Who Am I?

- +10 years developer experience
- + 6 years application security experience
- Software Architect / Security Consultant @ Sogeti Nederland B.V.
- Netherlands OWASP chapter board member
- OWASP Education Project Leader
- OWASP Speaker Buro
- OWSAP Capture The Flag
- OWASP Global Education Committee Member
- www.owasp.org
OWASP Global Committees:

• Projects
• Membership
• Education
• Conferences
• Industry
• Chapter
# Categorize (Organization) of educational materials

<table>
<thead>
<tr>
<th><strong>Target Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Benefit</strong></td>
</tr>
<tr>
<td>easier navigation to find relevant education material</td>
</tr>
<tr>
<td><strong>Short Description</strong></td>
</tr>
<tr>
<td>• categorization of the education material according to the CLASP roles</td>
</tr>
<tr>
<td>• categorization of the education material into 'management-ish', 'student-ish', technical-ish'</td>
</tr>
<tr>
<td><strong>Related Projects</strong></td>
</tr>
<tr>
<td>OWASP Education Project</td>
</tr>
<tr>
<td><strong>Deadline</strong></td>
</tr>
<tr>
<td>May 2009 - <a href="#">OWASP AppSec Europe 2009</a> - Poland</td>
</tr>
<tr>
<td><strong>Email Contacts &amp; Roles</strong></td>
</tr>
<tr>
<td><strong>Primary</strong></td>
</tr>
<tr>
<td>Martin Knobloch</td>
</tr>
</tbody>
</table>
# OWASP Boot Camp Project

<table>
<thead>
<tr>
<th><strong>Target Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Benefit</strong></td>
</tr>
<tr>
<td><strong>Short Description</strong></td>
</tr>
</tbody>
</table>
| **Related Projects**   | • all OWASP projects  
                         | • [OWASP Boot Camp Project](#) |
| **Deadline**           | October 2009 - [OWASP AppSec US 2009](#) - Washington, D.C. |

<table>
<thead>
<tr>
<th><strong>Email Contacts &amp; Roles</strong></th>
<th><strong>Primary</strong></th>
<th><strong>Secondary</strong></th>
<th><strong>Mailing list</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><a href="#">Martin Knobloch</a></td>
<td><a href="#">who</a></td>
<td>None</td>
</tr>
</tbody>
</table>
### OWASP CTF event

<table>
<thead>
<tr>
<th><strong>Activity Identification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity Name</strong></td>
</tr>
<tr>
<td><strong>Short Description</strong></td>
</tr>
<tr>
<td><strong>Related Projects</strong></td>
</tr>
<tr>
<td><strong>Email Contacts &amp; Roles</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
# Marketing efforts

## ACTIVITY IDENTIFICATION

<table>
<thead>
<tr>
<th>Activity Name</th>
<th>Select the target material</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Description</td>
<td>Promote OWASP projects, events, education material and OWASP mission.</td>
</tr>
<tr>
<td>Related Projects</td>
<td><strong>OWASP Education Project</strong> (Primary) and <strong>OWASP Positive Security Project</strong> (Secondary)</td>
</tr>
<tr>
<td>Email Contacts &amp; Roles</td>
<td>Eduardo Vianna de Camargo Neves</td>
</tr>
<tr>
<td></td>
<td><strong>e-mail</strong></td>
</tr>
<tr>
<td></td>
<td><strong>who</strong></td>
</tr>
</tbody>
</table>
# Internationalization of the training materials

**Activity Name**
- Internationalization of educational material a.k.a. translate materials

**Short Description**
- Perform translation and generation marketing material for distribution

**Related Projects**
- None

**Email Contacts & Roles**
- Eduardo Vianna de Camargo Neves
  - e-mail
- Secondary
  - who
- Mailing list
  - None
# Education material

<table>
<thead>
<tr>
<th><strong>ACTIVITY IDENTIFICATION</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity Name</strong></td>
<td>Training &amp; Academic Educational Services</td>
</tr>
<tr>
<td><strong>Short Description</strong></td>
<td>Consolidate all projects to create educational material</td>
</tr>
<tr>
<td><strong>Related Projects</strong></td>
<td>All OWASP Projects!</td>
</tr>
<tr>
<td><strong>Email Contacts &amp; Roles</strong></td>
<td><strong>Primary</strong> Martin</td>
</tr>
</tbody>
</table>
# Educational Academic Services

