OWASP

SOOM konference

Jan Kopecký
Czech chapter leader
rnmx123@gmail.com

O mě

- 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.

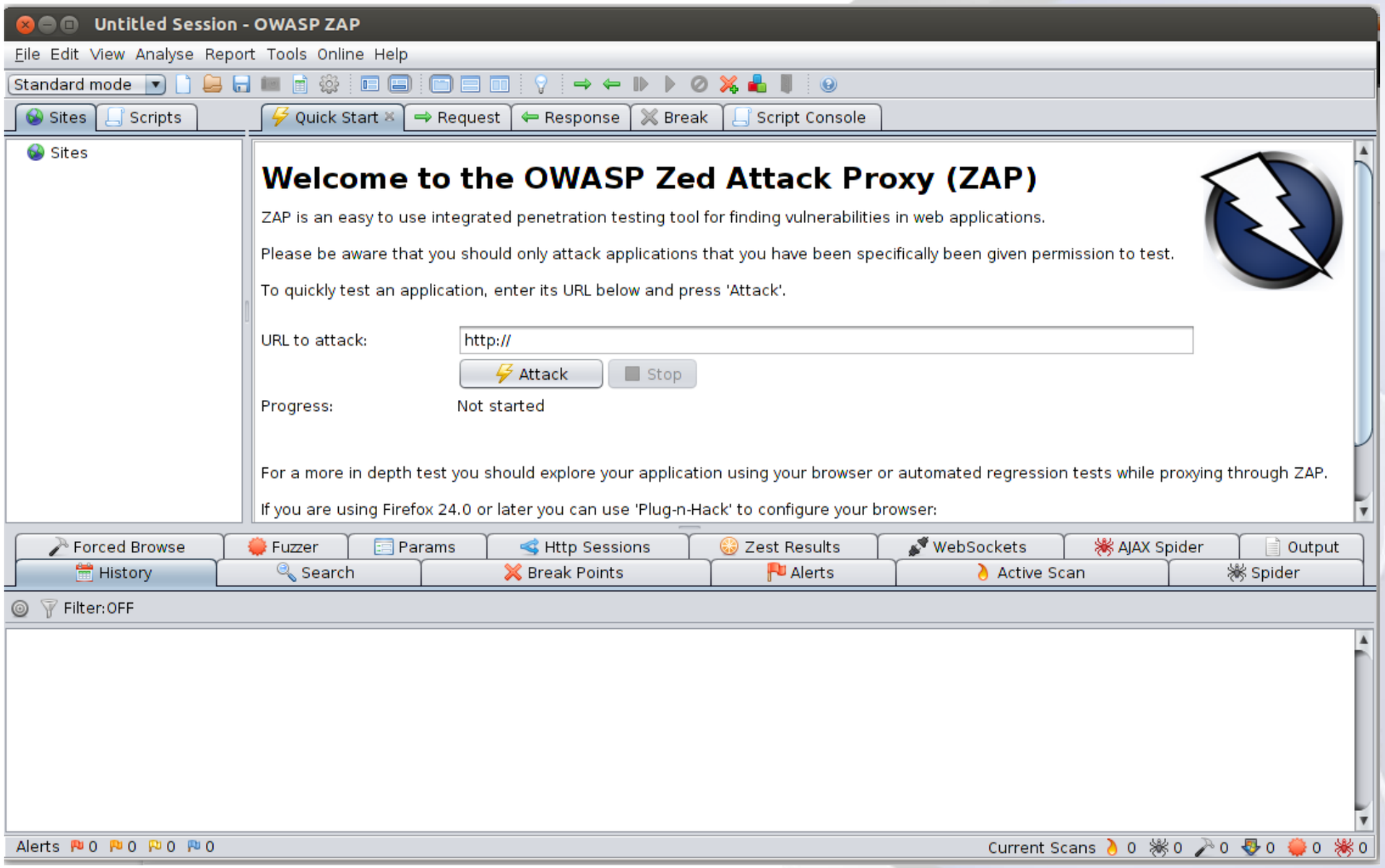
The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work.

