OWASP Romania Chapter

Chirita Ionel

Application Security Analyst @ EA

Romania Chapter Board Member

chirita.ionel@gmail.com

Romanian Chapter - Europe Tour 2013 - Agenda

- Penetration Testing - a way for improving our cyber security
- Android reverse engineering: understanding third-party applications
- The Trouble with Passwords
- Hacking the ViewState in ASP.NET
- Do you "GRANT ALL PRIVILEGES ..." in MySQL/MariaDB/Percona Server?

Who / What is OWASP?

The Open Web Application Security Project

OWASP !n Numbers

- 190 + local chapters
- Over 30K mailing list users

- 12 & counting years of service
- 55+ paid Corporate Members
- 2000 individual members from 70 countries
- 53+ Academic Supporters
- 88+ Government & industry citation
- 4 Global AppSec Conferences per Year

OWASP !n Numbers

More than …

250,000

…monthly unique visitors &

800,000

…page views.

OWASP !n Numbers

>> 140 ++

OWASP !n Numbers

OWASP's Core Values:

We are …

OWASP's Core Values:

...is our thinking

OWASP's Core Values:

We support …

OWASP's Core Values:

…is our creed

- Founded in 2011 by Claudiu Constantinescu
- 3 meeting organized yet, more to come
- OWASP Romania Chapter v2.0 – December 2012
- We are ~ 100 people on mailing list
- 40 member on linked in group, not yet a member **Join Now !**

OWASP Projects

… are distributed in 3 categories

- Protect
  - Documents & Tools used to prevent design and implementation flaws.
- Detect
  - Documents & tools created to identify design and implementation flaws.
- Lifecycle
  - tools and documents that can be used to add security-related activities into the Software Development Life Cycle (SDLC).

http://www.owasp.org/index.php/Category:OWASP_Project

OWASP Projects

Protect:

- ESAPI
- ModSecurity
- Security guides
- Appsec Tutorials
- Secure Coding Practices

Detect:

- Webscarab
- Zed Attack Proxy
- JBroFuzz
- Code review guide
- Cheat Sheet Series
- Live CD

Life Cycle:

