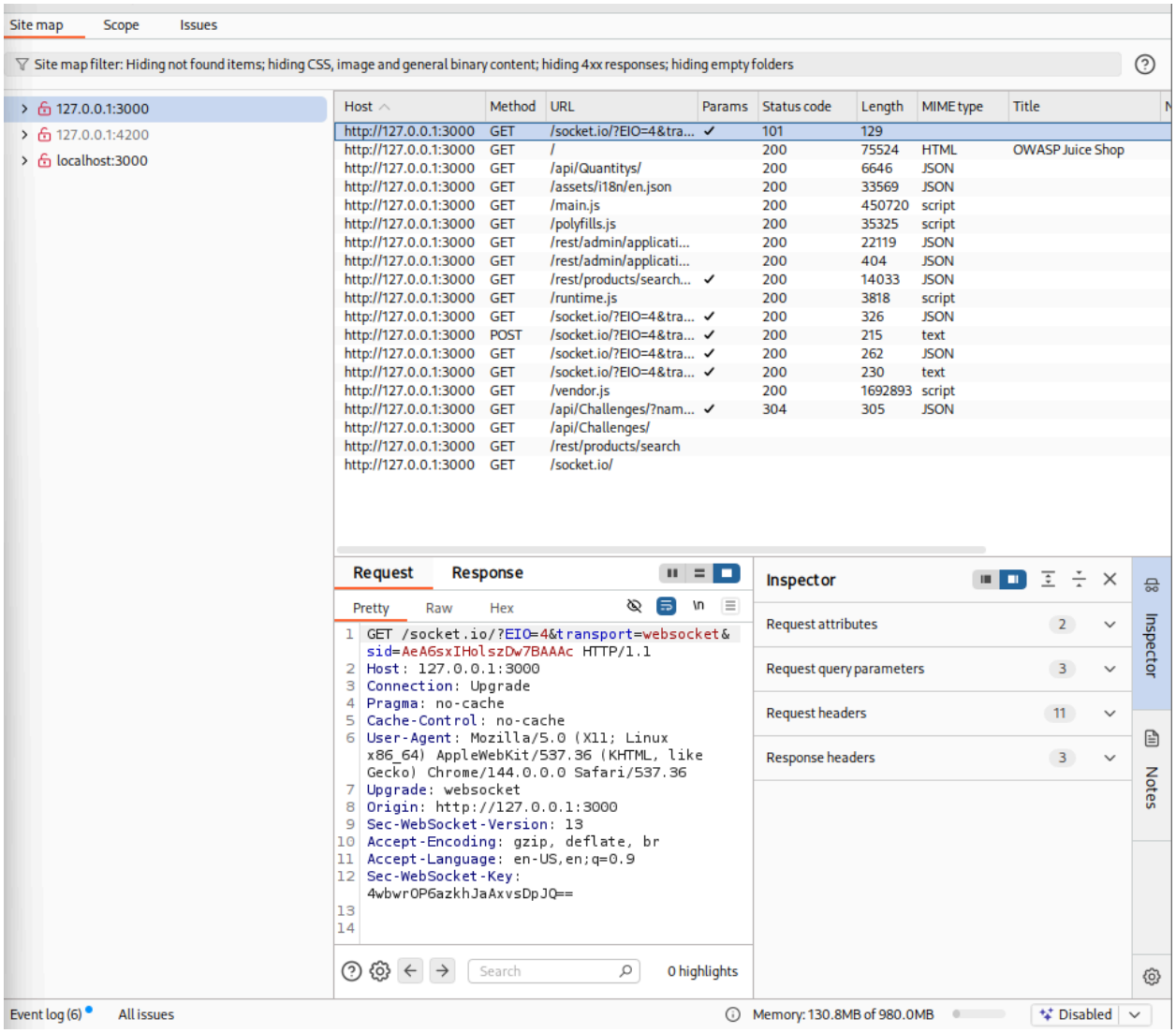
