Application Security Testing with ZAP

Open World Forum 2014
Paris – France

Sébastien Gioria
Sebastien.Gioria@owasp.org
Chapter Leader & Evangelist OWASP France

OWASP
The Open Web Application Security Project

OPEN WORLD FORUM

#OWF14

Warning !

- This talk is not ##pjlterrorisme compatible !
- This talk is not #LCEN compatible !
- Using the material from this talk could bring you to jail :
  - R323-1 to R323-5 Code Penal

OWASP
The Open Web Application Security Project

http://www.google.fr/#q=sebastien gioria

- Innovation and Technology @Advens && Application Security Expert

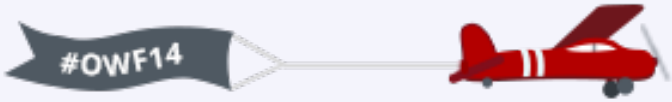
- OWASP France Leader & Founder & Evangelist,

- OWASP ISO Project & OWASP SonarQube Project Leader
- Application Security group leader for the CLUSIF

- Proud father of youngs kids trying to hack my digital life.

Twitter :@SPoint/@OWASP_France

OPEN WORLD FORUM



Agenda

OWASP
The Open Web Application Security Project

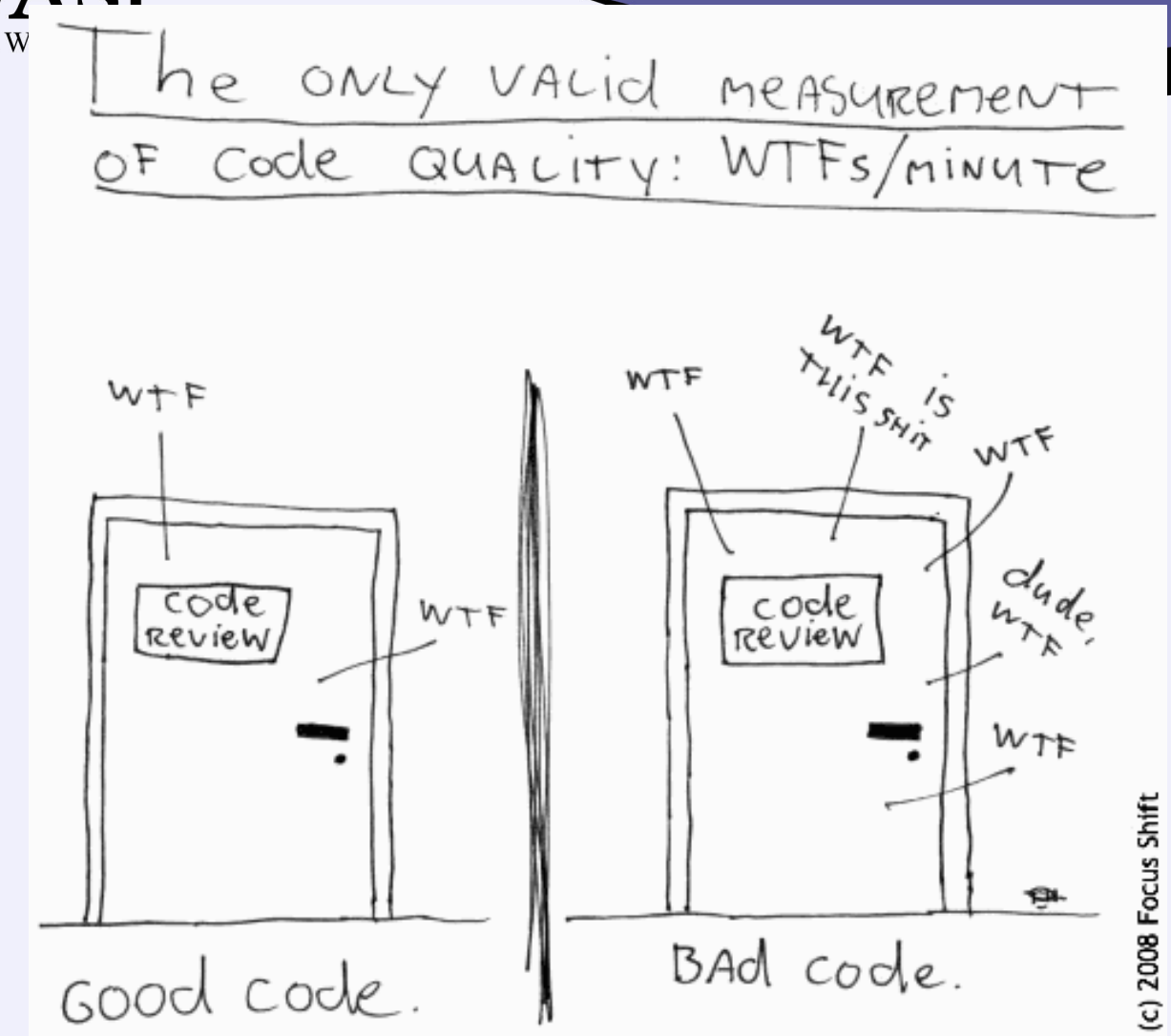
- Why you should be using ZAP
- Introduction to ZAP
- ZAP Use cases
- ZAP API
- ZAP Scripting
- Wrap up

