

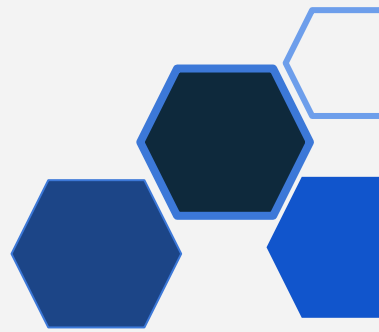
ROMHACK

CAMP



# OWASP Italian Chapter

ZAP Proxy  
An Open Source Web App Scanner





## \$ whoami

Giuseppe Porcu

Senior SW Security Consultant & Head of Training

@ IMQ Minded Security



Contacts:



giuseppe.porcu@mindedsecurity.com



www.linkedin.com/in/giuseppesorcu



# Agenda



The Open Web Application Security Project



OWASP Resources and Projects



Introduction to ZAP Proxy



Environment Set Up



Live Demo



Market & Add-ons

A cluster of four blue hexagonal icons in the top-left corner: a gear, a padlock, a person with glasses and a laptop, and a solid dark blue hexagon.

# Open **W**eb **A**pplication **S**ecurity **P**roject

**Nonprofit** foundation since 2001

Works to **improve the security** of software

Community-led **open-source projects**

Worldwide **local chapters** and members

Educational and training conferences





## OWASP Goals



**PROTECT**



**DETECT**



**LIFECYCLE**



# OWASP Core Values



## Open

**everything** at OWASP is radically **transparent** from our finances to our code



## Innovative

we encourage and **support innovation** and experiments for solutions to software security challenges



## Global

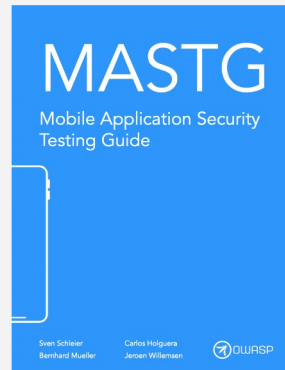
**anyone** around the world is **encouraged to participate** in the OWASP community



## Integrity

community is respectful, supportive, truthful and **vendor neutral**

# OWASP **Main** Guidelines





# OWASP Tools & Vulnerable Applications

Many **Open-Source & Free software** for security purpose

**Zap Proxy** - next slides for details ;)

**Dependency Checker**

**Vulnerable Applications**

JuiceShop online! at ***http://34.118.49.162:3000/***

...and so on...





