

SOOM.cz konference



The OWASP Foundation  
<http://www.owasp.org>

# OWASP

## SOOM konference

Jan Kopecký  
*Czech chapter leader*  
rnmx123@gmail.com

# O mě



The OWASP Foundation  
<http://www.owasp.org>

- OWASP chapter leader
- Senior ethical hacker pro ING
- Vlastník captes.cz
- Skills
  - Webová bezpečnost (server/client side)
  - Reverzní inženýrství
  - Psaní exploitů
  - Analýza malware
  - Penetrační testy



Co je OWASP  
OWASP projekty  
OWASP v ČR  
Jak pomoci?



# OWASP

The Open Web Application Security Project

<http://www.owasp.org>

**OWASP is a worldwide free and open community focused on improving the security of application software.**

**Our mission is to make application security visible so that people and organizations can make informed decisions about application security risks.**

**Everyone is free to participate in OWASP and all of our materials are available under a free and open software license.**

**The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.**

# Projekty



The OWASP Foundation  
<http://www.owasp.org>

- Co je OWASP TOP 10?
- TOP 10 2010 VS TOP 10 2013

| OWASP Top 10 – 2010 (Previous)                         | OWASP Top 10 – 2013 (New)                         |
|--|---|
| A1 – Injection   | A1 – Injection                                    |
| A3 – Broken Authentication and Session Management      | A2 – Broken Authentication and Session Management |
| A2 – Cross-Site Scripting (XSS)                        | A3 – Cross-Site Scripting (XSS)                   |
| A4 – Insecure Direct Object References                 | A4 – Insecure Direct Object References            |
| A6 – Security Misconfiguration                         | A5 – Security Misconfiguration                    |
| A7 – Insecure Cryptographic Storage – Merged with A9 → | A6 – Sensitive Data Exposure                      |
| A8 – Failure to Restrict URL Access – Broadened into → | A7 – Missing Function Level Access Control        |
| A5 – Cross-Site Request Forgery (CSRF)                 | A8 – Cross-Site Request Forgery (CSRF)            |
| <buried in A6: Security Misconfiguration>              | A9 – Using Known Vulnerable Components            |
| A10 – Unvalidated Redirects and Forwards               | A10 – Unvalidated Redirects and Forwards          |
| A9 – Insufficient Transport Layer Protection           | Merged with 2010-A7 into new 2013-A6              |

