

Week 1: Security Assessment – Summary

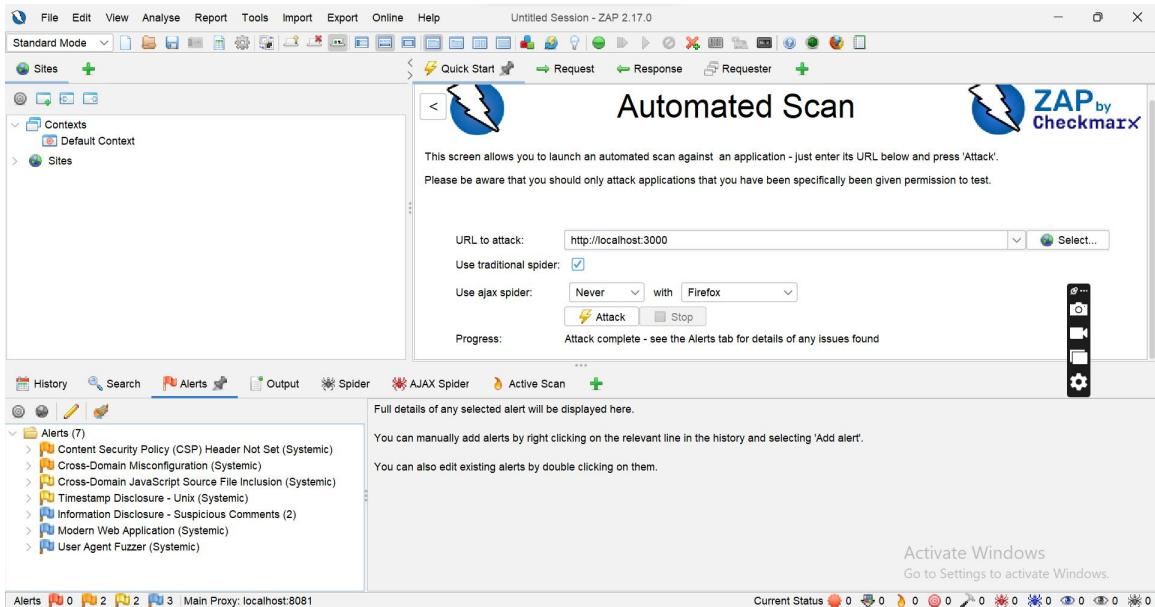
Vulnerabilities Found

- 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.

