# Application Security Awareness

Martin Knobloch
martin.knobloch@owasp.org

OWASP

OWASP



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

# 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
The Open Web Application Security Project

OWASP Germany AppSec 2009

OWASP Global Committees:

- Projects
- Membership
- Ecucation
- Conferences
- Industry
- Chapter

# Categorize (Organization) of educational materials

| Target Description | | | |
|---|---|---|---|
| **Benifit** | **easier navigation to find relevant education material** | | |
| **Short Description** | •categorization of the education material according to the CLASP roles<br>•categorization of the education material into 'management-ish', 'student-ish', technical-ish' | | |
| **Related Projects** | OWASP Education Project | | |
| **Deadline** | May 2009 - OWASP AppSec Europe 2009 - Poland | | |
| **Email Contacts & Roles** | **Primary**<br>**Martin Knobloch** | **Secondary**<br>**who** | **Mailing list**<br>None |

# OWASP Boot Camp Project

| Target Description | | | |
|---|---|---|---|
| **Benefit** | Presentabel overview of OWASP Projects | | |
| **Short Description** | Request, validate and categorize Boot Camp presentations | | |
| **Related Projects** | •all OWASP projects<br>•OWASP Boot Camp Project | | |
| **Deadline** | October 2009 - OWASP AppSec US 2009 - Washington, D.C. | | |
| **Email Contacts & Roles** | **Primary**<br>**Martin Knobloch** | **Secondary**<br>**who** | **Mailing list**<br>None |

# OWASP CTF event

| ACTIVITY IDENTIFICATION | | | |
|---|---|---|---|
| **Activity Name** | Capture the Flag | | |
| **Short Description** | Develop CtF contest | | |
| **Related Projects** | None | | |
| **Email Contacts & Roles** | **Primary**<br>Andrzej Targosz | **Secondary**<br>Martin Knobloch | **Mailing list**<br>ctf |

# Marketing efforts

| ACTIVITY IDENTIFICATION | | | |
|---|---|---|---|
| **Activity Name** | Select the target material | | |
| **Short Description** | Promote OWASP projects, events, education material and OWASP mission. | | |
| **Related Projects** | OWASP Education Project (Primary) and OWASP Positive Security Project (Secondary) | | |
| **Email Contacts & Roles** | **Eduardo Vianna de Camargo Neves** e-mail | **Secondary** who | **Mailing list** None |

# Internationalization of the training materials

| ACTIVITY IDENTIFICATION | | | |
|---|---|---|---|
| **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

| ACTIVITY IDENTIFICATION | | | |
|---|---|---|---|
| **Activity Name** | Training & Academic Educational Services | | |
| **Short Description** | Consolidate all projects to create educational material | | |
| **Related Projects** | All OWASP Projects! | | |
| **Email Contacts & Roles** | **Primary**<br>Martin | **Secondary**<br>Fabio | **Mailing list**<br>education_material |

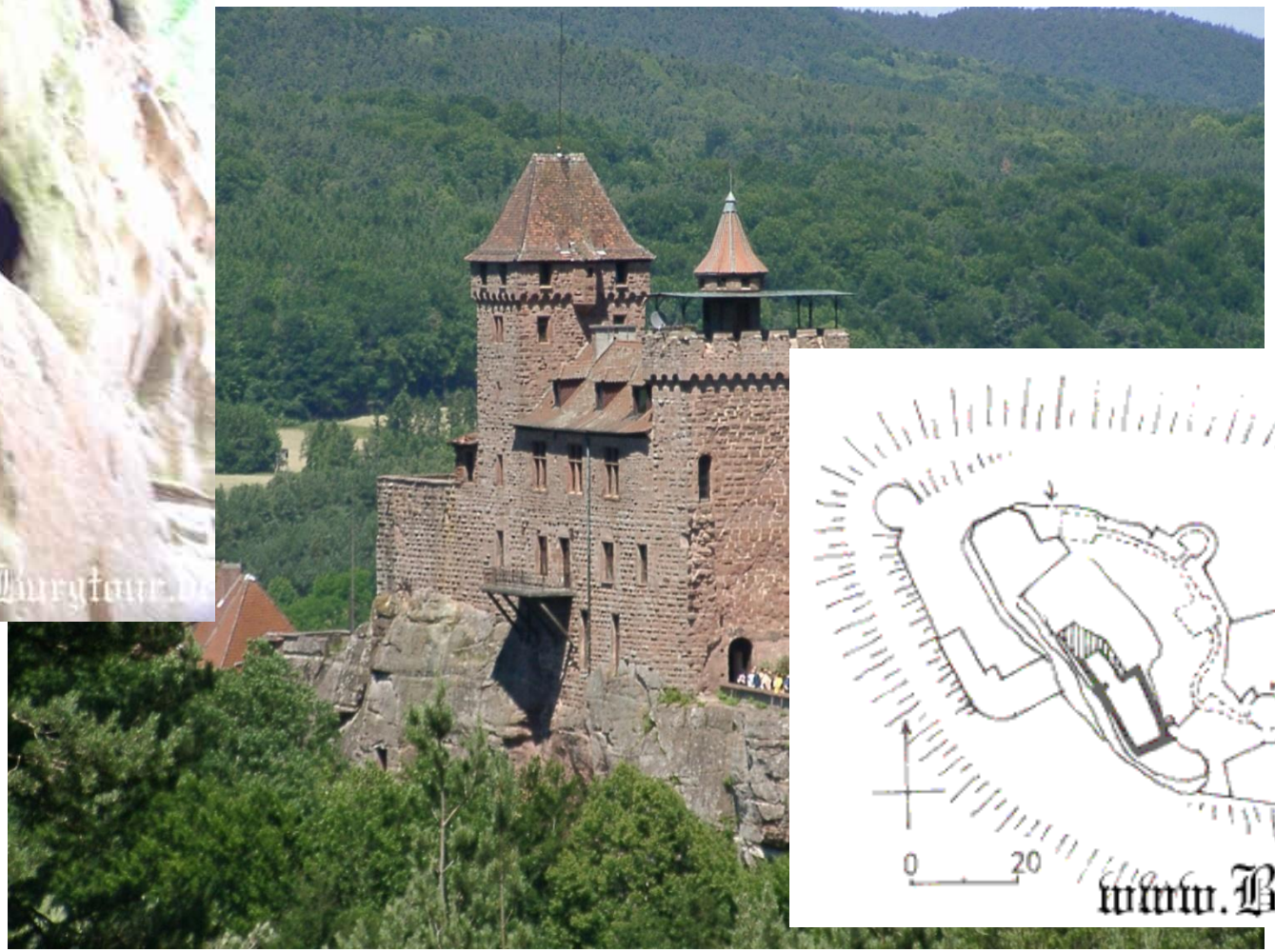
# Educational Academic Services

| ACTIVITY IDENTIFICATION | | | |
|---|---|---|---|
| **Activity Name** | Educational Academic Services. | | |
| **Short Description** | Reach out to Academic Institutions worldwide | | |
| **Related Projects** | Education Project | | |
| **Email Contacts & Roles** | **Primary**<br>Kuai Hinojosa | **Secondary**<br>Andrzej Targosz | **Mailing list**<br>edu_academic_services |

| PROJECT IDENTIFICATION | | | | | | |
|---|---|---|---|---|---|---|
| **Project Name** | **OWASP Education Project Project** | | | | | |
| **Short Project Description** | 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. | | | | | |
| **Key Project Information** | Project Leader<br>**Martin Knobloch** | Project Contributors<br>**Sebastien Deleersnyder**<br>**Martin Knobloch**<br>**Tom Brennan** | Mailing List<br>**Subscribe here**<br>**Use here** | License<br>**Creative Commons Attribution Share Alike 3.0** | Project Type<br>**Documentation** | Sponsors<br>**OWASP SoC 08** |

- OWASP Top Ten
- OWASP Tooling
- OWASP Documentation
- Profession / Interest
- CLASP roles
- SAMM Disciplines & Functions

