



OWASP

Open Web Application
Security Project

Security Knowledge Framework

Making the web secure by design



OWASP

Open Web Application
Security Project

Authors:

Glenn ten Cate

Security Engineer @



Riccardo ten Cate

Security researcher

Agenda

- Why?
- Software (AND Security) development life cycle
- What is security knowledge framework
- Stages of development
- Guide
- Community



Why SKF?

- Security by design
- Information is hard to find
- Examples lack security details
- Security is hard
- Together we can create secure web applications
- Defensive coding approach
- SKF is the first step in SDLC



Software (AND Security) development life cycle

- OWASP Security knowledge framework
- Static code analysis
- Code reviews
- Security automation testing (Seccubus)
- Penetration test



What is S.K.F?

- **Guide to secure programming**

By adapting your design to security, not securing your design

- **Security awareness**

It informs you about threats even before you wrote a single line of code.

- **Clear and transparent**

Provides information applicable for your specific needs on the spot.



Stages of development

- Pre development stage

Here we detect threats before hand and we provide developers with secure development patterns as well as providing feedback and solutions on how to handle their threats.

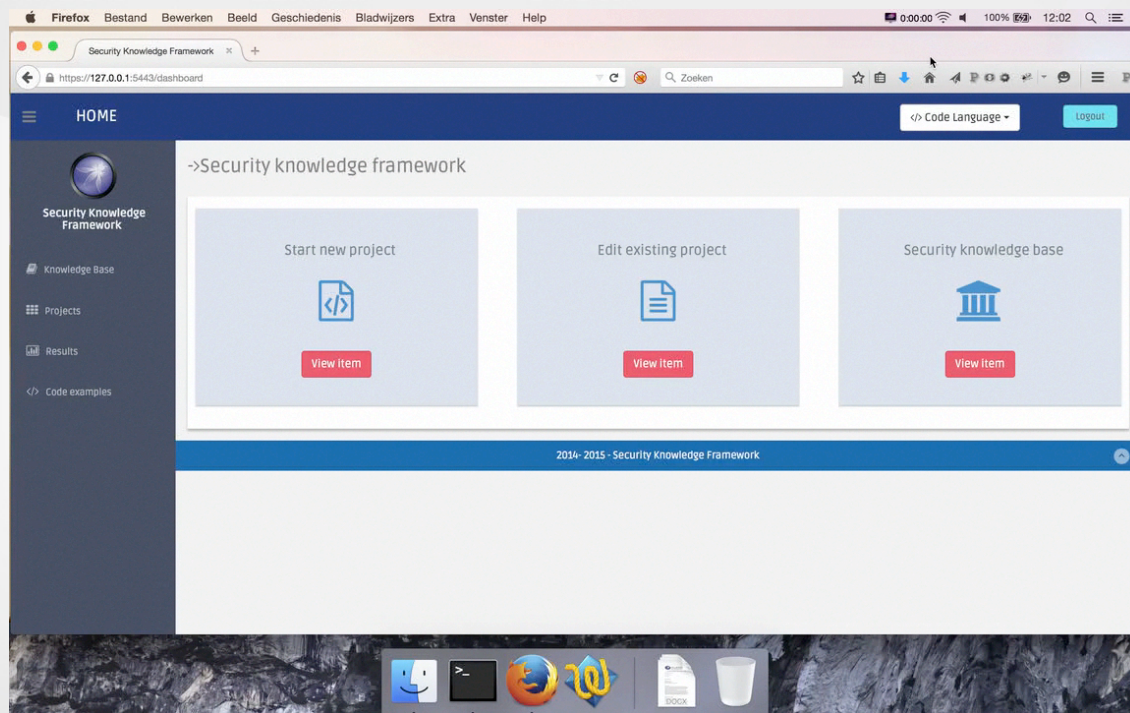
- Post development stage

By means of checklists we guide developers through a process where we harden their application infrastructure and functions by providing feedback and solutions