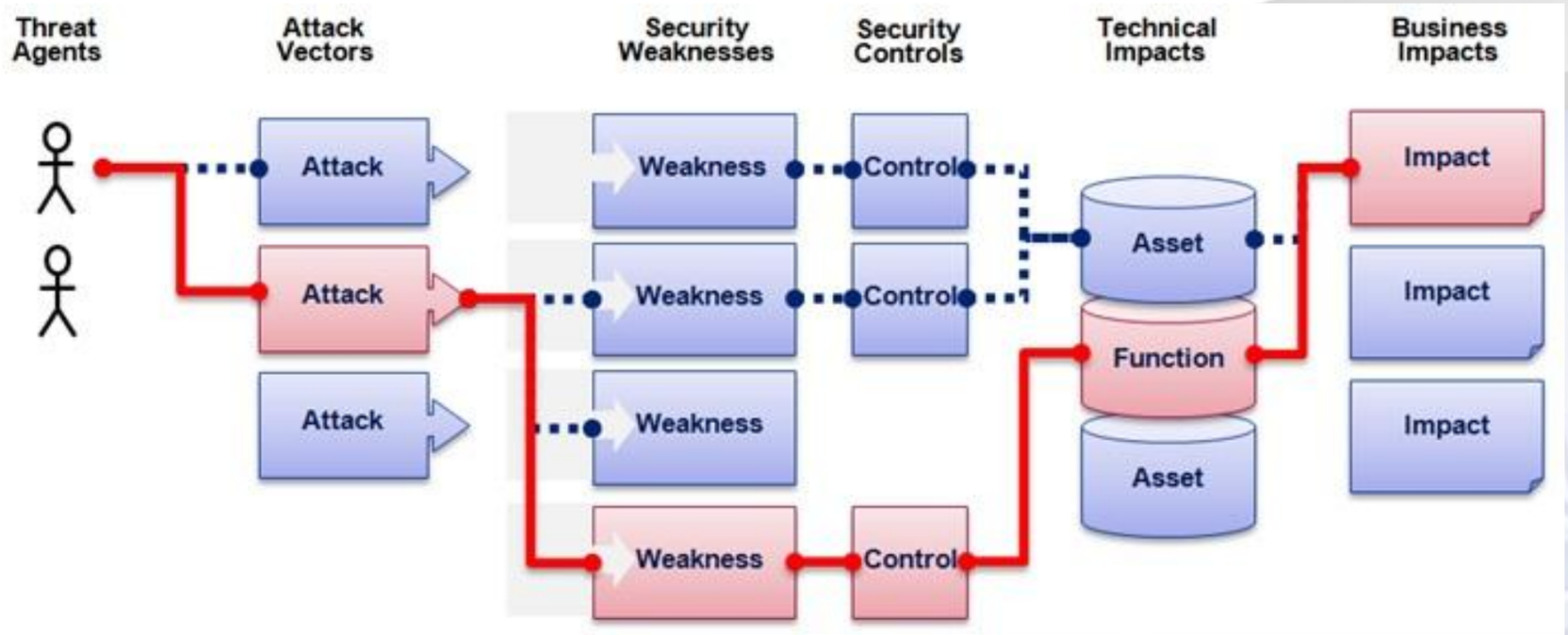
- SAMM
- WebGoat
- Legal Project

OWASP Top 10

- A1: Injection
- A2: Broken Authentication and Session Management
- A3: Cross-Site Scripting (XSS)
- A4: Insecure Direct Object References
- A5: Security Misconfiguration
- A6: Sensitive Data Exposure
- A7: Missing Function Level Access Control
- A8: Cross Site Request Forgery (CSRF)
- A9: Using Known Vulnerable Components
- A10: Unvalidated Redirects and Forwards

http://www.owasp.org/index.php/Top_10

OWASP Top 10 Risk Rating Methodology



To determine the risk to your organization, you can evaluate the likelihood associated with each threat agent, attack vector, and security weakness, when they rich boiling point add technical and business impact flavor taking in consideration your organization.

OWASP Code Review Guide

- Most effective technique for identifying security flaws.
- Focuses on the mechanics of reviewing code for certain vulnerabilities.
- A key enabler for the OWASP fight against software insecurity.
- v2 – January 2014

https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project

OWASP Testing Guide

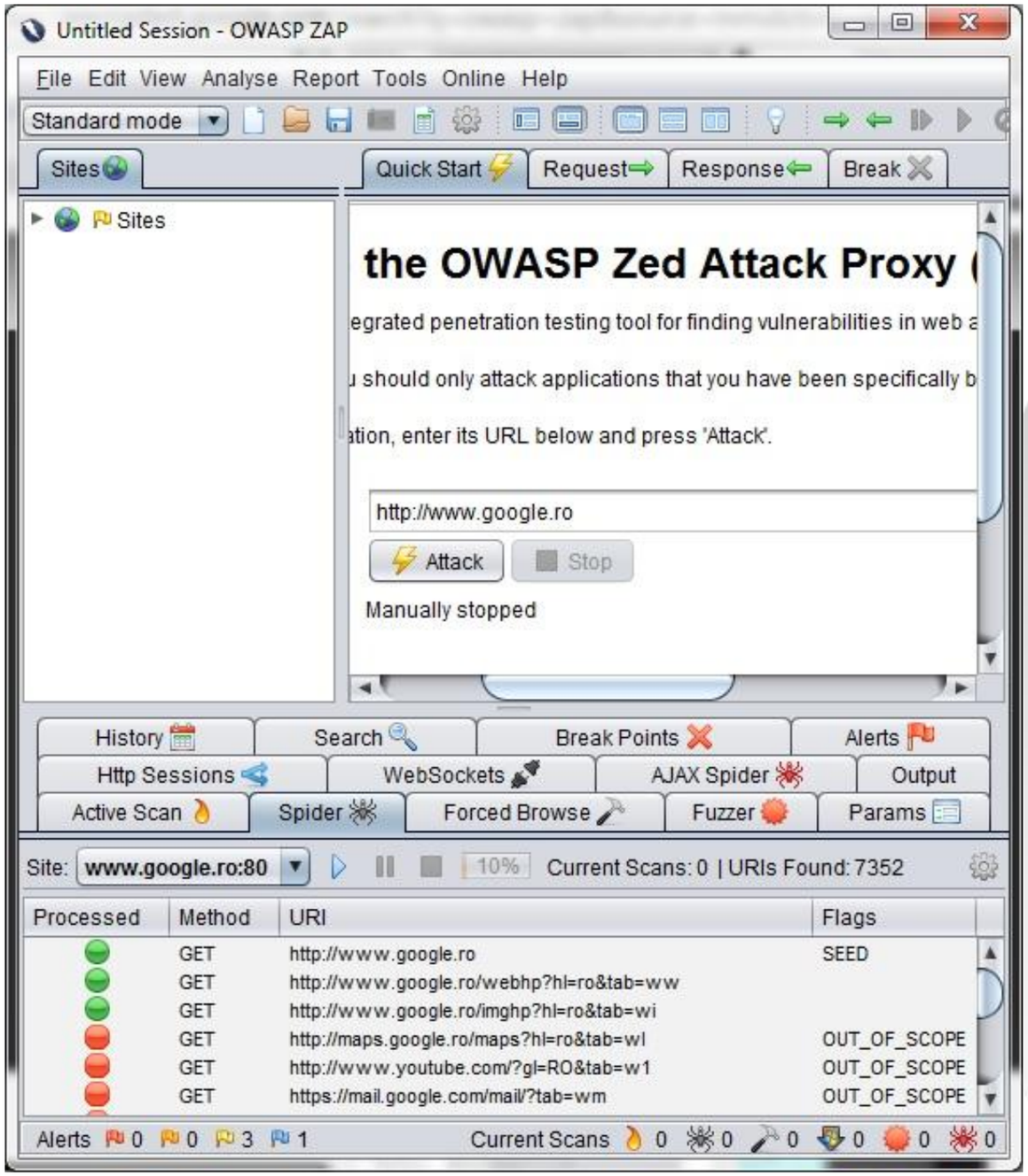
- Web application penetration test framework.
- what, why, when, where, and how of test an web application
- More than a checklist
- v4 in progress.

