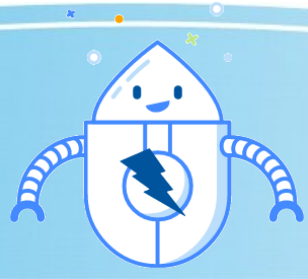
IWCON 2023

The SOFTWARE SECURITY PROJECT

A Decade + of Maintaining ZAP

Why I've done it and what I've learn along the way

Simon Bennetts
ZAP Project Lead
Software Security Project



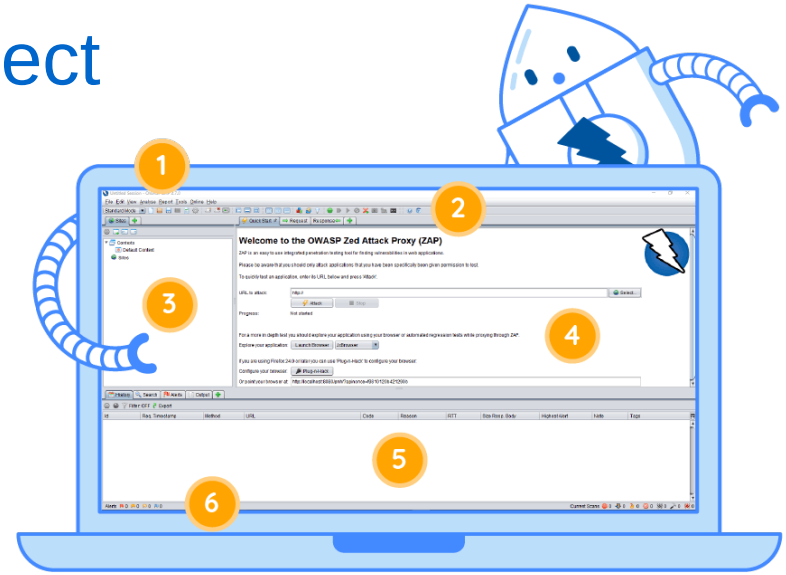
2023 December 17

This Talk

- An introduction to ZAP
- Why did I create ZAP?
- Running a successful open source project
- Ongoing challenges
- Conclusion

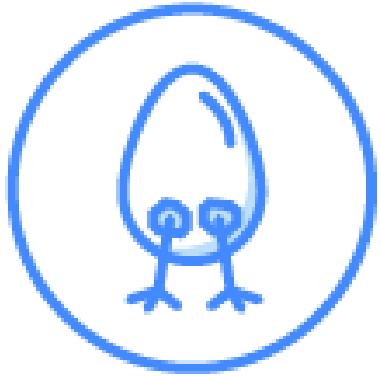
An Introduction to ZAP

- Tool for finding vulnerabilities in web apps
- Completely free and open source
- Welcoming community based project
- Ideal for newcomers and experts
- Great for automation
- The worlds most frequently used web app scanner!



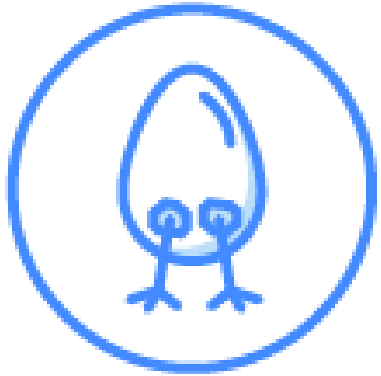
Why Did I Create ZAP?

- Developer / Team Lead
- No security training
- The pentest!
- Wanted a tool to automate security tests
- Wanted to learn more about web security
- Wanted to join a friendly open source project



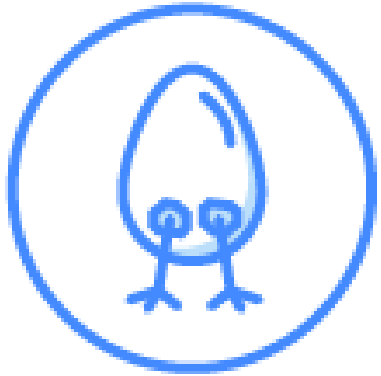
Why Did I Create ZAP?

