



# 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

Untitled Session - OWASP ZAP 2.5.0

File Edit View Analyse Report Tools Online Help

Protected Mode

Sites + Quick Start Request Response +

Contexts

- Default Context
- Sites
  - https://hisnakiomotors.122.2o7.net
  - https://kdartstage.kdealer.com
    - Dashboard
      - GET:viewDashboard
      - GET:GetWidgetTree
      - GET:GetWidgetTree(id)
      - POST:GetKpiDataByWidgetID\_Read(ChartType)
      - POST:readGraph(MonthID,YearID,chart,dlr,dst)
    - FixedOperationReport
      - GET:ViewFixedOperationReportRevise
    - Home
      - POST:ActivityDetailHome\_Read(filter,group,pag
      - GET:Logout
      - GET:Login
      - POST:GridAssignmentsNew\_Read(filter,group
      - POST:HomeGrid\_Read(aggregate,filter,group,p
      - POST:Login(Password,UserName,Req

Header: Text Body: Text

GET https://kdartstage.kdealer.com/Home/Login HTTP/1.1  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: br  
Cookie: s\_fid=2DB5F53E89AA5399-2BA38143FF6BD6A9; ASP.NET\_SessionId=i5eet0qyuc54rzs2xfbhqjrw8NjbwizStYKOLod9sX5NdVcF00s; s\_cc=true; s\_sq=%5B%5B%5D%5D; \_\_RequestVerificationToken=QXIDTSBngiURcXAZRiGaGFuhClK90yTed3S\_7aocS2w7Q459LdHiXMi6tKu76KwQmTqOJCHRARw3JqZa9\_UJr-z5Zc1  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Host: kdartstage.kdealer.com

History Search Alerts Output Spider +

New Scan Progress: 2: Context: Default Context 100% Current Scans: 0 URIs Found: 6 Show Messages

Processed	Method	URI	Flags
	GET	https://kdartstage.kdealer.com/Home/Login	SEED
	GET	https://kdartstage.kdealer.com/Content/Site.css	OUT_OF_CONTEXT
	POST	https://kdartstage.kdealer.com/Home/Login	
	POST	https://kdartstage.kdealer.com/Home/Login	
	POST	https://kdartstage.kdealer.com/Home/Login	

Alerts 0 0 2 7 0 Current Scans 0 0 0 0 0 0 0 0 0 0

# 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 mode 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

