



ZAP

Advanced Features

Simon Bennetts

OWASP ZAP Project Lead

Mozilla Security Team

psiinon@gmail.com

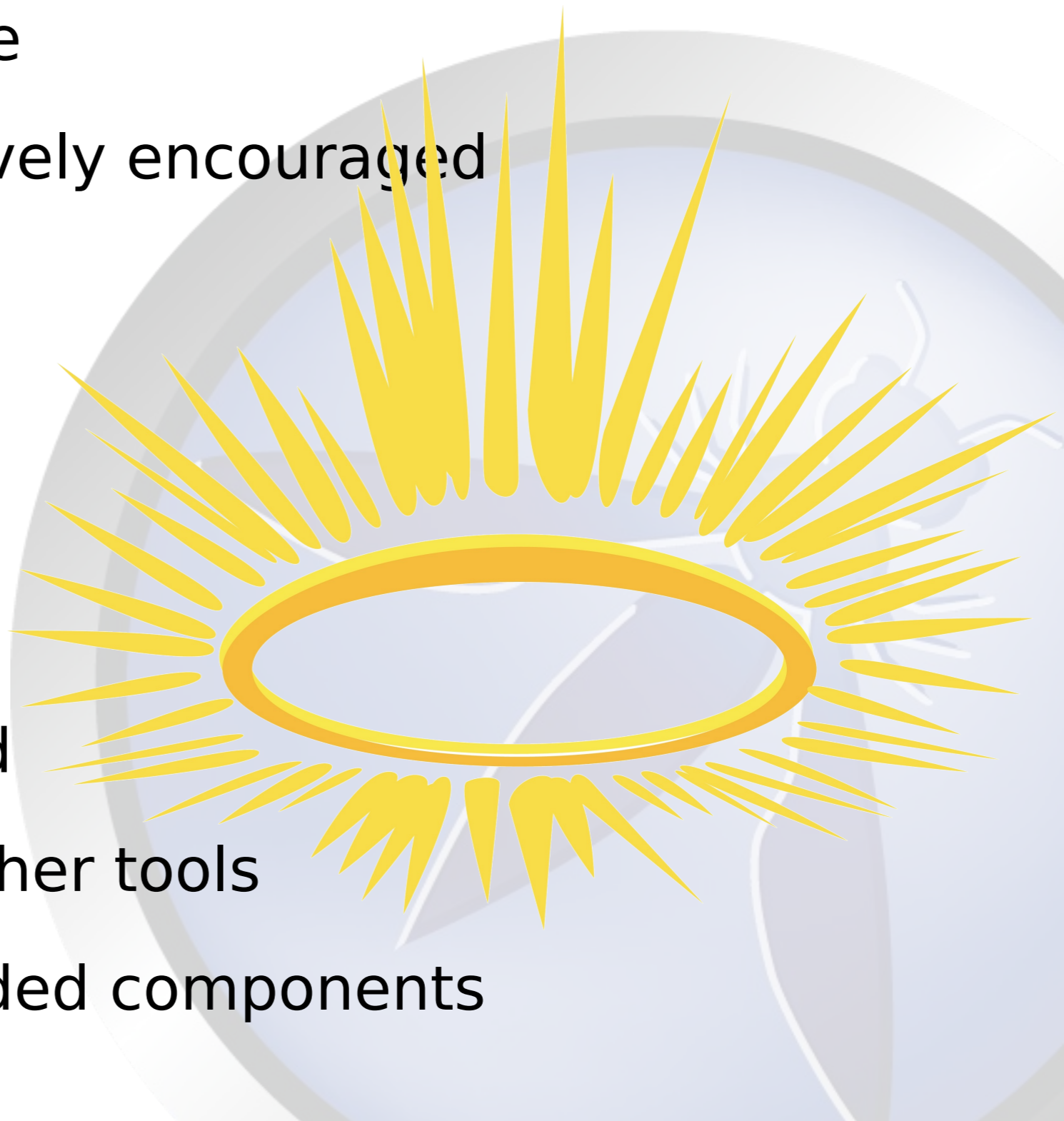
What is ZAP?