- No actively maintained websec projects
- Started playing with abandoned ones
- Started learning with OWASP Top 10
- Started giving Top 10 presentations
- First questions was always: “What tools should we use?”
- My requirements: Free, open source, cross platform, easy to use, maintained



How Did I Create ZAP?

- Had already started to tweak Paros Proxy
- So this version was now being maintained
- Forked and rebranded it
- Added help pages, misc improvements
- Created ZAP Developer Google Group
- Nearly derailed by Andiparos
- Announced on Bugtraq..



ZAP Launch

The Zed Attack Proxy (ZAP) version 1.0.0

From: psiinon <psiinon () gmail com>
Date: Mon, 6 Sep 2010 21:21:56 +0100

Hello

I'd l
https
to be

Why h

There are many excellent pen test tools, but few of them are really
suitable for people with little pen test experience.
ZAP is really
new to pen t
as well.
While ZAP ca
primarily de
In order to
available bo

ZAP is a for
cross platfo
Note that there will NOT be a 'Pro' version of ZAP, so there will be
no incentive to restrict the features available in the 'free' version
:)
Involvement in the development of ZAP is actively encouraged.

Regards,

Psiinon

ZAP is really intended for developers and functional testers who are new to pen testing. However experienced pen testers may find it useful as well.

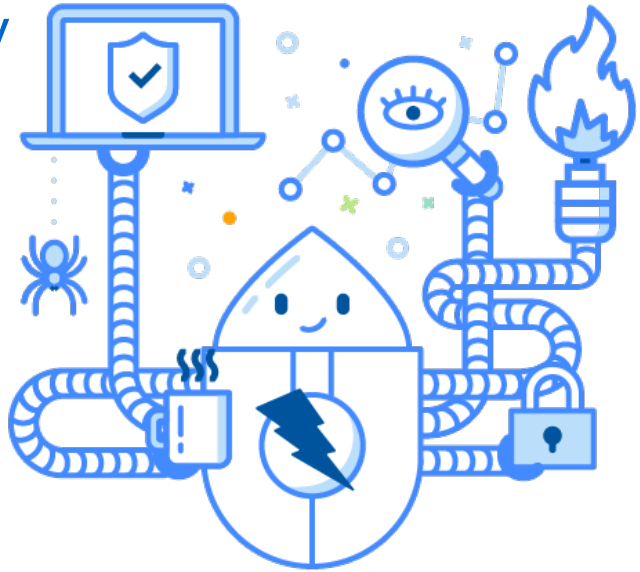
Note that there will NOT be a ‘Pro’ version of ZAP, so there will be no incentive to restrict the features available in the ‘free’ version :)
Involvement in ZAP is actively encouraged.

Promoting ZAP

- Bugtraq post
- Becoming an OWASP project
- Posting everywhere, esp if Paros Proxy or WebScarab mentioned
- Toolsmith Tool of the Year 2011
- AppSec Dublin 2012
- Security Conferences
- Developer Conferences
- Videos .. over 100 to date ..

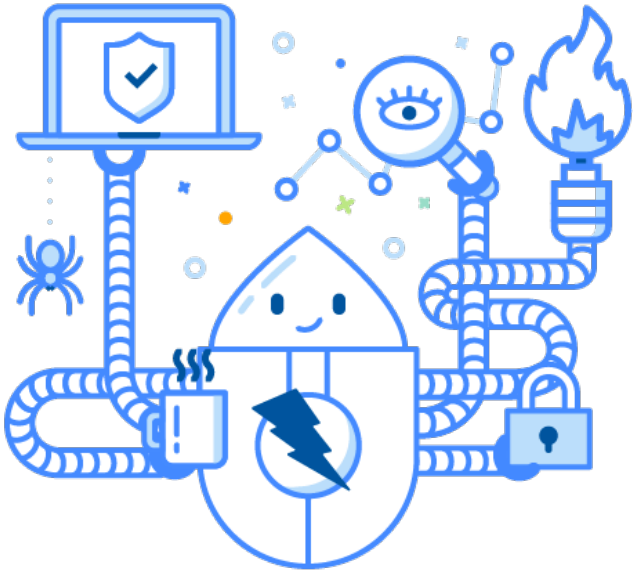
ZAP Today

- 4 Core Team – myself, thc202, kingthorin, and ricekot
- Very actively maintained – myself and thc202 full time
- Average ~ 2 releases a year, plus weekly + daily
- 42 repositories in zaproxy GitHub org
- Part of a large number of commercial offerings
- Worlds most popular webapp scanner
- A GitHub top 1000 project!