Before we start

OWASP
The Open Web Application Security Project

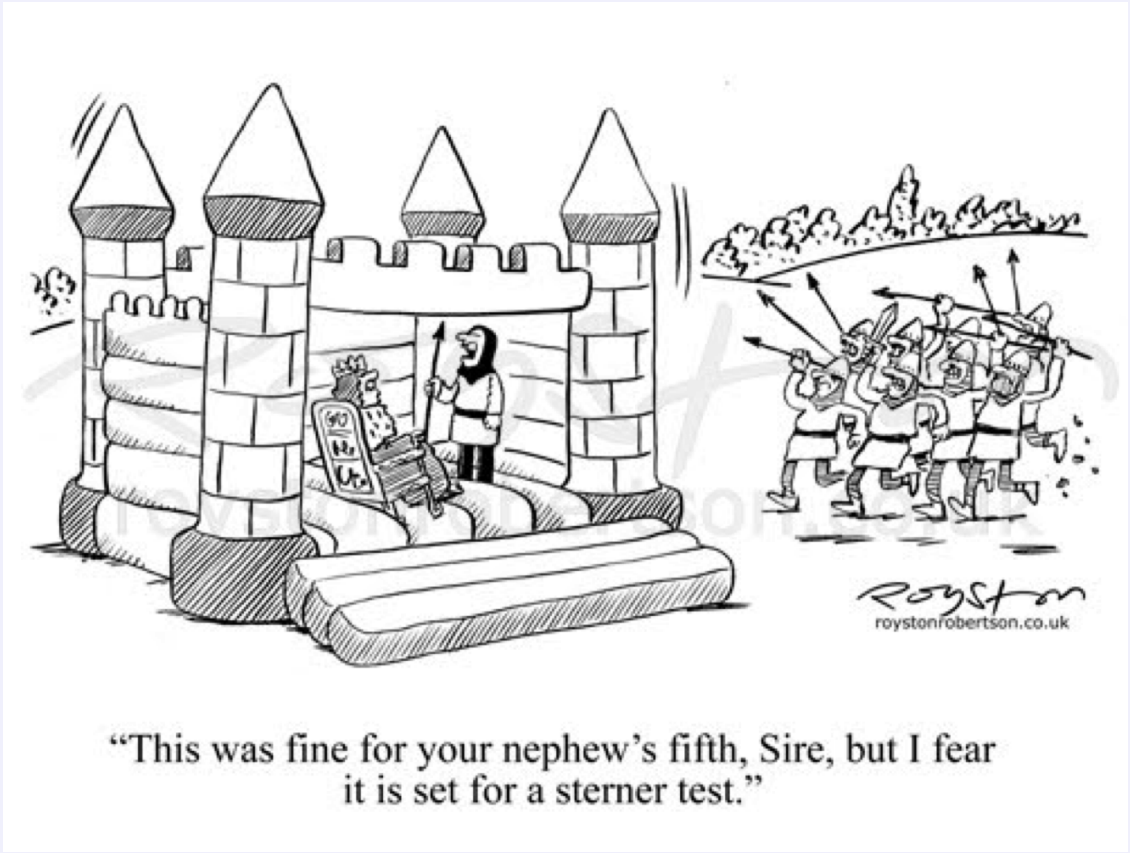
- Who's heard of OWASP?
- Who's heard of ZAP?
- Who's used ZAP?
- Who does *any* security testing in development?
- Who thinks they do *enough* security testing in development?

