Web Application Security Basics

Objective

The objective of this task is to understand the fundamentals of **web application security**, identify common vulnerabilities, and demonstrate how they can impact real-world applications if not mitigated properly.

Concepts

- Web application architecture
- Client–Server interaction
- Common web vulnerabilities (OWASP Top 10 overview)

Tools Used

- Web Browser (Chrome / Firefox)
- OWASP WebGoat / DVWA (for learning purpose)
- Burp Suite Community Edition
- Online OWASP Documentation

---

1. **SQL Injection** – Manipulating database queries via user input
2. **Cross-Site Scripting (XSS)** – Injecting malicious scripts into web pages
3. **Broken Authentication** – Weak login/session handling
4. **Security Misconfiguration** – Default credentials, open directories

---

- Unsanitized user input can directly lead to data breaches
- Lack of proper authentication mechanisms increases attack surface
- Simple validation and secure coding practices can prevent most attacks

---

Mitigation Techniques

- Input validation and parameterized queries

- Use of HTTPS
- Secure session handling
- Regular vulnerability testing

Web application interface
Example of vulnerable input field
Burp Suite intercepting requests
OWASP reference page

Conclusion

Web application security is a critical component of modern development. Understanding basic vulnerabilities helps developers and security professionals build safer and more resilient applications.