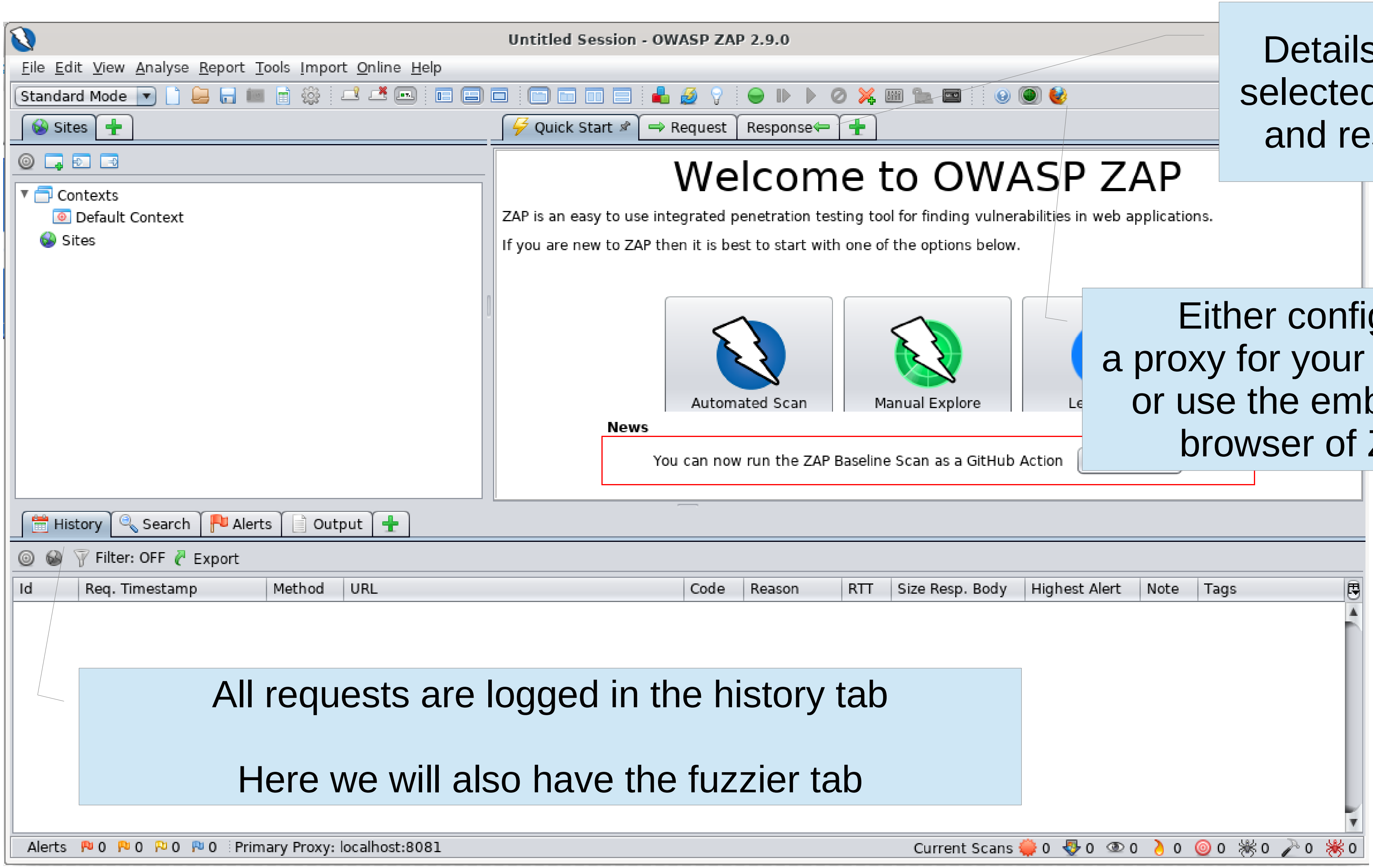
OWASP ZAP

Mario Alviano

OWASP Zed Attack Proxy

- Acts as a proxy for web requests
- Logs everything
- Forges custom requests
- Provides a repeater
- Provides a fuzzer
- Many other features