- 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
- 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 2.3.1 released in May 2014
- V 2.3.1 downloaded > 20K times
- Translated into 20+ languages
- Over 90 translators
- Mostly used by Professional Pentesters?
- Paros code: ~20% ZAP Code: ~80%



Ohloh Statistics

- 🏗️ Very High Activity
- The most active OWASP Project
- 29 active contributors
- 278 years of effort



Source: <http://www.ohloh.net/p/zaproxy>

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



Some Additional Features

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



The Advanced Stuff :)

- Contexts
- Advanced Scanning
- Scripts
- Zest
- Plug-n-Hack

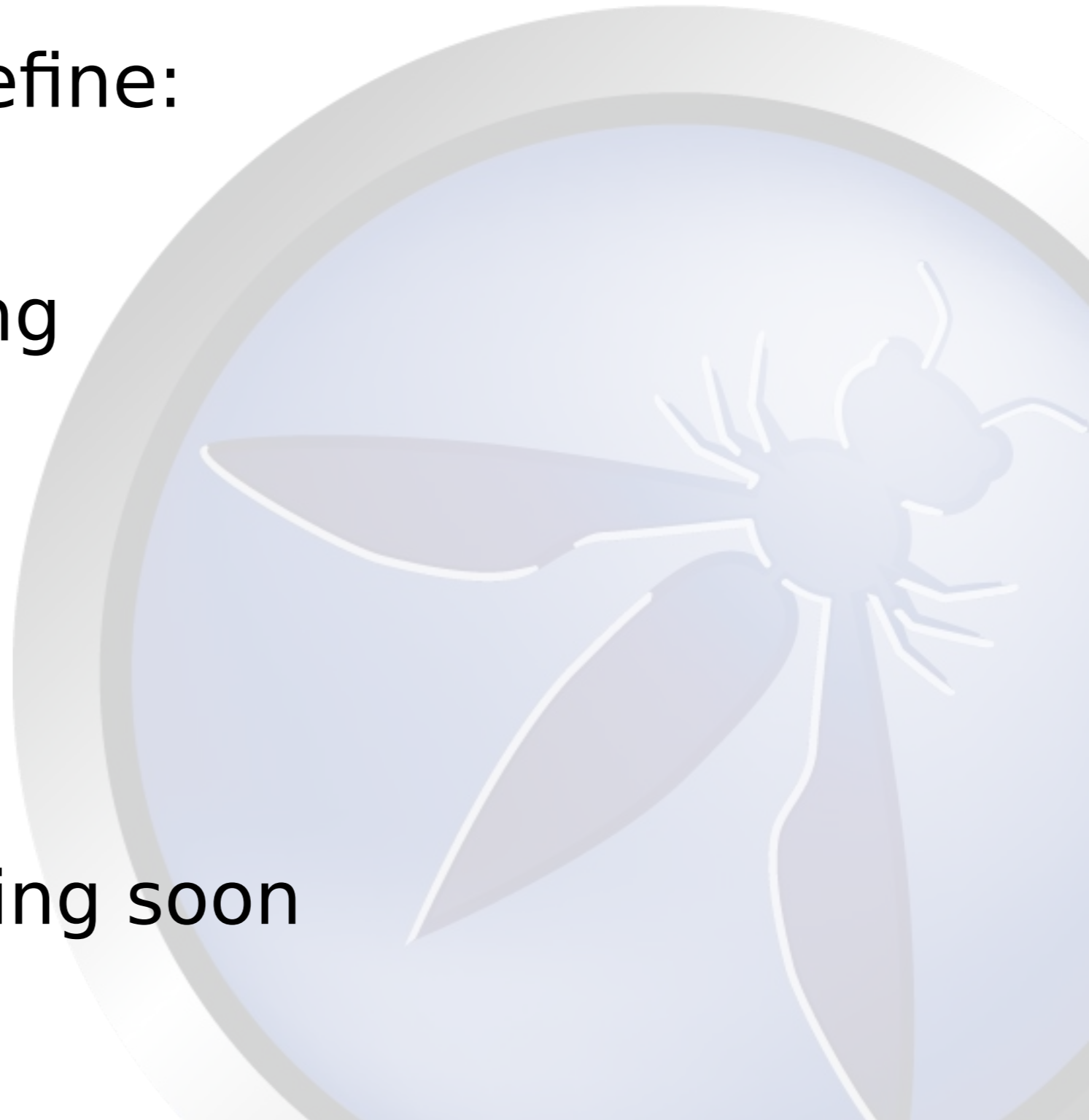


Contexts

- Assign characteristics to groups of URLs
- Like an application:
 - Per site:
 - <http://www.example.com>
 - Site subtree:
 - <http://www.example.com/app1>
 - Multiple sites:
 - <http://www.example1.com>
 - <http://www.example2.com>