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

OWASP Cheat Sheet Series

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

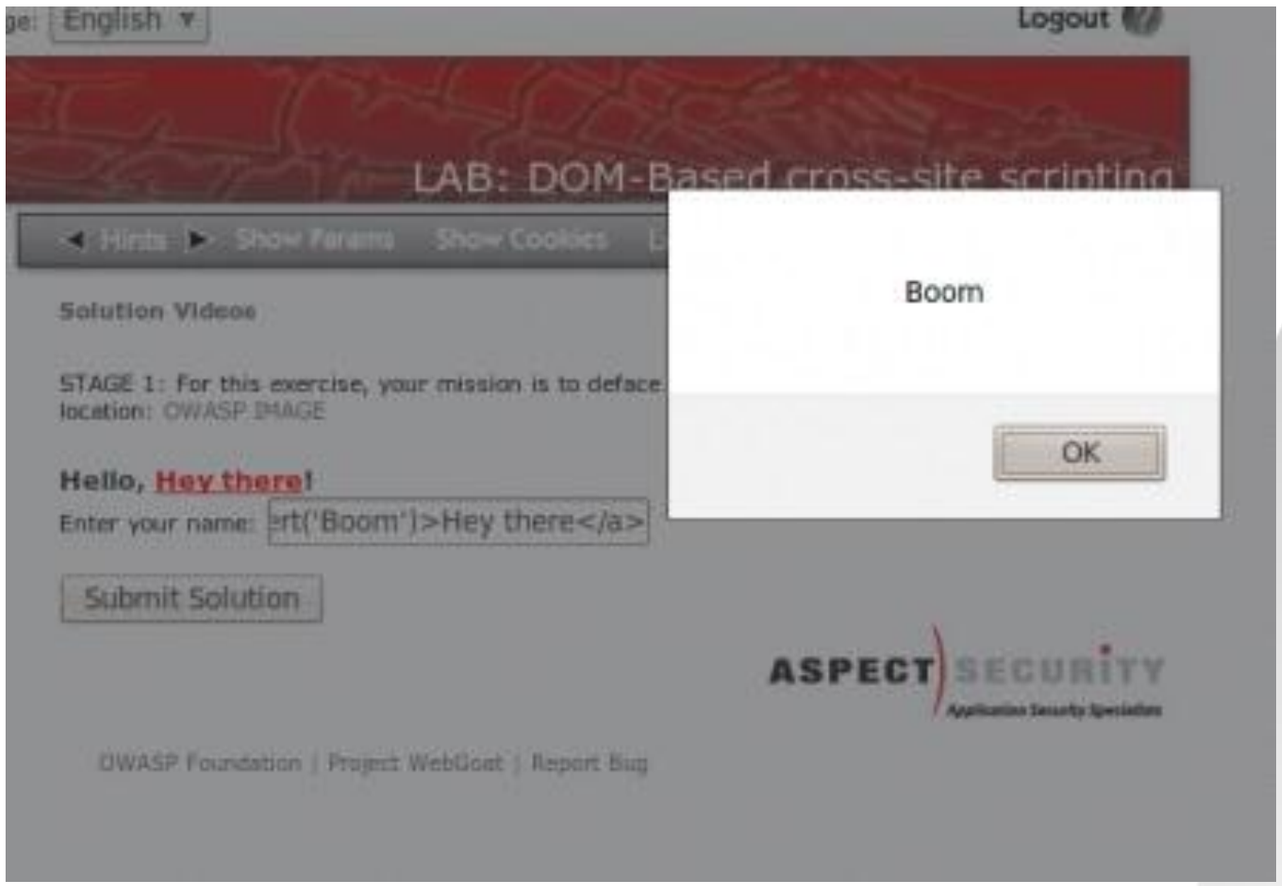
OWASP – Zed Attack Proxy (ZAP)



