



OWASP Zed Attack Proxy

Simon Bennetts

OWASP ZAP Project Lead

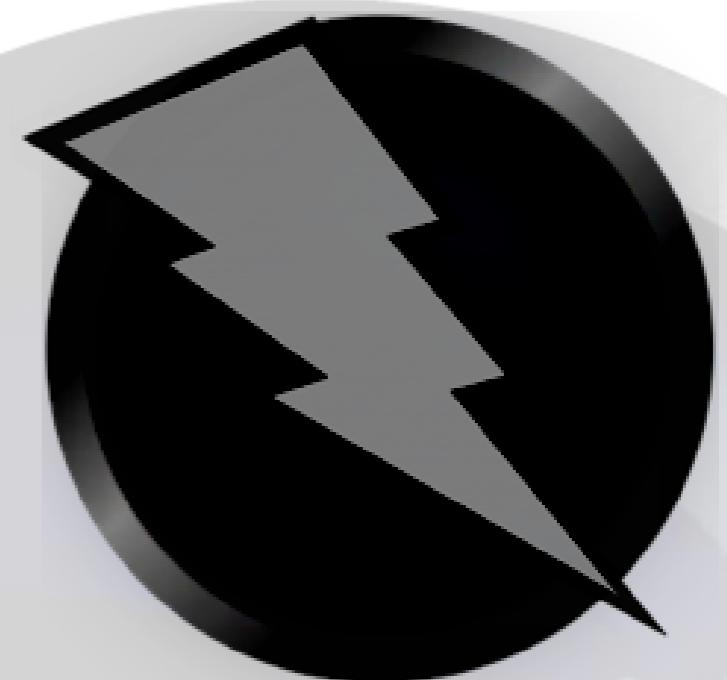
Mozilla Security Team

`psiinon@gmail.com`



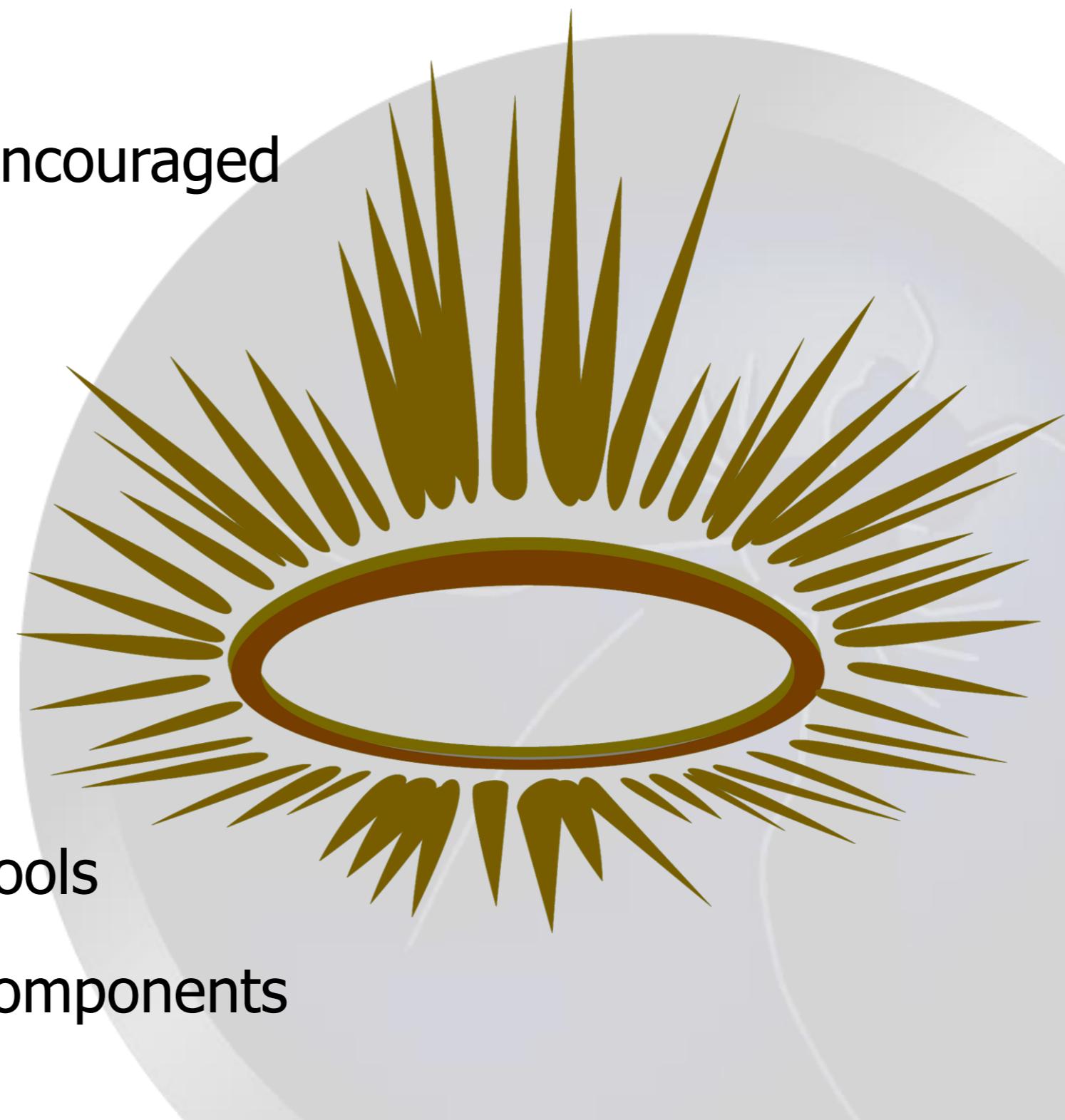
What is ZAP?