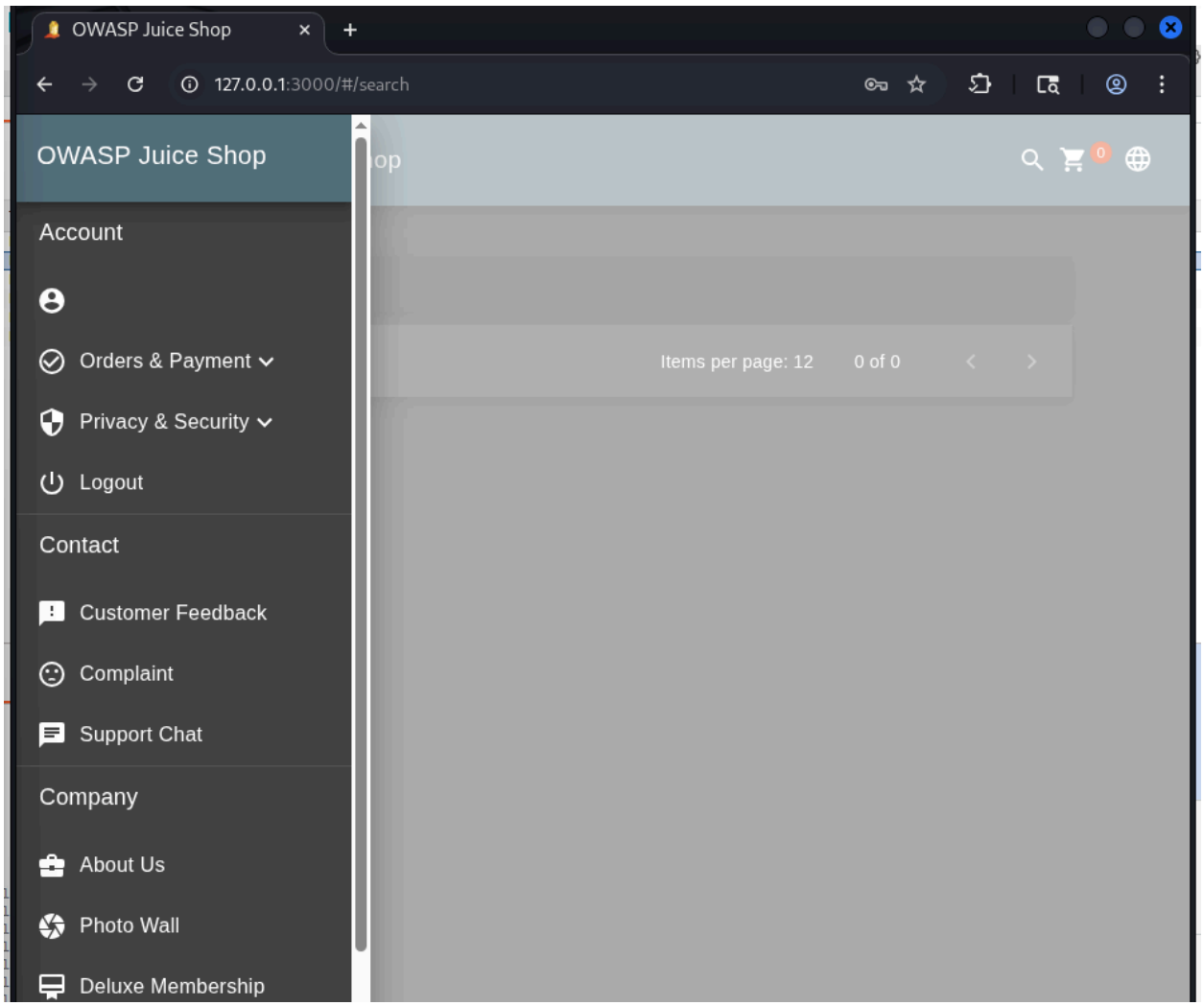
Task 1