Application Security in a nutshell



OWASP
The Open Web Application Security Project

- "You cannot build secure web applications unless you know how they will be attacked"



OPEN WORLD FORUM

- Thanks to Royston Robertson www.roystonrobertson.co.uk for permission to use his cartoon!

The problems

OWASP
The Open Web Application Security Project

- Most devs know little about security
- Most companies have too few appsec folk
- External appsec people cost $$$
- Security testing is done late in the development lifecycle (if at all)

Part of the solution

OWASP
The Open Web Application Security Project

- Use a security tool like ZAP in development :)

- In addition to a security training, secure development lifecycle, threat modeling, static source code analysis, code reviews, professional pentesting...

What's ZAP ?

OWASP
The Open Web Application Security Project

- An easy to use webapp pentest tool
- Completely free and open source
- Ideal for beginners
- But also used by professionals
- Ideal for devs, esp. for automated security tests
- Becoming a framework for advanced testing
- Included in all major security distributions
- ToolsWatch.org Top Security Tool of 2013
- Not a silver bullet!

Zap principles

OWASP
The Open Web Application Security Project

- Free, Open source
- Involvement actively encouraged
- Cross platform (Yes, build in Java)
- Easy to use
- Easy to install
- Internationalized
- Fully documented
- Work well with other tools
- Reuse well regarded components

Some stats

OWASP
The Open Web Application Security Project

- Released September 2010, fork of Paros
- V 2.3.1 released in May 2014
- V 2.3.1 downloaded > 70K times
- Translated into 20+ languages
- Over 100 translators
- Mostly used by Professional Pentesters?
- The most active OWASP Project
- 27 active contributors
- 329 years of effort

Why would you use Zap ?

OWASP
The Open Web Application Security Project

- Explore your application
- Configure ZAP for your application
- Passive scanning runs automatically
- Run active scanner
- Fine tuning?
- Perform manual testing?

What you need to configure to use it

OWASP
The Open Web Application Security Project

- Pages to ignore (logout, duplicates)
- Anti CSRF tokens
- Session handling
- Authentication
- Users
- Structure (single page apps)
- 'Non standard' separators e.g. aaa:bbb;ccc:ddd