# Projekty



The OWASP Foundation  
<http://www.owasp.org>

- OWASP Zed Attack Proxy

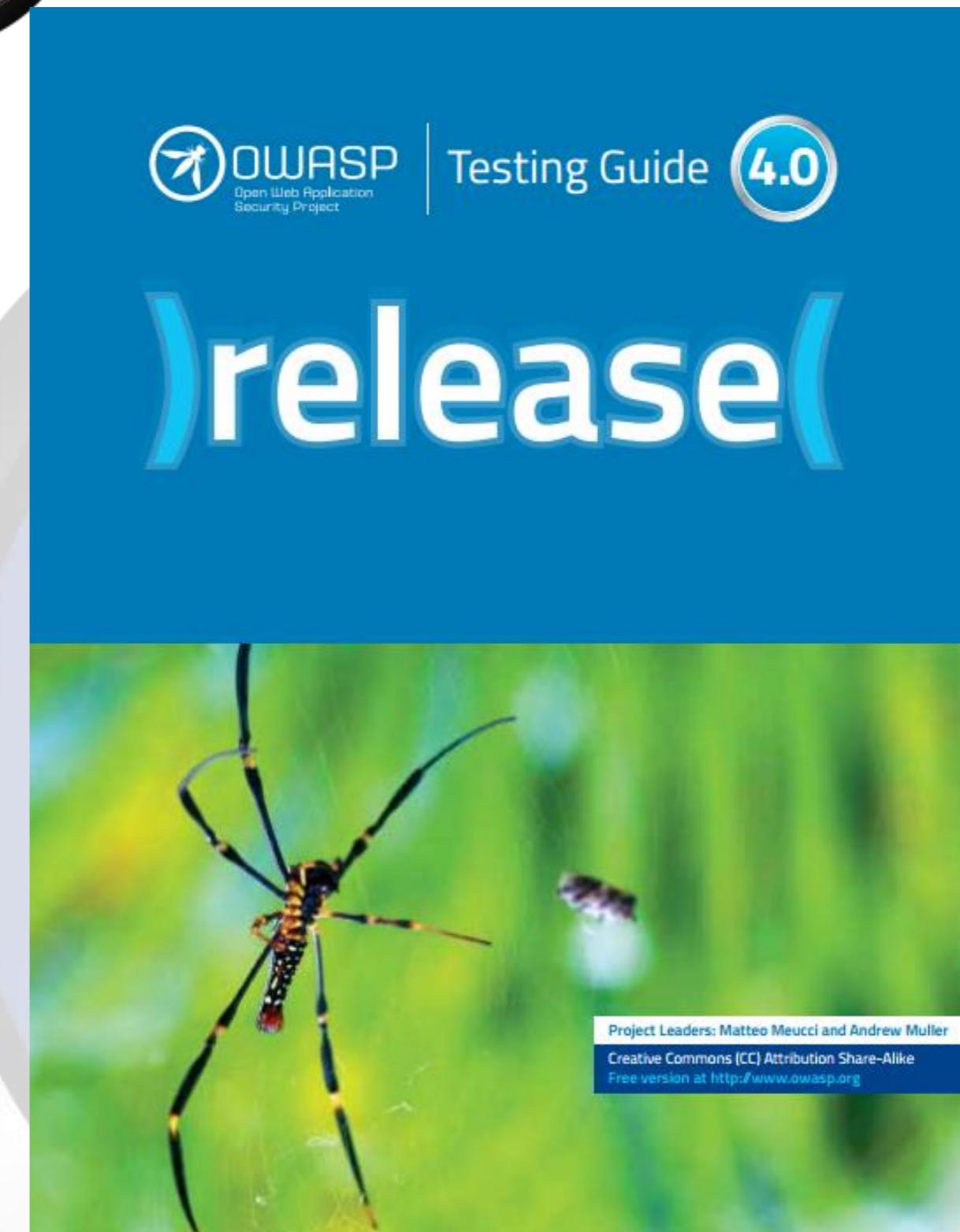
The screenshot shows the main interface of OWASP ZAP. The title bar reads "Untitled Session - OWASP ZAP". The menu bar includes File, Edit, View, Analyse, Report, Tools, Online, and Help. The toolbar below has icons for Standard mode, Sites, Scripts, Quick Start, Request, Response, Break, and Script Console. The left sidebar is titled "Sites" and contains a tree view. The main panel displays the "Welcome to the OWASP Zed Attack Proxy (ZAP)" message. It includes instructions: "ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.", "Please be aware that you should only attack applications that you have been specifically been given permission to test.", and "To quickly test an application, enter its URL below and press 'Attack'". A "URL to attack:" field contains "http://", and there are "Attack" and "Stop" buttons. The "Progress:" status is "Not started". Below the main panel, a note says "For a more in depth test you should explore your application using your browser or automated regression tests while proxying through ZAP." and "If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:". The bottom navigation bar includes tabs for Forced Browse, Fuzzer, Params, Http Sessions, Zest Results, WebSockets, AJAX Spider, Output, History, Search, Break Points, Alerts, Active Scan, and Spider. A filter icon and "Filter: OFF" are at the bottom left. The bottom status bar shows "Alerts 0 0 0 0 0" and "Current Scans 0 0 0 0 0 0 0".

# Projekty



The OWASP Foundation  
<http://www.owasp.org>

- OWASP testing guide



Project Leaders: Matteo Meucci and Andrew Muller

Creative Commons (CC) Attribution Share-Alike  
Free version at <http://www.owasp.org>



- OWASP CSRFGuard && OWASP ESAPI
- ESAPI (The OWASP Enterprise Security API) is a free, open source, web application security control library that makes it easier for programmers to write lower-risk applications.
- The OWASP CSRFGuard library is integrated through the use of a JavaEE Filter and exposes various automated and manual ways to integrate per-session or pseudo-per-request tokens into HTML.