# Ultimate Security?!?

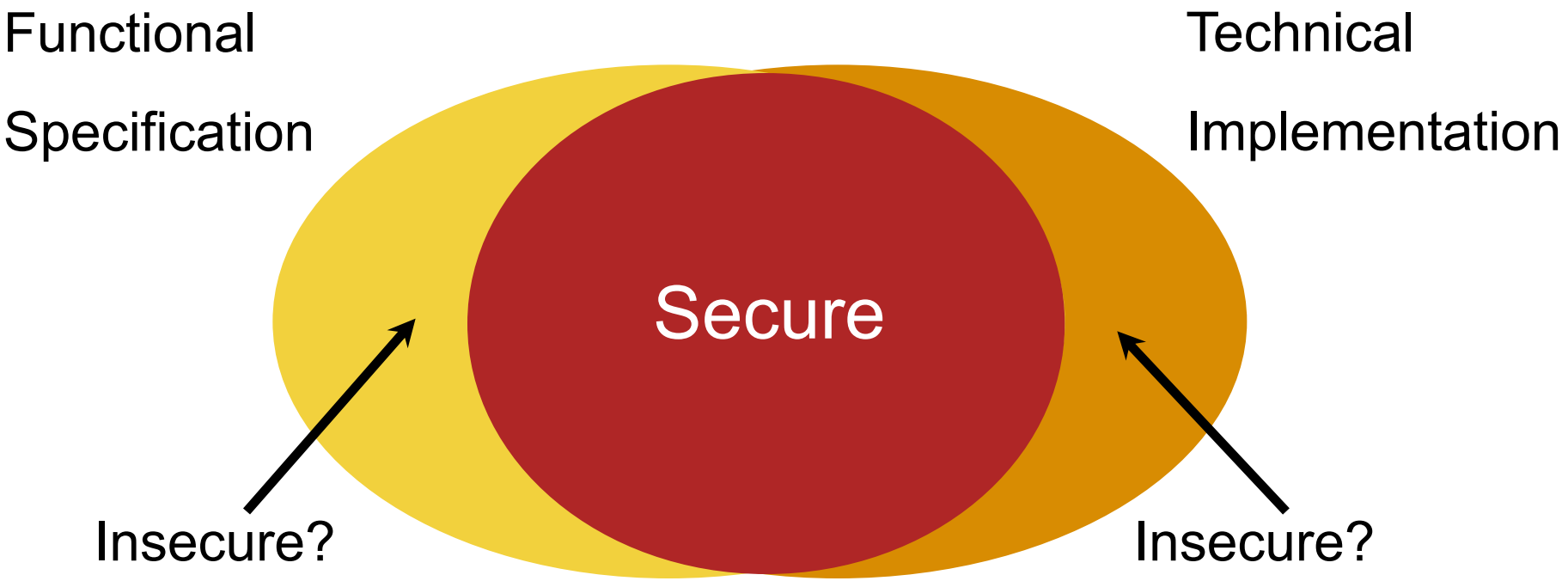





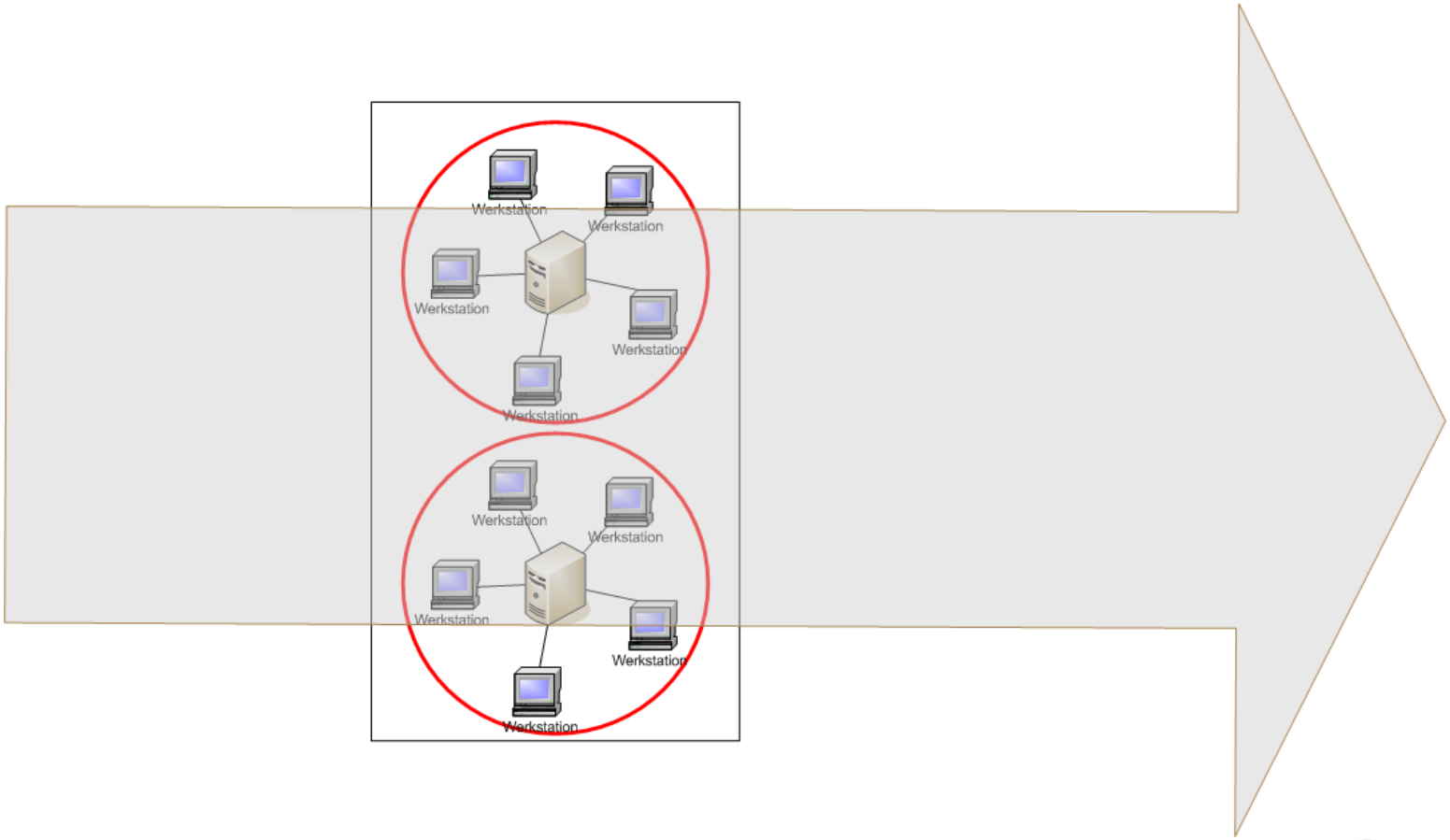

OWASP

# What is secure Software?

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



# Applications over time

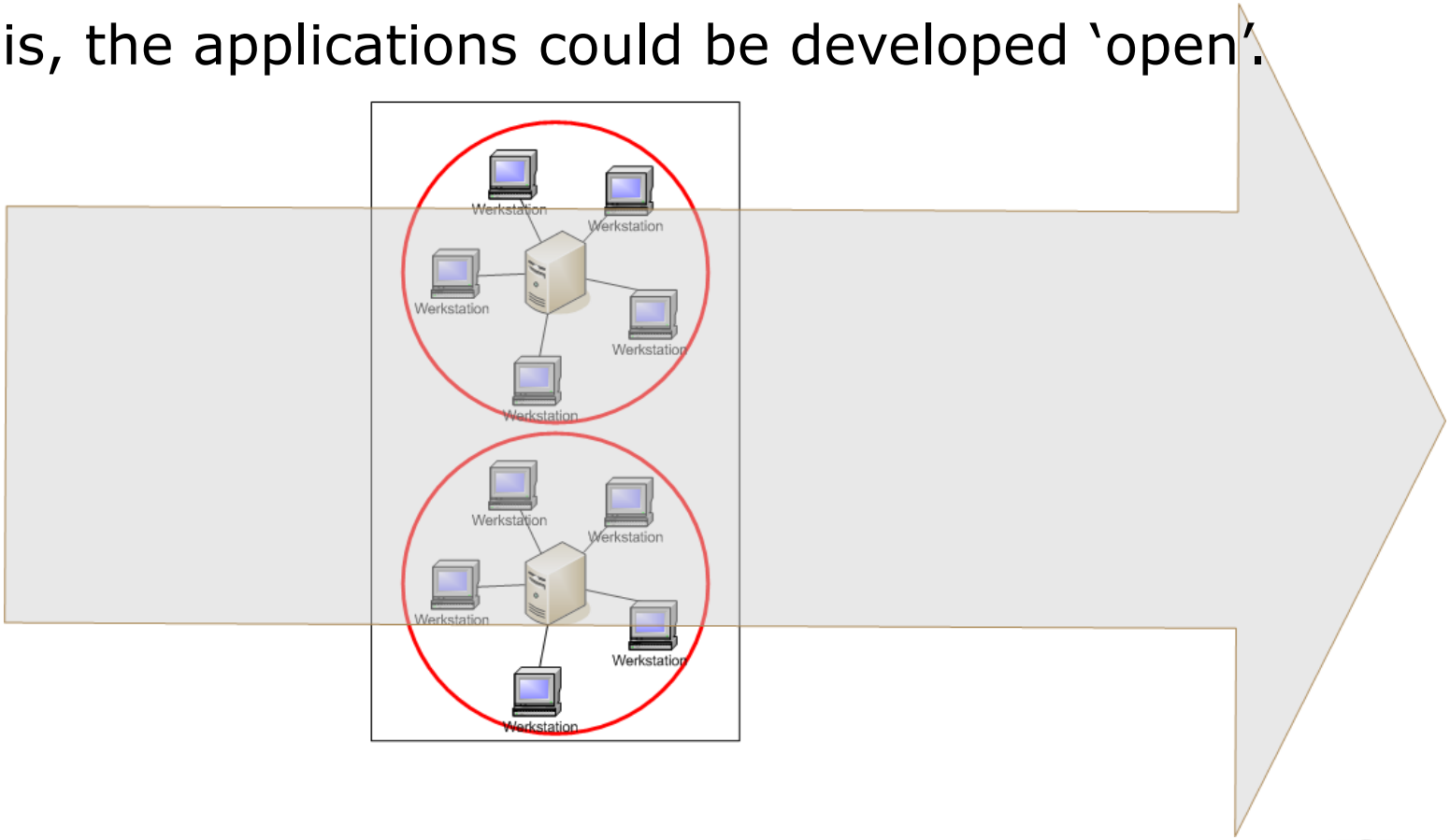



OWASP

# Applications over time

The environments in where the software applications run where closed.

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