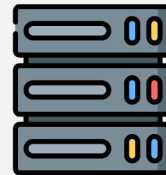
# ZAP 101

**Free** and **open-source** web app scanner

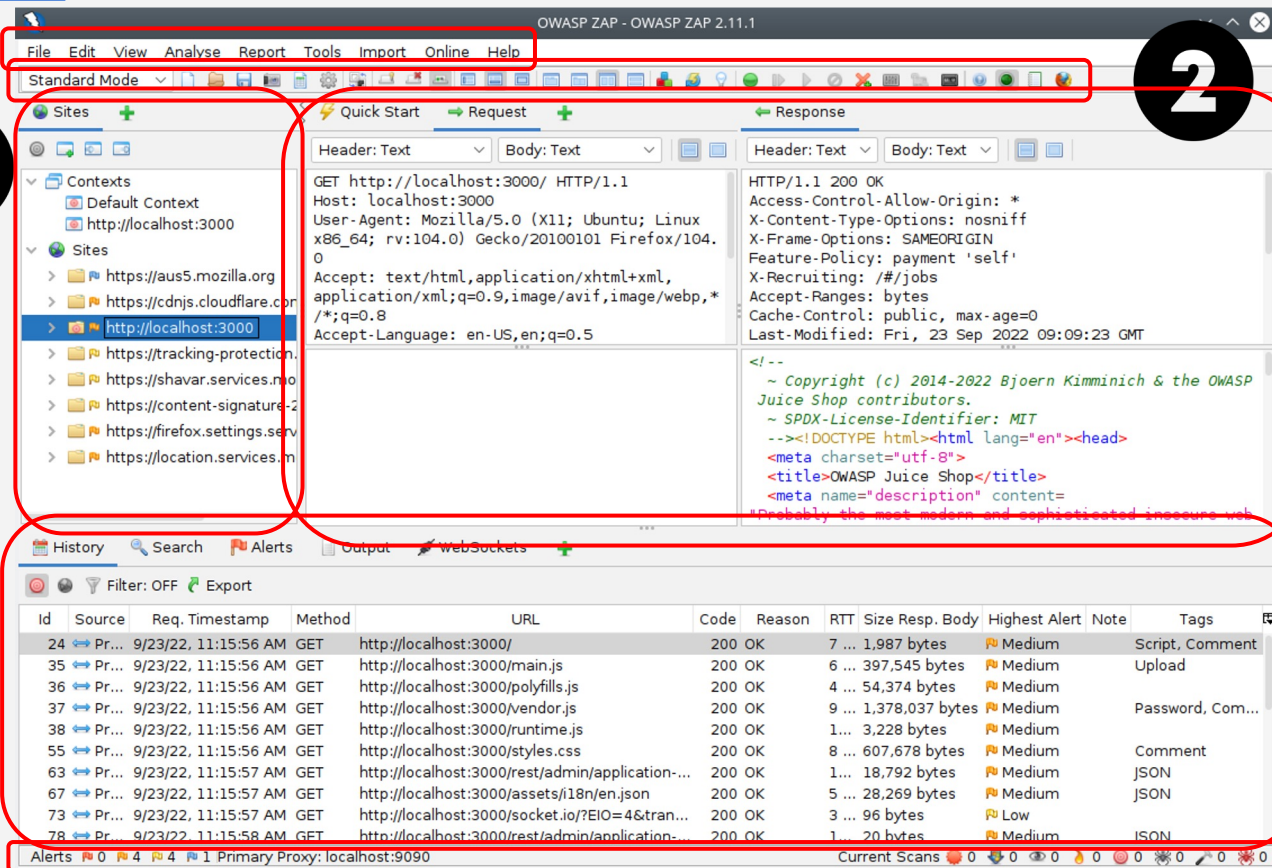
Maintained by **international team of volunteers**

**Customizable** with market or custom **add-ons**

Works with:   



# ZAP Overview



The screenshot shows the OWASP ZAP 2.11.1 interface. The menu bar (1) includes File, Edit, View, Analyse, Report, Tools, Import, Online, and Help. The toolbar (2) contains various icons for site management and analysis. The left sidebar (3) shows the 'Sites' tree with a list of sites, including 'http://localhost:3000'. The main pane (4) displays the 'Request' and 'Response' details for a GET request to 'http://localhost:3000/'. The 'Response' tab shows the HTTP status '200 OK' and the HTML body content. The bottom pane (5) shows the 'History' table with columns for Id, Source, Req. Timestamp, Method, URL, Code, Reason, RTT, Size, Resp. Body, Highest Alert, Note, and Tags. The status bar (6) at the bottom shows 'Alerts: 0', 'Primary Proxy: localhost:9090', and 'Current Scans: 0'.

1

2

3

4

5

6

A cluster of four hexagonal icons in the top-left corner. The top-left hexagon is dark blue with a white gear icon. The middle-left hexagon is dark blue with a white padlock icon. The bottom-left hexagon is light blue with a white icon of a person wearing a hood and glasses, sitting at a laptop. The top-right hexagon is dark blue.

## Environment Set-Up 1/2

**Download and install Zap Proxy** (or use standalone version)

- <https://www.zaproxy.org/download/>

**Set-up proxy on ZAP and Browser**

- ZAP: Tools > Options > Local Proxies
- Browser (eg. Firefox): Settings > General > Network Settings

## Environment Set-Up 2/2

### Add a ZAP Root CA to Browser Certificates

- ZAP: Tools > Options > Dynamic SSL Certificates > {Generate} > Save
- Browser (eg. Firefox): Settings > Privacy & Security > Certificates > View Certificate > Import (under Authorities tab) > Select certificate and check all boxes

### It is also possible to use Manual Explore on ZAP!

- Built-in browser already configured
- ZAP: Quick Start > Select URL > Launch Browser

