Week 1: Security Assessment – Summary

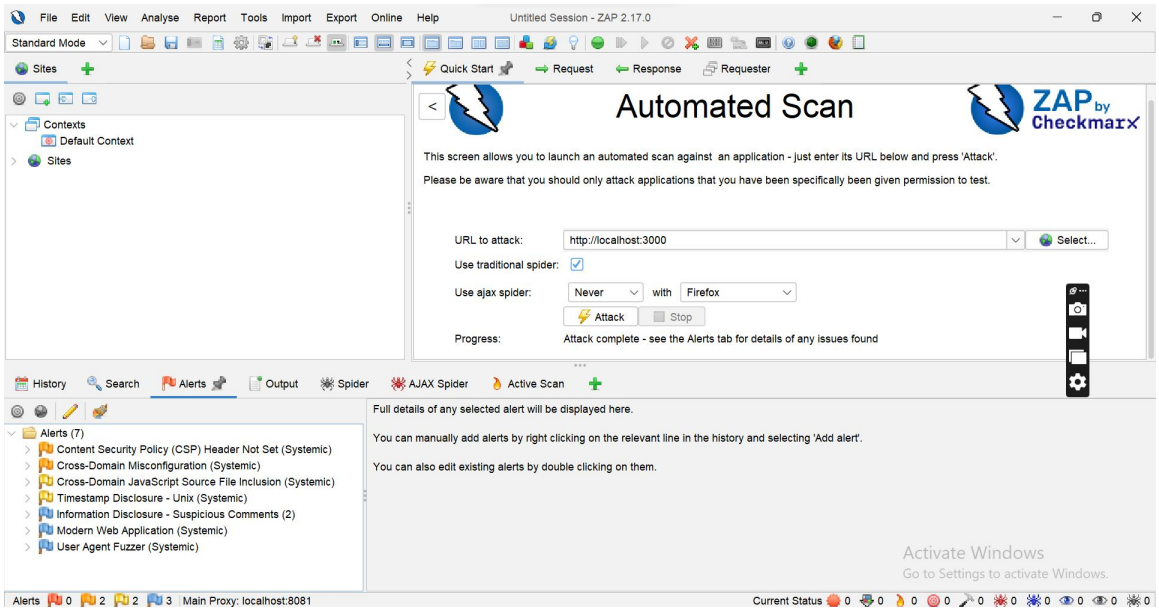
Vulnerabilities Found

- Cross-Site Scripting (XSS): User inputs were accepted without proper sanitization, allowing script injection.
- Weak Input Validation: Server-side validation was insufficient, enabling malformed data submission.
- Insecure Password Handling: Passwords were not adequately protected using strong hashing mechanisms.
- Missing Security Headers: HTTP security headers such as CSP and X-Frame-Options were not properly configured.
- Authentication Weakness: Login mechanisms lacked protection against common authentication attacks.