Contexts

- Allows you to define:
 - Scope
 - Session handling
 - Authentication
 - Users
 - 'Forced user'
 - Structure
 - with more coming soon



Advanced Scanning

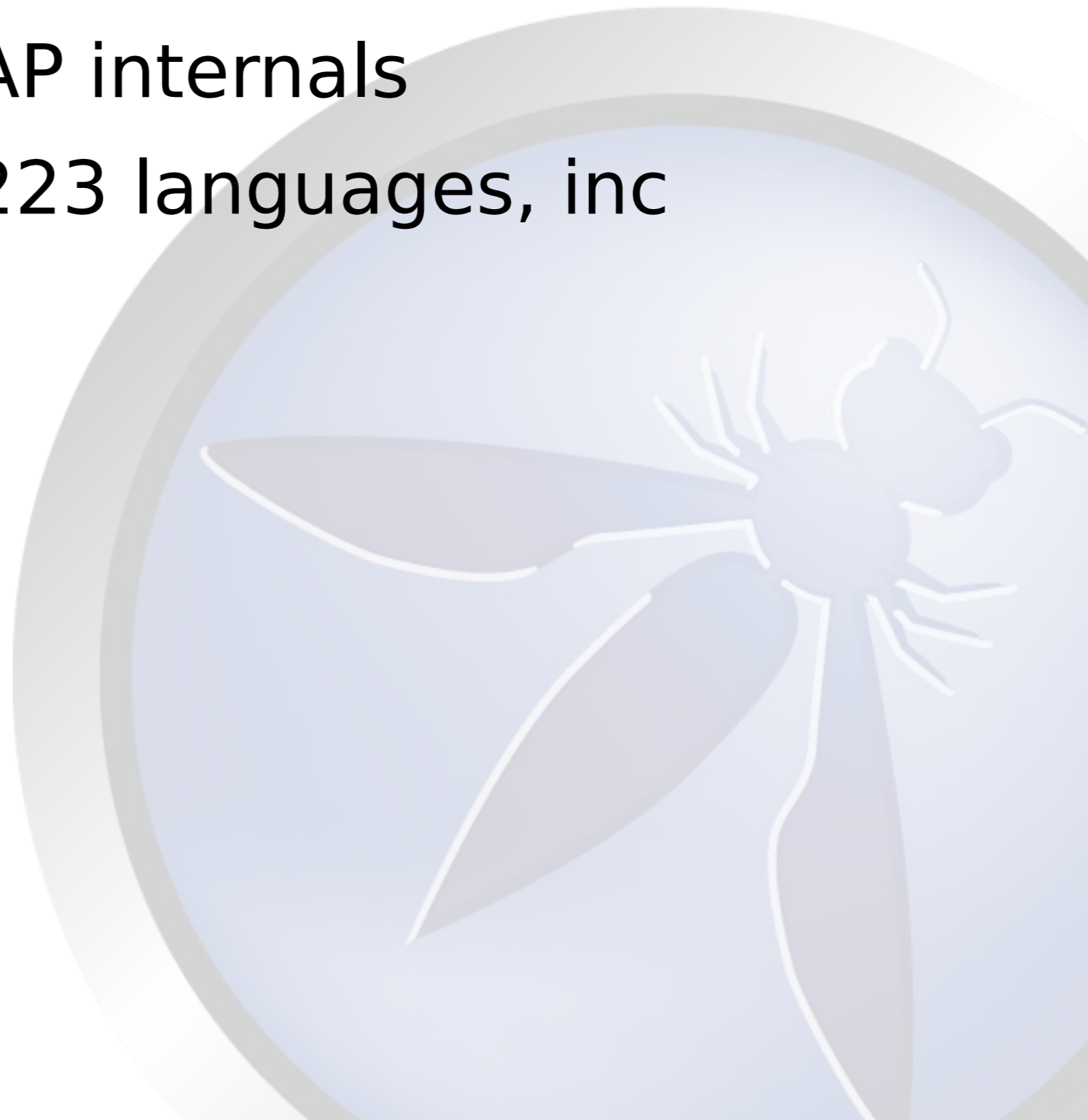
- Accessed from:
 - Right click Attack menu
 - Tools menu
 - Key board shortcut (default Ctrl-Alt-A)
- Gives you fine grained control over:
 - Scope
 - Input Vectors
 - Custom Vectors
 - Policy

