ZAP Automation in CI/CD

Simon Bennetts
ZAP Project Lead
StackHawk Inc

2021 February 9

This Talk

- ZAP Overview
- Automation Options
- The Automation Process
- ZAP Configuration
- Automation Framework WIP

What is ZAP?

- A tool for finding vulnerabilities in web applications
- An OWASP Flagship Project
- Free and Open Source
- Cross platform
- Well maintained
- Probably the worlds most frequently used web scanner!

Who is ZAP For?

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

ZAPCon!

March 9 2021 https://zapcon.io

Automation Options

- Command Line
- Jenkins Plugin
- Packaged Scans
- Github Actions
- Daemon + API

Command Line Quick Scan

- `./zap.sh -quickurl http://localhost:8080/bodgeit/ -quickprogress -cmd`

Jenkins Plugin – no longer supported :(

Packaged Scans

- https://www.zaproxy.org/docs/docker/
- Baseline Scan
- Full Scan
- API Scan
- Scan hooks

Github Actions

- https://github.com/marketplace/actions/owasp-zap-baseline-scan
- https://github.com/marketplace/actions/owasp-zap-full-scan

API and Daemon

- https://www.zaproxy.org/docs/api/

Automation Process

- What tests do you want to run?
- Test locally - manually first!
- Test locally - automated next
- Where should the results go to?
- Authentication is a pain!

ZAP Configuration

- Default directory
  - config.xml
  - contexts/
  - policies/
  - scripts/
  - plugin/

New ZAP Automation Framework WIP!

```yaml
env:
  contexts:
    - name: bodgeit
      url: http://localhost:8080/bodgeit/  # The top level url
      includePaths:                        # An optional list of regexes to include
      excludePaths:                        # An optional list of regexes to exclude
        - 'http://localhost:8080/bodgeit/logout'
      authentication:                      # TBA - in time to cover all auth configs
  parameters:
    failOnError: true
    failOnWarning: false
    progressToStdout: true
```

New ZAP Automation Framework WIP!

```yaml
jobs:
  - type: addOns                    # Any non standard add-ons to install
    parameters:
      updateAddOns: false           # Default: true
    install:
  - type: passiveScan-config        # The passive scanner jobs
    parameters:
      maxAlertsPerRule: 10          # Int: Maximum number of alerts to raise per rule
    rules:                          # Can be used to override default settings
      - id: 2
        desc: Private IP Disclosure # Not used - just for documentation
        threshold: high
```

New ZAP Automation Framework WIP!

```yaml
- type: spider                    # The traditional spider
  parameters:
    warnIfFoundUrlsLessThan: 50
    failIfFoundUrlsLessThan: 20
    maxDuration: 2                #
- type: activeScan                # The active scanner
  rules:                          # Can be used to override default settings
    - id: 0
      desc: Directory Browsing    # Not used - just for documentation
      strength: high
      risk: high                  # Will create an alert filter to change the risk
```

Find Out More

- www.zaproxy.org
- zapcon.io