### Start Testing Your Application!



# Most used Features - **Breakpoint**

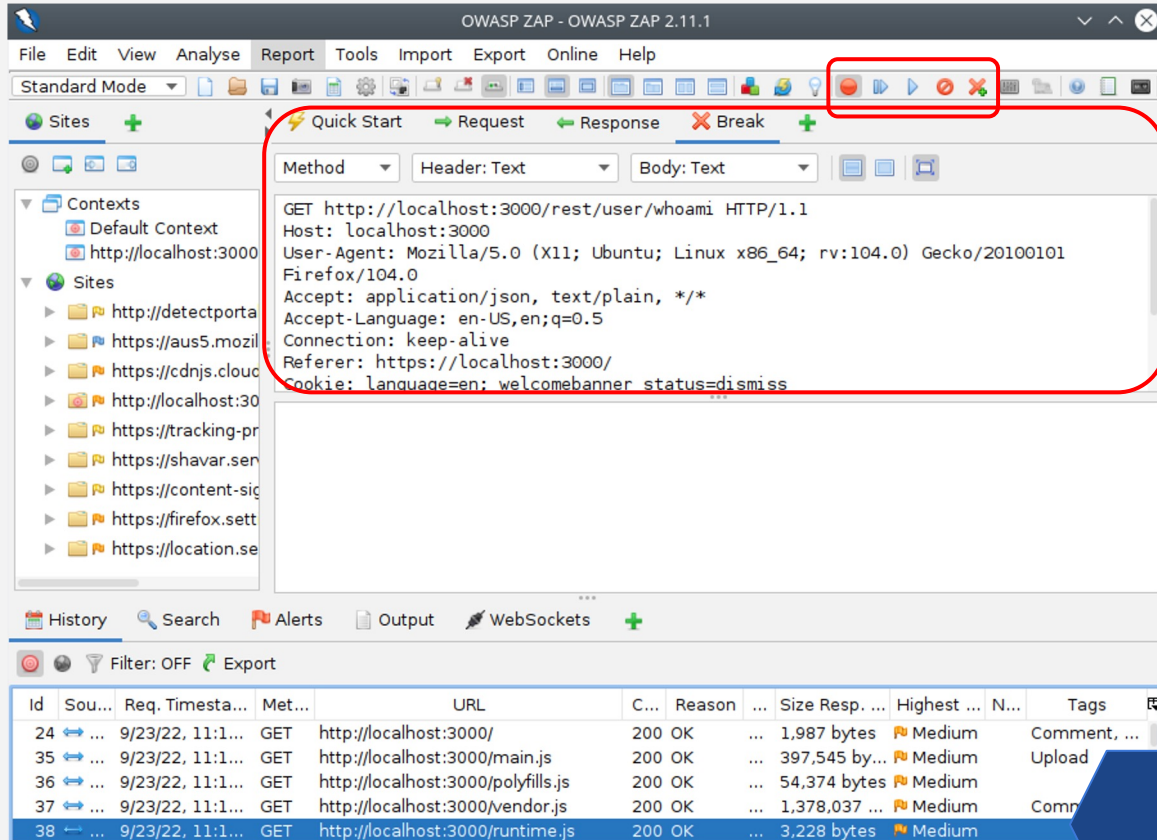
## **ZAP Breakpoint aka ZAP Proxy Interceptor**

- allows to intercept any request/response sent by browser
- once intercepted it is possible to modify them to perform security testing
- add/remove header, parameters, changing HTTP methods and so on

## **It is possible to set-up custom rules for breakpoints**

- intercept only request/response in context
- intercept on specific condition (URLs, methods, keyword ....)

# ZAP Breakpoint



OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Quick Start Request Response Break

Method: GET Header: Text Body: Text

GET http://localhost:3000/rest/user/whoami HTTP/1.1  
Host: localhost:3000  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:104.0) Gecko/20100101 Firefox/104.0  
Accept: application/json, text/plain, \*/\*  
Accept-Language: en-US,en;q=0.5  
Connection: keep-alive  
Referer: https://localhost:3000/  
Cookie: language=en; welcomebanner status=dismiss