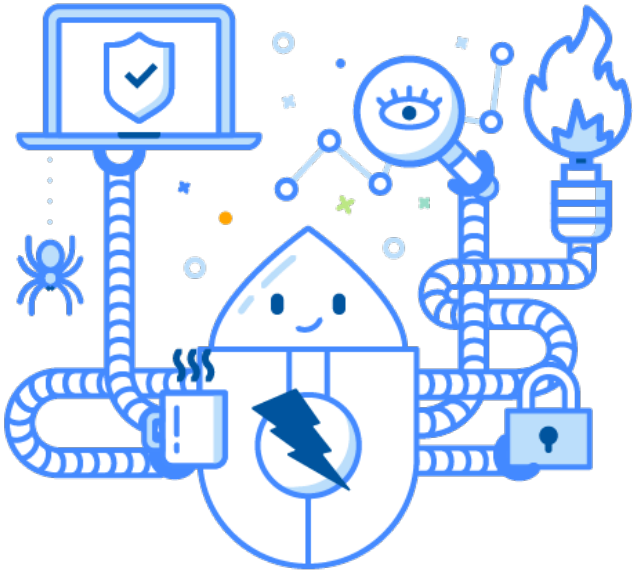
Running a Successful Open Source Project

- Community Vs small focussed team
- Spending time with new contributors
- Accepting it is no longer just your project
- Spinning plates
- Focus and ignoring distractions
- Documentation
- Persistence, ignoring detractors



Wearing Many Hats

- Designer, Implementer, Tester
- Technical Author
- Graphical Artist
- User Support
- Evangelist
- Project Manager
- Team Manager
- Marketeer



Getting Contributors

- ZAP has always been a community project
- Security people
  - Tend to contribute to another commercial tool
- Developers
  - Nervous about contributing to a security tools?
- Students
  - Lots of very significant contributions!

Student Hall of Fame

- https://www.zaproxy.org/student-hall-of-fame/

Student(s)	Contact	Title	Date	Program	Links
Vitika Soni		Postman Support	2023 Summer	GSoC	Blog, add-on
Aryan Gupta		Browser Recorder	2023 Summer	GSoC	Blog, add-on
Arkaprabha Chakraborty		Param Digger	2022 Summer	GSoC	Blog, add-on
Akshath Kothari		Out-of-band Application Security Testing	2021 Summer	GSoC	Blog, add-on
Pranav Saxena		Retesting Alerts	2021 Summer	GSoC	Blog, add-on
Akshath Kothari		GraphQL Support	2020 Summer	GSoC	Blog, add-on
Nirojan Selvanathan		ZAP GitHub actions	2020 Spring	Direct	Blog, blog
Nirojan Selvanathan		ZAP API documentation	2019 Autumn	GSoD	Blog, docs, repo
Manos Kirtas		Scanning websockets (phase 2)	2019 Summer	GSoC	Blog, wiki
David Scrobonia		The ZAP HUD	2016-2018	Direct	Repo, video
Kajan Mohanagandhirasa		Authentication helper	2018 Summer	GSoC	Wiki
Manos Kirtas		Scanning websockets (phase 1)	2018 Summer	GSoC	Blog
Ryan Webb		Form handling (team project)	2016 Winter	MWoS	Wiki