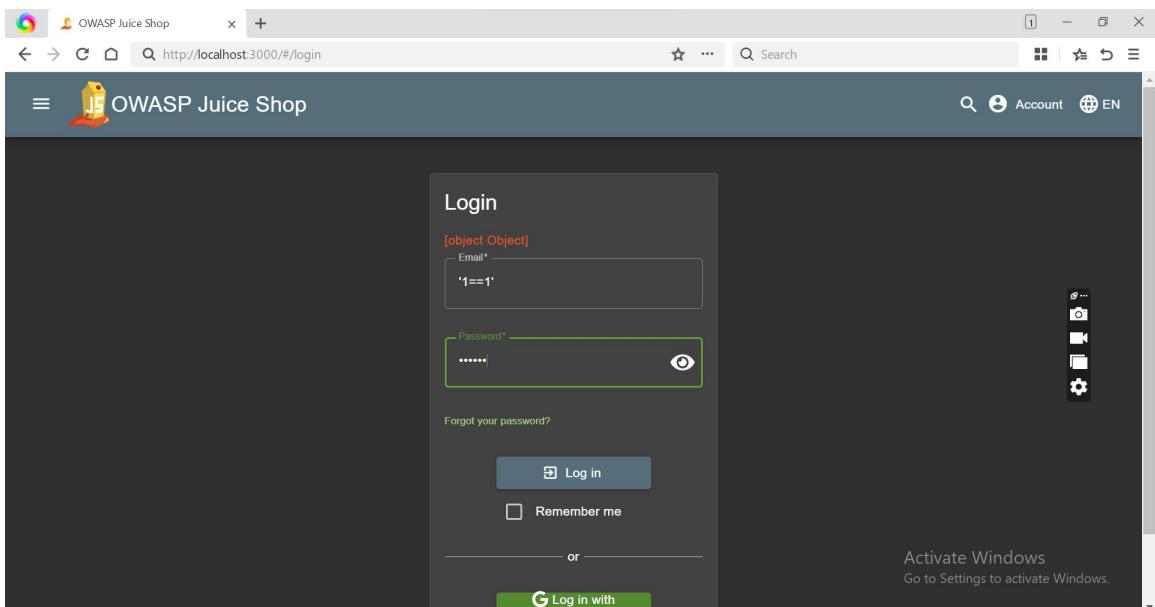
Areas of Improvement

- 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.

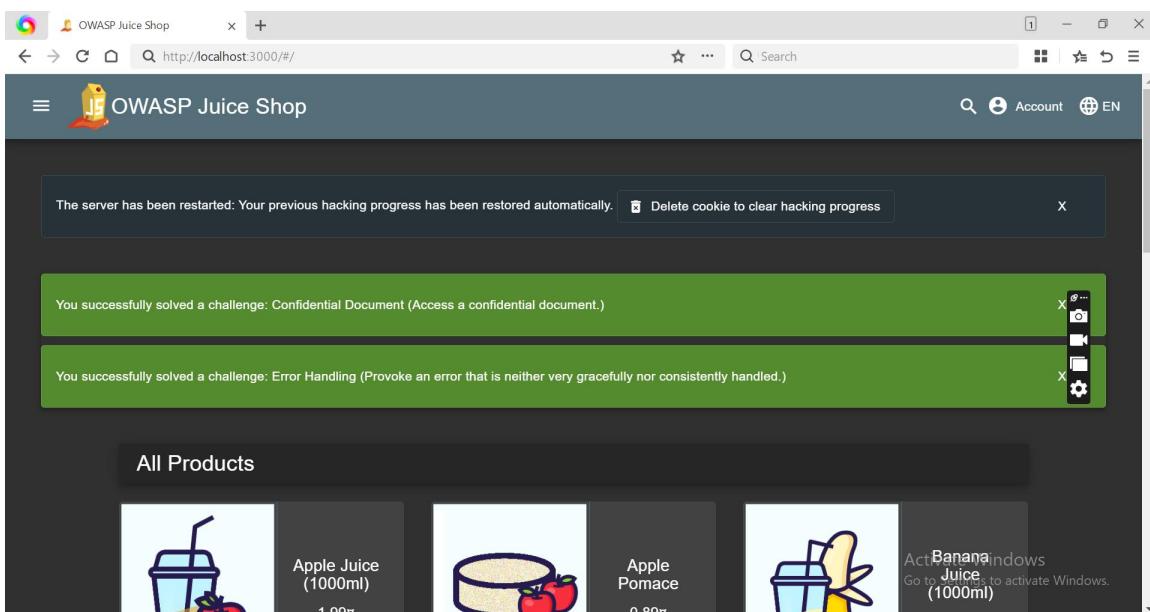
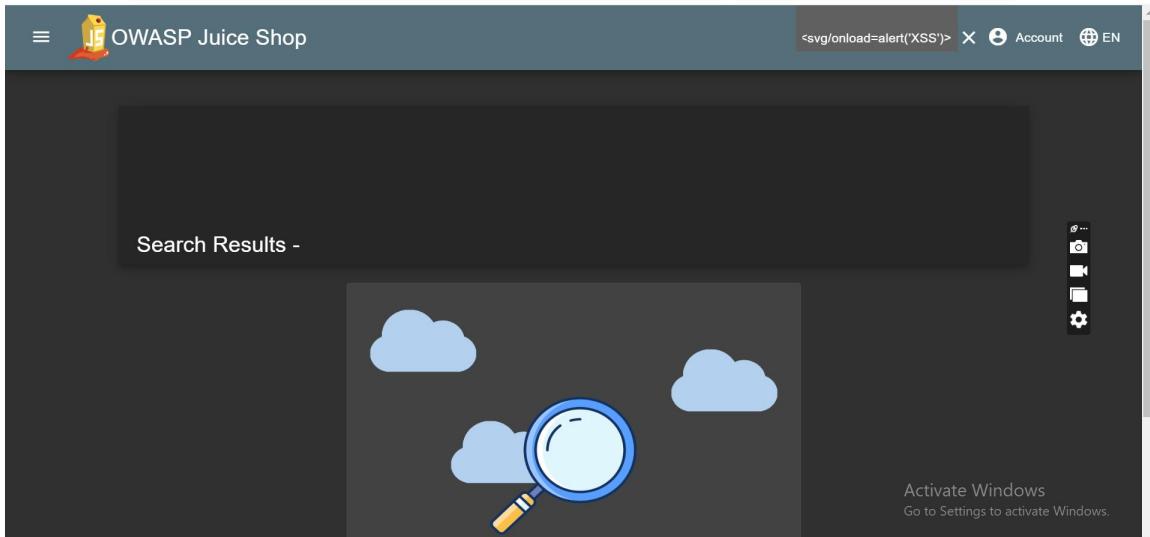
Some vulnerabilities detection screenshots are mentioned below:



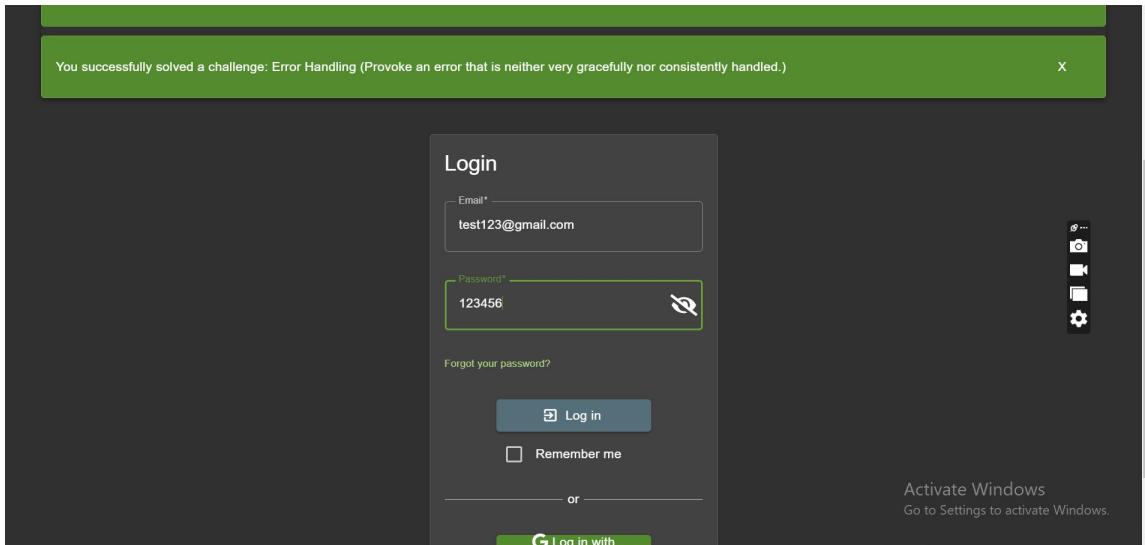
Using Owasp Zap I am being able to find the vulnerabilities in the web application which I get from GitHub which is OWASP JUICE.
There were 7 alerts detected which are clearly shown in the screenshots.



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.

A screenshot of the OWASP Juice Shop application. At the top, the header includes the logo, the name "OWASP Juice Shop", a search bar, an "Account" link with a notification count of 0, a "Your Basket" link, and language selection ("EN"). A user menu is open, showing options: "test123@gmail.com", "Orders & Payment", "Privacy & Security", and "Logout". The main content area shows two green banners: "The server has been restarted: Your previous hacking progress has been restored automatically." and "You successfully solved a challenge: Confidential Document (Access a confidential document.)". Below these, another banner says "You successfully solved a challenge: Error Handling (Provoked an error that is neither very gracefully nor consistently handled.)". The "All Products" section displays five items: "Apple Juice (1000ml)" for 1.99\$, "Apple Pomace" for 0.89\$, and "Banana Juice (1000ml)" for 1.99\$. There is also a "Activate Windows" section with the text "Go to Settings to activate Windows".