https://owasp.org/www-project-zap/



Untitled Session - OWASP ZAP 2.9.0

Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

News

You can now run the ZAP Baseline Scan as a GitHub Action

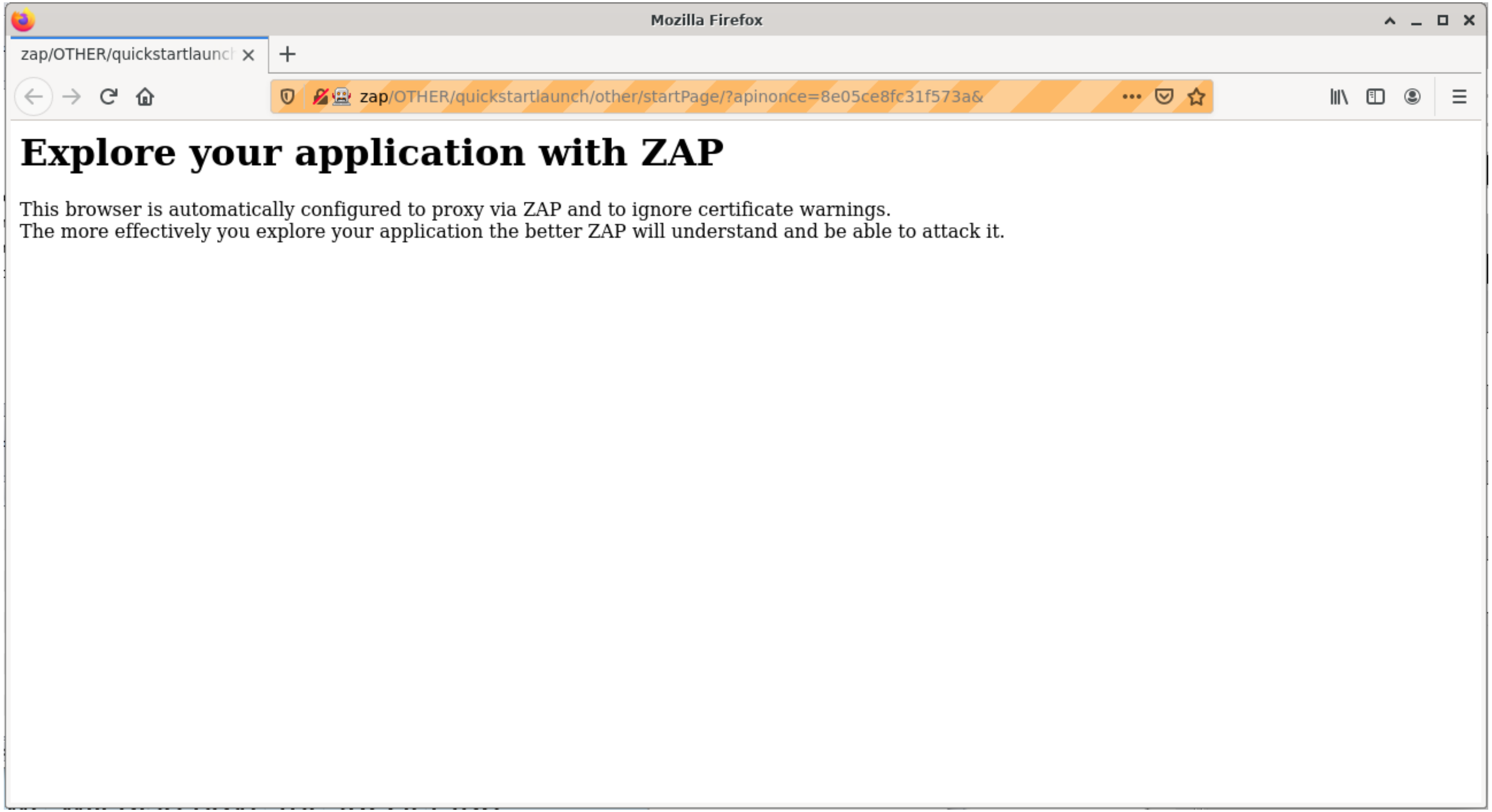
Primary Proxy: localhost:8081

Details on the selected request and response

Either configure a proxy for your browser, or use the embedded browser of ZAP

All requests are logged in the history tab

Here we will also have the fuzzier tab



Mozilla Firefox
zap/OTHER/quickstartlaunc
zap/OTHER/quickstartlaunch/other/startPage/?apinonce=8e05ce8fc31f573a&

Explore your application with ZAP

This browser is automatically configured to proxy via ZAP and to ignore certificate warnings.
The more effectively you explore your application the better ZAP will understand and be able to attack it.

