

# Application Security Testing with ZAP



## Open World Forum 2014 Paris – France

**Sébastien Gioria**

[Sebastien.Gioria@owasp.org](mailto:Sebastien.Gioria@owasp.org)

Chapter Leader & Evangelist OWASP France



# OWASP

The Open Web Application Security Project

**OPEN  
WORLD  
FORUM**

#OWF14



Warning !



# OWASP

The Open Web Application Security Project

- 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**



Attribution - Pas d'Utilisation  
Commerciale - Partage dans  
les Mêmes Conditions 3.0  
France





- 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?





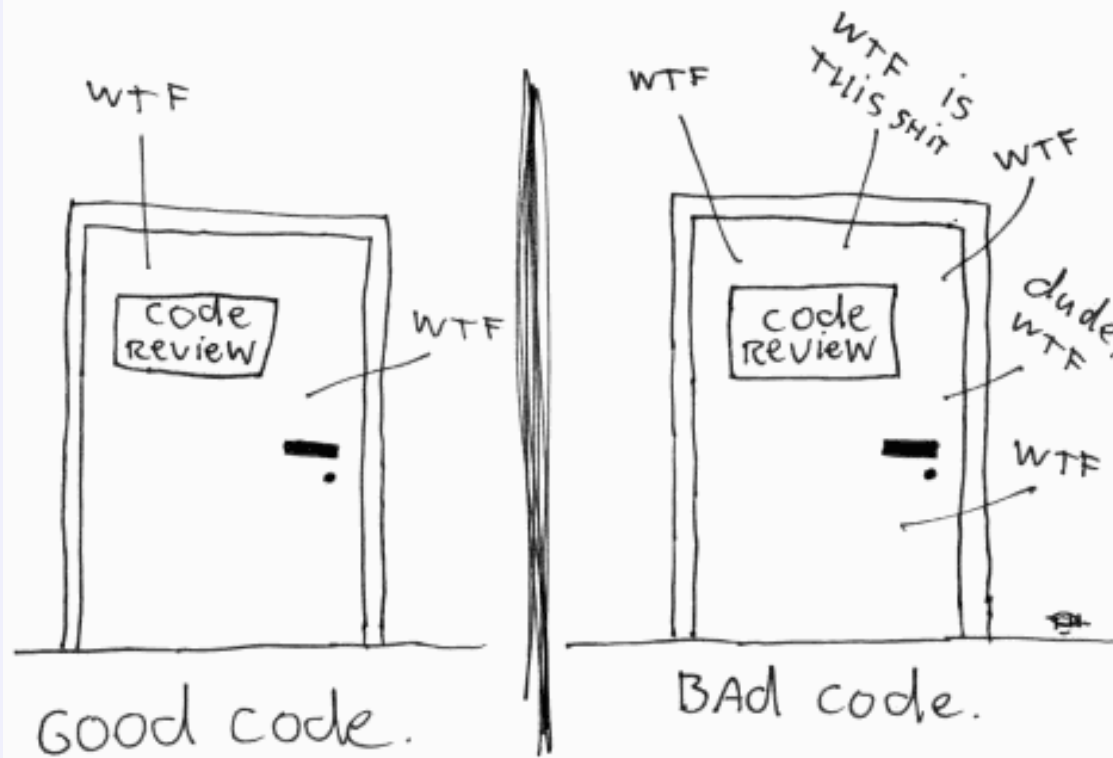
# Application Security in a nutshell



**OWASP**

The Open W

The ONLY VALID MEASUREMENT  
OF CODE QUALITY: WTFs/MINUTE



(c) 2008 Focus Shift

**OPEN  
WORLD  
FORUM**

#OWF14



Attribution - Pas d'Utilisation  
Commerciale - Partage dans  
les Mêmes Conditions 3.0  
France

