



# ZAP 2.4.0 and beyond...

**Simon Bennetts**

*OWASP ZAP Project Lead*

*Mozilla Security Team*

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

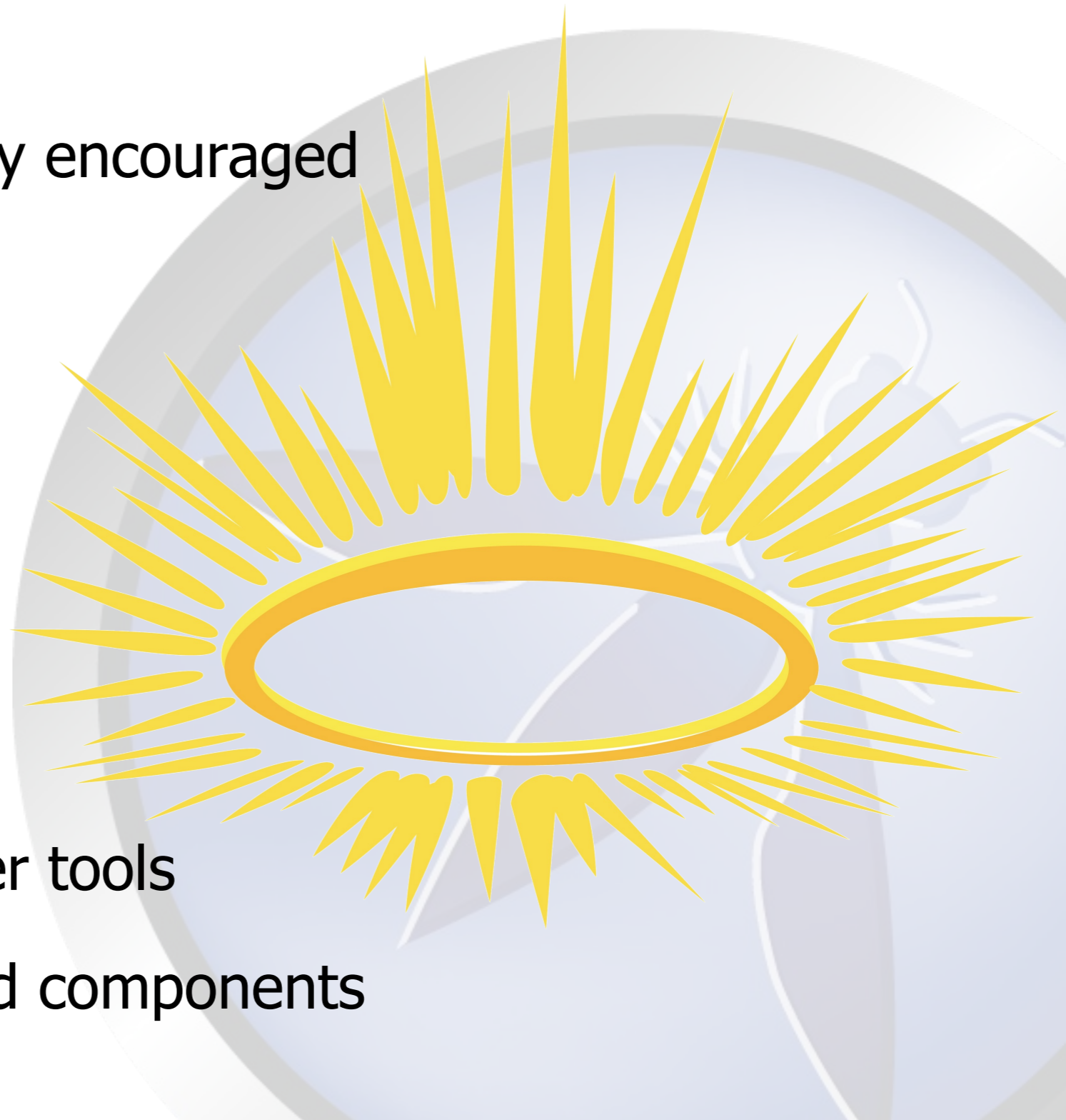
# What is ZAP?