Scripting

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

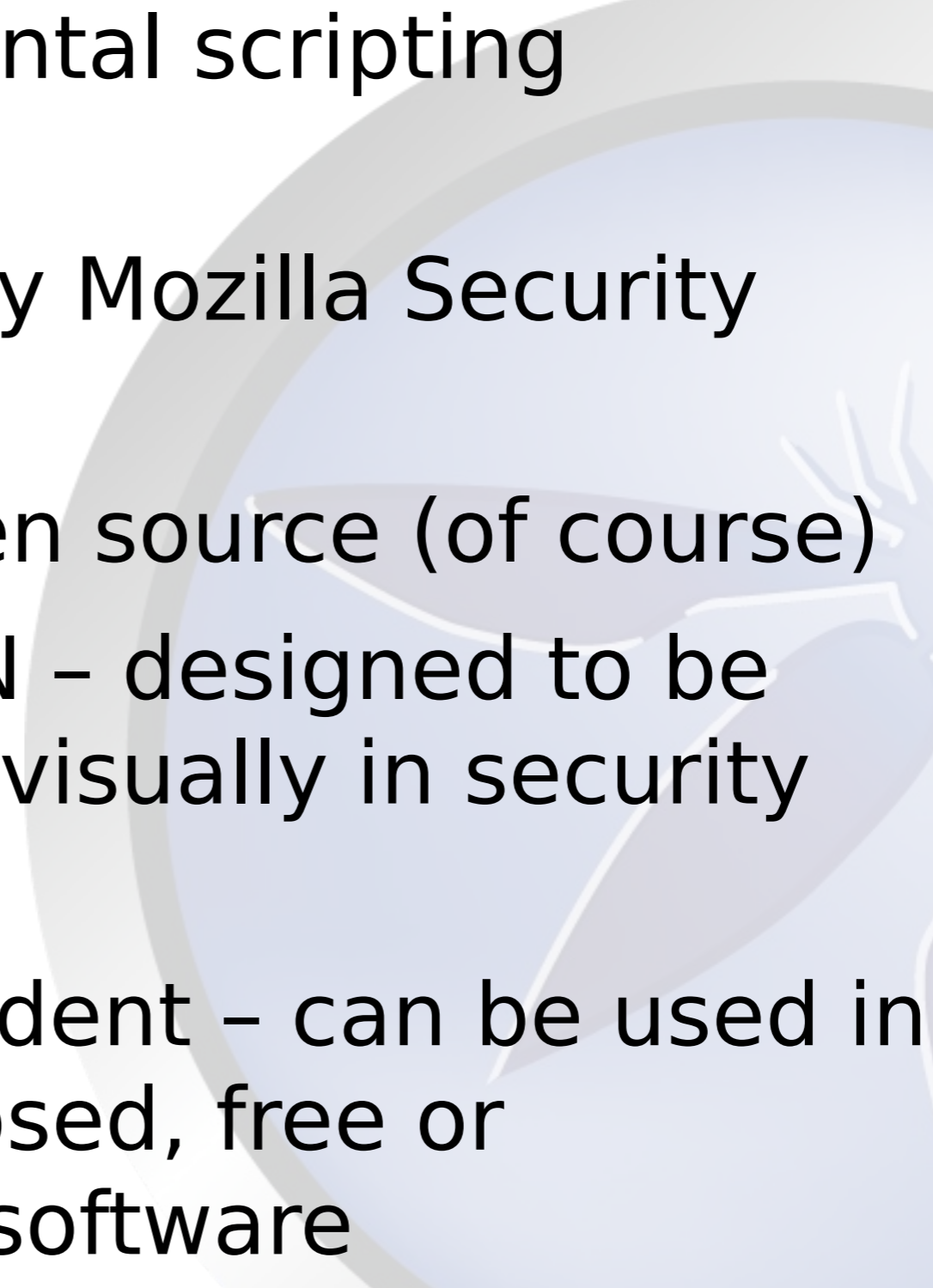
Scripting

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






Zest - Overview

- 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
 - Is included by default in ZAP from
- 