<table>
<thead>
<tr>
<th>ACTIVITY IDENTIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activity Name</strong></td>
</tr>
<tr>
<td><strong>Short Description</strong></td>
</tr>
<tr>
<td><strong>Related Projects</strong></td>
</tr>
<tr>
<td><strong>Email Contacts &amp; Roles</strong></td>
</tr>
</tbody>
</table>
  **Primary** Kuai Hinojosa  
  **Secondary** Andrzej Targosz  
  **Mailing list** edu_academic_services |
# OWASP Education Project Project

The project will continuously deliver education material about OWASP tooling and documentation. This aims to create an easy entrance towards understanding application security and usage of the OWASP tooling. By creating education documentation papers, screen scrape video courses and setting up an OWASP Boot camp, a controlled education process of a standardized quality can be created continuously. With the setup of a OWASP Boot camp, the OWASP word can be spread in a controlled manner and deliver high quality training, both inside and outside of the OWASP community. The OWASP Education Project will setup and standardize OWASP trainings manuals and materials to ensure a certain level of quality of the trainings. Trainings about the OWASP tooling and projects will have to be reviewed by the Projects.

<table>
<thead>
<tr>
<th>Project Name</th>
<th>OWASP Education Project Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Short Project Description</td>
<td>The project will continuously deliver education material about OWASP tooling and documentation. This aims to create an easy entrance towards understanding application security and usage of the OWASP tooling. By creating education documentation papers, screen scrape video courses and setting up an OWASP Boot camp, a controlled education process of a standardized quality can be created continuously. With the setup of a OWASP Boot camp, the OWASP word can be spread in a controlled manner and deliver high quality training, both inside and outside of the OWASP community. The OWASP Education Project will setup and standardize OWASP trainings manuals and materials to ensure a certain level of quality of the trainings. Trainings about the OWASP tooling and projects will have to be reviewed by the Projects.</td>
</tr>
</tbody>
</table>

## Key Project Information

<table>
<thead>
<tr>
<th>Project Leader</th>
<th>Martin Knobloch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contributors</td>
<td>Sebastien Deleersnyder, Martin Knobloch, Tom Brennan</td>
</tr>
<tr>
<td>Mailing List</td>
<td><a href="#">Subscribe here</a> <a href="#">Use here</a></td>
</tr>
<tr>
<td>License</td>
<td>Creative Commons Attribution Share Alike 3.0</td>
</tr>
<tr>
<td>Project Type</td>
<td>Documentation</td>
</tr>
<tr>
<td>Sponsors</td>
<td>OWASP SoC 08, OWASP Germany AppSec 2009: Application Security Awareness, Martin Knobloch</td>
</tr>
</tbody>
</table>
• OWASP Top Ten
• OWASP Tooling
• OWASP Documentation
• Profession / Interest
• CLASP roles
• SAMM Disciplines & Functions
Ultimate Security?!?
What is secure Software?

An application is secure if it acts and reacts, as it expected, at any time!
Applications over time
Applications over time

The environments in which the software applications run were closed.

- By this, the applications could be developed ‘open’.
Applications over time

The environments in which the software applications run were closed.

- By this, the applications could be developed ‘open’.

The environments became more open over time.
Applications over time

The environments in which the software applications run became more open over time. By this, the applications could be developed ‘open’.

What means, the applications have to become more closed.
Security Design & Architectuur
The problem:

- Cookies, HTTP authentication, SSL
- Low learning curve
- Easy to attack (web) applications
OWASP Top 10 2007

- A1 - Cross Site Scripting (XSS)
- A2 - Injection Flaws
- A3 - Malicious File Execution
- A4 - Insecure Direct Object Reference
- A5 - Cross Site Request Forgery (CSRF)
- A6 - Information Leakage & Improper Error Handling
- A7 - Broken Authentication & Session Management
- A8 - Insecure Cryptographic Storage
- A9 - Insecure Communications
- A10 - Failure to Restrict URL Access
Where do attacks come from?