- An easy to use webapp pentest tool
- Completely free and open source
- 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
- Included in all major security distributions
- 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

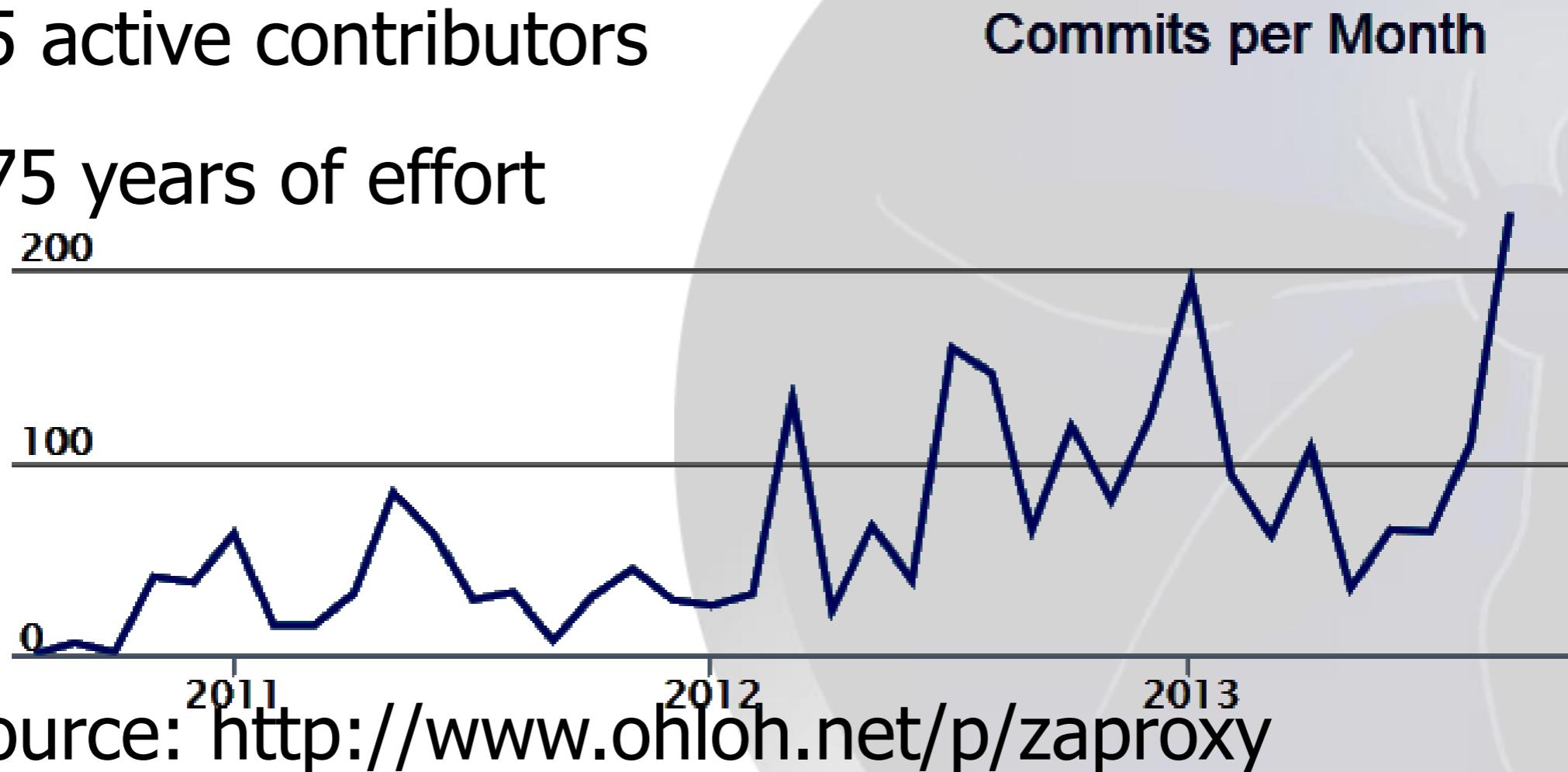
- Released September 2010, fork of Paros
- V 2.2.2 released in Sept 2013
- V 2.2.2 downloaded > 60K times
- Translated into 20+ languages
- Over 80 translators
- Mostly used by Professional Pentesters?
- Paros code: ~20% ZAP Code: ~80%