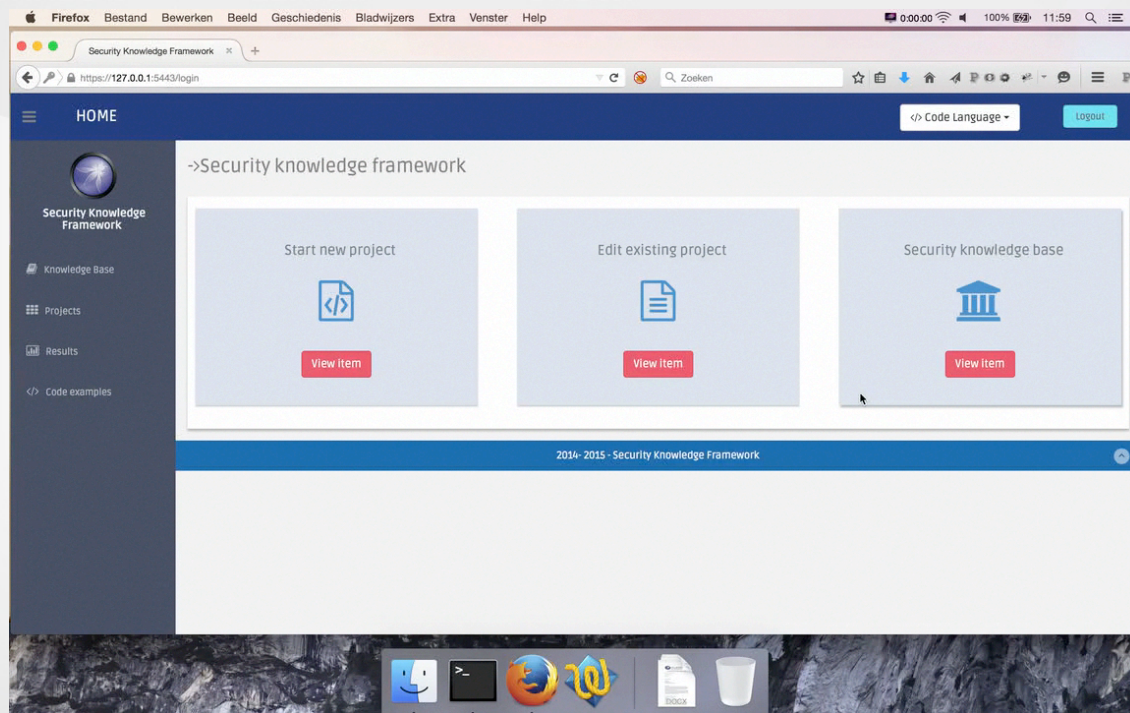
Guide

Pre development



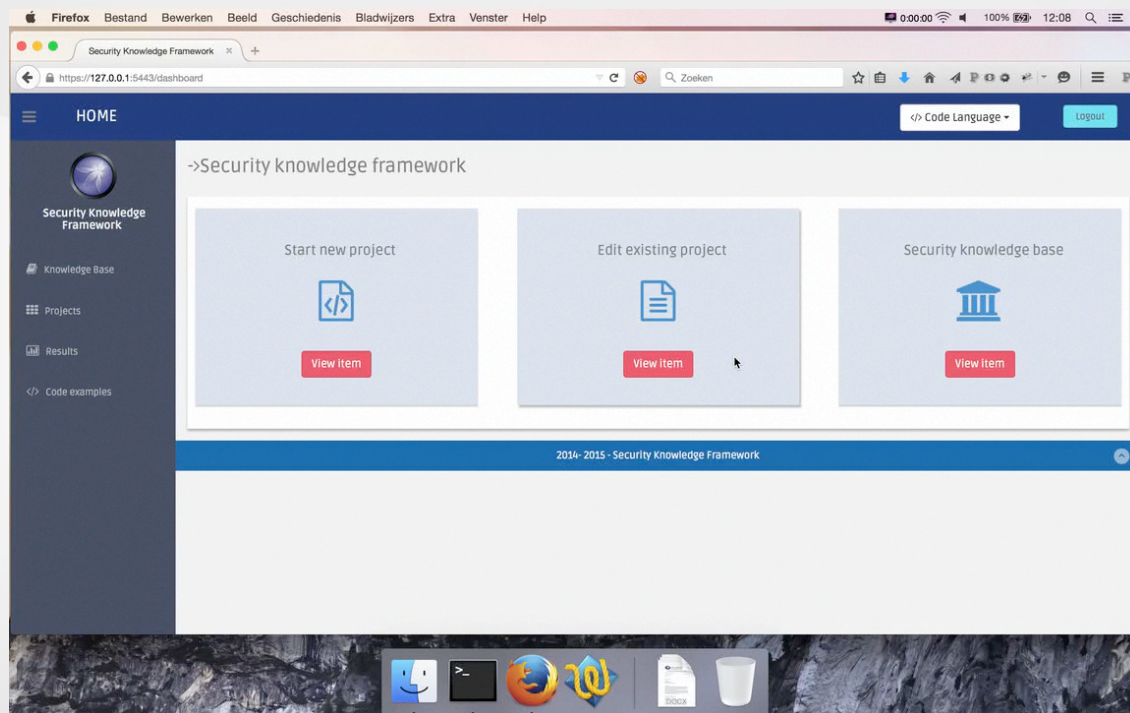
Guide

Post development



Guide

Knowledge base



Community

- Getting involved?

[https://www.owasp.org/index.php/
OWASP_Security_Knowledge_Framework](https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework)

Together we can make it Big, strong, and helpful!



CONNECT.

LEARN.

GROW.

Questions?



OWASP
Open Web Application
Security Project