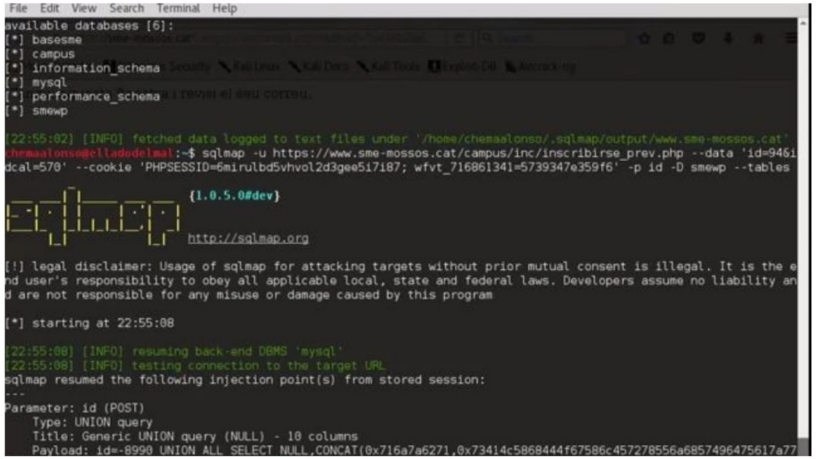
You Never Know Whats Coming Next...

A Notorious Hacker Just Released a How-To Video Targeting Police

The hacker behind the Hacking Team breach is hoping to get others into the game.

