



# An Introduction to ZAP

## **OWASP**

### ***Zed Attack Proxy***

Simon Bennetts

*OWASP ZAP Project Lead*

*Mozilla Security Team*

[psiinon@gmail.com](mailto:psiinon@gmail.com)

# What is ZAP?

- An easy to use webapp pentest tool
- Completely free and open source
- An OWASP flagship project
- Ideal for beginners
- But also used by professionals
- Ideal for devs, esp. for automated security tests
- Becoming a framework for advanced testing
- Not a silver bullet!



# ZAP Principles

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



# Statistics

- Released September 2010, fork of Paros
- V 2.1.0 released in April 2013
- V 2.1.0 downloaded > 10K times
- 16 active contributors (Ohloh)
- 120 Person years (Ohloh)
- Translated into 17 languages
- Mostly used by Professional Pentesters?
- Paros code: ~30%    ZAP Code: ~70%

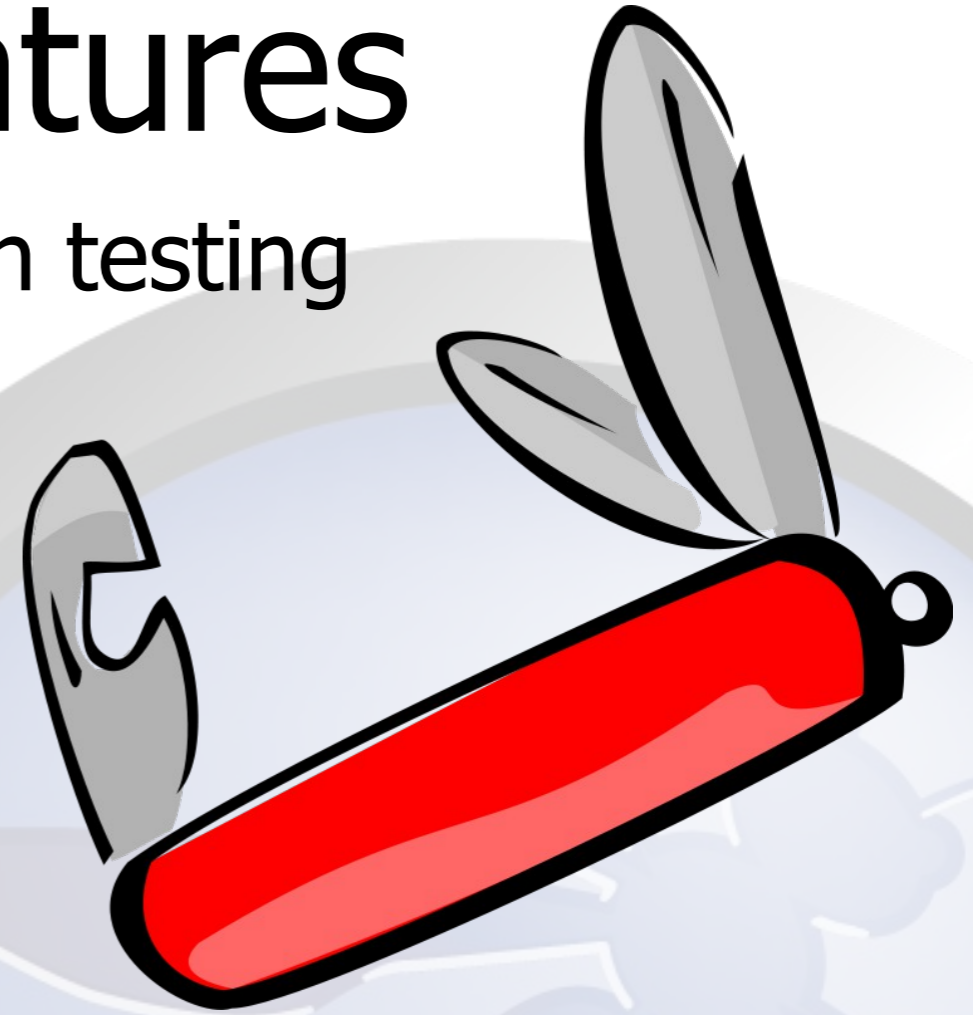




# The Main Features

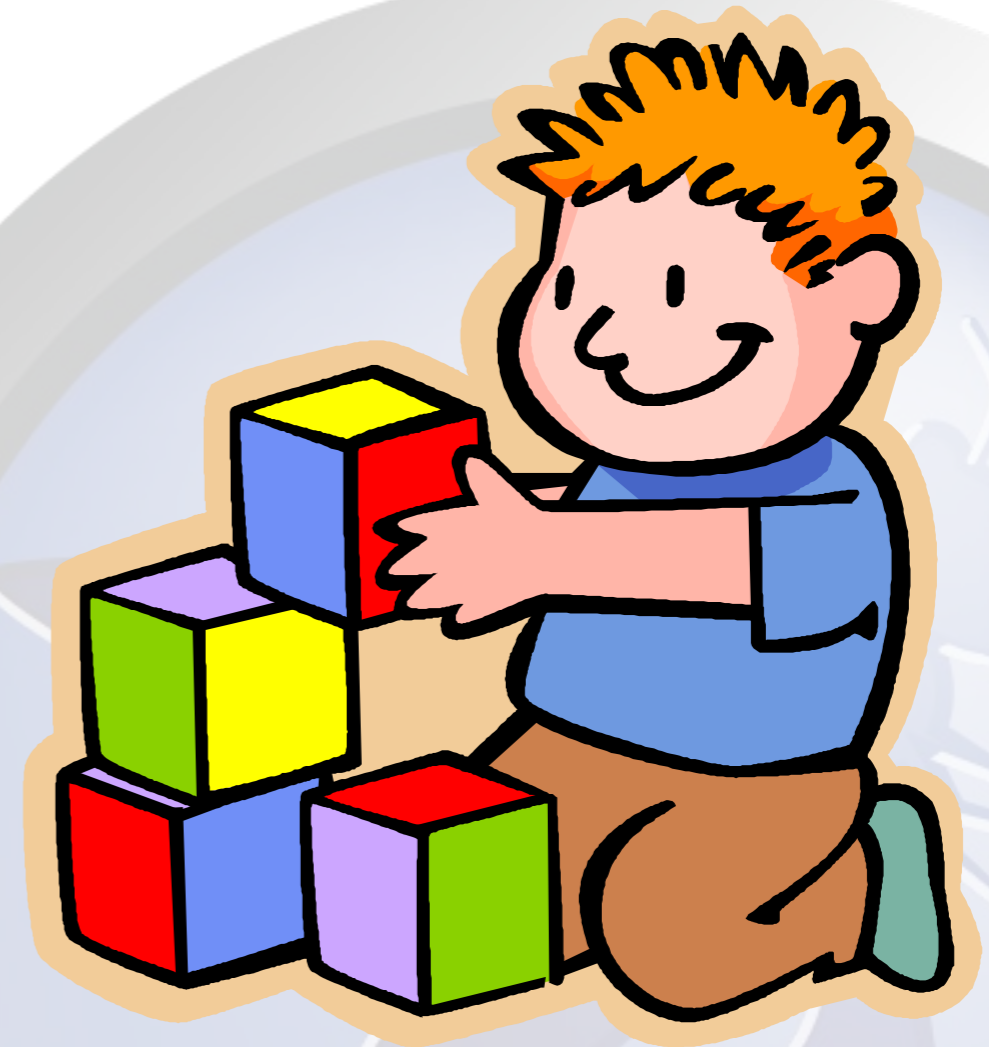
All the essentials for web application testing

- Intercepting Proxy
- Active and Passive Scanners
- Traditional and Ajax Spiders
- WebSockets support
- Forced Browsing (using OWASP DirBuster code)
- Fuzzing (using fuzzdb & OWASP JBroFuzz)
- Online Add-ons Marketplace



# Developer Features

- ⑤ Quick start
- ⑤ REST API
- ⑤ Java and Python clients
- ⑤ Headless mode
- ⑤ Anti CSRF token handling
- ⑤ Authentication support
- ⑤ Auto updating
- ⑤ Modes



# Some Additional Features

- ⑤ Auto tagging
- ⑤ Port scanner
- ⑤ Script Console
- ⑤ Report generation
- ⑤ Smart card support
- ⑤ Contexts and scope
- ⑤ Session management
- ⑤ Invoke external apps
- ⑤ Dynamic SSL Certificates

