Introduction

- Web applications are a part of our life, either as part of our vocation or in order to access our email, view a news item of interest, etc.
- Web applications become main threat to secrecy and integrity of company’s sensitive data.
- OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate and maintain applications that can be trusted.
- The OWASP Top Ten is a powerful awareness document for web application security. It represents a broad consensus about what the most critical web application security flaws are.

Methodology

- **Introduction**: A description of each threat, a definition and some statistics about it.
- **Types of Attacks**: Main attack methods and their subcategories, using Web Hacking Incident Database (WHID) which has real life examples and new entries for many attack methods.
- **Detection**: Detection methods and tools, emphasizing to the most important ones.
- **Prevention**: Prevention techniques and tools separately for every attack, examining the more suitable way to prevent the attacker from being harmful.

**Figure 1: Comparison of OWASP Top Ten Entries**

**Figure 2: Variety of hacking actions within Web**

Main attack methods

- SQL Injection
- Cross Site Scripting (XSS)
- Phishing attack
- Brute force attack
- Path traversal

Detection & Prevention methods

- Web Application Firewall
- Intrusion Detection System (IDS)
- Data Encryption
- Password Hashing
- Security Awareness of Users
- Penetration Testing

References