ZAP Proxy is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

- Flagship OWASP Project
- Cross platform tool
- Features:
  - Intercepting proxy
  - Port scanner
  - Brute force tool
  - Spider
  - Fuzzer
  - Automatic & passive scanner

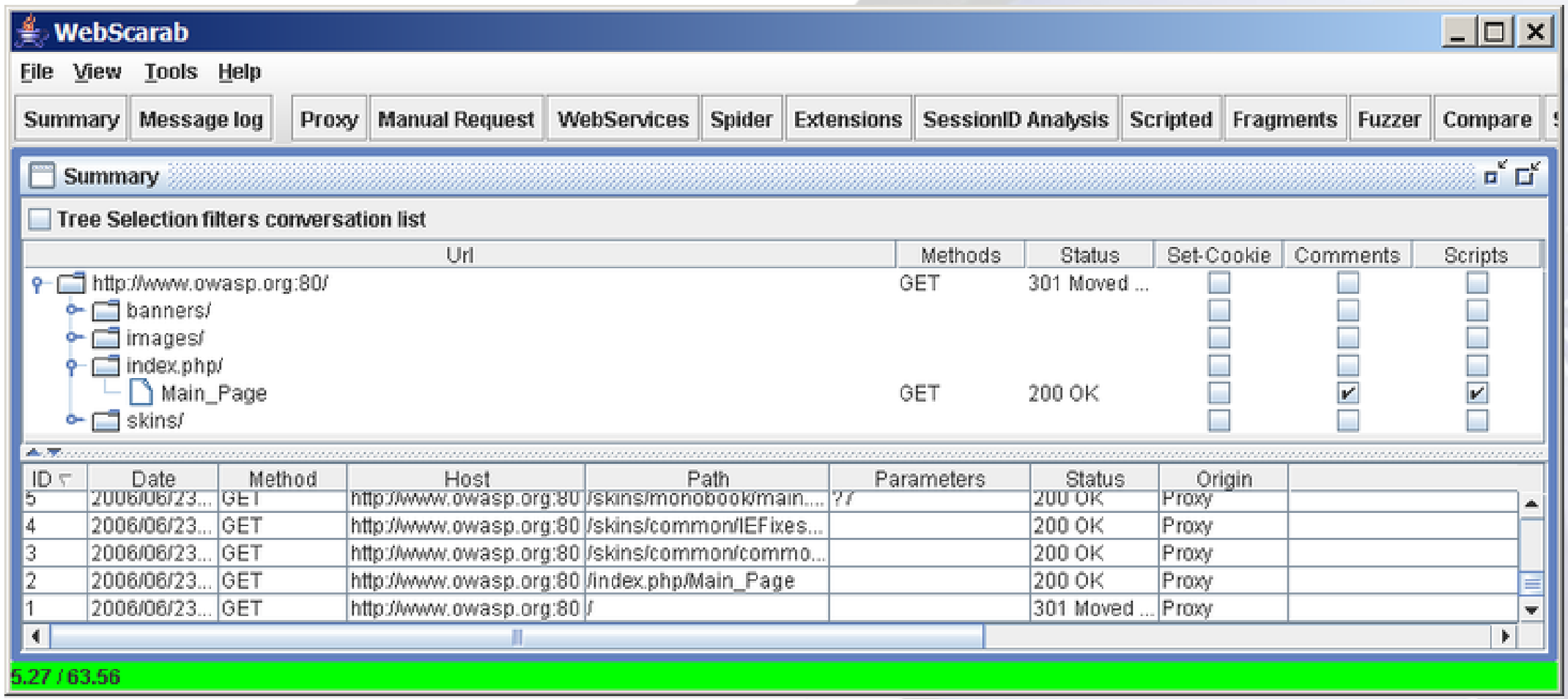
OWASP WebGoat Java Project



- Deliberately vulnerable J2EE web application
- Guide for secure programming
- Realistic teaching environment
- More than 30 hands on lessons including:
  - XSS
  - Access control
  - SQLi
  - Hidden form manipulation
  - Weak session cookies
  - … + many more.