Ohloh Statistics

-  Very High Activity
- The most active OWASP Project
- 25 active contributors
- 275 years of effort

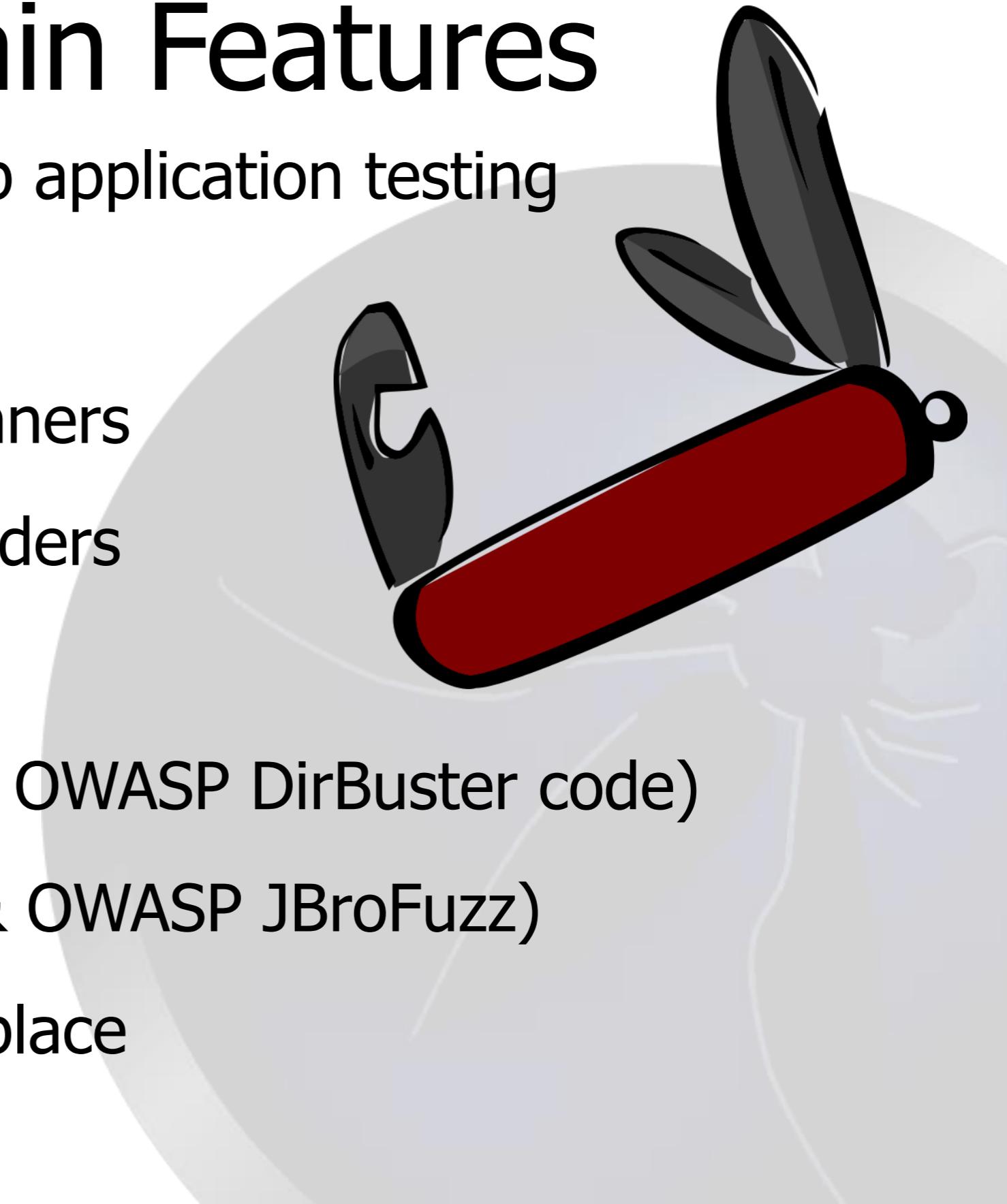


- Source: <http://www.ohloh.net/p/zaproxy>

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

