Spring Security

Beginner to Guru

Common Web Vulnerabilities

Common Web Vulnerabilities

- OWASP - Open Web Application Security Project - https://owasp.org
  - Nonprofit organization working to improve the security of software
  - Provides:
    - Tools and Resources
    - Community and Networking
    - Education and Training
- OWASP Top 10 Web Application Security Risks

OWASP Top 10 Web Application Security Risks

1. **Injection** - Injection of malicious code, such as SQL Injection attacks
   - Mitigation typically using proper encoding and bind variables
2. **Broken Authentication** - Authentication and session management implemented incorrectly
   - Mitigation - Use framework, don't roll your own
3. **Sensitive Data Exposure** - Not protecting sensitive data
   - Mitigation - Proper error handling, don't expose stack traces

OWASP Top 10 Web Application Security Risks

4. **XML External Entities**- Poorly Configured XML Processors
   - Mitigation - Patch XML Processors frequently
5. **Broken Access Control** - User Restrictions not properly enforced
   - Mitigation - Automated Testing, verify restrictions
6. **Security Misconfiguration** - Unintentionally not protecting resources
   - Mitigation - Security Audits

OWASP Top 10 Web Application Security Risks

7. **CrossSite Scripting** - XSS Allows Users to inject HTML or Javascript
   - Mitigation - Use proper validation and escaping
8. **Insecure Deserialization** - Insecure deserialization can allow remote code execution
   - Mitigation - Use open source, patch frequently
9. **Using Components with Known Vulnerabilities** - Popular components often have known vulnerabilities
   - Mitigation - Patch frequently

OWASP Top 10 Web Application Security Risks

10. **Insufficient Logging & Monitoring** - Time to detect breaches often over 200 days
    - Mitigation - Properly monitor systems
- Further information available on OWASP
    - Highly recommended reviewing

Spring Security for Common Vulnerabilities

- Spring Security has built in support to address several common vulnerabilities
  - Cross-site Scripting (XSS)
  - Cross-Site Request Forgery (CSRF)
  - Security HTTP Response Headers
    - Variety of headers can be set to improve browser security
  - Redirect to HTTPS

SPRING FRAMEWORK

GURU