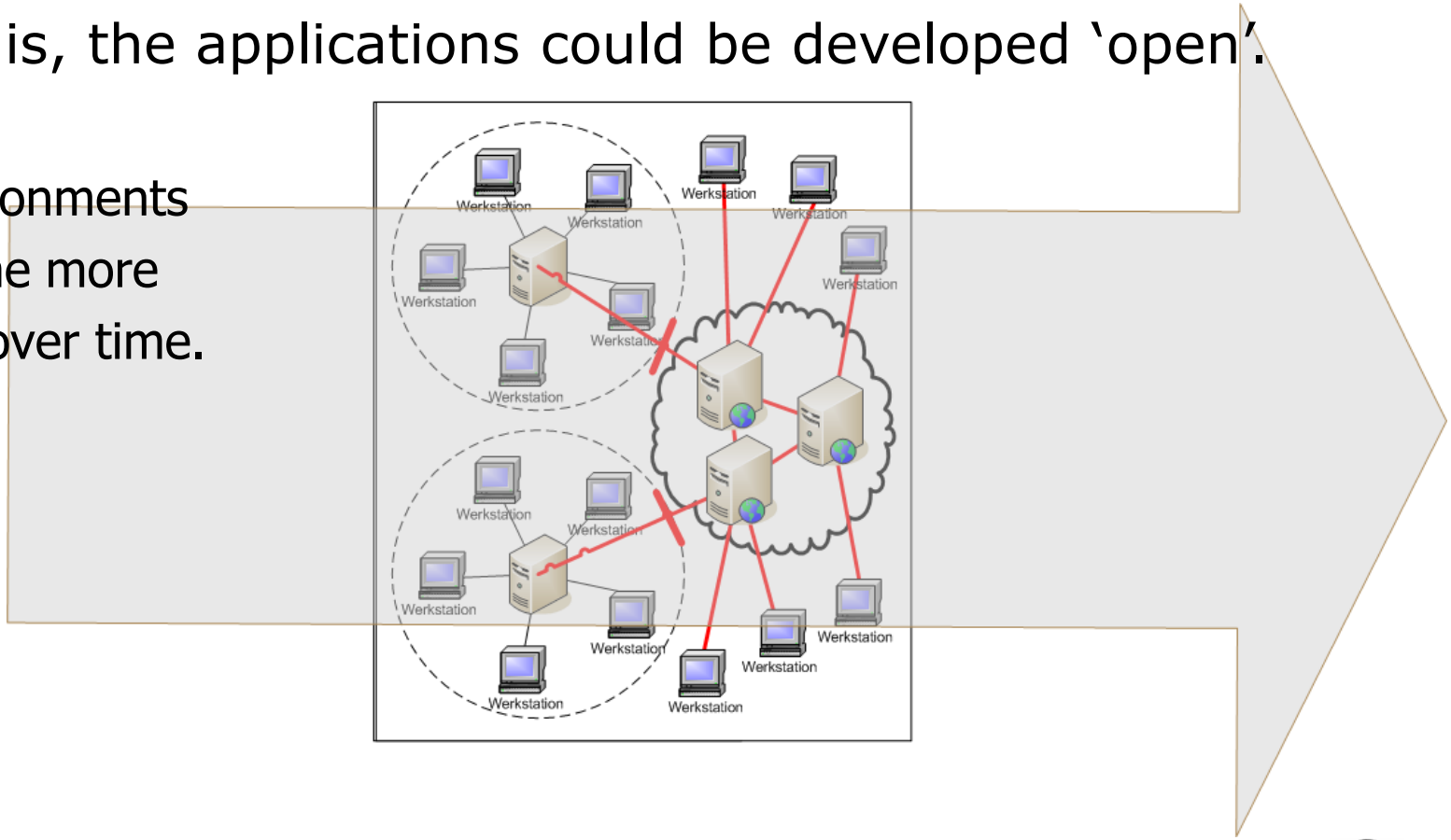

OWASP

# Applications over time

The environments in where the software applications run where closed.

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

The environments became more open over time.




OWASP

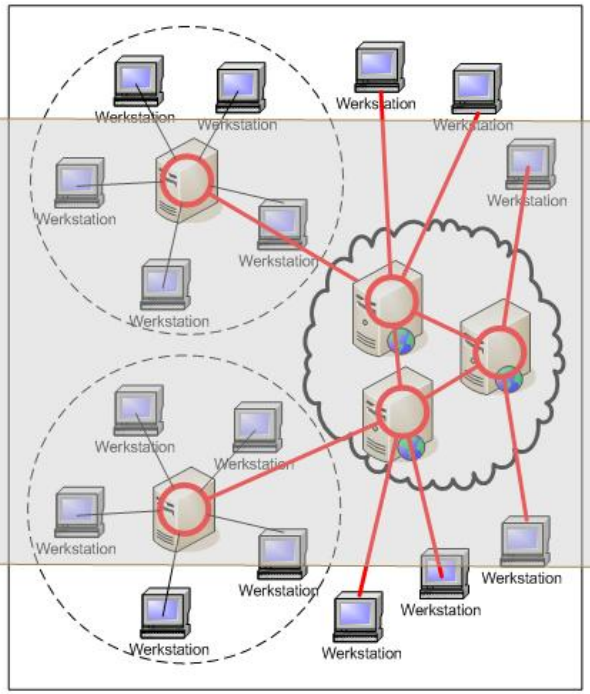
# Applications over time

The environments in where the software applications run where closed.