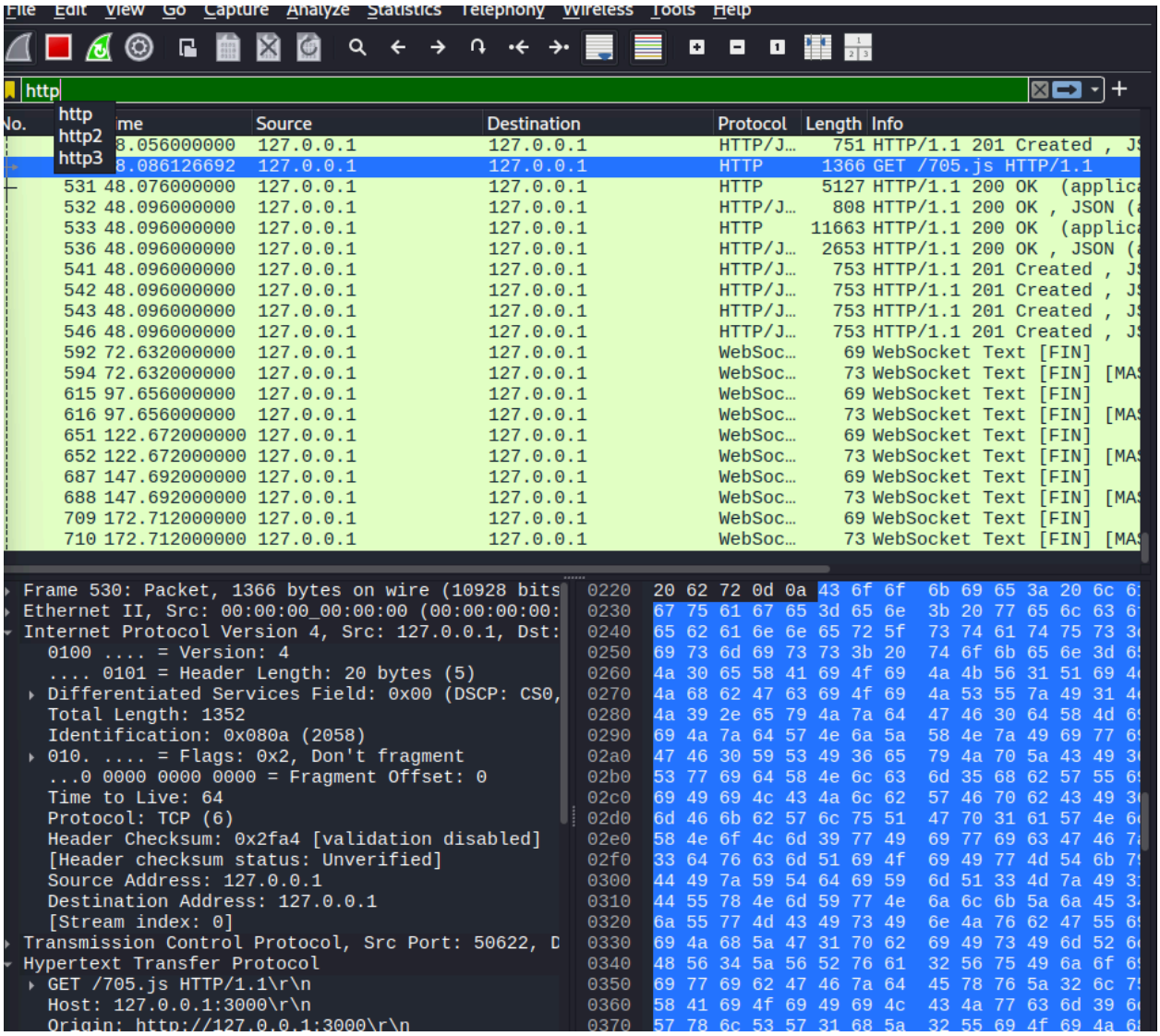
Hidden paths can tell an attacker what services exist, application architecture, technologies used and give information on where to focus an attack. Authentication exists but APIs may not enforce it properly, some endpoints (unused or outdated/old) may skip auth check

Task 2



The input ' OR 1=1 -- alters the SQL logic by forcing the authentication condition to always evaluate as true and commenting out the remaining checks. As a result, the database returns a user record regardless of credentials, causing the application to treat the login as successful.

Task 3



Without HTTPS, attackers could extract credentials, session cookies, personal data, and application endpoints from plaintext HTTP traffic, enabling account hijacking, privacy breaches, and further targeted attacks.

Reflection

The vulnerabilities demonstrated in this lab closely reflect techniques used by real-world cyberattackers. Information disclosure through exposed paths and metadata allows attackers to map applications and identify weak points without authentication, often serves as the first step in an attack chain. SQL injection demonstrates how improper input handling can directly compromise authentication mechanisms and lead

to unauthorized access or data breaches. Observing plaintext network traffic highlights how lack of encryption enables credential theft and session hijacking exploited together rather than in isolation, increasing the overall impact and potential danger of an attack