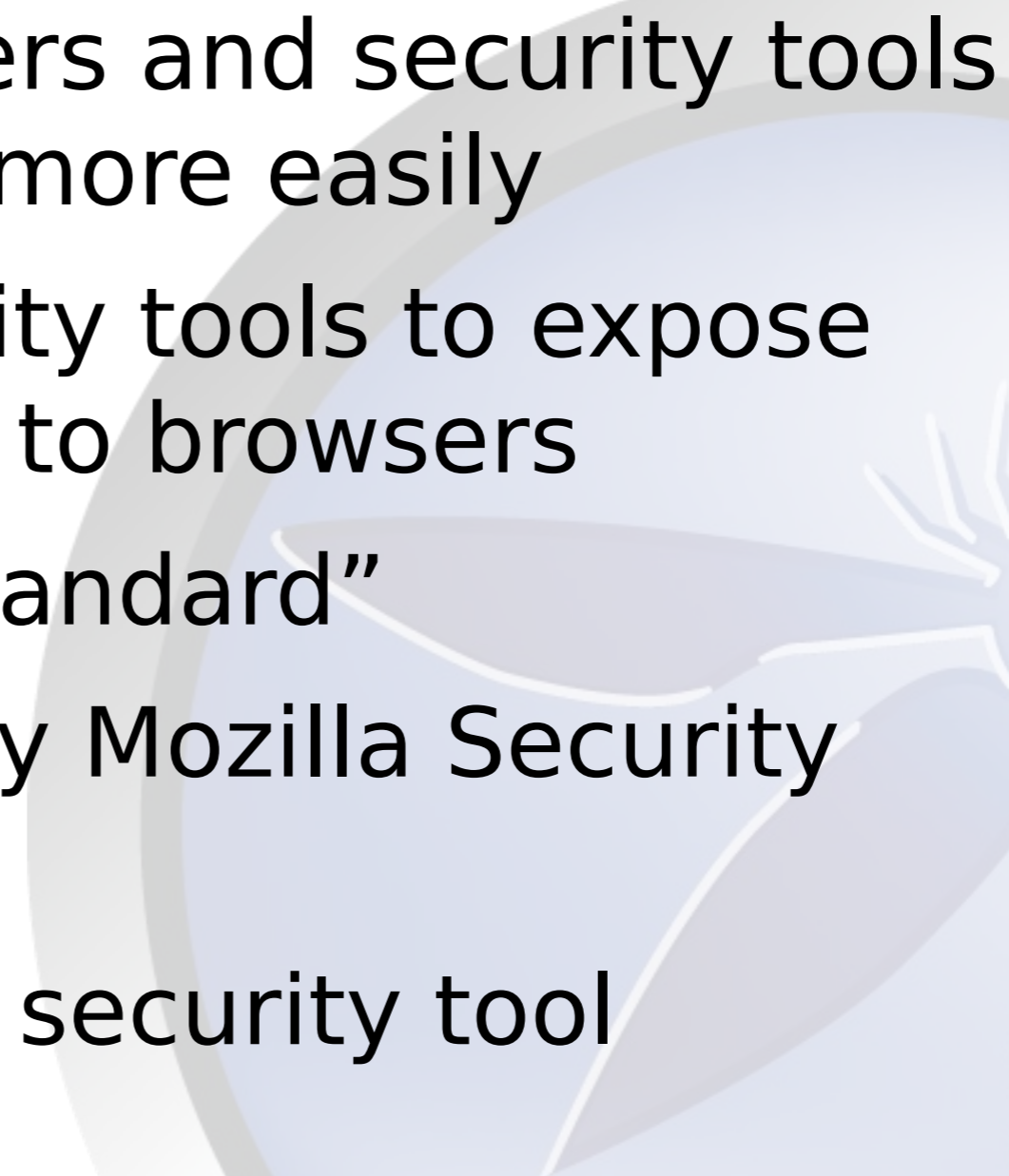


Zest - Use cases

- Reporting vulnerabilities to companies
 - Reporting vulnerabilities to developers
 - Defining tool independent active and passive scan rules
 - Deep integration with security tools
- 

