# OWASP
# Zed Attack Proxy

## OWASP
Tbilisi Chapter
May, 2019

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

## The OWASP Foundation
http://www.owasp.org

# The Introduction

- The statement
  - You cannot build secure web applications unless you know how to attack them
- The problem
  - For many developers (including functional testers) ‘penetration testing’ is a black art
- The solution
  - Teach basic penetration techniques to developers

# Overview

- Why you should be using ZAP
- Introduction to ZAP
- ZAP Use cases
- Wrap up

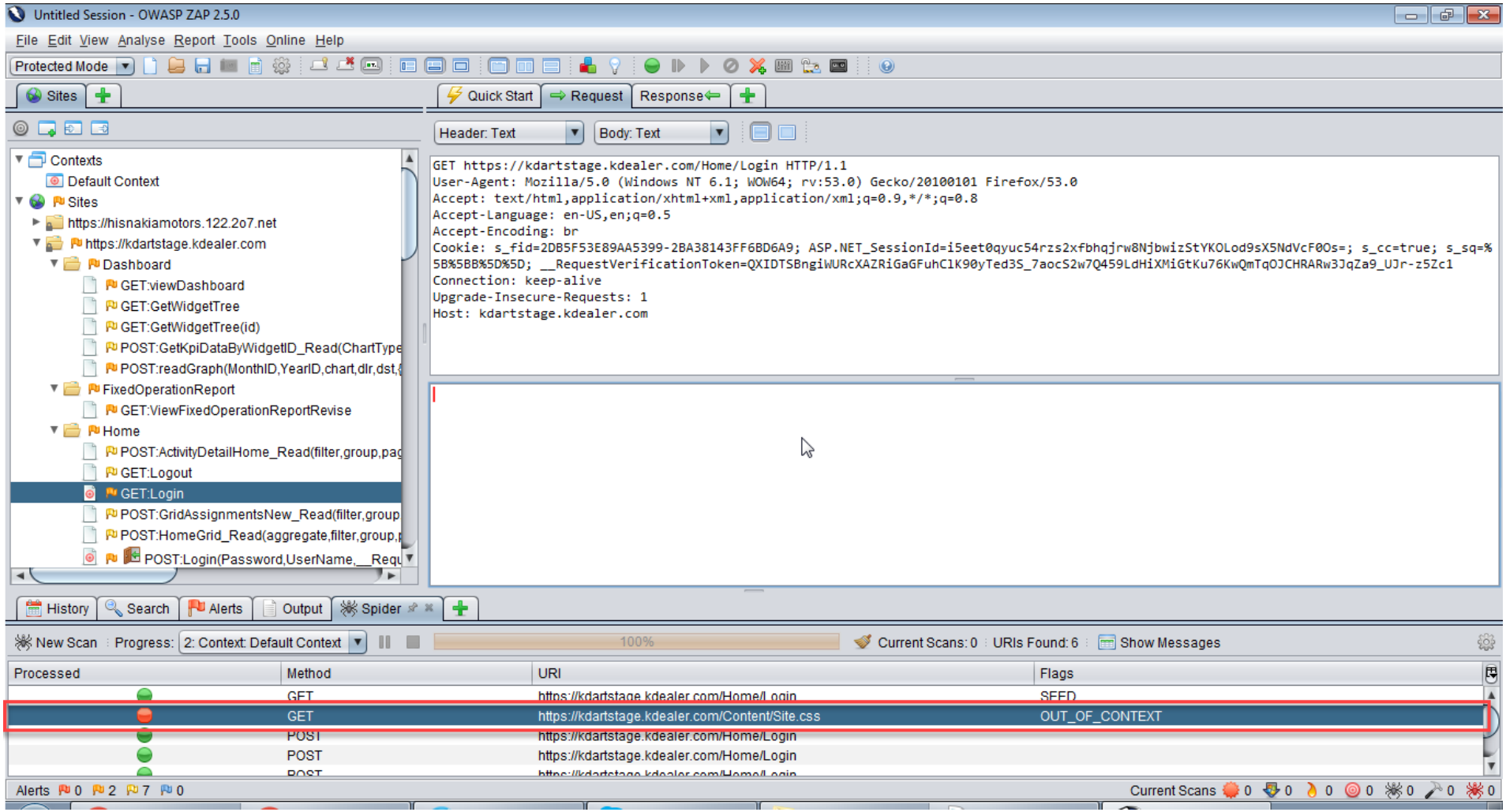
# Introducing OWASP ZAP

- An integrated penetration testing tool for finding vulnerabilities in web applications.
- Easy to use
- Easy to install
- Fully documented
- Free, Open source
- Cross platform
- Fully internationalized
- Works well with other tools
- Under active development
- Involvement actively encouraged

# The Features

- All the essentials for web application testing
- Intercepting proxy
- Automated scanner
- Passive scanner
- Spider
- Brute force scanner
- Port scanner
- Plus lots of useful things:
  - Fuzzing
  - Report generation
  - Web Sockets
  - REST API

# The screenshot



# Suggested use cases

- Point and shoot - Quick start
- Proxying via ZAP, and then scanning
- Spider to find missed content
- Brute force to find unreferenced content
- Automated security regression tests
- Active scan to find basic vulnerabilities
- Examine the requests and responses for more subtle issues
- Running in headless more and integrating in DevOps pipelines
- …

# The Summary

- Ideal for developers new to penetration testing
- Ideal for professional penetration testers
- Useful addition to experienced pen testers toolbox
- Get involved:
  - Try it out
  - Find vulnerabilities in your apps
  - Report bugs
  - Localize
  - Suggest improvements
  - Implement improvements
- https://www.owasp.org/index.php/ZAP

# Questions