

OWASP ZAP

Intro & Latest Features

Simon Bennetts @psiinon
ZAP Project Lead
StackHawk Distinguished Engineer



2021 April 15 - OWASP Belgium



This Talk

- .ZAP Introduction
- .Automation Framework
- .Reporting Add-on



What is ZAP?

- A tool for finding vulnerabilities in web applications
- An OWASP Flagship Project
- Free and Open Source
- Cross platform
- Well maintained
- And ...



The worlds most widely used web scanner

- .~500K start pings every month
- .6M Docker pulls in Feb 2021
- .Used by large enterprises and individuals globally
- .Foundation for multiple commercial tools



Who is ZAP For?

- .Developers and functional testers (QA)
- .Students
- .Security Professionals



How can you run ZAP?

- Desktop GUI (requires Java)
- Heads Up Display
- Automation



How often is ZAP released?

- Full releases – averaging 2 a year
- Add-ons – released as and when required
- Weekly releases (zip and docker image)
- Live docker image



Any Questions
so far?



ZAP Automation

- .Command line scan
- .Packaged Scans
- .GitHub actions
- .Daemon + API
- .Automation Framework



New Automation Framework

- Runs entirely in ZAP
- No requirement for any containers
- Easily extensible
- Simple configuration – one YAML file
- Currently no GUI
- Expected to be most common way to automate ZAP

Command Line Options

- autorun <filename> Run the automation jobs specified in the file
- autogenmin <filename> Generate template automation file with the key parameters
- autogenmax <filename> Generate template automation file with all parameters
- autogenconf <filename> Generate template automation file using the current configs



Minimal YAML File

env:

contexts:

- name: example

url: <https://www.example.com/>

jobs:

- type: spider

- type: passiveScan-wait

- type: report



Automation Framework Demos

- .Minimal Generated Configuration
- .Maximum Generated Configuration
- .Baseline Scan
- .Full (restricted) Scan



Reporting

- .Core functionality not changed since Paros
- .3 reporting add-ons, none actively maintained
- .Now a forth add-on
- .This will be actively maintained
- .And will replace the core functionality



New Reporting Add-on

- Already much more flexible
- Supports
 - HTML, MD, JSON, XML, PDF
 - External resources like images and JS
- Uses Thymeleaf open source templating language
- Internationalized
- Can access much more data from ZAP



Reporting Demo

Generate Report

Scope Template Filter Options

Report Title:

Report Name:

Report Directory: ...


Description:

Contexts:

Sites:

Generate If No Alerts: ☐

Display Report: ☒



ZAP Reporting Competition

- \$100 for each HTML/PDF template we include with ZAP
- Aiming to accept around 10
- Looking for different styles, but must be practical
- Detail on the ZAP Blog: <https://www.zaproxy.org/blog/2021-03-12-report-competition/>
- Accepting submissions now!

Find Out More

[.www.zaproxy.org](http://www.zaproxy.org)

[.Twitter: @zaproxy](https://twitter.com/zaproxy)