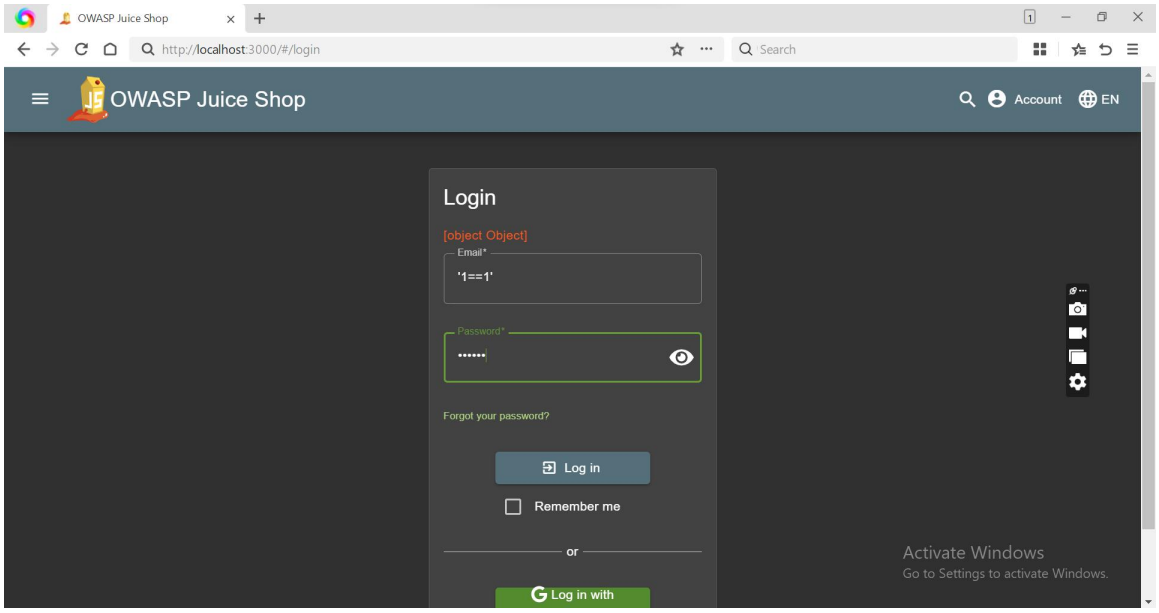
Areas of Improvement

- Input Validation: Implement strict server-side validation and sanitization for all user inputs.
- Password Security: Hash and salt passwords using secure algorithms such as bcrypt.
- Authentication Control: Introduce token-based authentication to strengthen user verification.
- Secure Configuration: Apply security headers using middleware like Helmet.
- Monitoring and Logging: Enable logging to track security events and suspicious activity.

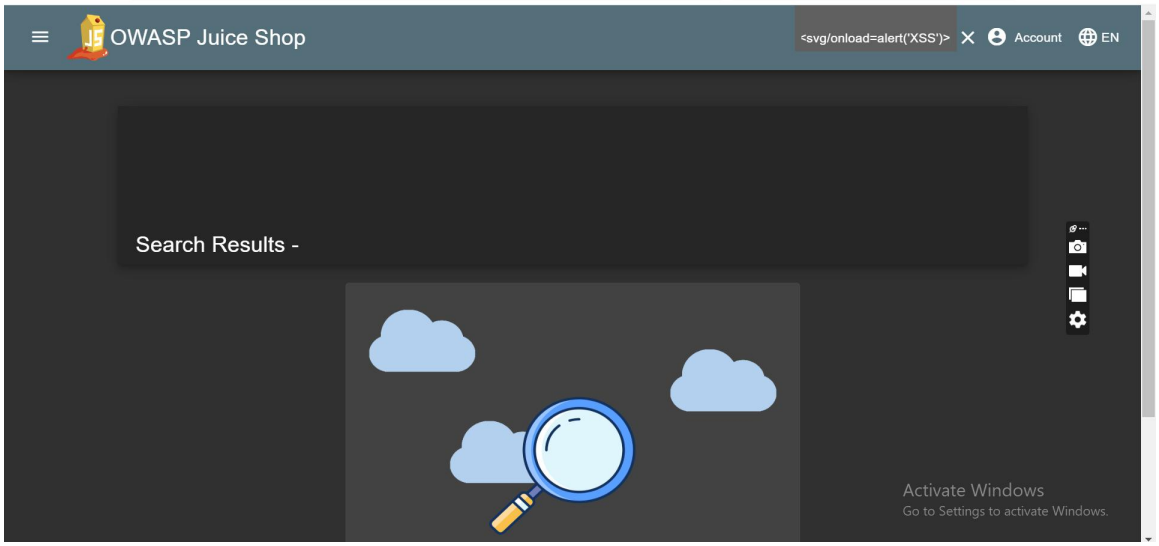
Some vulnerabilities detection screenshots are mentioned below:

