Week 3: Advanced Security and Final Reporting

1. Nmap Basic Penetration Testing

In the last stage of the project, I performed basic penetration testing with Nmap to assess the exposure and vulnerability of the application to threats at the network level. The emphasis was placed on open ports, active services, and confirmation of the local development environment's configuration.

Most Important Activities:

Scanned particular application port (3000) to check if only anticipated services were available.

Scanned for open common ports such as SSH (22), HTTP (80), and HTTPS (443) to make sure there were no unnecessary services active.

Conducted OS detection and version scanning to mimic an attacker attempting to collect system and service information.

Executed aggressive and stealth scans to determine how the application reacts under possible reconnaissance or intrusions.

The scans found no critical flaws. Only the anticipated ports were open, and sensitive service details were not leaked. These tests ensured that the security settings implemented (e.g., restricted access to ports, service hardening) successfully reduced the attack surface.

2. Logging and Monitoring

To provide more insight into user and system behavior, I enforced structured logging via a logging library. This enabled more complete tracking of authentication attempts and potential security incidents.

Key Activities:

Logged login attempts, both successful and failed, to detect abnormal activity.

Logged error messages, especially on authentication failures, to support debugging and incident containment.

Preserved logs in the console as well as in a separate log file, guaranteeing long-term access to historical information.

Outcome:

This logging configuration greatly enhances monitoring capacity and forms a basis for intrusion detection and forensic analysis in case of abnormal activity.

3. Security Best Practices Checklist

As a result of the hands-on security work done during the internship, the following is a customized security checklist based on the actual steps taken:

- Only required ports (such as 3000) are exposed, minimizing the attack surface.
- All incoming data is subject to input validation to avoid injection attacks and malformed input.
- Login attempts are logged to help identify brute-force attacks or strange login patterns.
- Error logging is used to aid in debugging and audit trails.
- Logs are stored in files, so they can be analyzed later on.
- There is no extraneous system or server version information revealed during scans.