
# Hamarosan kezdünk...

Biztonságos programozás haladóknak

Peter Veres
peter_veres2@epam.com

2016

# Biztonságos programozás haladóknak 13. nap

**Peter Veres**
**peter_veres2@epam.com**

2016


Java Security
OWASP TOP 10
Superdry

# OWASP

OWASP
Open Web Application Security Project

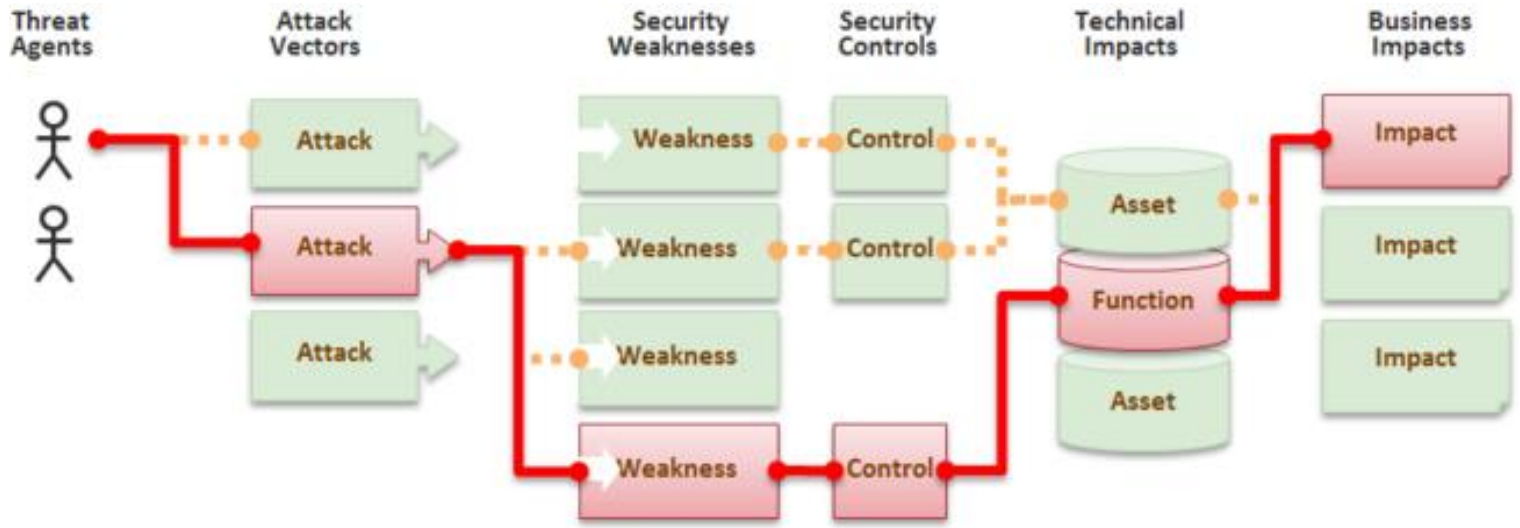
- Open Web Application Security Project
  - Worldwide not-for-profit charitable organization focused on improving the security of software
  - an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted
- www.owasp.org

# OWASP Top 10

OWASP
Open Web Application Security Project

- Raise awareness about application security by identifying some of the most critical risks facing organizations
- First released in 2003
- Current version released in 2013
- Can be used by organizations started with security

# Application Security Risk



# OWASP Top 10 - 2013 (Current Version)


Java Security
SPRING SECURITY
Superdry

# What is Spring Security?

- Integrated with Servlet API
- Integrated with Spring MVC
- Provides solutions to protect against hacker attacks (session fixation, CSRF etc.)
- Provides a JSP taglib
- Web socket support

# What is Spring Security?

- Supports wide range of authentication models and technologies
- Supported authentication technologies:
  - JAAS
  - LDAP
  - Form-based
  - HTTP Digest
  - Kerberos
  - Etc.

# Why not Java EE standard?

- Servlet API security and/or JAAS
- NOT portable
- lot of work to configure
- lacks important features/support of de-facto standards out-of the box
- out of scope


Java Security
SECURITY RULES
Superdry

# Tips for Java security

- Limit access to your classes, methods and vars
- Make everithing final
- Don’t depend to package scope
- Avoid inner classes
- Make classes uncloneable
- Make classes unserializable/undeserializble
- Secure app configuration (XML, database, etc.)
- Validate data
- Review code

# Tips for Application security

- Grant DB permissions carefully
- Always set root password (never keep empty)
- Never hardcode username/password into Java program/property file
- Use prepared statements

# Tips for Application security

- Enable SSL
- Disable BACK button
- Disable after more than 3 unsuccessful login attempts
- Use POST instead of GET
- Alert when hits from a given IP exceeds a spcified limit
- Perform client side validation as well
- Never story sensitive information in hidden fields
- Update login passwords periodically

# Tips for Application security

- Neer keep inportant information in a log file
- No „execute” permission in upload directory
- Avoid passing session id in URL
- Check size of files/arrays before processing
- Set proper session timeout


# Szünet, Hamarosan folytatjuk

Biztonságos programozás haladóknak

Peter Veres
peter_veres2@epam.com

2016


# Köszönöm a figyelmet!

**Biztonságos programozás haladóknak**

**Peter Veres**
**peter_veres2@epam.com**

2016