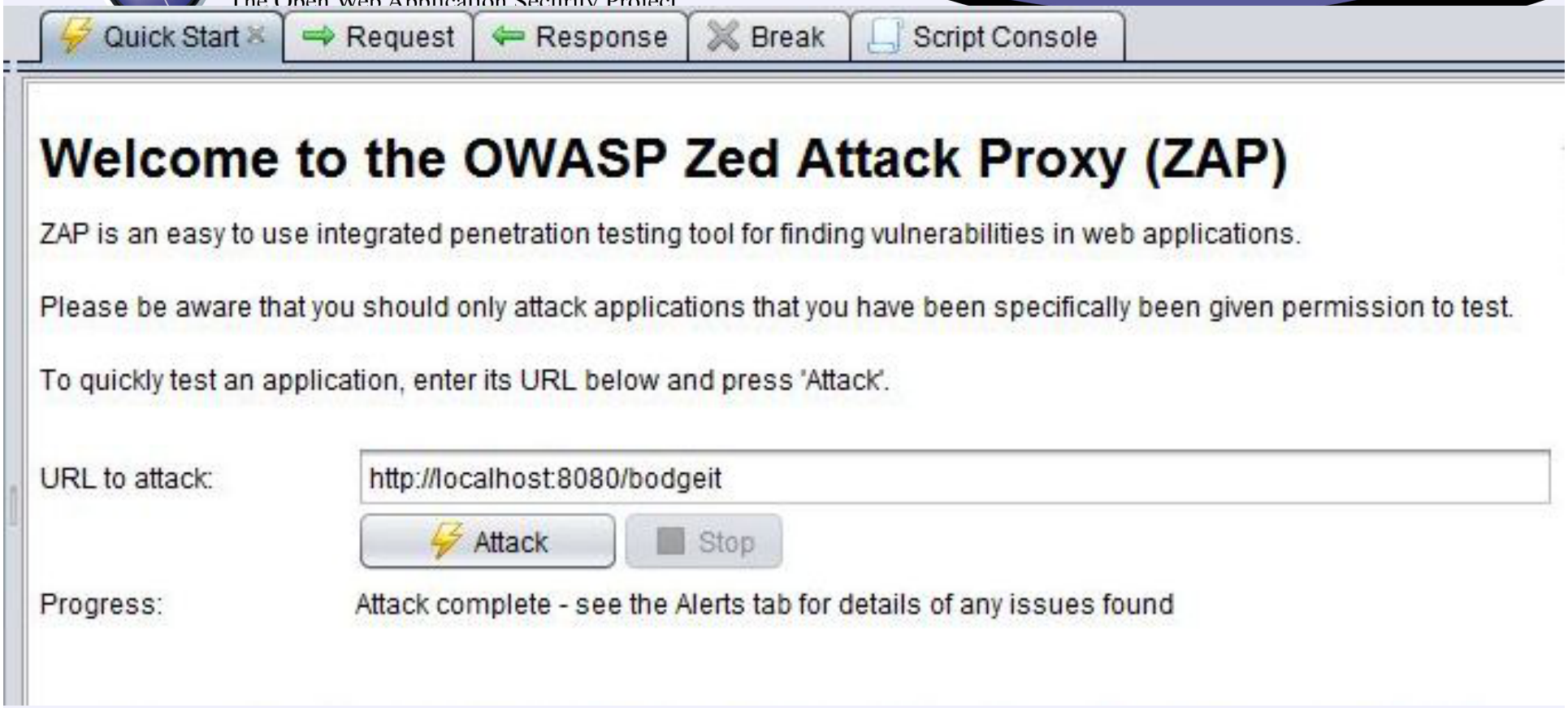
Zap use cases

OWASP
The Open Web Application Security Project

- Point and shoot – the Quick Start tab
- Proxying via ZAP, and then scanning
- Manual pentesting
- Automated security regression tests
- Debugging
- Part of a larger security program