Conscious
- Cracker
- Hacker
- Scriptkiddie

Risk = Threat \times Vulnerability

Unconscious
- System
- Environment
- User
What is Software Security about?

Applications are about information!

- 3 pillars of Information Security:
  - Confidentiality
  - Integrity
  - Availability
Security Requirements?

- ‘Why’
  - Business requirements
- ‘What’
  - User requirements
    - Business rules
    - External interfaces
  - System requirements
    - Constraints
- ‘How’
  - Functional
  - Non-functional

OWASP Germany AppSec 2009: Application Security Awareness, Martin Knobloch
What is Software Security about?

Who.. in what role?

..may do: in which process..

Where..

..on what data?

thus, with what rights?
Where ‘is’ Software Security?

- Database
- Web Service
- Presentation Service
- Business Services
- Application Services
- Batch
- Integration Service
- External Systems

Internet
Software Architectuur?
Security Development Lifecycles

Microsoft SDL

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Design</th>
<th>Implementation</th>
<th>Verification</th>
<th>Release</th>
<th>Support &amp; Servicing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Architecture &amp; Attack &amp; Threat Modeling</td>
<td>Threat Modeling</td>
<td>Accept Security</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

CLASP

Touchpoints

SECURITY REQUIREMENTS
ABUSE CASES
RISK ANALYSIS
EXTERNAL REVIEW
RISK BASED SECURITY TESTS
CODE REVIEW (TOOLS)
PENETRATION TESTING
SECURITY OPERATIONS

OWASP Germany AppSec 2009: Application Security Awareness, Martin Knobloch
• **Summary:**

  > Applications are about information
    > Confidentiality, Integrity & Availability
  > Explicit security requirements
    > Make security verifiable!
  > Security in depth
    > Security considered through the whole application
    > Propagation of credentials
  > Security by default
    > Who may do what?

**More code = more bugs!**
Any questions so far?
Agenda

- What is OWASP
- Secure Application
- OWASP Top Ten
- OWASP near you
OWASP TOP TEN

1. Cross Site Scripting
2. Injection Flaws
3. Malicious File Execution
4. Insecure Direct Object References
5. Cross Site Request Forgery
6. Information Leakage and Improper Error Handling
7. Broken Authentication and Session Management
8. Insecure Cryptographic Storage
9. Insecure Communication
10. Failure to Restrict URL access
A1 Cross-Site Scripting (XSS)

1. Web Server sends script to Client
2. Client executes script (possibly via user input)
3. Script Interpreter runs script
4. Script returns HTML Page
5. HTML Page with client-side script is returned

- HTML Page with client-side script is returned.
Unsafe content is stored in the dynamic part of the web content?

1. Unsafe content is retrieved from the database
2. That unsafe content becomes part of the site
3. The servers sends the response to the client
4. The client receives and interprets the received content.
5. The unsafe content (e.g. a script) causes the browser to send an request to another, unsafe, site!
A2 Injection Flaws
A2 Injection Flaws – SQL injection

Screen:
  USERNAME:[Admin]
  PASSWORD:[Secret01]

Server:
  Access if:
  the username is ‘Admin’
    &
  and the password is ‘Secret01’;
A2 Injection Flaws – SQL injection

Screen:
USERNAME: [Admin]
PASSWORD: [Secret01 OR 1 = 1]

Server:
Access if:
the username is ‘Admin’
&
and the password is ‘Secret01’ OR 1 = 1;
A2 Injection Flaws – SQL injection

Screen:
USERNAME: [Admin]
PASSWORD: [Secret01 OR 1 = 1]

Server:
Access if:
the username is ‘Admin’
&
and the password is ‘whatever’ OR 1 = 1;
A3 Malicious File Execution
A4 Insecure Direct Object Reference
A5 Cross-site Request Forgery (XSRF)
A6 Information Leakage / Improper Error Handling
A8 Insecure Cryptographic Storage
A9 Insecure Communication
A10 Failure to Restrict URL Access
That’s it...

..thank you!