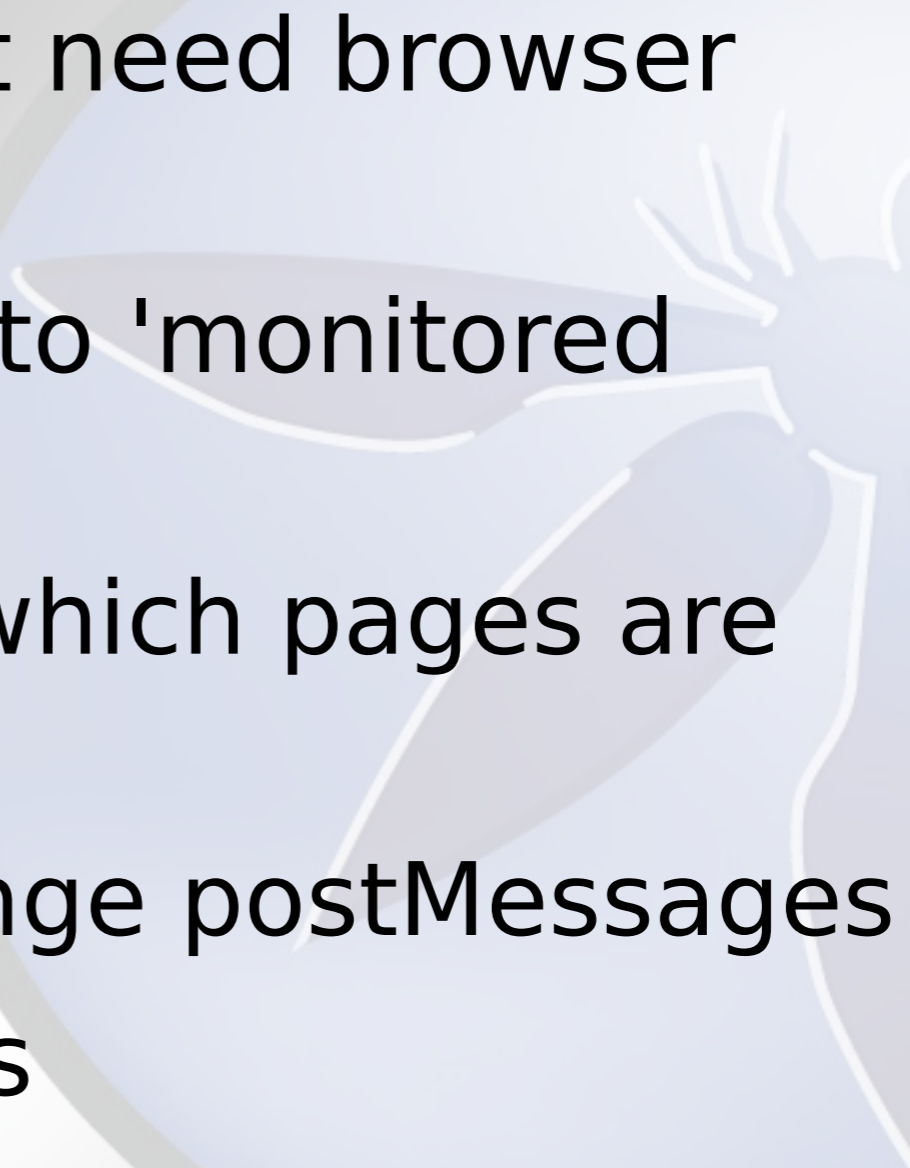


Plug-n-Hack – Phase 1

- Allow browsers and security tools to integrate more easily
 - Allows security tools to expose functionality to browsers
 - “Proposed standard”
 - Developed by Mozilla Security Team
 - Browser and security tool independent
- 



Plug-n-Hack – Phase 2

- Allows browsers to expose functionality to security tools
 - This phase doesn't need browser plugin
 - Inject javascript into 'monitored pages'
 - Heartbeat shows which pages are alive
 - Intercept and change postMessages
 - Fuzz postMessages
 - DOM XSS oracle
- 