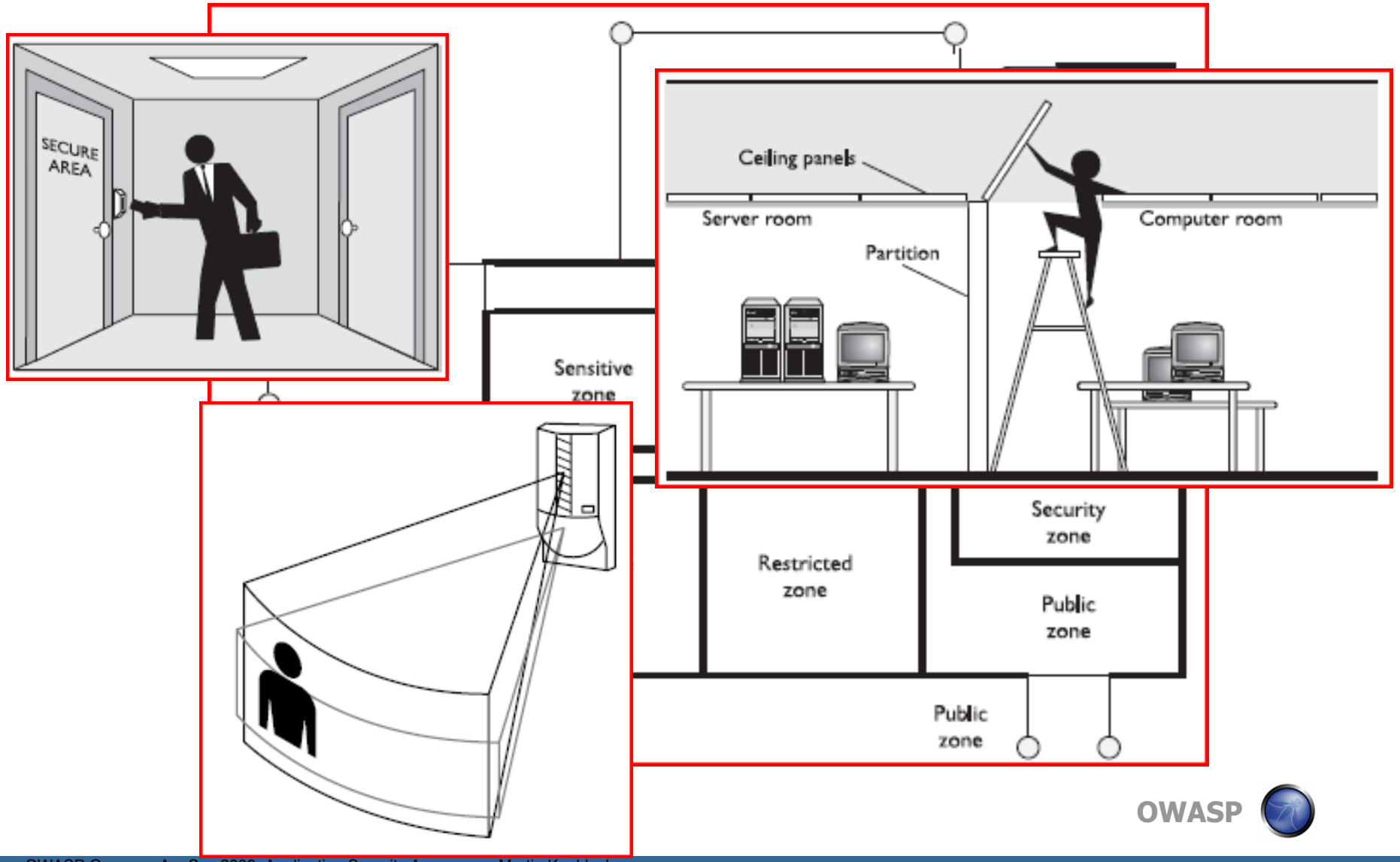
- By this, the applications could be developed ‘open’.

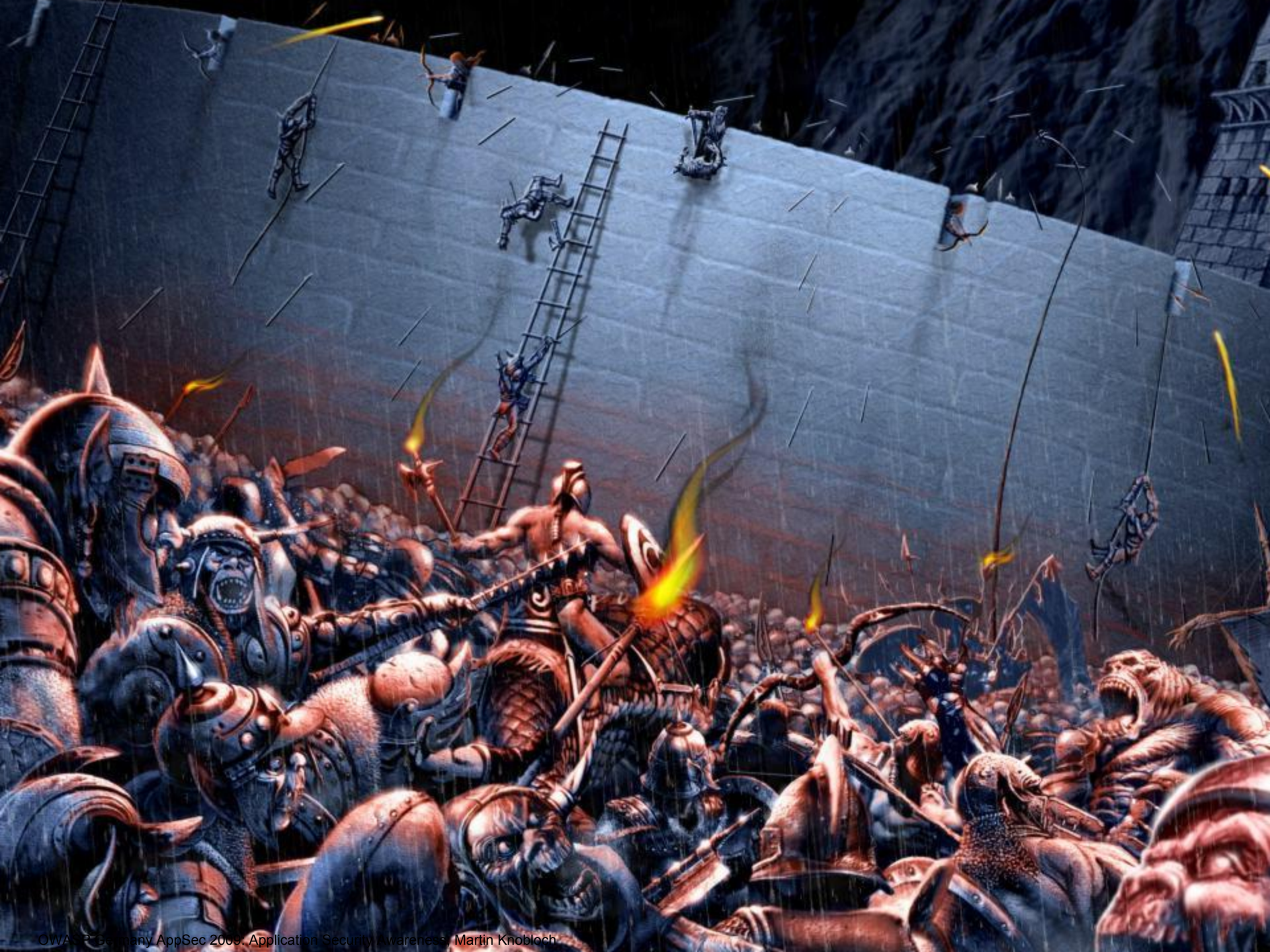
The environments became more open over time.

- What means, the applications have to become more closed.