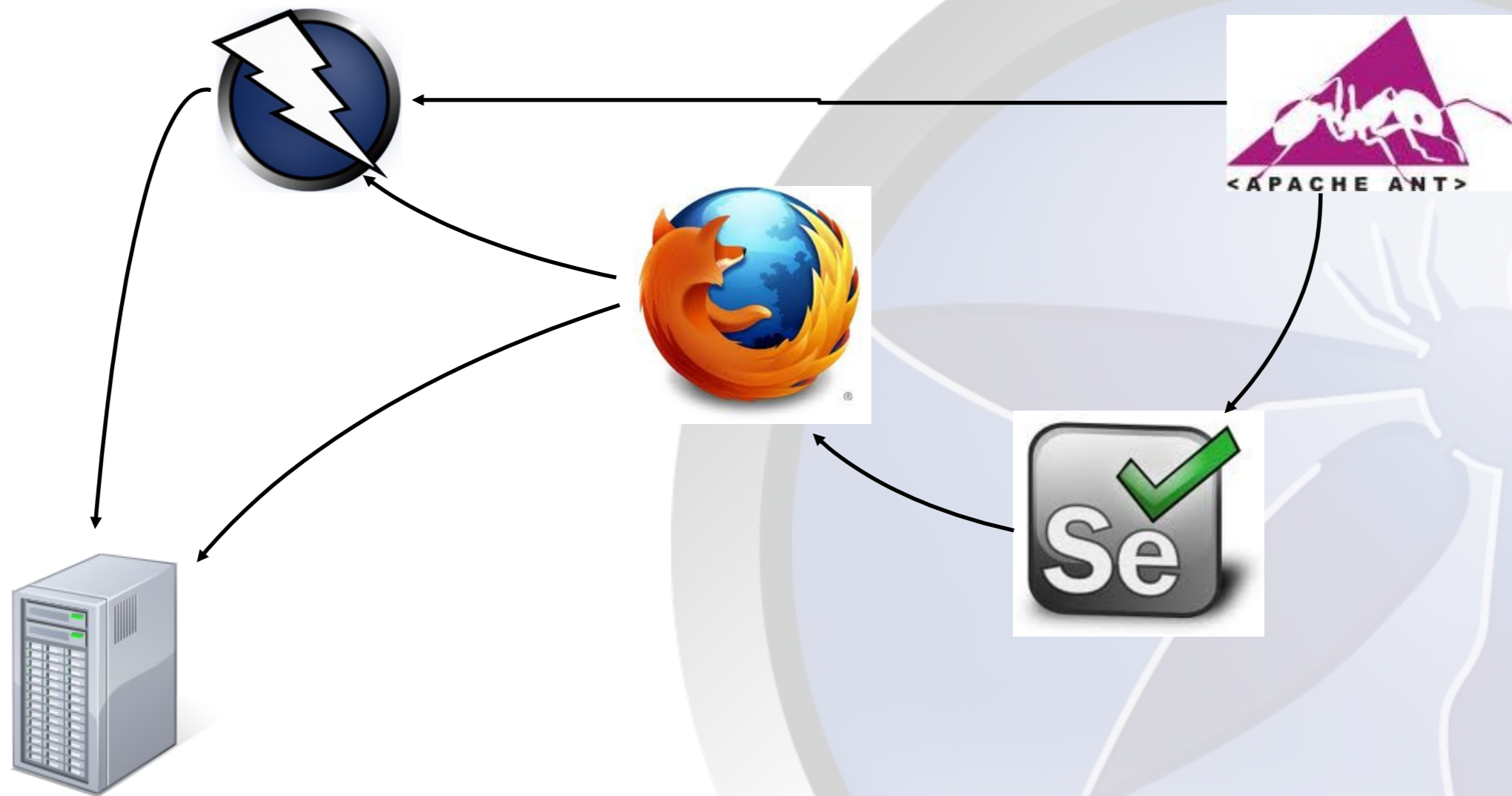


# How can you use ZAP?

- Point and shoot – the Quick Start tab
- Proxying via ZAP, and then scanning
- Manual pentesting
- Automated security regression tests



# Security Regression Tests



<http://code.google.com/p/zaproxy/wiki/SecRegTests>



- New Spider plus Session awareness  
Cosmin Stefan
- Ajax Spider via Crawljax  
Guifre Ruiz
- WebSockets support  
Robert Kock

