Blog 4: Web Application Penetration Testing – Securing the Online Realm

"Web applications are the doors to your kingdom. Guard them well." – Anonymous

With the internet becoming the core of business operations, web applications are prime targets for cyberattacks. Web Application Penetration Testing (WAPT) is a method of evaluating the security of a web app by simulating an attack.

What WAPT Involves

- **Reconnaissance**: Gathering information about the target
- **Enumeration**: Mapping the web application and its inputs
- **Exploitation**: Attempting to exploit vulnerabilities such as SQL injection, XSS, CSRF, etc.

Common Vulnerabilities

- **Injection Flaws**
- **Broken Authentication**
- **Sensitive Data Exposure**
- **Security Misconfiguration**

Methodologies

- **OWASP Top 10**: A foundational framework for identifying the most critical web vulnerabilities
- **Burp Suite**: The Swiss Army knife of web pentesting
- **Nikto**: Web server scanner for identifying vulnerabilities

Reporting & Remediation

Effective reporting includes:

- Risk rating
- Steps to reproduce
- Recommendations for fixing the vulnerability

References:

- OWASP Top 10
- Burp Suite