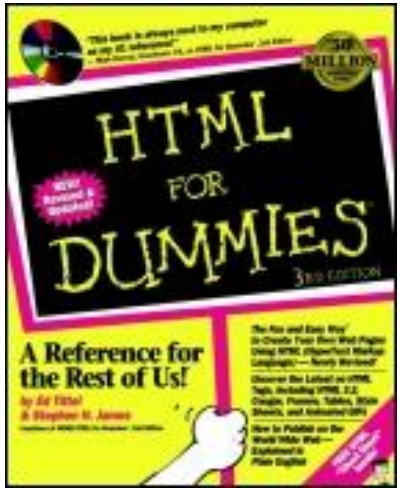
# Security Design & Architectuur

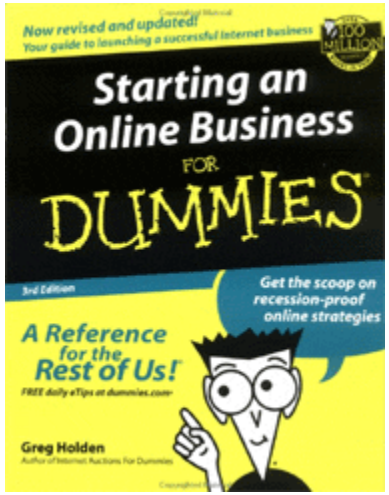


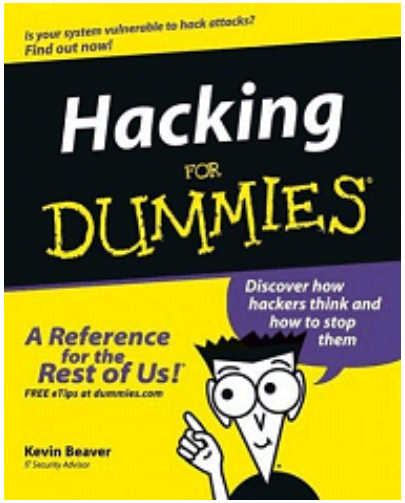


# The problem:

- Cookies, HTTP authentication, SLL..
- 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

OWASP

# Where do attacks come from?

Conscious us!

- Cracker
- Hacker ent
- Scriptki

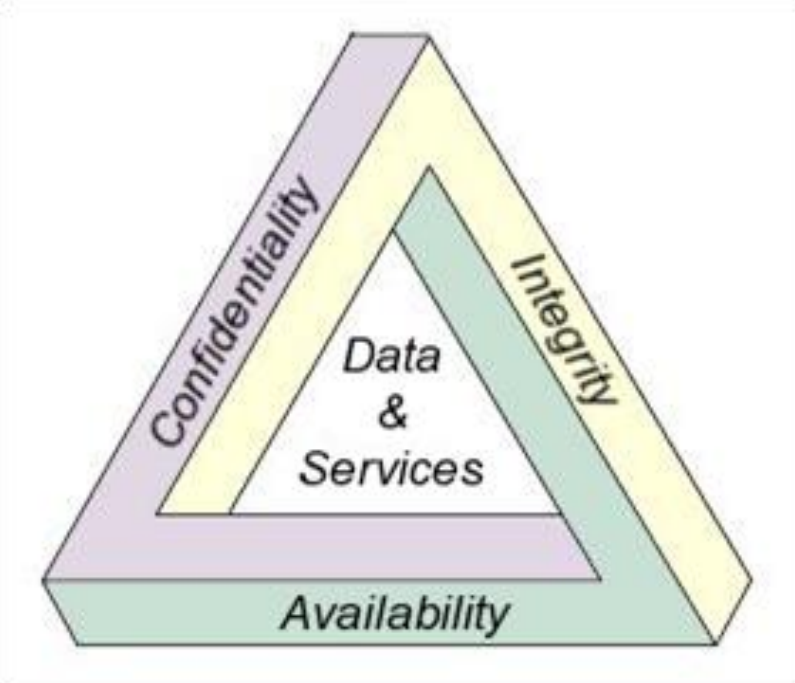
Risk= ue

OWASP

# What is Software Security about?

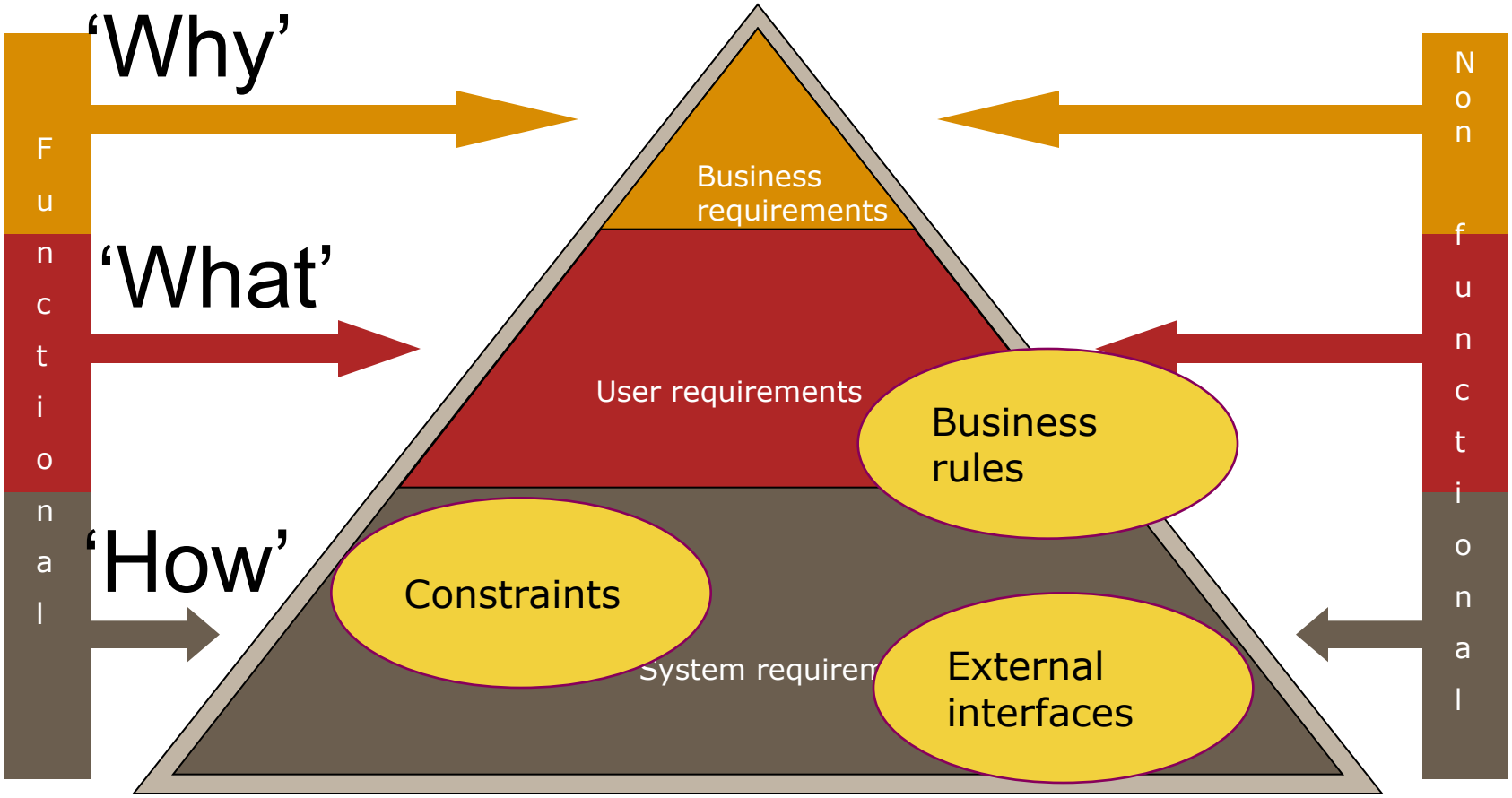
Applications are about information!

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




OWASP

# Security Requirements?



# What is Software Security about?

Who..

in what role?

thus, with what rights?

..may do..

..in which process..