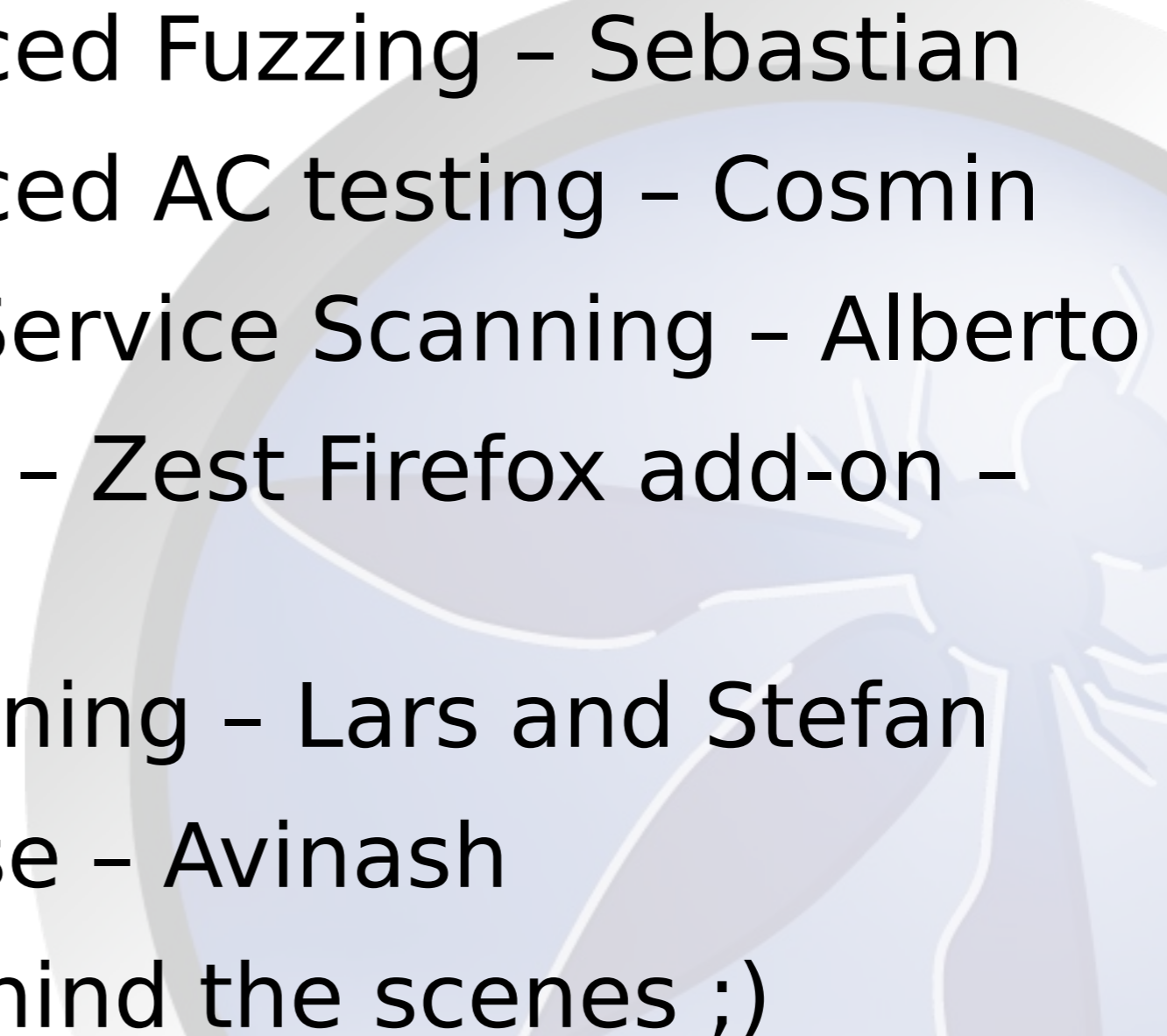
Plug-n-Hack – Phase 3

- Support more client side events..
- .. which enables client side Zest recording
- Work in progress!