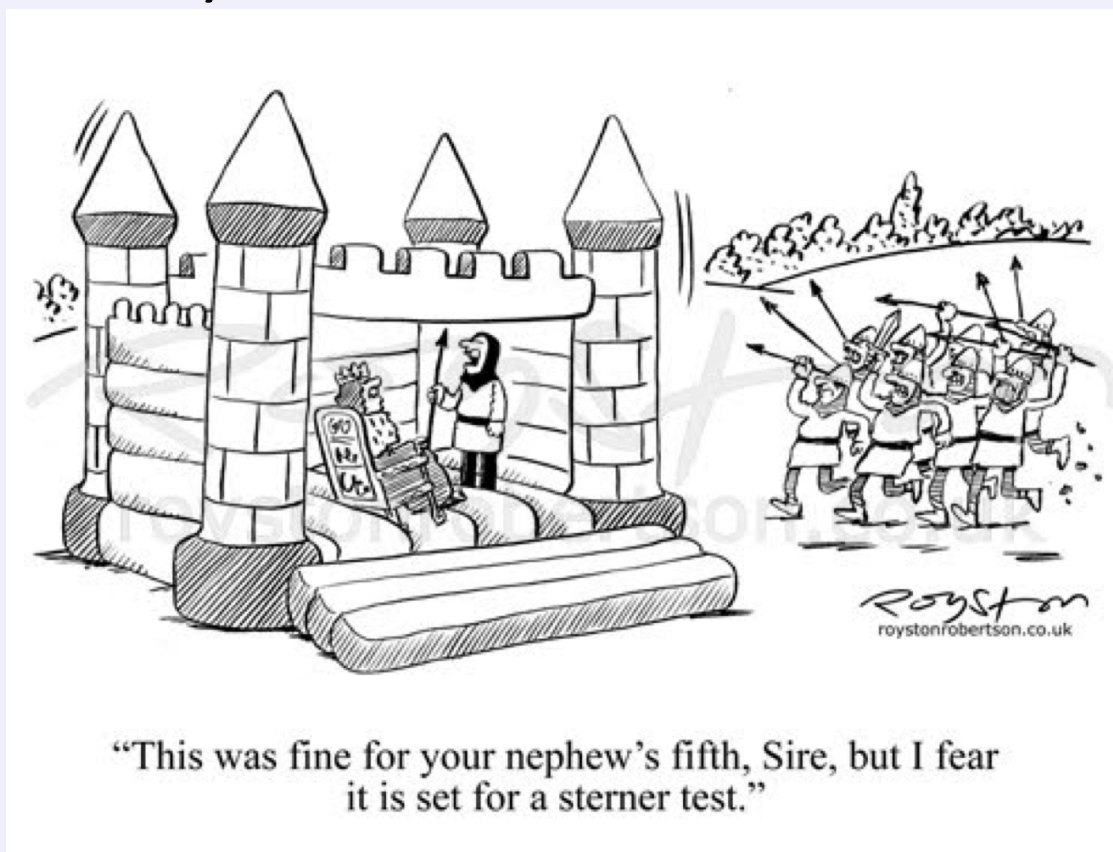




# OWASP

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](http://www.roystonrobertson.co.uk) for permission to use his cartoon!

Attribution - Pas d'Utilisation  
Commerciale - Partage dans  
les Mêmes Conditions 3.0  
France

# 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



Quick Start



Request



Response



Break



Script Console

## Welcome to the OWASP Zed Attack Proxy (ZAP)

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

Please be aware that you should only attack applications that you have been specifically given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack:

http://localhost:8080/bodgeit



Attack

Stop

Progress:

Attack complete - see the Alerts tab for details of any issues found

OPEN  
WORLD  
FORUM

#OWF14



Attribution - Pas d'Utilisation  
Commerciale - Partage dans  
les Mêmes Conditions 3.0  
France



# Using as a Proxy



## OWASP

The Open Web Application Security Project

- Options:
- Plug-n-Hack

If you are using Firefox 24.0 or later you can use 'Plug-n-Hack' to configure your browser:

Configure your browser:



Plug-n-Hack

Or point your browser at:

<http://localhost:8090/pnh/>

- Configure your browser's proxy manually



# Right Click program



## OWASP

The Open Web Application Security Project

**Sites** | **Scripts** | **Quick Start** | **Request** | **Response** | **Break**

Header: Text | Body: Text

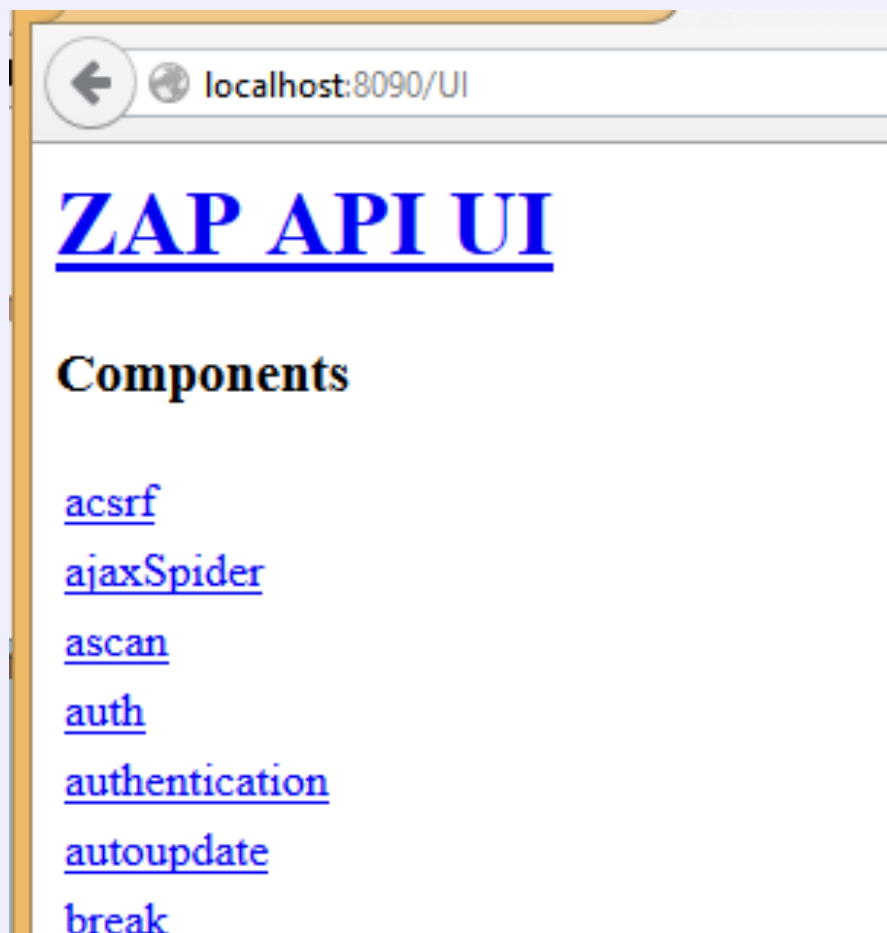
GET http://localhost:8080/bodgeit/home.jsp H  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0  
Pragma: no-cache

**Attack**

- Active Scan all in Scope
- Active Scan site
- Active Scan subtree
- Active Scan single URL
- Spider Context...
- Spider all in Scope
- Spider site
- Spider Subtree
- Spider URL
- Forced Browse site
- Forced Browse directory
- Forced Browse directory (and children)
- AJAX Spider in Scope
- AJAX Spider Site







- 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       |



## 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



OWASP

Sites Scripts

Quick Start Request Response Break Script Console

Run Zest: 301-302 body

Scripting

- Scripts
  - Passive Rules
    - 301-302 body
      - IF:OR
        - OR
          - Status Code (301)
          - Status Code (302)
        - THEN
          - IF:Length
            - Length (response.body = 0 +/- 0%)
          - THEN
          - ELSE
            - Action - Fail (Redirect contains a body)
          - ELSE
- Active Rules
- Proxy
- Stand Alone
- Targeted
- Templates
  - Passive Rules
    - Passive default template.js
    - 301-302 body.zest

```
1 {  
2   "about":  
3   "This is a Zest script. For more details about Zest visit https://de  
4   org/en-US/docs/Zest",  
5   "zestVersion": "0.3",  
6   "title": "301-302 body",  
7   "description": "Redirect (301-302) contains a body",  
8   "prefix": "",  
9   "type": "Passive",  
10  "parameters": {  
11    "tokenStart": "{{",  
    "tokenEnd": "}}",  
    "tokens": /
```

This is a graphical script that can only be edited via the Scripts tab on the left hand side.





# 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](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!



# OWASP

The Open Web Application Security Project

## Démo

**OPEN  
WORLD  
FORUM**

#OWF14



Attribution - Pas d'Utilisation  
Commerciale - Partage dans  
les Mêmes Conditions 3.0  
France



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

# License



## OWASP

The Open Web Application Security Project

Attribution - Pas d'Utilisation  
Commerciale - Partage dans  
les Mêmes Conditions 3.0  
France



## @SPoint



[sebastien.gioria@owasp.org](mailto:sebastien.gioria@owasp.org)

OPEN  
WORLD  
FORUM

