**✅ Week 4 Project Testing Summary (SmartGlass Project)**

1. Vulnerability Scanning:

- Performed final security scan on production environment using:

• OWASP ZAP (automated scan)

• Burp Suite (manual test)

- Identified potential risks such as:

• Insecure cookies (ZAP)

• Missing X-Frame-Options header

• Weak CORS policy (Burp)

2. Security Policy Checks:

- Verified that:

• JWT tokens are being used for authentication

• Firebase Auth correctly enforces login & logout sessions

• MongoDB database access is protected via environment config

- Checked `.env` configuration is not exposed in client code

3. API & Backend Tests:

- Used Postman to verify APIs:

• Login and Register endpoints return correct status codes

• AI model endpoint (if working) returns expected output

• Error handling on invalid tokens or missing fields tested

4. Improvements Suggested:

- Add rate limiting to prevent brute force login attacks

- Enable HTTPS for secure transmission

- Add helmet.js or security headers to Express backend

- Sanitize and validate all input (backend)

5. Screenshot Summary:

- `zap-scan.png` → ZAP vulnerability report

- `burp-scan.png` → Burp Suite intercepted requests

- `postman-tests.png` → Sample Postman API test

- `login-error.png` → Screenshot of Firebase 404 login bug (fixed)