QuickStart

OWASP
The Open Web Application Security Project



Using as a Proxy

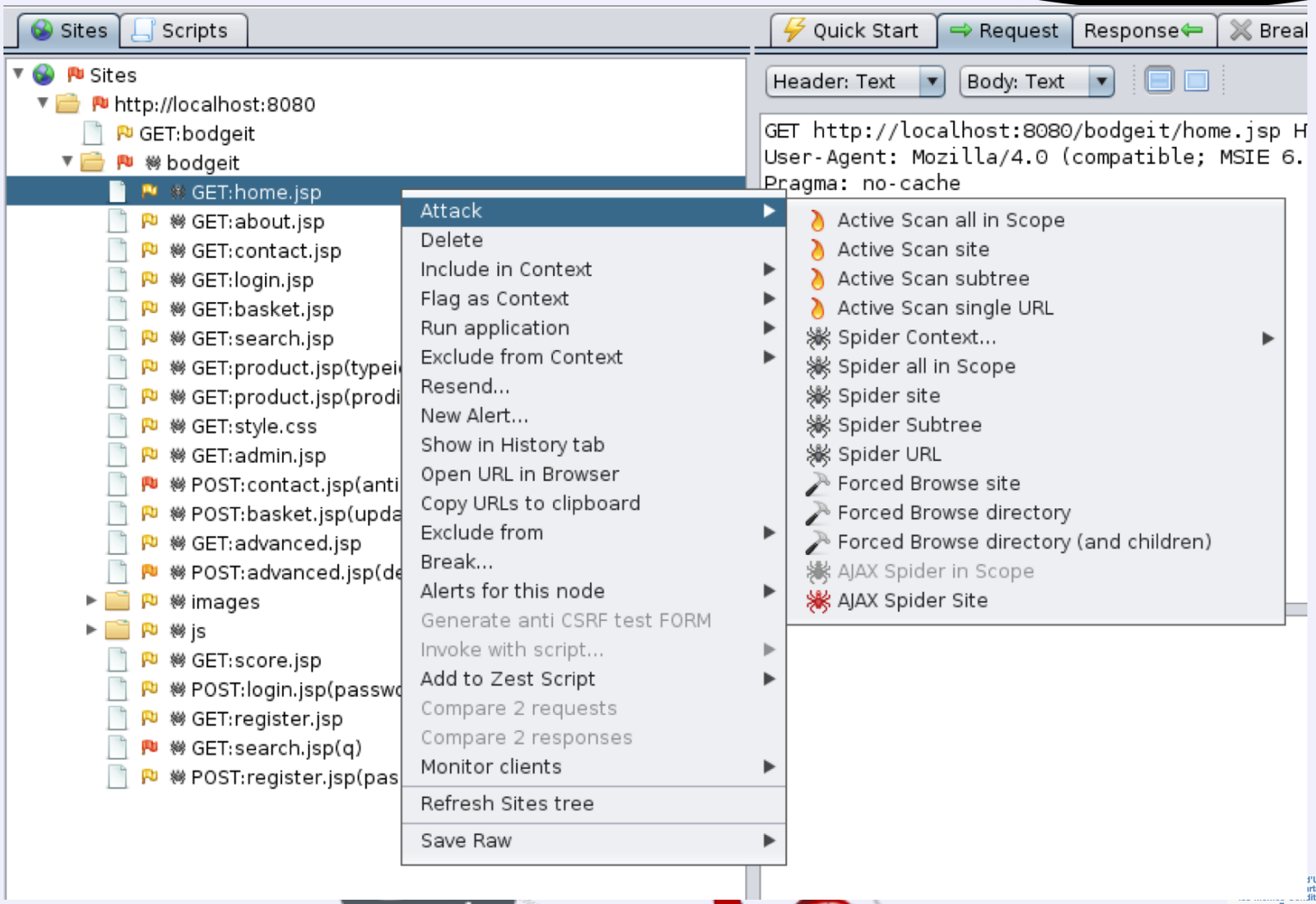
OWASP
The Open Web Application Security Project