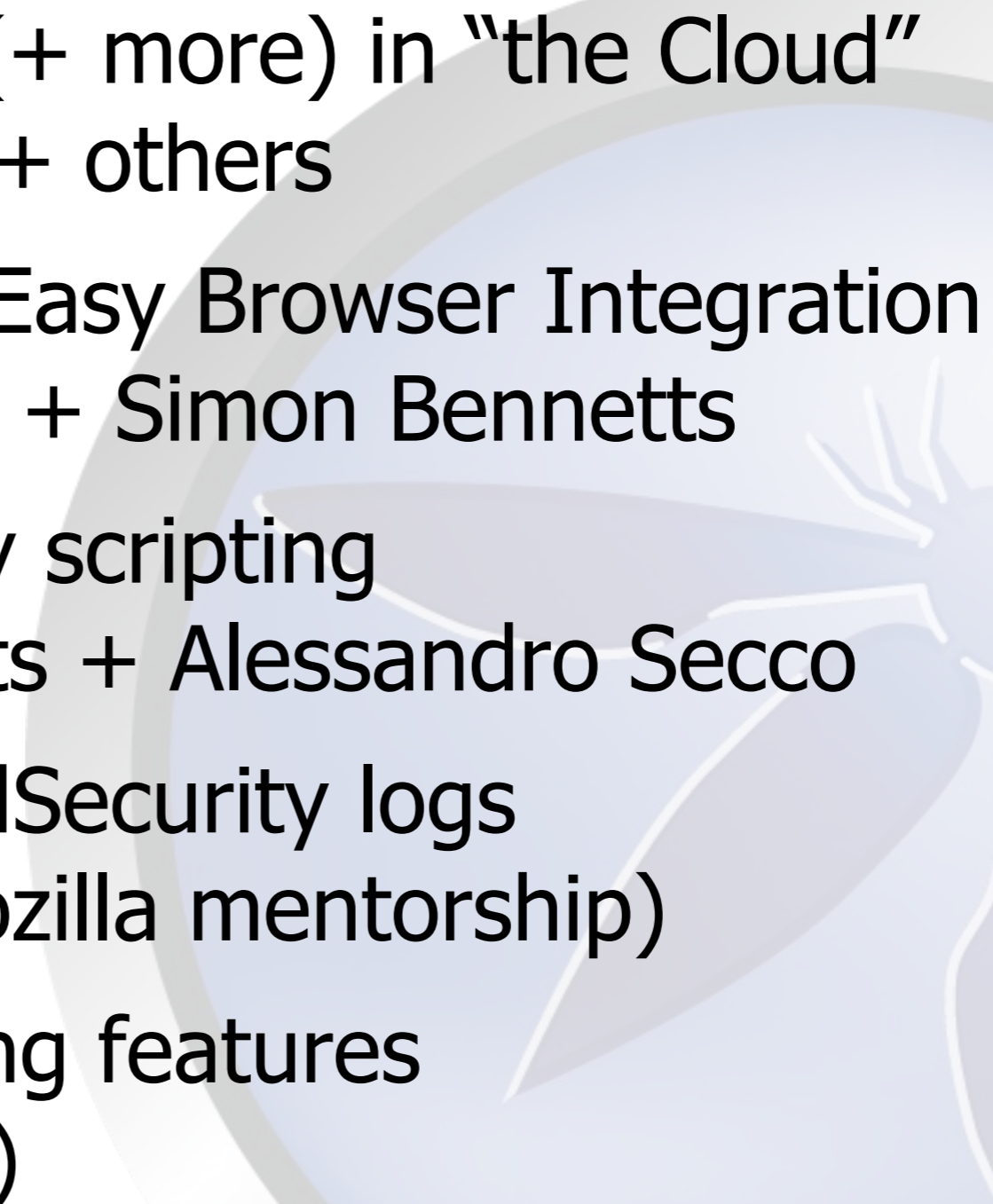
All in current release (2.1.0)



- Dynamically Configurable Actions  
Alessandro Secco
- SAML 2.0  
Pulasthi Mahawithana
- Enhanced HTTP Session Handling  
Cosmin Stefan
- Advanced Reporting using BIRT  
Rauf Butt
- CMS Scanner  
Abdelhadi Azouni



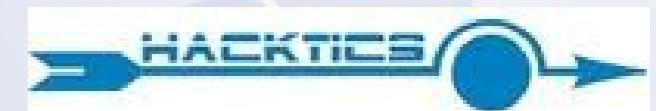
# But theres more!

- Minion – ZAP (+ more) in “the Cloud”  
Stefan Arentz + others
  - Plug-n-hack : Easy Browser Integration  
Mark Goodwin + Simon Bennetts
  - Zest – Security scripting  
Simon Bennetts + Alessandro Secco
  - Importing ModSecurity logs  
Joe Kirwin (Mozilla mentorship)
  - New networking features  
(Mozilla intern)
- 



# Collaborations

- Dradis – ZAP upload plugin
- OWASP ModSecurity Core Rule Set script – SpiderLabs
- ThreadFix – Denim Group
- Ultimate Obsolete File Detection – Hacktics ASC, Ernst & Young
- Grey-box plugin – BCC Risk Advisory







# Any Questions?

<http://www.owasp.org/index.php/ZAP>