Projekty

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

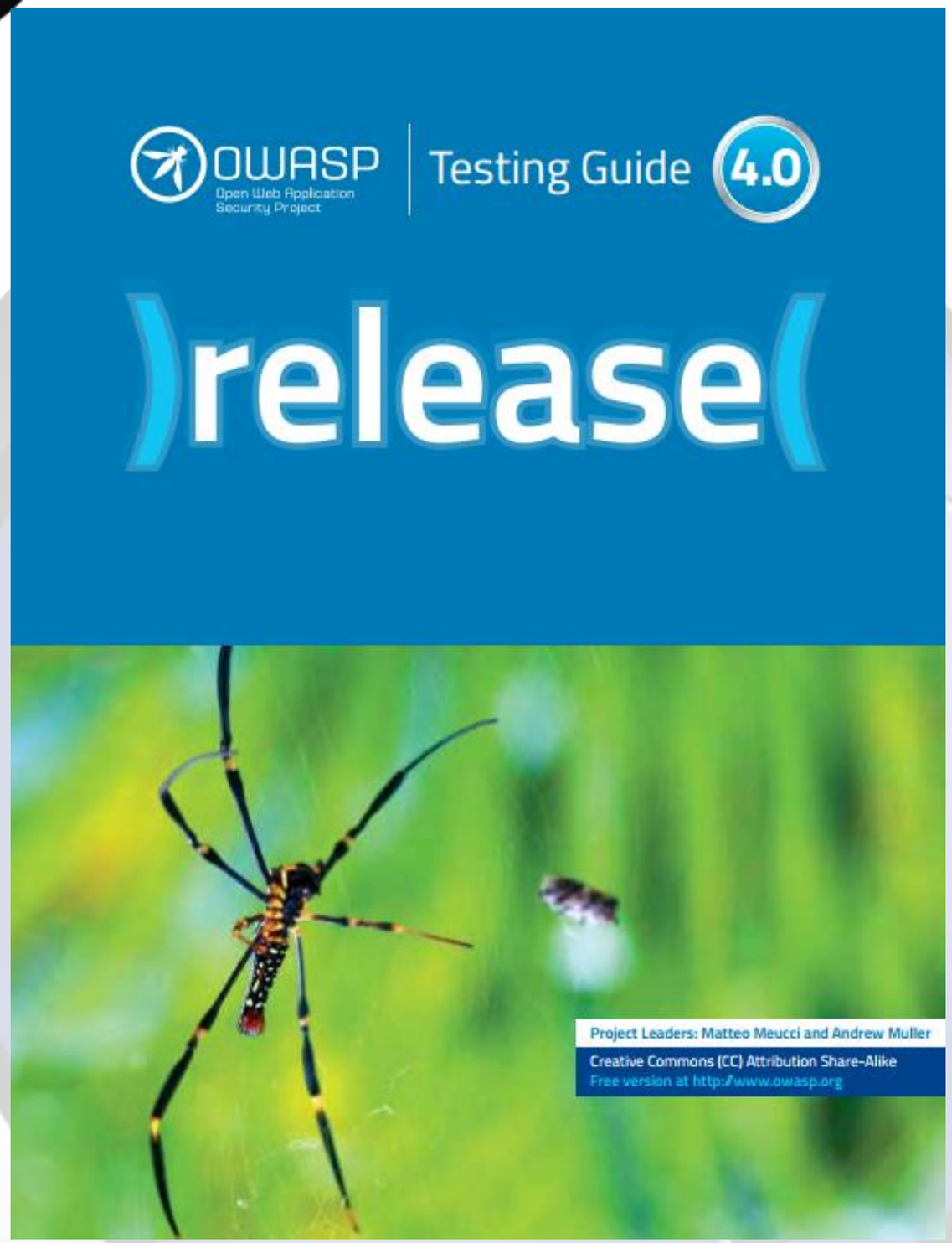
OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure 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

- OWASP Zed Attack Proxy



Projekty

- OWASP testing guide



Projekty

- 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.

Projekty

- OWASP CSRFGuard && OWASP ESAPI

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

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

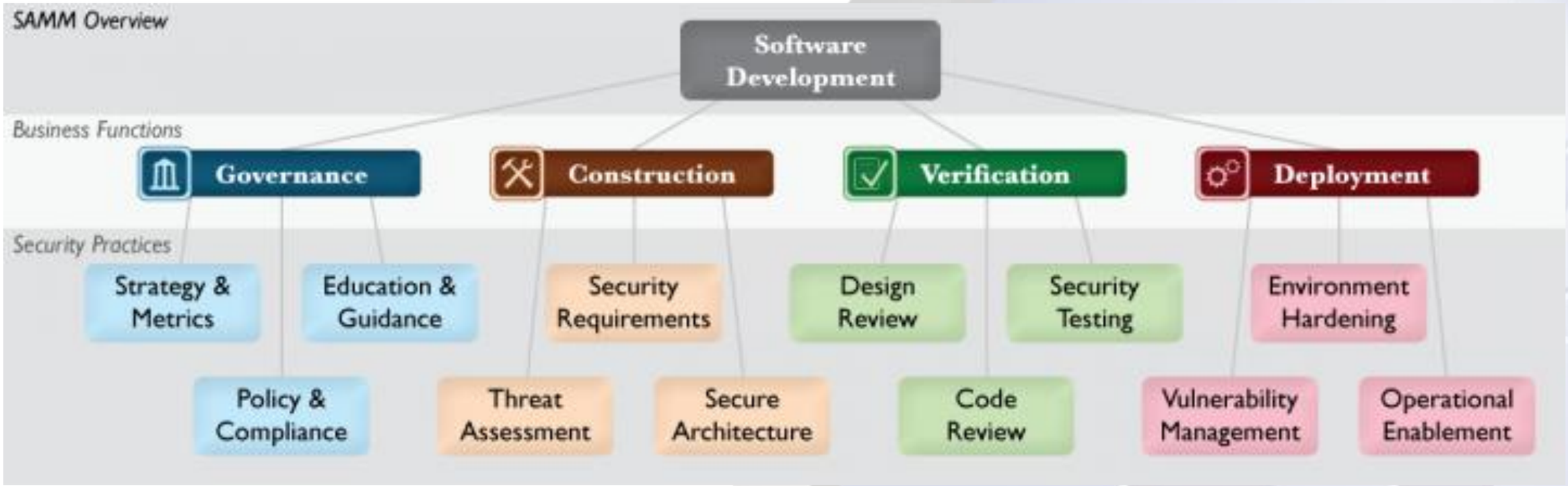
<div ...NEVER PUT UNTRUSTED DATA HERE...=test /> in an attribute name

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

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

Projekty

- OWASP Software Assurance Maturity Model (SAMM)



OWASP v ČR

- Hlavní cíl: fungující a aktivní komunita

- Naplnění cíle:
  - OWASP meetings
  - Mailing list
  - Twitter
  - OWASP pages

Komunita a komunikace

https://www.owasp.org/index.php/Czech_Republic

https://lists.owasp.org/mailman/admin/owasp-czech_republic

owasp.security-portal.cz

https://twitter.com/OWASP_Czech