Title ：Login Bypass Attempt via SQL Injection

Description

The login functionality of the OWASP Juice Shop application does not properly handle malicious input. During testing, a classic SQL Injection payload was supplied in the login request. Although the payload did not result in a fully authenticated session, the application redirected the user to the product listing page without valid credentials.

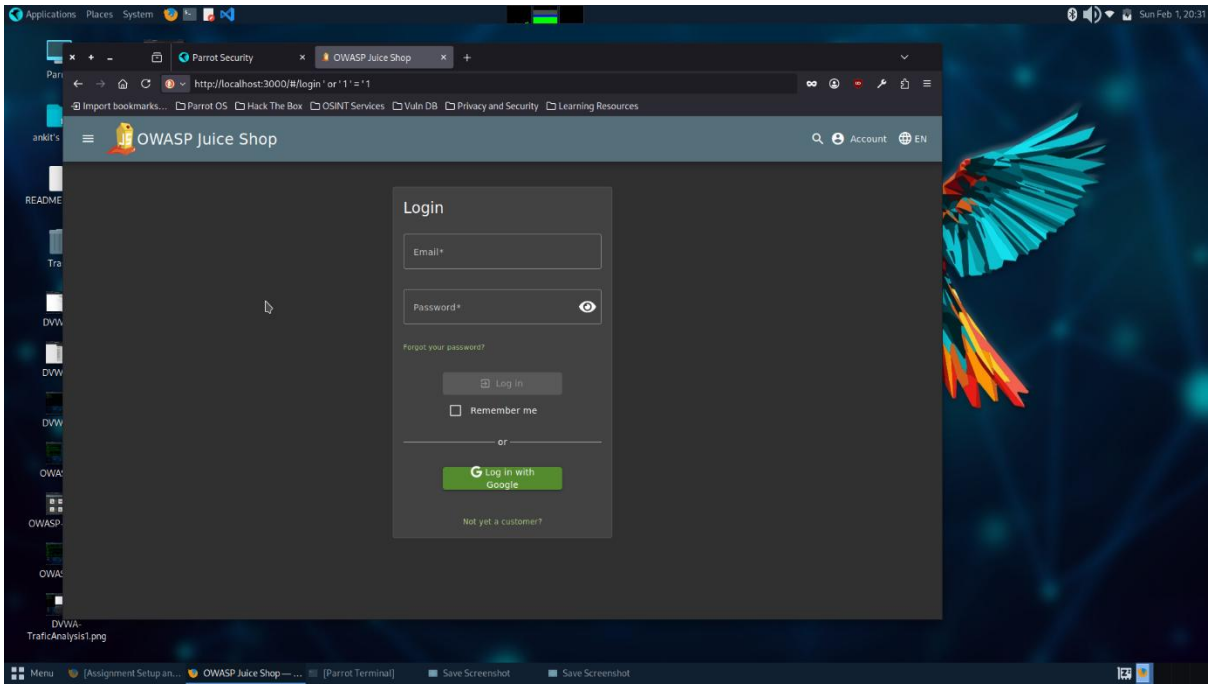
This behavior indicates a weakness in authentication logic and improper validation of login responses.

Impact

- Unauthorized users may gain unintended access to application resources
- Authentication flow can be abused or bypassed
- In real-world applications, this could lead to account takeover or privilege escalation

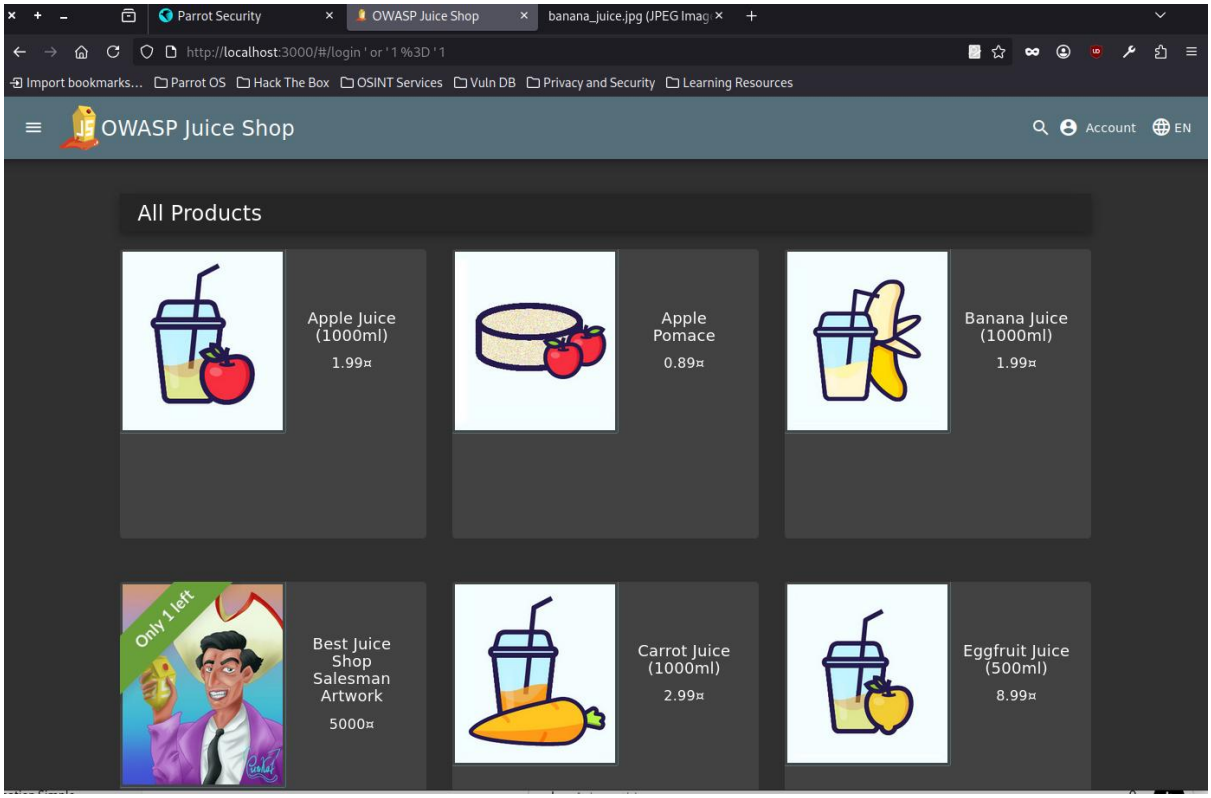
Evidence

- SQL Injection payload used:



Evidence

- SQL Injection payload used in login request:
- ' OR '1'='1
- URL tested:
- http://localhost:3000/rest/user/login
- Application redirected to the product listing page despite invalid credentials
- Screenshot attached showing redirection after injection attempt
- HTTP request captured using browser developer tools


Parrot Security
OWASP Juice Shop
banana_juice.jpg (JPEG Imag
http://localhost:3000/#/login ' or ' 1 %3D ' 1
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
OWASP Juice Shop
Account
EN
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤
Only 1 left
Best Juice Shop Salesman Artwork
5000¤
Carrot Juice (1000ml)
2.99¤
Eggfruit Juice (500ml)
8.99¤