PROJECT REPORT

Name Sudhir S Bhat

Title: Web Application Security Basics Practical Awareness of OWASP Top 10

1. Project Overview

Web applications are the backbone of modern digital businesses, but they are also one of the most targeted attack surfaces. As a intern, this project helped me understand **how web application attacks happen**, why they succeed, and **how organizations can reduce risk** using the **OWASP Top 10** framework.

Rather than performing exploitation, this project focuses on **practical security awareness**, **risk understanding**, and **defensive thinking**, which are critical for entry-level roles.

2. Objective of the Project

- To understand the **OWASP Top 10 Web Application Risks**
- To learn **how insecure design leads to real-world breaches**
- To identify common **developer and configuration mistakes**
- To build a **security-first mindset** as a fresher intern
- To document findings in a **professional, industry-ready format**

3. Why Web Application Security Matters

Most cyber attacks today do not rely on advanced malware — they exploit

- Weak authentication
- Poor access control
- Input validation failures
- Misconfigured servers

A single vulnerable web application can lead to

- Data breaches
- Account takeovers

- Financial fraud
- Reputation loss

According to industry reports, **over 70% of breaches originate from web-layer attacks**, making OWASP Top 10 knowledge a baseline requirement for security roles.

4. OWASP Top 10 – Practical Awareness

4.1. Broken Access Control

- Occurs when users can access resources they shouldn't.

Example

- A normal user accessing /admin pages by changing the URL.

Impact

- Privilege escalation, data exposure.

4.2. Cryptographic Failures

- Sensitive data is not properly protected.

Example

- Passwords stored without hashing.

Impact

- Credential theft, identity compromise.

4.3. Injection

- Untrusted input is interpreted as commands.

Example

- User input altering database queries.

Impact

- Data leakage, system compromise.

4.4. Insecure Design

- Security is not considered during application planning.

Example

- No rate-limiting on login attempts.

Impact

- Brute-force attacks, abuse.

4.5. Security Misconfiguration

- Default or unsafe configurations.

Example

- Debug mode enabled in production.

Impact

- Information disclosure.

4.6. Vulnerable & Outdated Components

- Using old libraries with known flaws.

Impact

- Attackers reuse public exploits.

4.7. Identification & Authentication Failures

- Weak password policies or session handling.

Impact

- Account takeover.

4.8. Software & Data Integrity Failures

- Untrusted updates or code.

4.9. Logging & Monitoring Failures

- Attacks go unnoticed.

Impact

- Delayed response, greater damage.

4.10. Server-Side Request Forgery (SSRF)

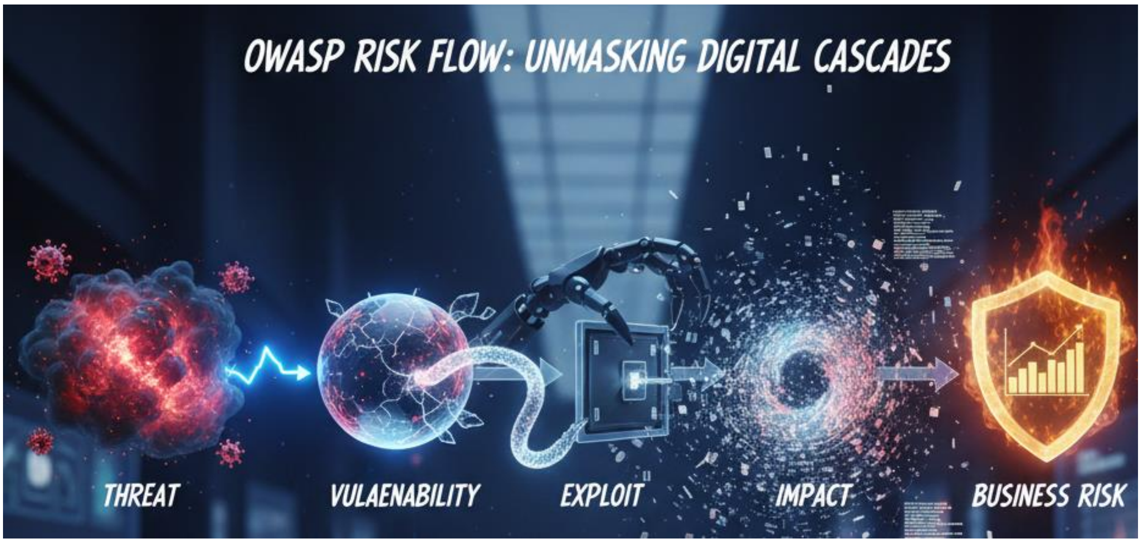
- Server makes unintended requests.

Diagrams

Web Application Architecture

WEB APPLICATION ARCHITECTURE:
INNOVATION IN CONNECTIVITY
WEB SERVER
BROWSER
APPLICATION LOGIC
DATABASE
2026
2026

OWASP Risk Flow



Secure Authentication Flow

SECURE AUTHENICTATION FLOW: THE DIGITAL GAUNTLET
LOGIN
MFA
USER
LOGIN
MFA
ACCESS VALIDATION

5. Outcomes

- Strong understanding of OWASP Top 10 risks
- Improved ability to **think like a defender**
- Learned how attackers exploit design flaws
- Developed professional security documentation skills

6. Lessons Learned

- Most attacks succeed due to **basic mistakes**
- Security is not just technical — it's **design + process**
- Logging and monitoring are as important as prevention
- Awareness can prevent more incidents than tools alone

7. Challenges Faced

- Translating theory into real-world scenarios
- Understanding technical terms without hands-on exploitation
- Structuring a professional security report
- Learning to think from an attacker’s perspective safely

8. Conclusion

This project helped me build a solid foundation in **web application security awareness** using the OWASP Top 10 framework. As a intern, it strengthened my analytical thinking, documentation skills, and understanding of how real-world web attacks impact organizations.