History Search Alerts Output WebSockets

Filter: OFF Export

ID	Source	Req. Timesta...	Met...	URL	C...	Reason	Size Resp. ...	Highest ...	N...	Tags
24	...	9/23/22, 11:1...	GET	http://localhost:3000/	200	OK	1,987 bytes	Medium		Comment, ...
35	...	9/23/22, 11:1...	GET	http://localhost:3000/main.js	200	OK	397,545 bytes	Medium		Upload
36	...	9/23/22, 11:1...	GET	http://localhost:3000/polyfills.js	200	OK	54,374 bytes	Medium		
37	...	9/23/22, 11:1...	GET	http://localhost:3000/vendor.js	200	OK	1,378,037 bytes	Medium		Comm
38	...	9/23/22, 11:1...	GET	http://localhost:3000/runtime.js	200	OK	3,228 bytes	Medium		



# Most used Features - Request Editor

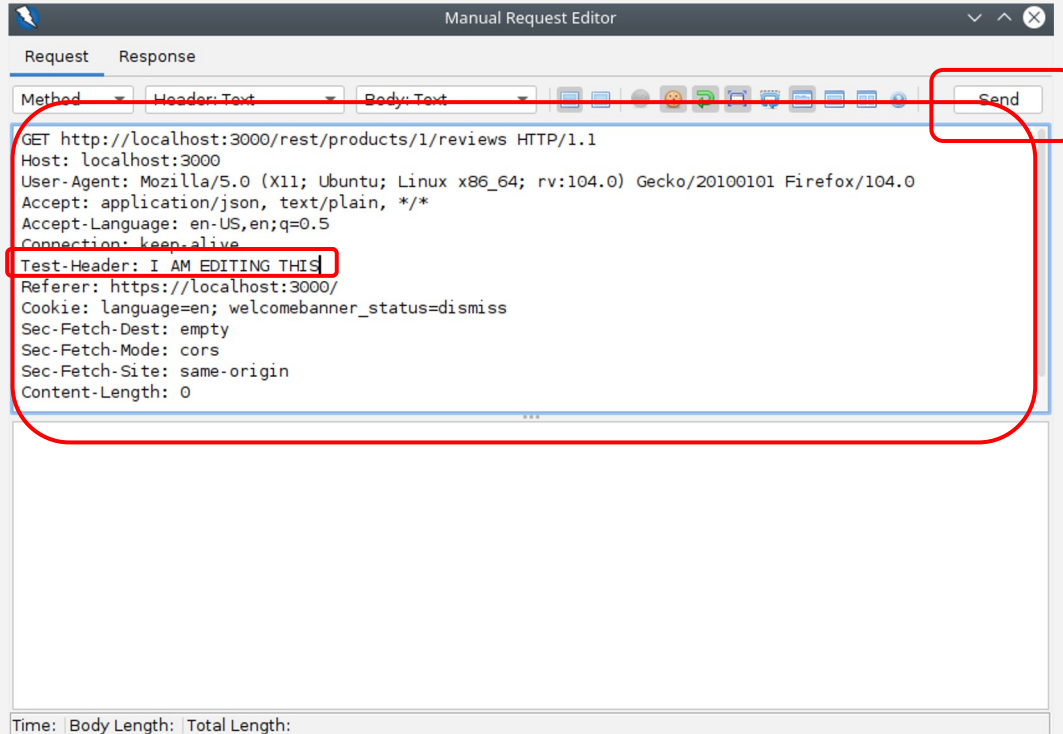
## ZAP Request Editor

- to test request **without intercepting each time**
- select the target request > right click, **Open/Resend in Request Editor**
- add/remove header, parameters, changing HTTP methods and so on

## Used to execute multiple test on the same request

- finding XSS, Injection, used parameters etc...

# ZAP Request Editor



The image shows the ZAP Manual Request Editor window. It has a title bar with a ZAP logo and the text 'Manual Request Editor'. Below the title bar are two tabs: 'Request' and 'Response'. The 'Request' tab is active. Below the tabs are three dropdown menus: 'Method' (set to GET), 'Header: Text' (set to Text), and 'Body: Text' (set to Text). To the right of these dropdowns is a 'Send' button. Below the dropdowns is a large text area containing the following request details:

```
GET http://localhost:3000/rest/products/1/reviews HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:104.0) Gecko/20100101 Firefox/104.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Test-Header: I AM EDITING THIS
Referer: https://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
```

At the bottom of the window, there are three labels: 'Time:', 'Body Length:', and 'Total Length:'.