By Joseph Cox

19 May 2016, 6:52pm Share Tweet Snap



MORE LIKE THIS

Tech

Meet the Environmental Hacktivists Trying to 'Sabotage' Mining Companies

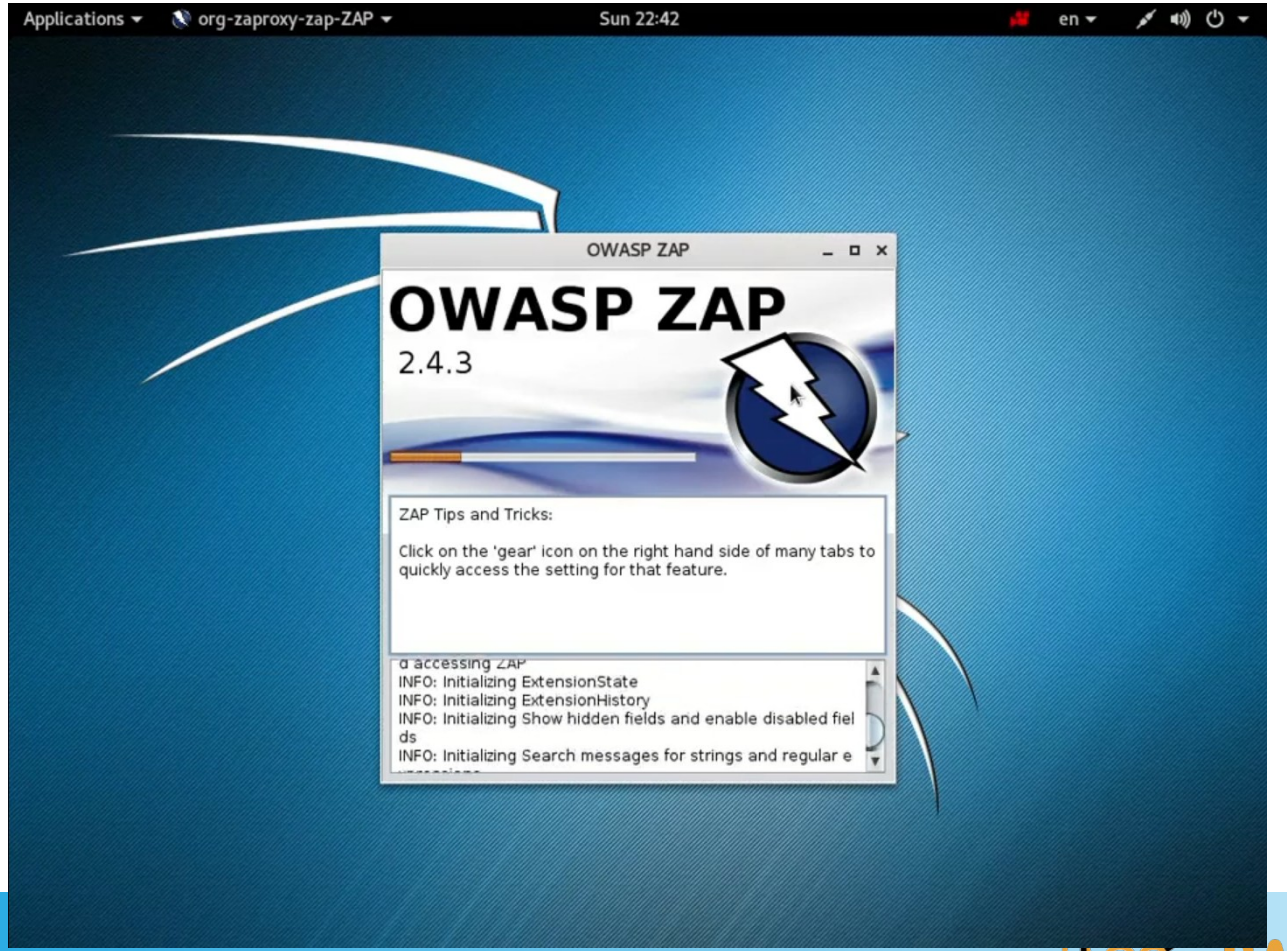
LORENZO FRANCESCHI-BICCHIERAI

08.16.22

Tech

BMW Wants to Charge for Heated Seats. These Grey

You Never Know Whats Coming Next...



You Never Know Whats Coming Next...

CVE-2021-44228 PUBLISHED

View JSON

Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints

Important CVE JSON 5 Information +

Assigner: Apache Software Foundation
Published: 2021-12-10 **Updated:** 2023-04-03

Zed Attack Proxy @zaproxy · Dec 10, 2021
Important advice re **ZAP** and **Log4Shell**:

zaproxy.org
ZAP and Log4Shell
ZAP appears to be impacted by the Log4Shell vulnerability - CVE-2021-44228. We have release...

30 47

Zed Attack Proxy @zaproxy · Dec 12, 2021
New **ZAP** alpha active scan rule: **Log4Shell** (CVE-2021-44228) detection: zaproxy.org/docs/desktop/a...
Note this does depend on OAST support: zaproxy.org/docs/desktop/a...
Great work by @ricekot_
Blog post coming soon... **#Log4Shell** #log4j #owasp #dast

3 61 121

IWCON 2023

OSS Competitors Come and Go

- https://github.com/psiinon/open-source-web-scanners

Main Site	Last Commit	Committers	Stars
ZAP	last commit yesterday	contributors 205	stars 12k
- ZAP Extensions	last commit yesterday	contributors 162	stars 772
Hetty	last commit march 2022	contributors 8	stars 5.8k
W3af	last commit june 2020	contributors 58	stars 4.4k
Arachni	last commit may	contributors 19	stars 3.6k
Astra	last commit february	contributors 9	stars 2.4k
Wapiti	last commit december	contributors 26	stars 871
Skipfish	last commit december 2012	contributors 1	stars 631
Sitadel	last commit november	contributors 3	stars 528

Ongoing Challenges

- Getting more (longterm) contributors
- Getting more (actionable) feedback
- Keeping up with emails, issues, slack, groups, twitter, mastodon, stackoverflow, etc etc
- Focus - doing the right things at the right times
- Funding...

Funding

- First 2 years – own time
- Mozilla – 40-80% of my time 2012-2020
- 2020 – 2023 100% my time, c/o 2 startups
- 2023 + Software Security Project
- Google Summer of Code – 21 student projects!
- Mozilla Winter of Security – 3 students (1 team)
- Google Season of Docs – 1 student
- Competitions – scripts, unit tests, report templates

Funding

- Build it and they will come ✓
- Build it and they will fund ✗
- Companies that rely on OSS projects don’t support them
- Startups cannot be relied upon to fund OSS projects
- Building an OSS revenue stream is **hard**

Conclusions

- Luck plays a big part – right place, right time
- An open source project is for life, not just Xmas / Divali ;)
- A successful open source project opens many doors
- Get involved – it really pays dividends
- Don’t be afraid to start a new open source project
- But be aware it can be a long term commitment
- Funding is important and **really** hard
- Keep plugging away!

More About ZAP