- Options:
- Plug-n-Hack

- Configure your browser's proxy manually

Right Click program

OWASP
The Open Web Application Security Project

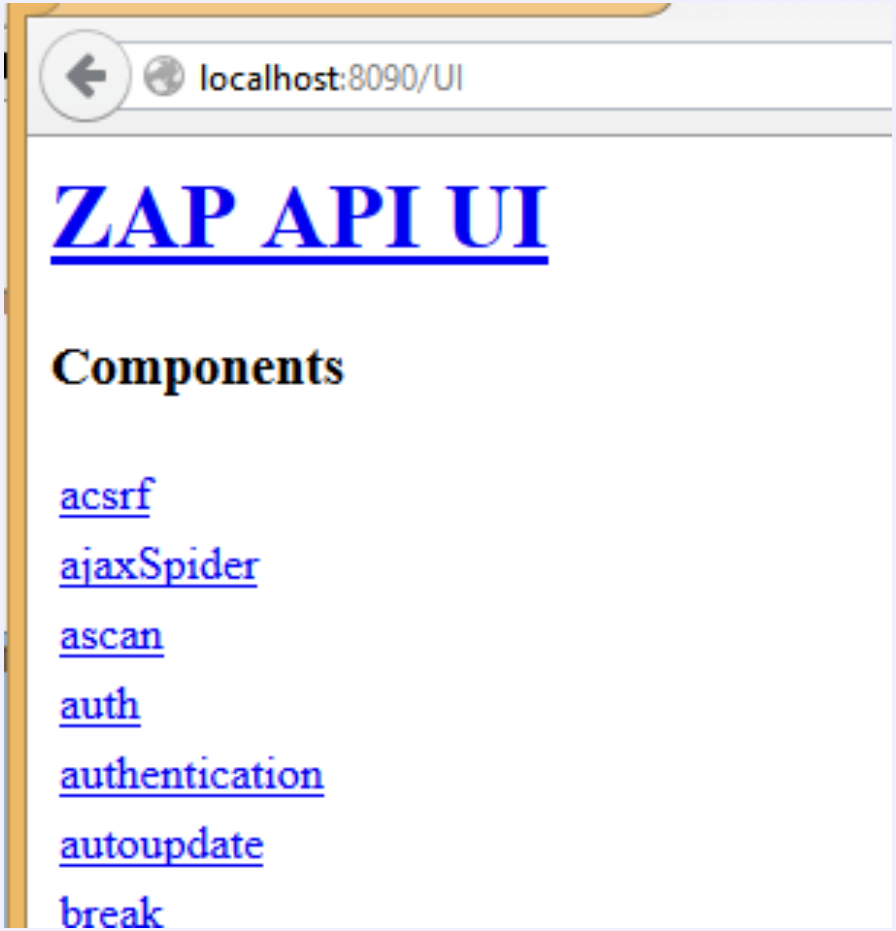


OPEN WORLD FORUM

#OWF14

ZAP Api

OWASP
The Open Web Application Security Project



- Direct access via:
- http://zap/ (if proxying through ZAP)
- http://<ip address>:<port>
- API Clients:
- Java
- Python
- Node.js
- PHP
- https://code.google.com/p/zaproxy/wiki/ApiDetails

Scripting ?

OWASP
The Open Web Application Security Project

- Full access to ZAP internals
- Support all JSR 223 languages, inc
- JavaScript
- Jython
- JRuby
- Zest :)