- OWASP CSRFGuard && OWASP ESAPI

<script>...NEVER PUT UNTRUSTED DATA HERE...</script> directly in a script

<!--...NEVER PUT UNTRUSTED DATA HERE...--> inside an HTML comment

<div ...NEVER PUT UNTRUSTED DATA HERE...=test /> in an attribute name

<NEVER PUT UNTRUSTED DATA HERE... href="/test" /> in a tag name

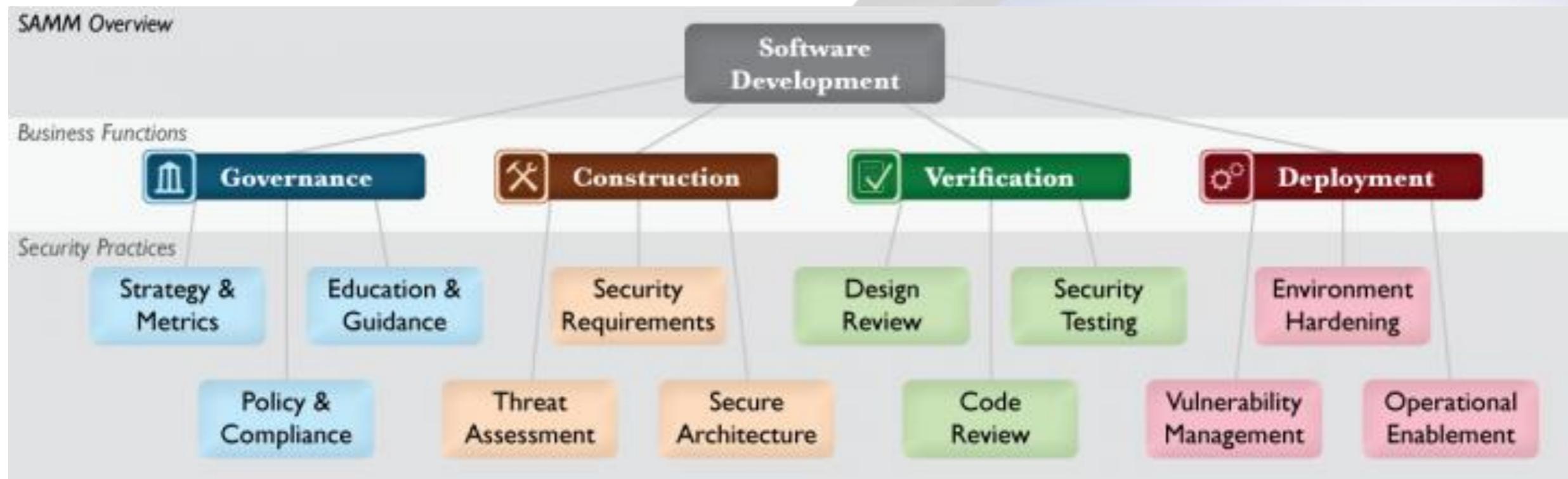
<style>...NEVER PUT UNTRUSTED DATA HERE...</style> directly in CSS

# Projekty



The OWASP Foundation  
<http://www.owasp.org>

- OWASP Software Assurance Maturity Model (SAMM)





- Hlavní cíl: fungující a aktivní komunita
- Naplnění cíle:
  - OWASP meetings
  - Mailing list
  - Twitter
  - OWASP pages





The OWASP Foundation  
<http://www.owasp.org>

# Komunita a komunikace



[https://www.owasp.org/index.php/Czech\\_Republic](https://www.owasp.org/index.php/Czech_Republic)

[https://lists.owasp.org/mailman/admin/owasp-czech\\_republic](https://lists.owasp.org/mailman/admin/owasp-czech_republic)

[owasp.security-portal.cz](http://owasp.security-portal.cz)

[https://twitter.com/OWASP\\_Czech](https://twitter.com/OWASP_Czech)