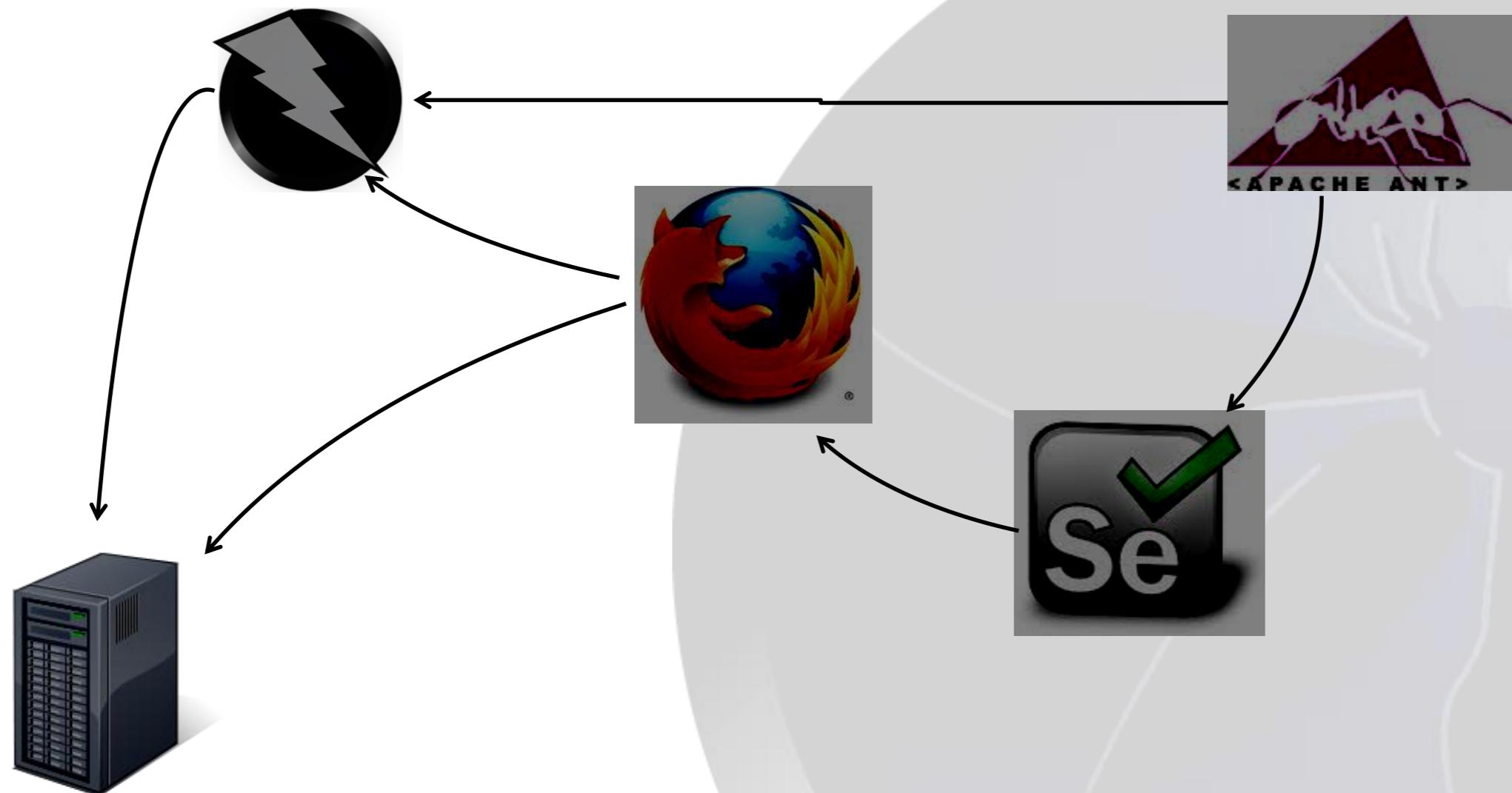
- Auto tagging
- Port scanner
- Script Console
- Report generation
- Smart card support
- Contexts and scope
- Session management
- Invoke external apps
- Dynamic SSL Certificates



