

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.

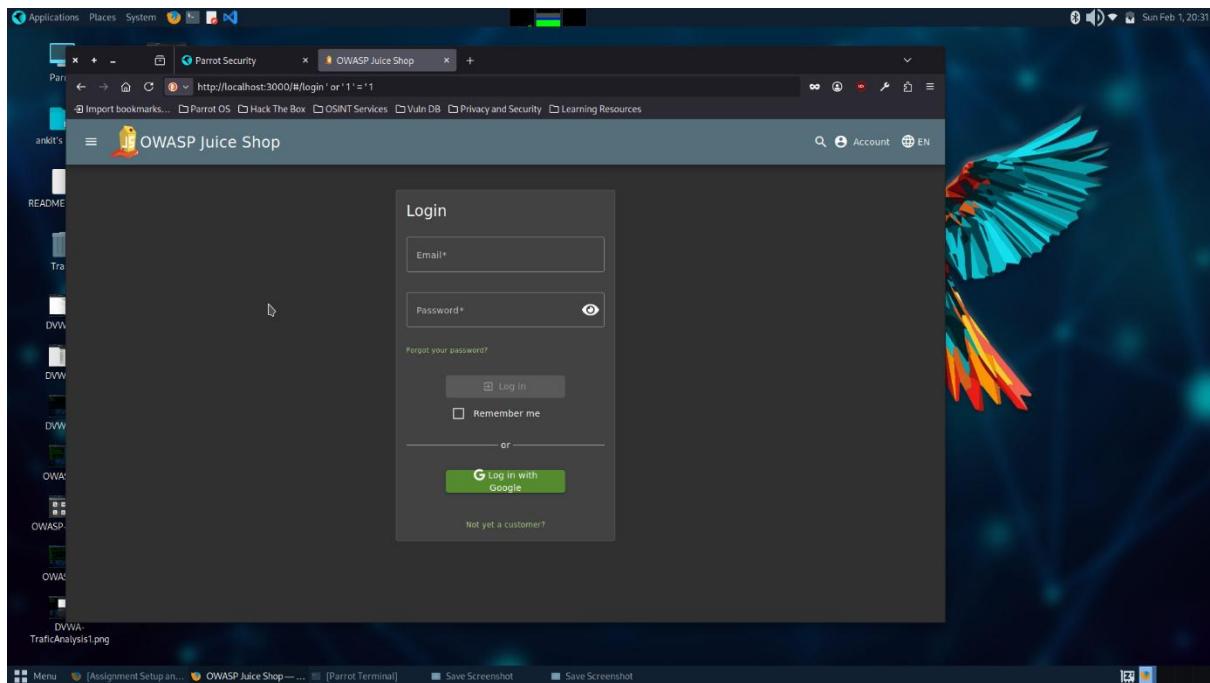
This behavior indicates a weakness in authentication logic and improper validation of login responses.

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

A screenshot of a web browser showing the OWASP Juice Shop application. The title bar indicates the page is "banana_juice.jpg (JPEG Image)". The address bar shows the URL "http://localhost:3000/#/login' or '1%3D'1". The navigation bar includes links for "Import bookmarks...", "Parrot OS", "Hack The Box", "OSINT Services", "Vuln DB", "Privacy and Security", and "Learning Resources". The top right corner shows account information and language settings ("Account EN").

The main content area displays a grid of products under the heading "All Products". There are six items visible:

- Apple Juice (1000ml)**: Price 1.99¤. Image shows a juice glass and an apple.
- Apple Pomace**: Price 0.89¤. Image shows a juicer with apples.
- Banana Juicce (1000ml)**: Price 1.99¤. Image shows a juice glass and a banana.
- Best Juice Shop Salesman Artwork**: Price 5000¤. Image shows a cartoon salesman holding a juice glass, with a green overlay that says "Only 1 left".
- Carrot Juice (1000ml)**: Price 2.99¤. Image shows a juice glass and a carrot.
- Eggfruit Juice (500ml)**: Price 8.99¤. Image shows a juice glass and an eggplant.