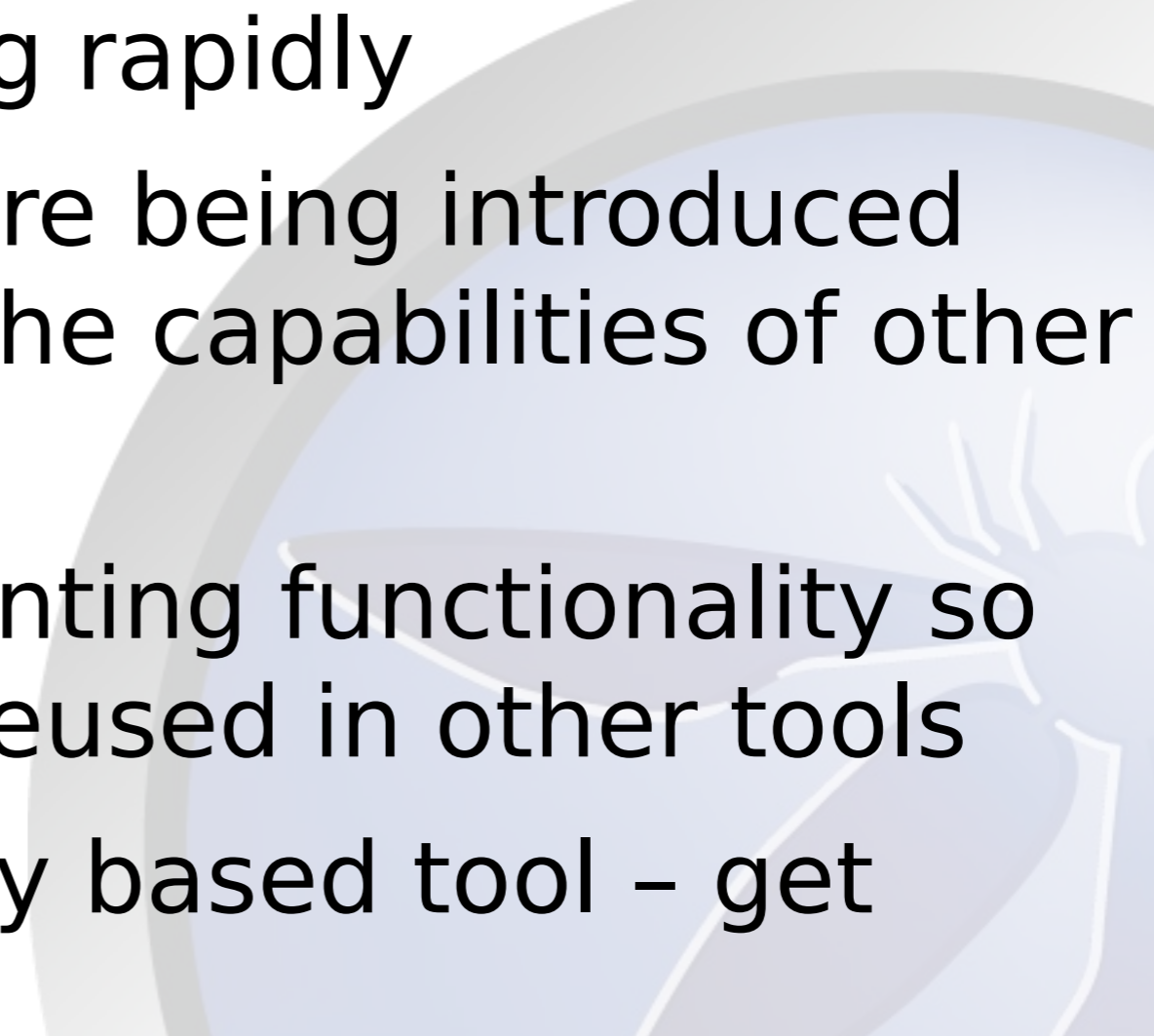


Work In Progress

- GSOC - Advanced Fuzzing - Sebastian
 - GSOC - Advanced AC testing - Cosmin
 - GSOC - SOAP Service Scanning - Alberto
 - GSOC (Mozilla) - Zest Firefox add-on - Sunny
 - Sequence scanning - Lars and Stefan
 - Sequence abuse - Avinash
 - .. and more behind the scenes ;)
- 



Conclusion

- ZAP is changing rapidly
 - New features are being introduced which exceed the capabilities of other tools
 - We're implementing functionality so that it can be reused in other tools
 - Its a community based tool - get involved!
- 



Questions?

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