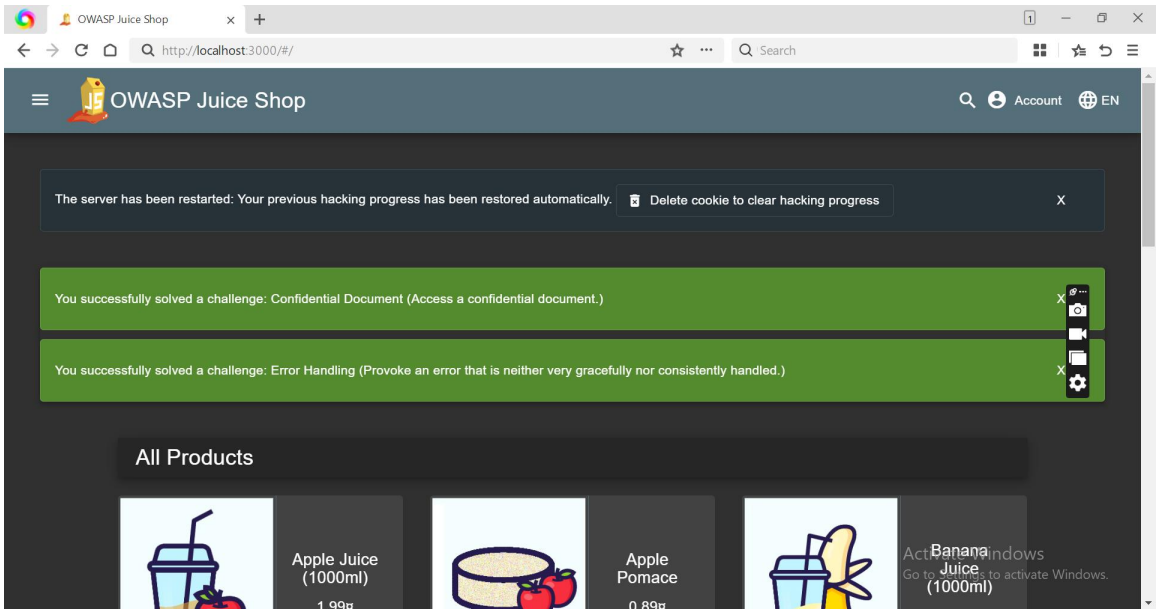


Using Owasp Zap I am being able to find the vulnerabilities in the web application which I get from GitHub which is OWASP JUICE.
There were 7 alerts detected which are clearly shown in the screenshots.

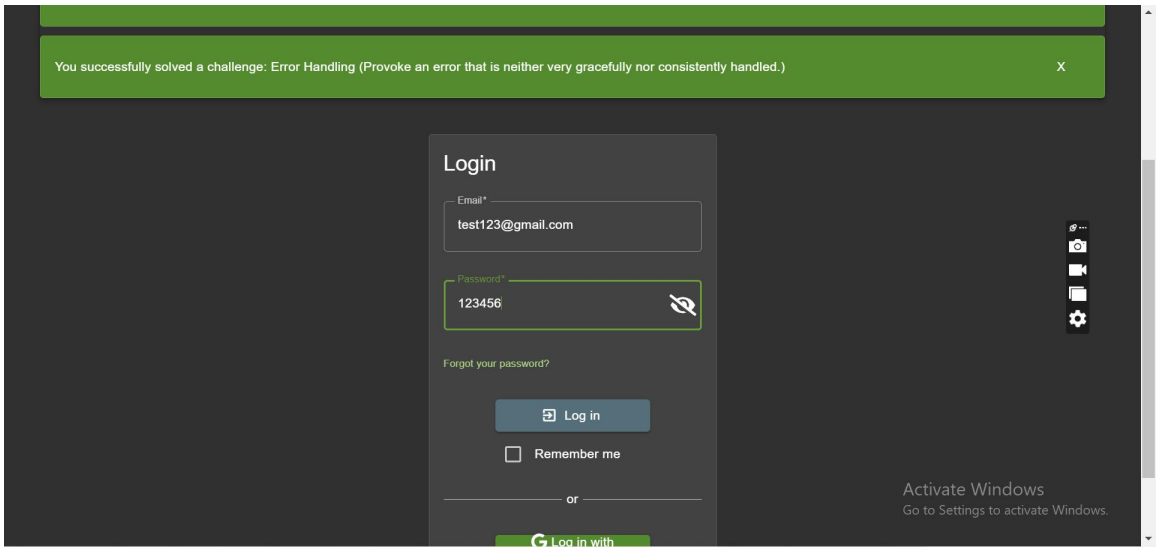


Here I am being able to detect sql injection attack vulnerability as after injecting '1==1' its showing object object which means that the injections is successful but is not logging in due to some database errors





Here I have applied XSS vulnerability testing which clearly shows that something fishy is there.



Here I also have shown that there is a weakness that it is accepting weaker passwords which are easily be able to be exploited by the hackers and can be easily attacked by the hacking communities.
I have registered my account with 123456 password and now I am going to login which will easily be let me login in the account.