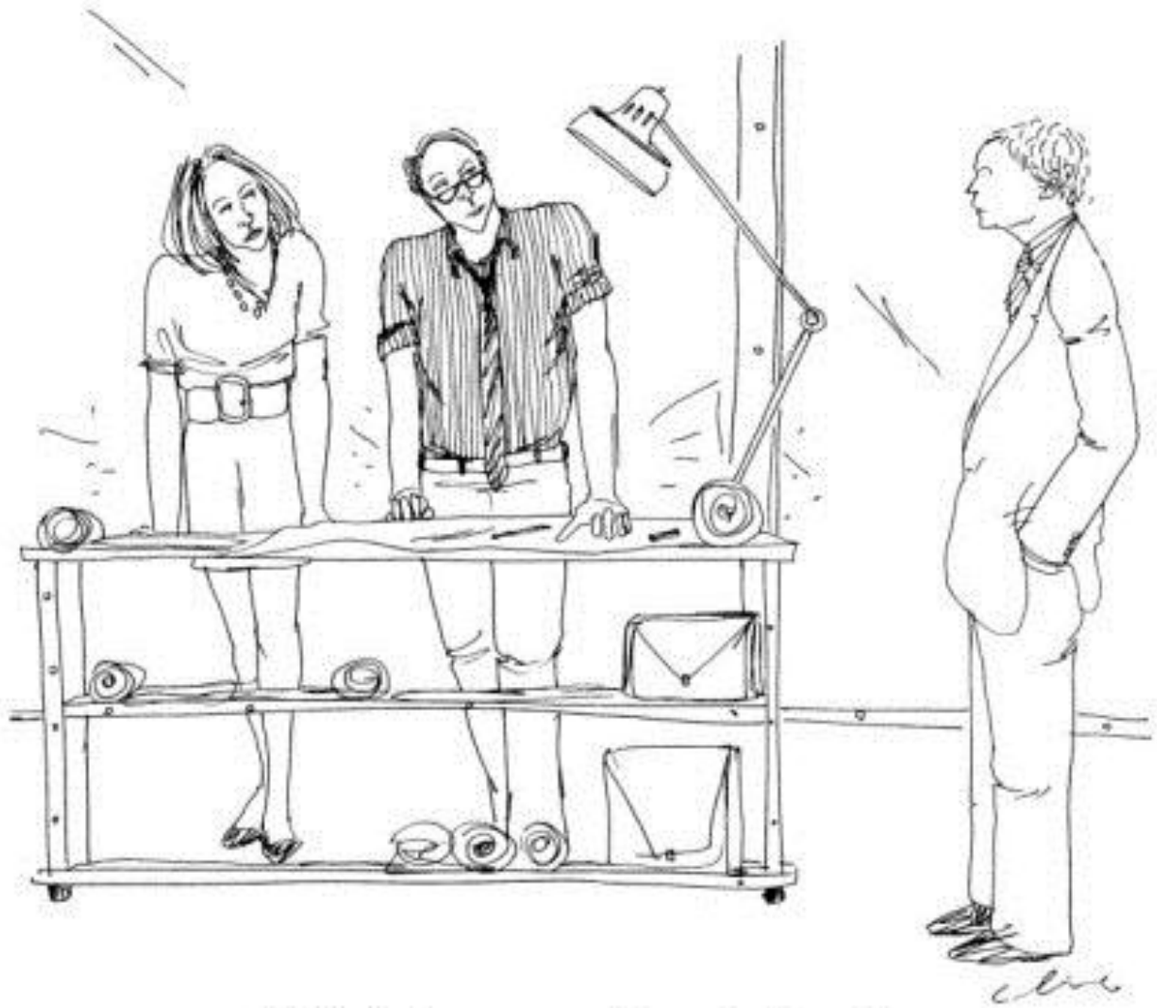
Webscarab

Java based framework used for analyzing web applications and web services that communicate over http & httpS



https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project

This is a part of what OWASP offers



"Did I leave any ideas in here?"

What about you?

- **OPEN** our door, join as a member
- **Innovate** and participate in an OWASP project
- Attend **GLOBAL** OWASP AppSec series conference
- Act with **INTEGRITY**

What next? Consider…

- Donating
- Attending local chapter regular meeting
- Contributing to an OWASP project
  - Developers, beta testers, etc.
- Attend on Europe OWASP AppSec series Conference

Affiliation and Membership

Categories of Membership and Supporters:

- Individual Supporters
- Single Meeting Supporter
- Event Sponsorship
- Organization Supporters
- Accredited University Supporters

Benefits…?

Ethics and principals of OWASP Foundation

- Underscore your awareness of web application software security
- Attend OWASP conferences at a discount
- Expand your personal network of contacts
- Support a local chapter of your choice
- Get your @owasp.org email address
- Have individual vote in elections

https://owasp.org/index.php/Membership

OWASP Romania