- An easy to use webapp pentest tool
- Completely free and open source
- OWASP Flagship project
- Ideal for beginners
- But also used by professionals
- Ideal for devs, esp. for automated security tests
- Included in all major security distributions
- ToolsWatch.org Top Security Tools of 2013/2014
- On the ThoughtWorks Tech Radar (as of May)
- 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



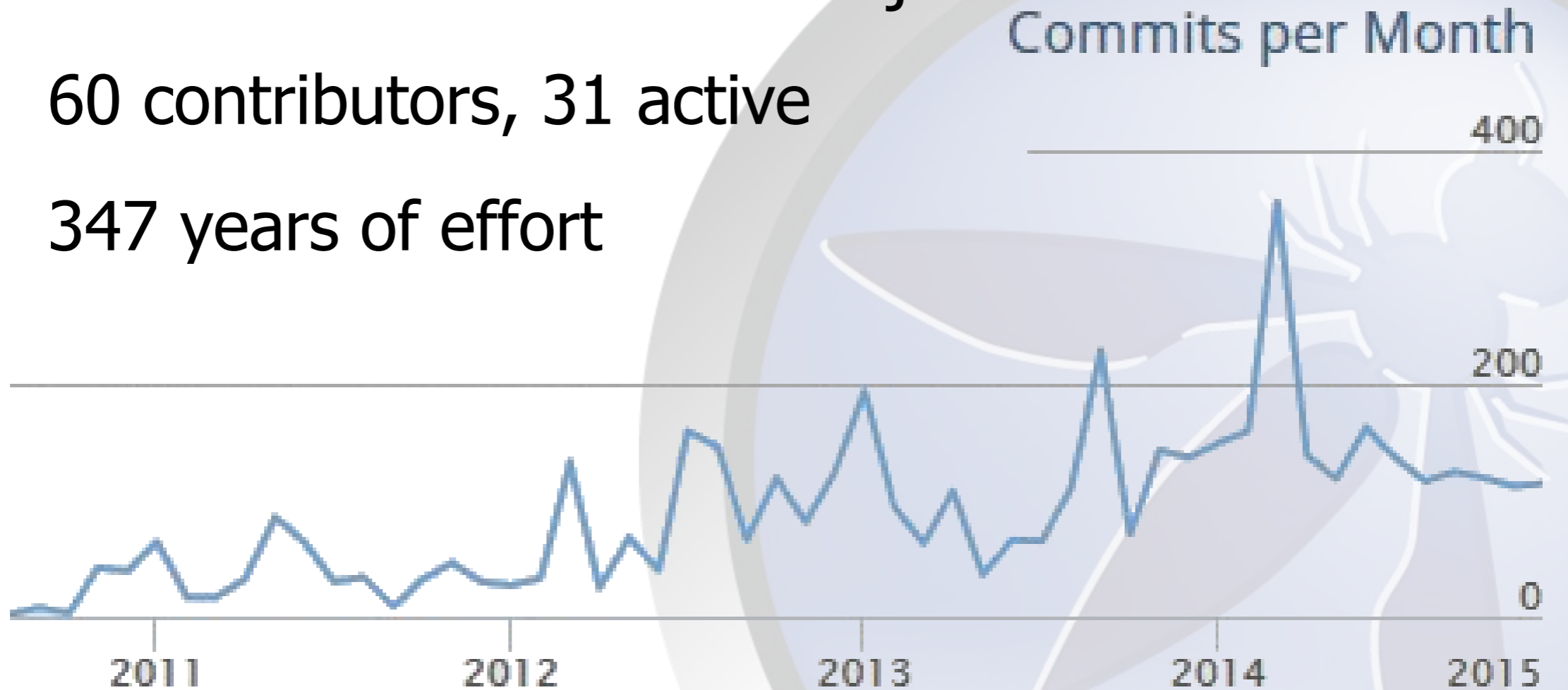
# Statistics

- Released September 2010, fork of Paros
- V 2.4.0 released in April 2015
- V 2.4.0 downloaded > 32K times
- Translated into 30 languages
- Over 130 translators
- Mostly used by Professional Pentesters?
- Paros code: ~20%    ZAP Code: ~80%