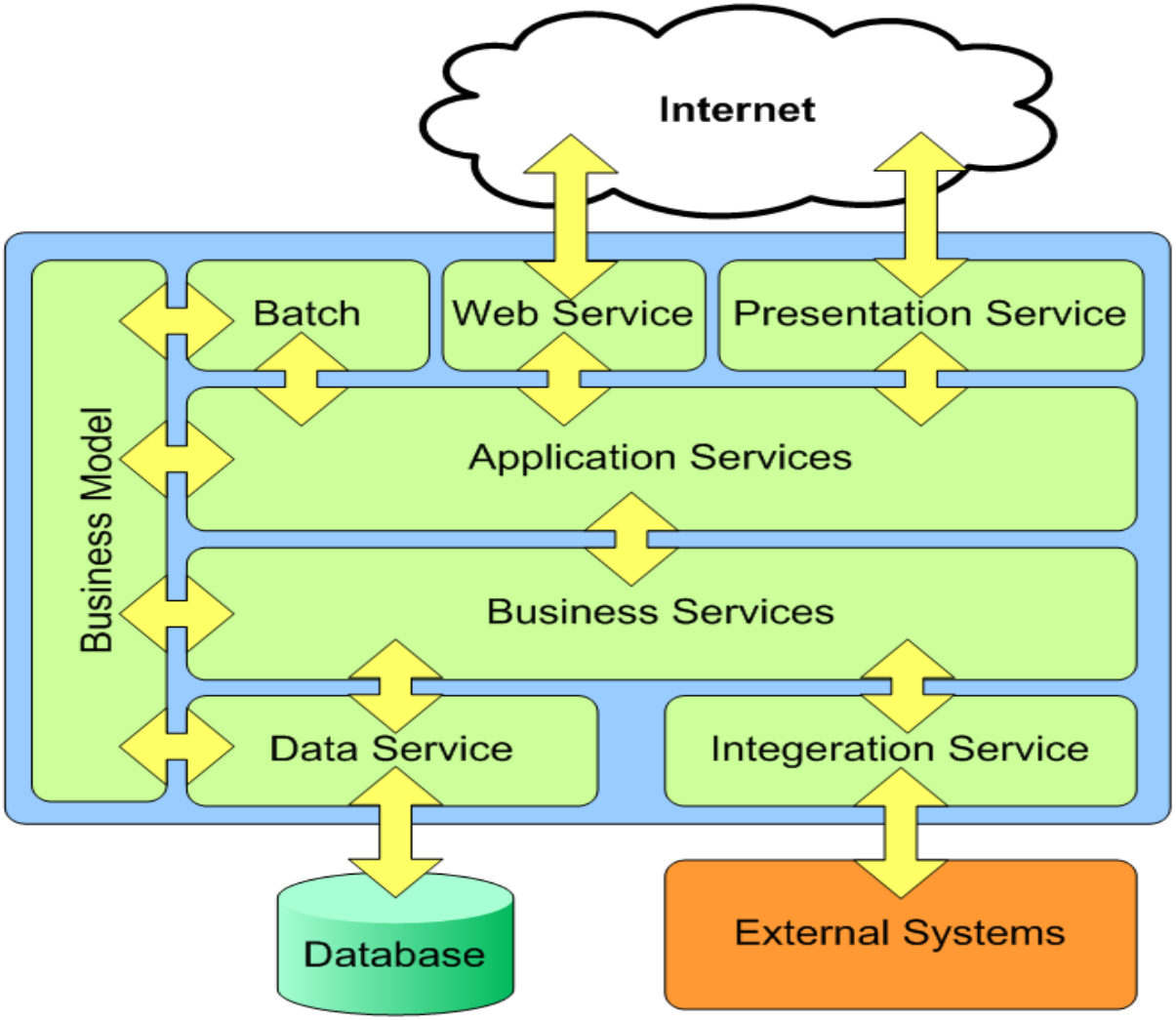
| | A | B | C |
|---|---|---|---|
| 1 | NAME PRODUCT | REFERENCE | PRICE |
| 2 | | | |
| 3 | PRODUCT 1 | REF : 452_KL | $ 44,10 |
| 4 | PRODUCT 2 | REF : 598_EW | $ 73,10 |
| 5 | PRODUCT 3 | REF : 1043_PO | $ 65,50 |
| 6 | PRODUCT 4 | REF : 1043_PO | $ 16,90 |
| 7 | PRODUCT 5 | REF : 581_EW | $ 40,30 |
| 8 | PRODUCT 6 | REF : 523_KL | $ 24,80 |
| 9 | PRODUCT 7 | REF : 946_OT | $ 41,00 |
| 10 | PRODUCT 8 | REF : 43_AL | $ 38,20 |
| 11 | PRODUCT 9 | REF : 1070_PO | $ 75,30 |
| 12 | PRODUCT 10 | REF : 394_HY | $ 59,30 |
| 13 | PRODUCT 11 | REF : 158_CF | $ 77,80 |
| 14 | PRODUCT 12 | REF : 779_IS | $ 41,10 |

Where..

..on what data?

OWASP

# Where 'is' Software Security?

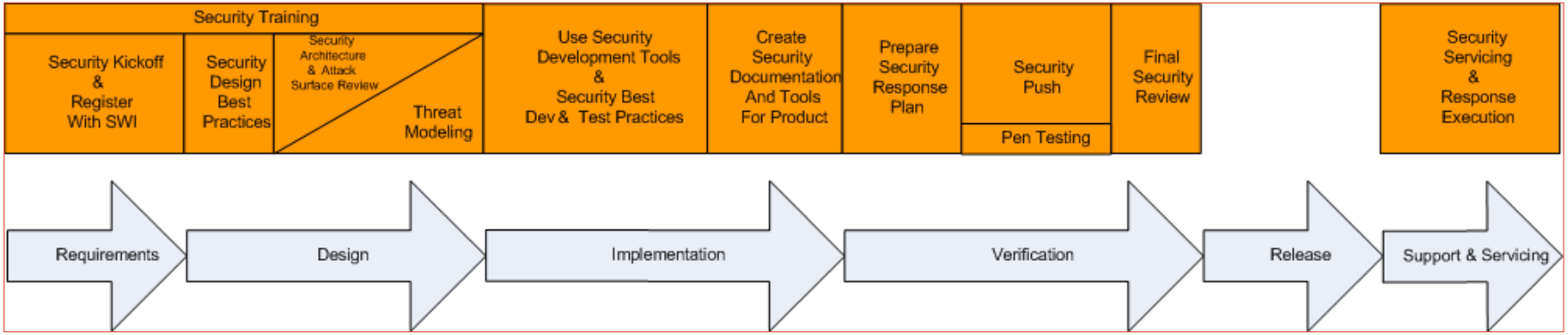


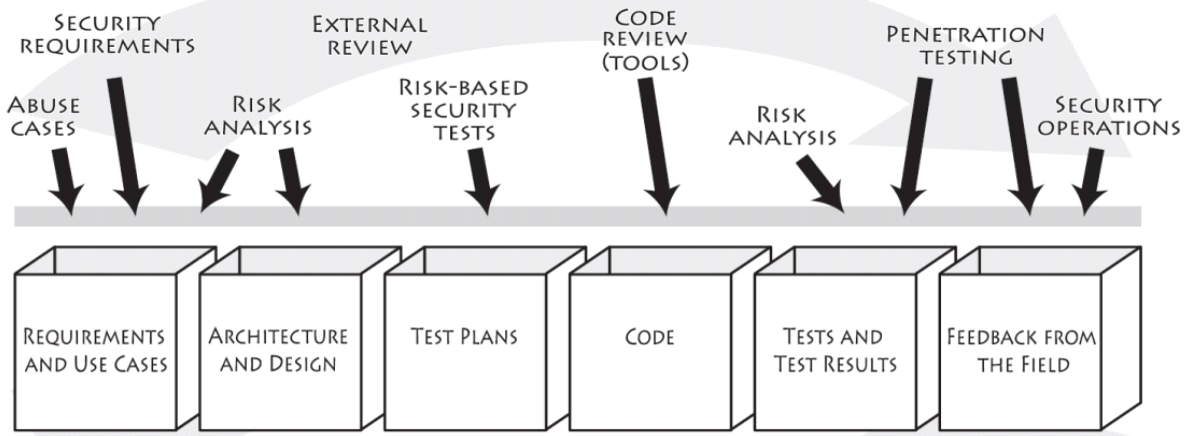

OWASP

# Software Architectuur?

# Security Development Lifecycles

## Microsoft SDL




CLASP

## Touchpoints

- 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?