Zero configuration approach: use the embedded browser of ZAP

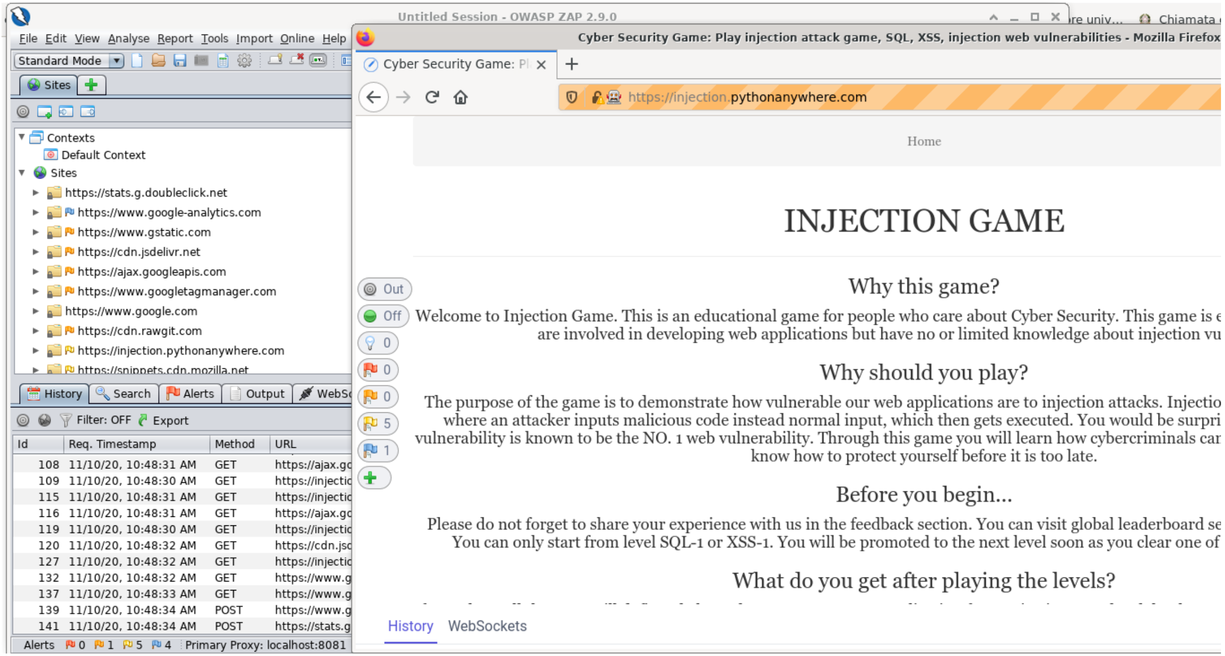
Examples

- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)

From the following

deliberately vulnerable website

https://injection.pythonanywhere.com/


Untitled Session - OWASP ZAP 2.9.0
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
History
Search
Alerts
Output
WebSo
Filter: OFF
Export
Cyber Security Game: Play injection attack game, SQL, XSS, injection web vulnerabilities - Mozilla Firefox
Cyber Security Game: Pl
re univ...
Chiamata
Out
Off
0
0
0
5
1
Home
History
WebSockets

Contexts
Default Context
Sites
https://stats.g.doubleclick.net
https://www.google-analytics.com
https://www.gstatic.com
https://cdn.jsdelivr.net
https://ajax.googleapis.com
https://www.googletagmanager.com
https://www.google.com
https://cdn.rawgit.com
https://injection.pythonanywhere.com
https://snippets.cdn.mozilla.net

Id	Req. Timestamp	Method	URL
108	11/10/20, 10:48:31 AM	GET	https://ajax.go
109	11/10/20, 10:48:30 AM	GET	https://injectio
115	11/10/20, 10:48:31 AM	GET	https://injectio
116	11/10/20, 10:48:31 AM	GET	https://ajax.go
119	11/10/20, 10:48:30 AM	GET	https://injectio
120	11/10/20, 10:48:32 AM	GET	https://cdn.jsd
127	11/10/20, 10:48:32 AM	GET	https://injectio
132	11/10/20, 10:48:32 AM	GET	https://www.g
137	11/10/20, 10:48:33 AM	GET	https://www.g
139	11/10/20, 10:48:34 AM	POST	https://www.g
141	11/10/20, 10:48:34 AM	POST	https://stats.g

Alerts 0 1 5 4 Primary Proxy: localhost:8081

https://injection.pythonanywhere.com

INJECTION GAME

Why this game?

Welcome to Injection Game. This is an educational game for people who care about Cyber Security. This game is e
are involved in developing web applications but have no or limited knowledge about injection vu

Why should you play?

The purpose of the game is to demonstrate how vulnerable our web applications are to injection attacks. Injectio
where an attacker inputs malicious code instead normal input, which then gets executed. You would be surpri
vulnerability is known to be the NO. 1 web vulnerability. Through this game you will learn how cybercriminals car
know how to protect yourself before it is too late.

Before you begin...

Please do not forget to share your experience with us in the feedback section. You can visit global leaderboard se
You can only start from level SQL-1 or XSS-1. You will be promoted to the next level soon as you clear one of

What do you get after playing the levels?

Live demo

- Intercept a request
- Inspect arguments
- Repeat a request
- Run the fuzzer
- Exploit (blind) SQLi to dump confidential content
- Reflected and stored XSS

Questions