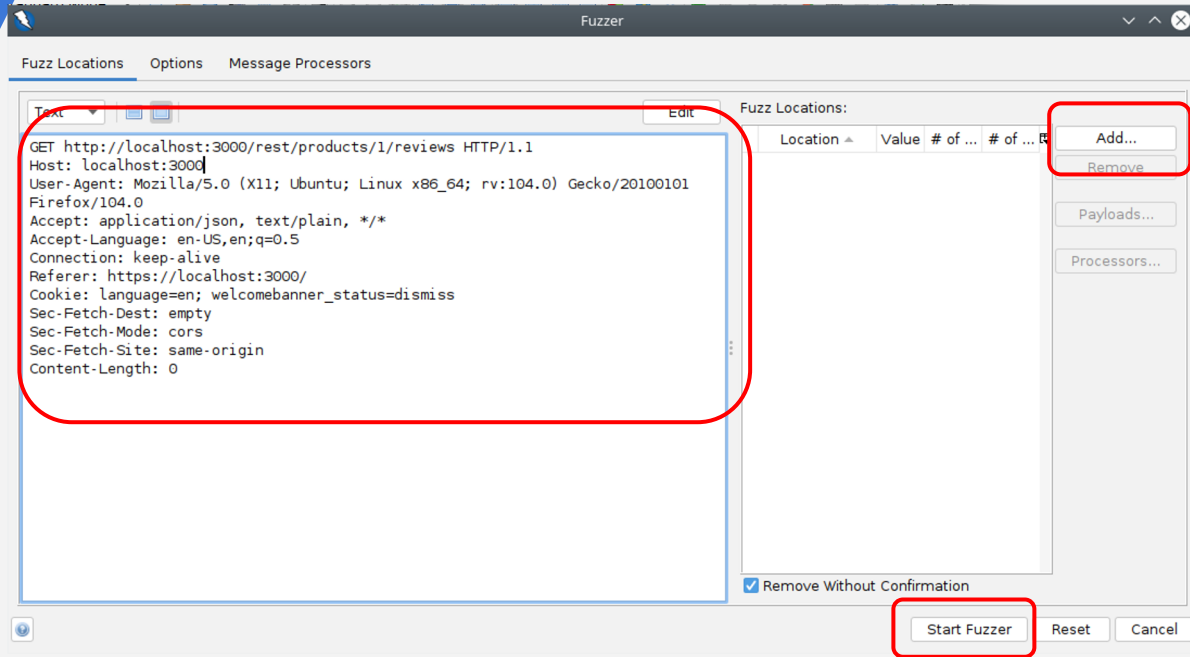


A cluster of four hexagonal icons in the top-left corner. The icons are: a gear, a padlock, a person wearing a hood and glasses, and a laptop.