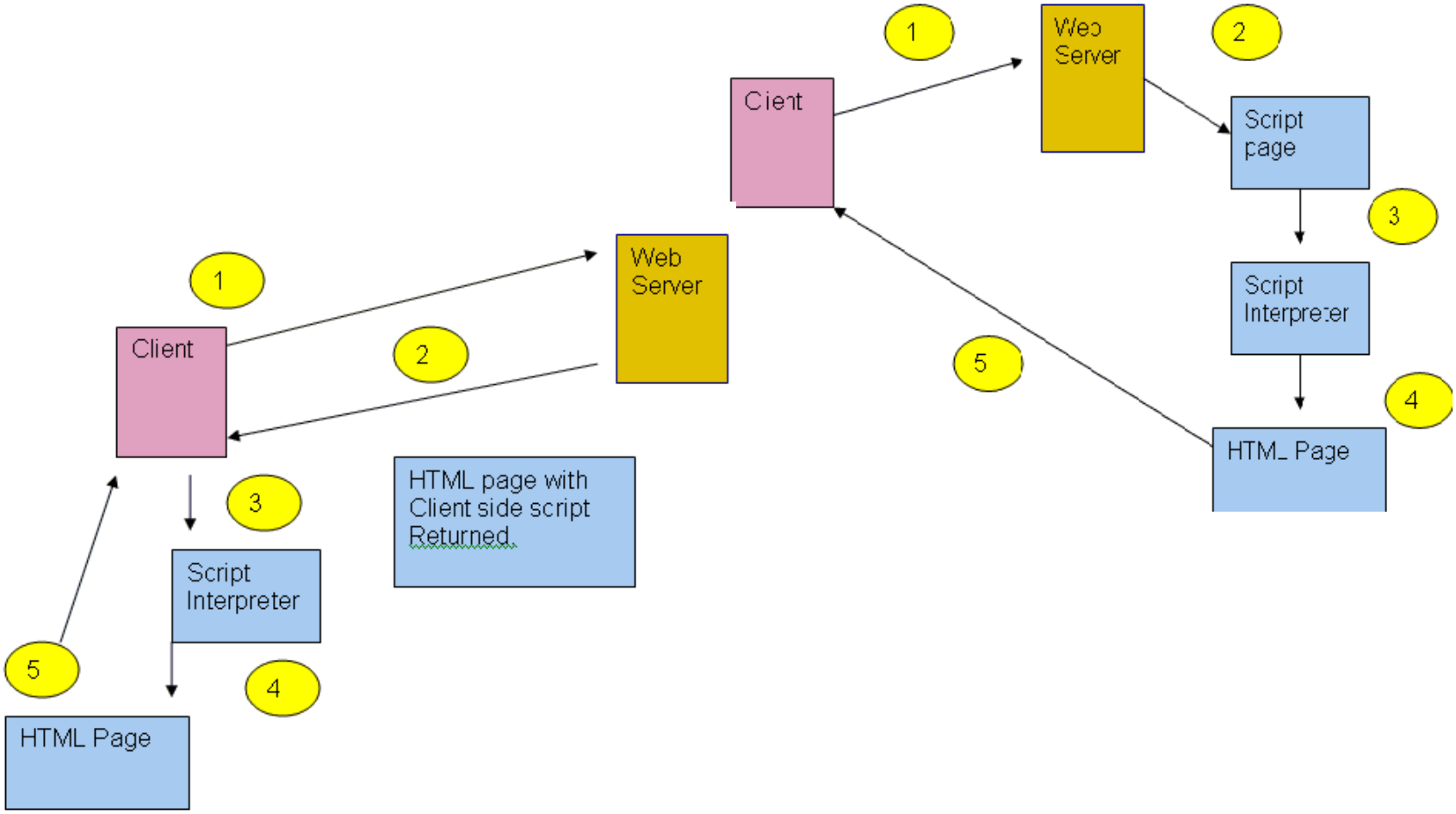
# Agenda

- What is OWASP
- Secure Application
- **OWASP Top Ten**
- OWASP near you

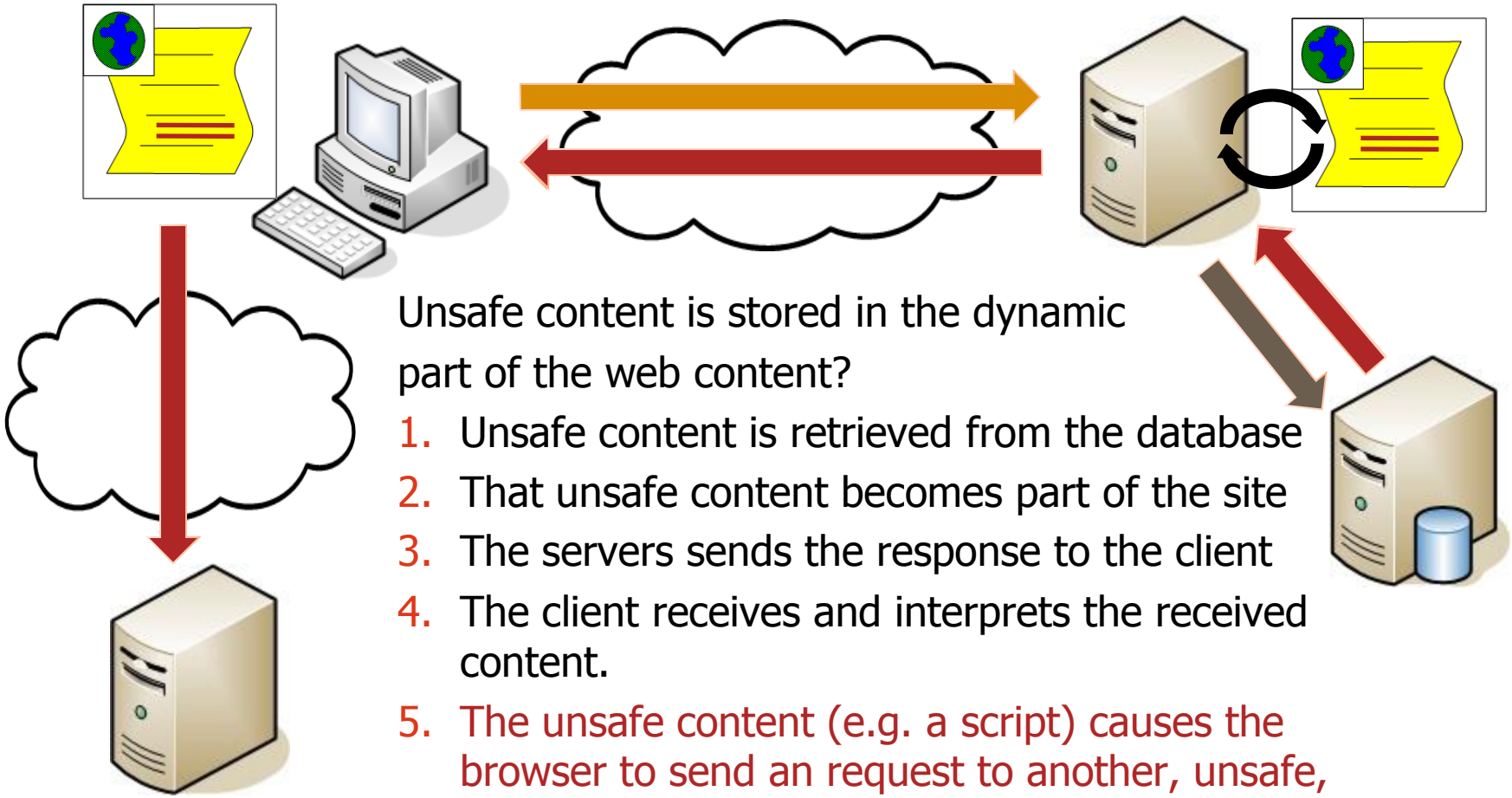
# OWASP TOP TEN

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)