# Open HUB Statistics

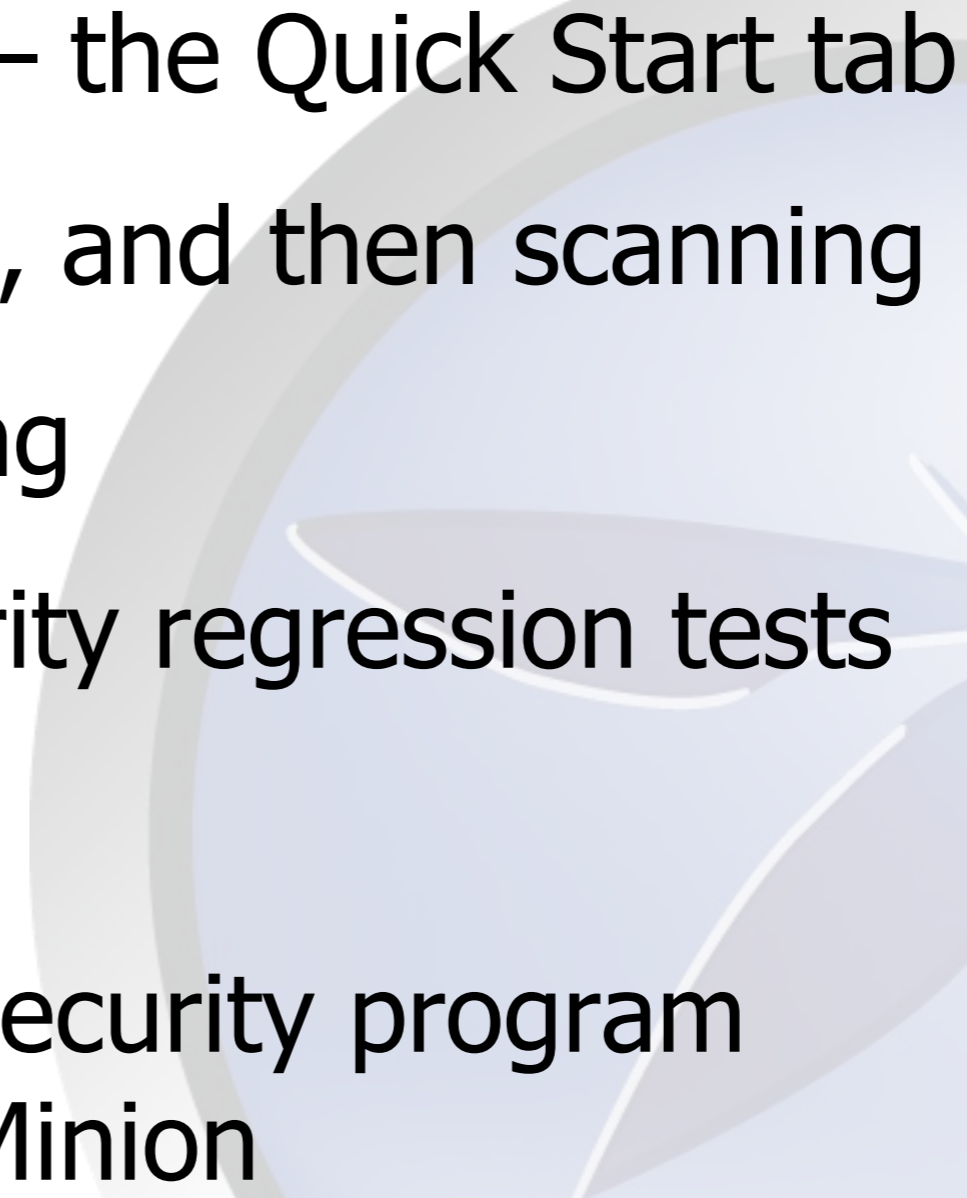
- 🏗️ Very High Activity
- The most active OWASP Project
- 60 contributors, 31 active
- 347 years of effort



Source: <https://www.openhub.net/p/zaproxy>



# Some ZAP use cases

- 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  
e.g. ThreadFix, Minion
- 

# Version 2.4.0

- UI Changes
- Scan Dialogs
- Scan Policies
- Attack Mode
- Advanced Fuzzer
- API Changes
- Lots of minor enhancements and bug fixes!




# And some more new stuff

- Alpha add-ons:
  - Access Control Testing
  - Sequence scanning
  - New scan rules
- Community Scripts  
<https://github.com/zaproxy/community-scripts>







So whats  
next?

# More of the same..

- 2.4.0.1 Bugfix release “coming soon”
- New/improved active + passive scan rules
- New/improved add-ons
- Migration to GitHub
- Adoption of Maven/Gradle/??
- ...

# ZAP properties

Database	Local HSQLDB
Data Structures	Db and in process
Processes	One
Deployment	Single machine
Users	One
Roles	One
Process Lifetime	Hours
Access	Swing UI / API
Licence	Apache V2



# ZaaS

## ZAP as a Service



# ZAP (desktop) properties

Database	Local HSQLDB
Data Structures	Db and in memory
Processes	One
Deployment	Single machine
Users	One
Roles	One
Access	Swing UI / API
Application Lifetime	Hours
Licence	Apache V2

# ZaaS properties

Database	Enterprise (eg MySQL)
Data Structures	Db
Processes	Multiple
Deployment	Distributed
Users	Multiple
Roles	Multiple
Process Lifetime	Five Nines capability
Access	Web UI / API
Licence	Apache V2

# ZaaS properties

Database	Enterprise (eg MySQL)
Data Structures	Db
Processes	Multiple
Deployment	Distributed
Users	Multiple
Roles	Multiple
Access	Web UI / API
Application Lifetime	Five nines capability
Licence	Apache V2

# ZaaS todo list

- ✓ Introduce db independence layer
- ✓ Support MySQL
- ✓ Low memory *option*
  - Multi-process *option*
  - Support multiple users and roles
  - Add scheduler
  - Develop web UI
  - Full security review





# Questions?

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