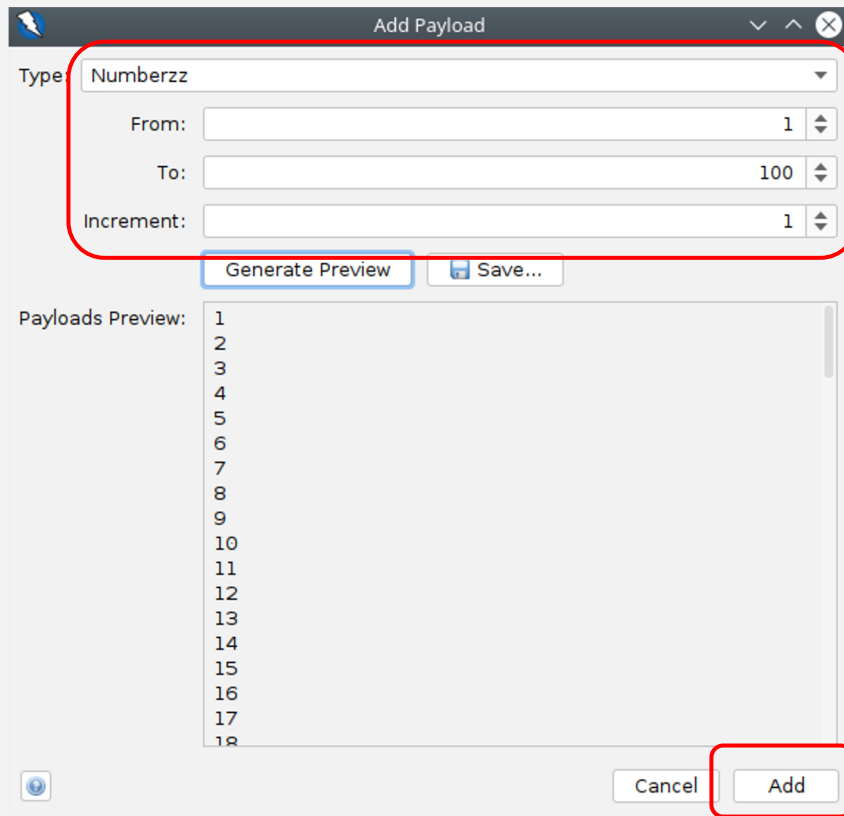
## Most used Features - **Fuzzer**

### ZAP Fuzzer

- sending multiple request in order to find sensitive information
- eg. config files, test page, information gathering on framework
- also used for bruteforce attacks (eg. usernames, ids ...)
- basically a machine-gun against the target
- select the target request > right click, **Fuzz**



# ZAP Fuzzer Options



The image shows the 'Add Payload' dialog box in ZAP. A red rectangle highlights the configuration area for a 'Numberzz' payload, which includes fields for 'From' (1), 'To' (100), and 'Increment' (1). Below this, there are 'Generate Preview' and 'Save...' buttons. The 'Generate Preview' button is also highlighted with a blue rectangle. The 'Payloads Preview' section shows a list of 18 generated payloads. At the bottom right, the 'Add' button is highlighted with a red rectangle.

Type:

From:

To:

Increment:

Payloads Preview:

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18

# ZAP Fuzzer Results

OWASP ZAP - OWASP ZAP 2.11.1

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites Quick Start Request Response Break

Text

Contexts

- Default Context
- http://localhost:3000

Sites

- http://detectport
- https://aus5.mo
- https://cdnjs.clou
- http://localhost:3
- https://tracking-p
- https://shavar.se
- https://content-s

```
GET http://localhost:3000/rest/products/4/reviews HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:104.0) Gecko/20100101 Firefox/104.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Referer: https://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
```

History Search Alerts Output WebSockets Fuzzer

New Fuzzer Progress: 0: HTTP - http://localhost:3000/rest/products/4/reviews 100% Current fuzzers: 0

Messages Sent: 100 Errors: 0 Show Errors

Task...	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
0	Original	200	OK	42 ...	385 bytes	172 bytes	Medium		
1	Fuzzed	200	OK	77 ...	385 bytes	172 bytes		Reflected	1
2	Fuzzed	200	OK	25 ...	385 bytes	184 bytes		Reflected	2
3	Fuzzed	200	OK	81 ...	385 bytes	185 bytes		Reflected	3
4	Fuzzed	200	OK	79 ...	384 bytes	30 bytes			4
5	Fuzzed	200	OK	44 ...	384 bytes	30 bytes			5
6	Fuzzed	200	OK	41 ...	385 bytes	170 bytes		Reflected	6
7	Fuzzed	200	OK	18...	384 bytes	30 bytes			7
8	Fuzzed	200	OK	69 ...	384 bytes	30 bytes			8
9	Fuzzed	200	OK	50 ...	384 bytes	30 bytes			9
10	Fuzzed	200	OK	24...	384 bytes	30 bytes			10