# A1 Cross-Site Scripting (XSS)



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


OWASP

# 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'

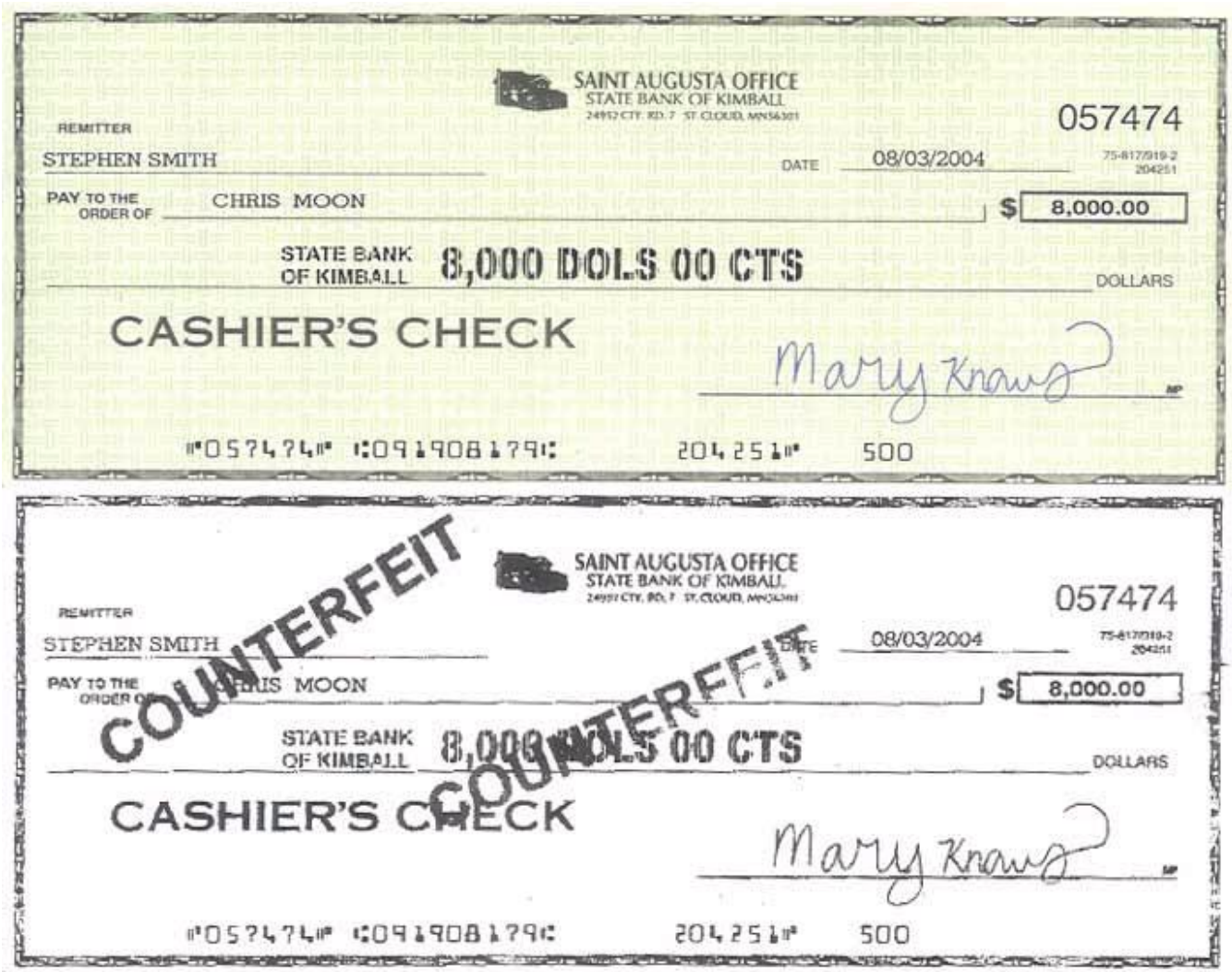
&

and the password is 'whatever' OR 1 = 1;

# A3 Malicious File Execution

# A4 Insecure Direct Object Reference

# A5 Cross-site Request Forgery (XSRF)

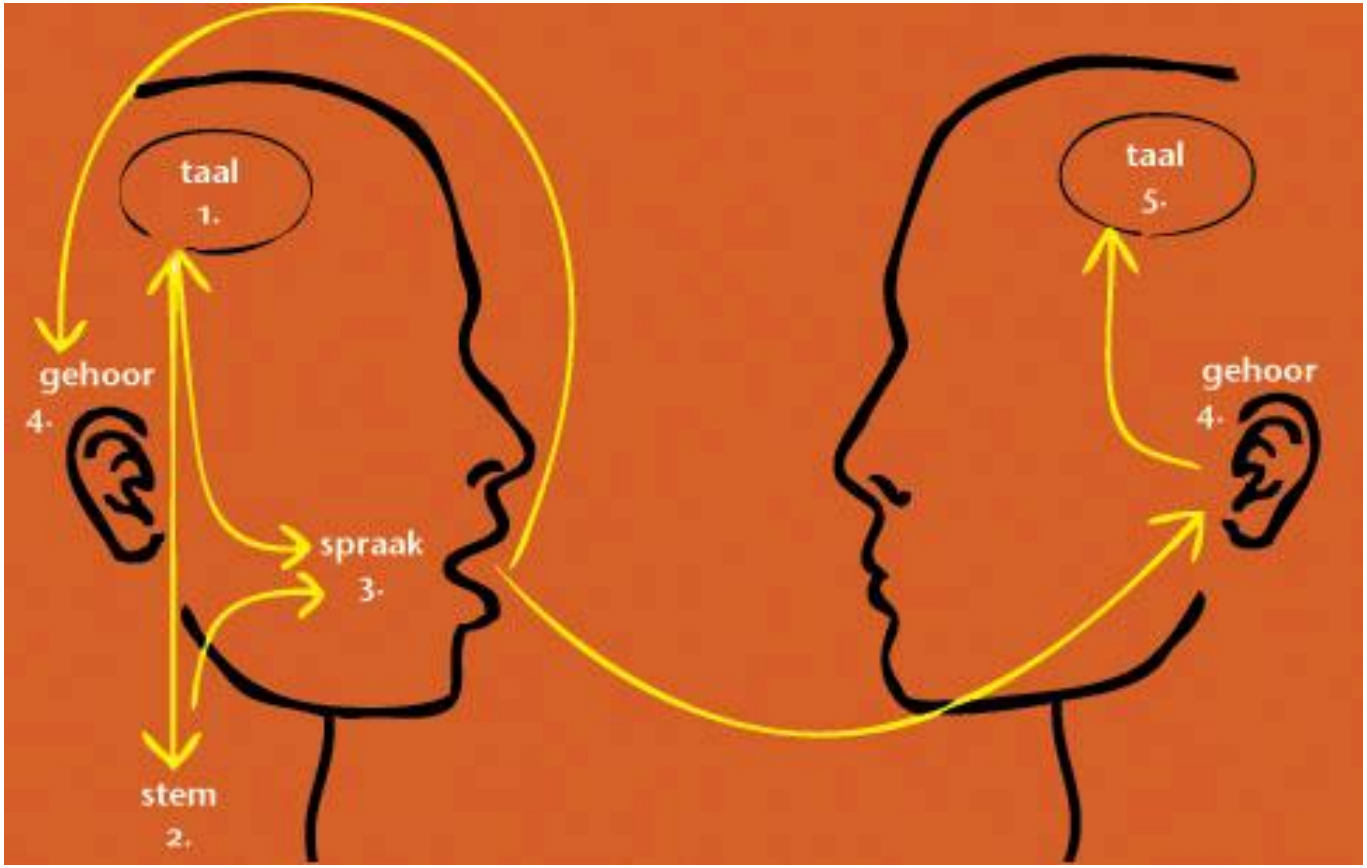


# A6 Information Leakage / Improper Error Handling

OWASP

# A8 Insecure Cryptographic Storage

# A9 Insecure Communication



# A10 Failure to Restrict URL Access

OWASP

# That's it...

..thank you!