OWASP
The Open Web Application Security Project

Different types of scripts

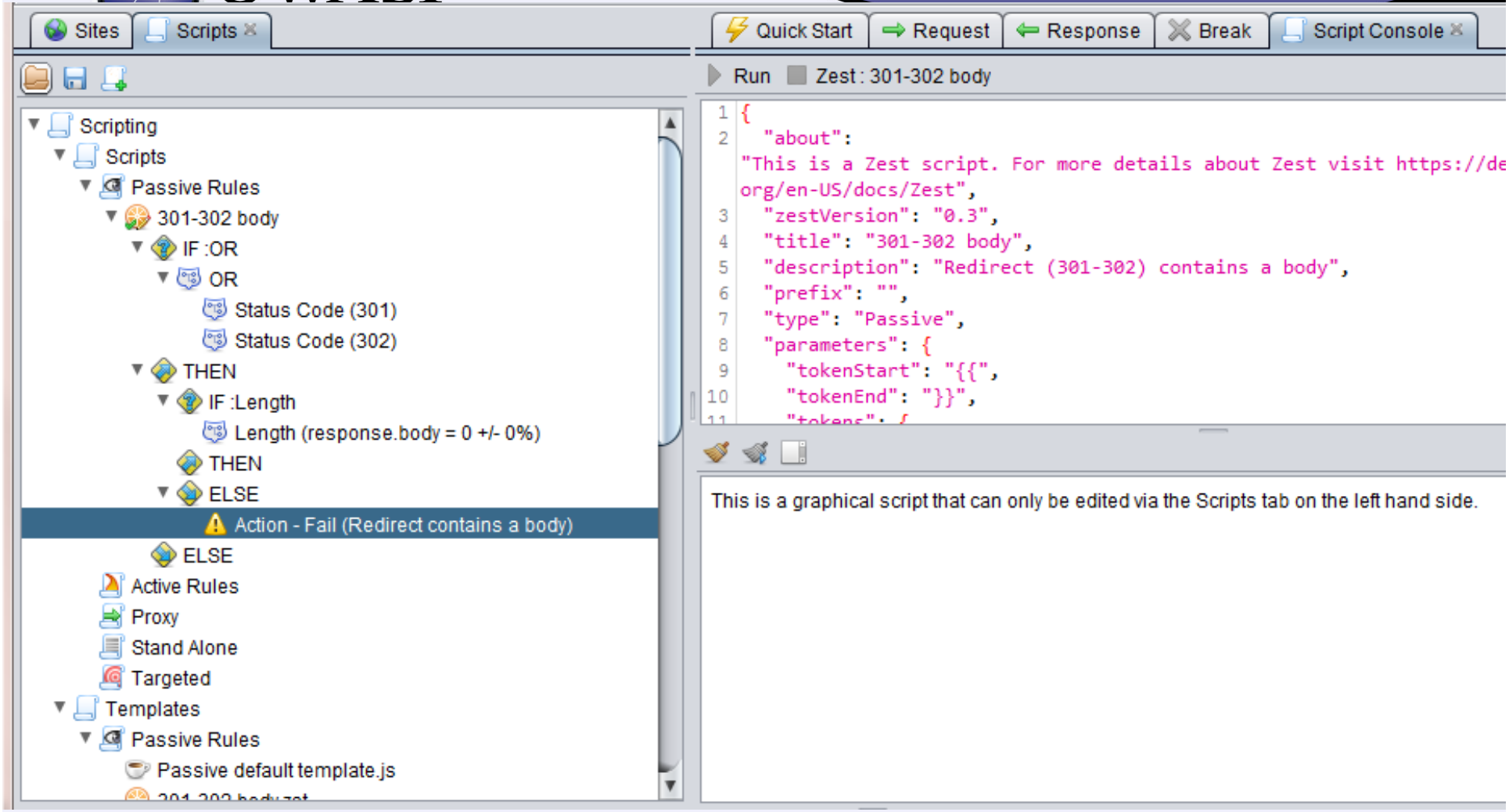
• Stand alone	Run when you say
• Targeted	Specify URLs to run against
• Active	Run in Active scanner
• Passive	Run in Passive scanner
• Proxy	Run 'inline'
• Authentication	Complex logins
• Input Vector	Define what to attack

Zest, experimental scripting

OWASP
The Open Web Application Security Project

- An experimental scripting language
- Developed by Mozilla Security Team
- Free and open source (of course)
- Format: JSON – designed to be represented visually in security tools
- Tool independent – can be used in open and closed, free or commercial software
- Essentially ZAP's macro language
- Supports all ZAP default script types

Zest Script



Where to find ZAP ?

OWASP
The Open Web Application Security Project

- OWASP Zap Official Page :
  - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
- Code :
  - Currently on Google Code
  - Will probably move to GitHub when time allows
- Hacking ZAP blog series: https://code.google.com/p/zaproxy/wiki/Development
- ZAP Internals: https://code.google.com/p/zaproxy/wiki/InternalDetails
- ZAP Dev Group: http://groups.google.com/group/zaproxy-develop

You must use ZAP !

OWASP
The Open Web Application Security Project

- You need to consider security in all stages of development
- ZAP is an ideal tool for automating security tests
- Its also a great way to learn about security
- Its a community based tool – get involved!

Démo

Thanks

OWASP
The Open Web Application Security Project

- Simon Bennetts (@psiinon) ; principal author of Zap and of this slides

- @SncfMonAmour: who was in time yesterday ☺
- @AsahiUK and @GuinnessIreland : giving energy
- @BushmillsGlobal ; giving strenght

OPEN WORLD FORUM

#OWF14

License

OWASP
The Open Web Application Security Project

@SPoint

sebastien.gioria@owasp.org