Alerts 0 5 4 3 Primary Proxy: localhost:9090 Current Scans 0 0 0 0 0 0 0 0 0 0



# Most used Features - **ATTACK**

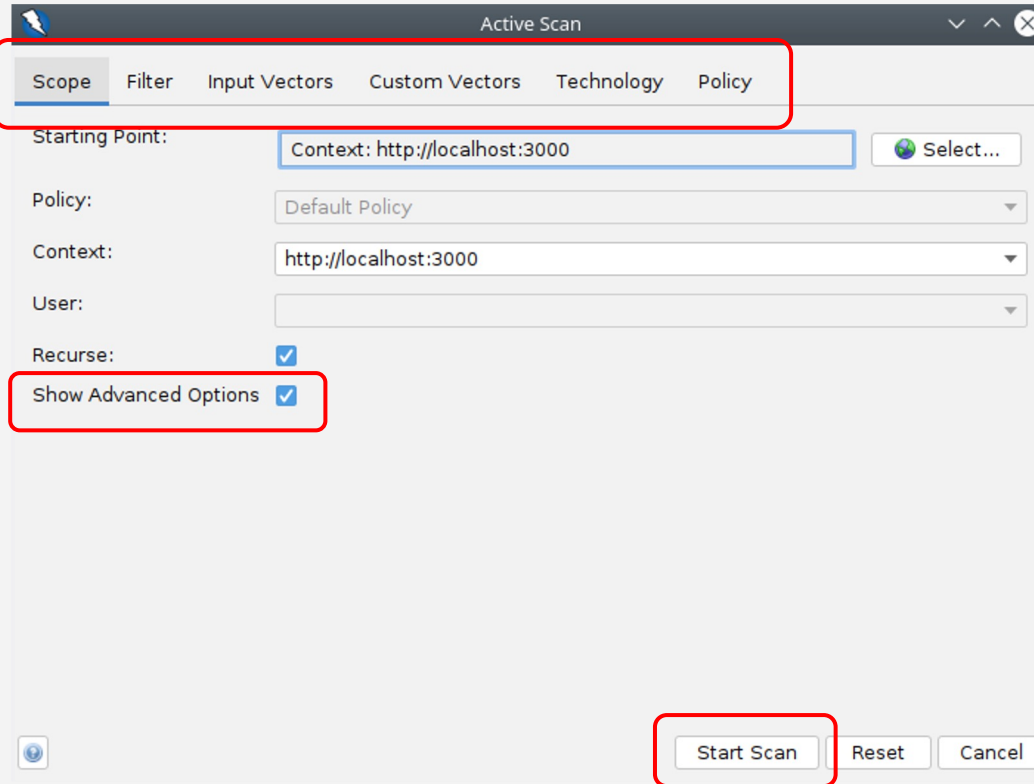
## ZAP ATTACK

- Active Scan
- passive scans are less intrusive and they are usually preferable in a real scenario
- vulnerabilities scanner
- basically a fuzzer against all the target
- used to find common vulnerabilities

## Once started...

- the request sent are showed in the **Active Scan** tab
- vulnerabilities found are showed in the **Alerts** tab


# ZAP ATTACK



The image shows the 'Active Scan' dialog box in ZAP. The 'Scope' tab is selected and highlighted with a red box. The 'Starting Point' is set to 'Context: http://localhost:3000'. The 'Policy' is 'Default Policy'. The 'Context' is 'http://localhost:3000'. The 'User' field is empty. The 'Recurse' checkbox is checked. The 'Show Advanced Options' checkbox is checked and highlighted with a red box. The 'Start Scan' button is highlighted with a red box. The 'Reset' and 'Cancel' buttons are also visible.

Active Scan

Scope Filter Input Vectors Custom Vectors Technology Policy

Starting Point: Context: http://localhost:3000  Select...


