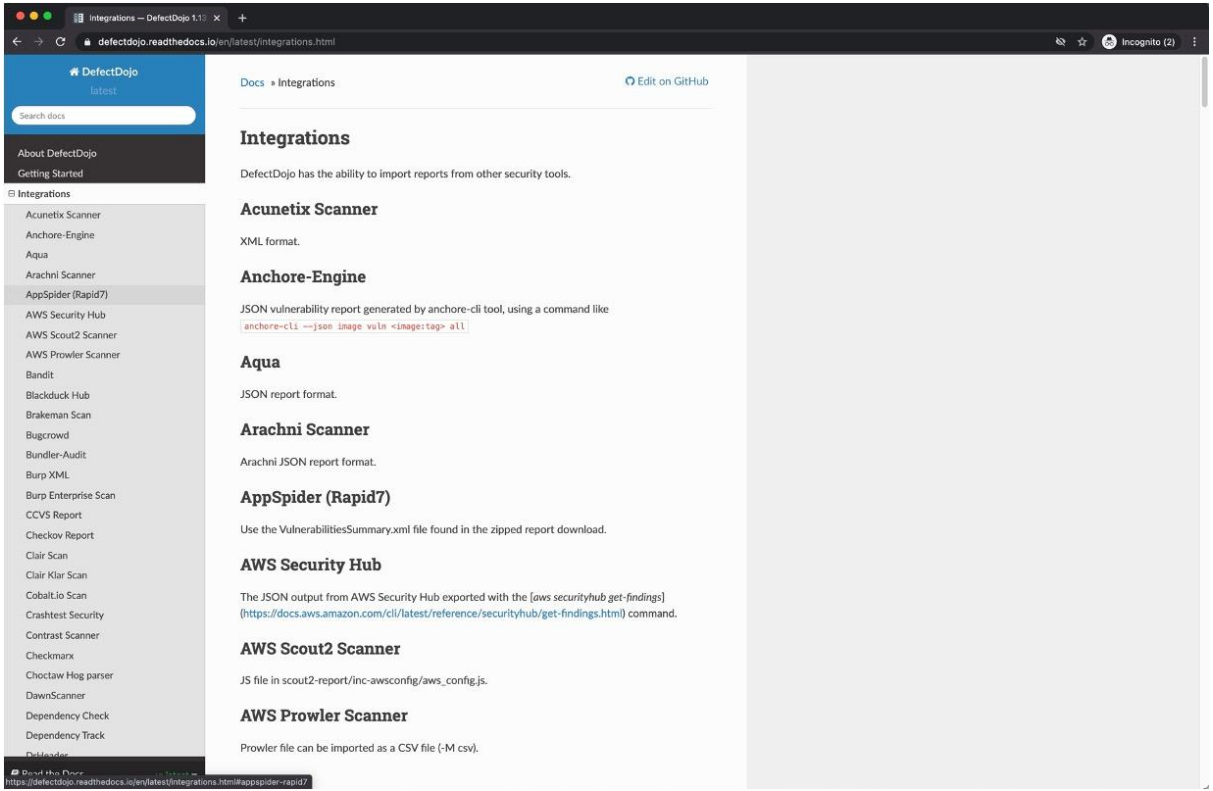
1. DefectDojo is another tool-based OWASP flagship project
2. Open source security program, application vulnerability management and correlation, and security orchestration tool
3. Enables and streamlines application security testing process
4. CI/CD automation and tracking

DefectDojo Website & GitHub

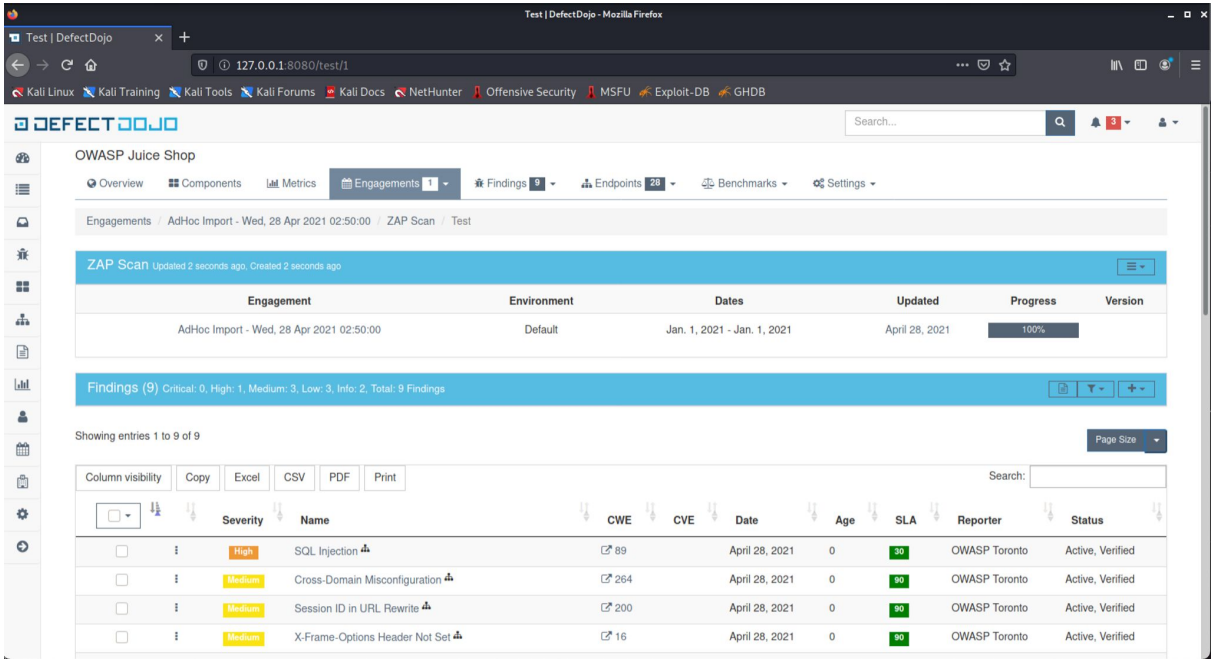


https://owasp.org/www-project-defectdojo/
https://github.com/DefectDojo/django-DefectDojo

DefectDojo integrations



DefectDojo with ZAP results



Questions?

Yuk Fai Chan
OWASP Toronto
yukfai.chan@owasp.org