How can you use ZAP?

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

Security Regression Tests



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

ZAP – Embedded

ThreadFix – Denim Group

Software vulnerability aggregation and management system

Main Menu ThreadFix						Bug 235 processed
https://localhost:8443/threadfix/organizations/2/applications/2/vulnerabilities/35?nonce=D8E29CED1552E2F4F5F17B83398DE012						 Google
Scanner Name	Severity	Vulnerability Type	Path	Parameter	Number Merged Results	
Skipfish		6/30/11 9:43:04 AM				
OWASP Zed Attack Proxy		9/23/11 9:31:41 PM				
w3af		7/6/11 9:24:45 AM				
WebInspect		11/4/11 3:53:29 PM				
Findings						
Arachni	HIGH	Cross-Site Scripting (XSS)	/demo/XSS-reflected2.php	username	1	
Burp Suite	High	Cross-site scripting (reflected)	/demo/XSS-reflected2.php	username	1	
IBM Rational AppScan	High	Cross-Site Scripting	/demo/XSS-reflected2.php	username	1	
Mavituna Security Netsparker	Important	Cross-site Scripting	/demo/XSS-reflected2.php	username	1	
Nessus	2	CGI Generic HTML Injections (quick test)	/demo/XSS-reflected2.php	username	1	
Nessus	2	CGI Generic Cross-Site Scripting Vulnerability (quick test)	/demo/XSS-reflected2.php	username	1	
Skipfish	3	XSS vector in document body	/demo/XSS-reflected2.php	username	1	
OWASP Zed Attack Proxy	3	Cross site scripting	/demo/XSS-reflected2.php	username	2	
w3af	Medium	Cross site scripting vulnerability	/demo/XSS-reflected2.php	username	1	
WebInspect	4	Cross-Site Scripting	/demo/XSS-reflected2.php	username	1	

Minion – Mozilla Security automation platform

Minion		Administration		Logged in as yeukhon@mozilla.com - Sign out					
		zap	---	-	-	-	-	-	Details Scan
		skipfish	---	-	-	-	-	-	Details Scan
http://testaspnet.vulnweb.com	basic	---	-	-	-	-	-	-	Details Scan
		zap	---	-	-	-	-	-	Details Scan
		skipfish	---	-	-	-	-	-	Details Scan
http://testfire.net	basic	---	-	-	-	-	-	-	Details Scan
		zap	---	-	-	-	-	-	Details Scan
		skipfish	---	-	-	-	-	-	Details Scan
http://zero.webappsecurity.com	basic	---	-	-	-	-	-	-	Details Scan
		zap	---	-	-	-	-	-	Details Scan
		skipfish	---	-	-	-	-	-	Details Scan



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



- Enhanced HTTP Session Handling

Cosmin Stefan

- SAML 2.0

Pulasthi Mahawithana

- Advanced Reporting using BIRT

Rauf Butt

- CMS Scanner

Abdelhadi Azouni

- Dynamically Configurable Actions

Alessandro Secco



- OWASP has just been allocated 14 slots
- We dont know how many will be assigned to ZAP :/



2.3 – coming very soon!

- ZAP 'lite'
- Support browser side events
- Enhanced authentication
- Non standard apps
- Fine grained scan policy
- Advanced active scan
- Extended command line
- More API support





2.3 – continued...

- Internationalized help file, inc
 - Bosnian, French, Japanese, Spanish
- Keyboard shortcuts
- New UI options
- More functionality as add-ons
- New and improved scan rules
- Over 240 enhancements + fixes!



Demo Time





Questions?

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