Policy: Default Policy

Context: http://localhost:3000

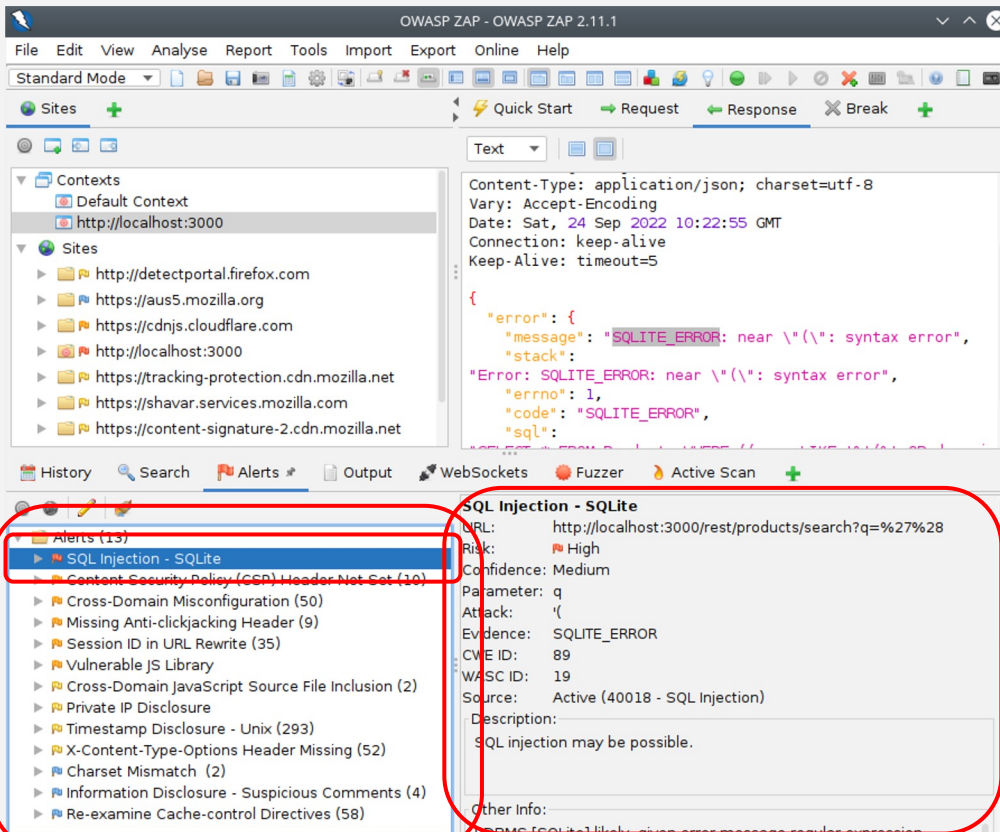
User:

Recurse: ☒

Show Advanced Options ☒

 Start Scan Reset Cancel

# ZAP ATTACK Result



The screenshot displays the OWASP ZAP 2.11.1 interface. The left sidebar shows a tree view with 'Contexts' and 'Sites'. The 'Alerts' tab is active, showing a list of alerts. A red box highlights the 'SQL Injection - SQLite' alert. The right pane shows the details of this alert, including the URL, risk, confidence, parameter, attack, evidence, CVE ID, WASC ID, source, description, and other info.

**Alerts (13)**

- SQL Injection - SQLite
- Content Security Policy (CSP) Header Not Set (10)
- Cross-Domain Misconfiguration (50)
- Missing Anti-clickjacking Header (9)
- Session ID in URL Rewrite (35)
- Vulnerable JS Library
- Cross-Domain JavaScript Source File Inclusion (2)
- Private IP Disclosure
- Timestamp Disclosure - Unix (293)
- X-Content-Type-Options Header Missing (52)
- Charset Mismatch (2)
- Information Disclosure - Suspicious Comments (4)
- Re-examine Cache-control Directives (58)

**SQL Injection - SQLite**

URL: http://localhost:3000/rest/products/search?q=%27%28

Risk: High

Confidence: Medium

Parameter: q

Attack: '('

Evidence: SQLITE\_ERROR

CVE ID: 89

WASC ID: 19

Source: Active (40018 - SQL Injection)

Description: SQL injection may be possible.

Other Info:   
The SQL query is likely using a regular expression.

# LIVE DEMO





## Market & Add-ons

ZAP is customizable with add-ons from the **Market Place**

It is also possible to write your own extension

- <https://www.zaproxy.org/docs/developer/creating-new-addon-in-zap-extensions/>
- <https://www.zaproxy.org/addons/>

### Collection: Pentester Pack

- ViewState, JWT, Fuzzer, File Upload

### GraphQL Support

- advanced support for GraphQL endpoints



Questions?





# Try ZAP in our Web Vulnerable Application!

**Juice Shop** accessible from the **WiFi network RHC22-hackspace**

- Register your team and solve some challenges
- The top 5 teams (with the most challenges solved) will win an exclusive OWASP/RomHack Camp Trophy
- The shop closes on Sunday at 9AM





Giuseppe Porcu

