



## Zed attack proxy cookbook : hacking tactics, techniques, and procedures for testing web applications and APIs /

Soper, Ryan,  
author

Monografía

Dive into security testing and web app scanning with ZAP, a powerful OWASP security tool Purchase of the print or Kindle book includes a free PDF eBook Key Features Master ZAP to protect your systems from different cyber attacks Learn cybersecurity best practices using this step-by-step guide packed with practical examples Implement advanced testing techniques, such as XXE attacks and Java deserialization, on web applications Book Description Maintaining your cybersecurity posture in the ever-changing, fast-paced security landscape requires constant attention and advancements. This book will help you safeguard your organization using the free and open source OWASP Zed Attack Proxy (ZAP) tool, which allows you to test for vulnerabilities and exploits with the same functionality as a licensed tool. Zed Attack Proxy Cookbook contains a vast array of practical recipes to help you set up, configure, and use ZAP to protect your vital systems from various adversaries. If you're interested in cybersecurity or working as a cybersecurity professional, this book will help you master ZAP. You'll start with an overview of ZAP and understand how to set up a basic lab environment for hands-on activities over the course of the book. As you progress, you'll go through a myriad of step-by-step recipes detailing various types of exploits and vulnerabilities in web applications, along with advanced techniques such as Java deserialization. By the end of this ZAP book, you'll be able to install and deploy ZAP, conduct basic to advanced web application penetration attacks, use the tool for API testing, deploy an integrated BOAST server, and build ZAP into a continuous integration and continuous delivery (CI/CD) pipeline. What you will learn Install ZAP on different operating systems or environments Explore how to crawl, passively scan, and actively scan web apps Discover authentication and authorization exploits Conduct client-side testing by examining business logic flaws Use the BOAST server to conduct out-of-band attacks Understand the integration of ZAP into the final stages of a CI/CD pipeline Who this book is for This book is for cybersecurity professionals, ethical hackers, application security engineers, DevSecOps engineers, students interested in web security, cybersecurity enthusiasts, and anyone from the open source cybersecurity community looking to gain expertise in ZAP. Familiarity with basic cybersecurity concepts will be helpful to get the most out of this book

<https://rebiunoda.pro.baratznet.cloud:28443/OpacDiscovery/public/catalog/detail/b2FpOmNlbGVicmF0aW9uOmVzLmJhcmF0ei5yZW4vMzM4MDg5NDM>

**Edición:** 1st ed

**Editorial:** Birmingham, England Mumbai Packt Publishing [2023]

**Descripción física:** 1 online resource (284 pages)

**Contenido:** Cover -- Title Page -- Copyright and Credits -- Dedication -- Contributors -- Table of Contents -- Preface -- Chapter 1: Getting Started with OWASP Zed Attack Proxy -- Downloading ZAP -- Getting ready -- How to do it... -- Installing Docker -- See also -- Setting up the testing environment -- Getting ready -- How to do it... -- How it works... -- There's more... -- Setting up a browser proxy and certificate -- Getting ready -- How to do it... -- How it works... -- Testing the ZAP setup -- Getting ready -- How to do it... -- How it works... -- Chapter 2: Navigating the UI -- Technical requirements -- Persisting a session -- Getting ready -- How to do it... -- How it works... -- Menu bar -- Getting ready -- How to do it... -- How it works... -- There's more... -- Toolbar -- Getting ready -- How to do it... -- How it works... -- See also -- The tree window -- Getting ready -- How to do it... -- How it works... -- Workspace window -- Getting ready -- How to do it... -- How it works... -- Information window -- Getting ready -- How to do it... -- How it works... -- There's more... -- Footer -- Getting ready -- How to do it... -- How it works... -- Encode/Decode/Hash dialog -- Getting ready -- How to do it... -- How it works... -- See also -- Fuzzing with Fuzzer -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Chapter 3: Configuring, Crawling, Scanning, and Reporting -- Technical requirements -- Setting scope in ZAP -- Getting ready -- How to do it... -- How it works... -- Crawling with the Spider -- Getting ready -- How to do it... -- How it works... -- Crawling with the AJAX Spider -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Scanning a web app passively -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Scanning a web app actively -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Generating a report -- Getting ready -- How to do it... -- How it works... -- See also -- Chapter 4: Authentication and Authorization Testing -- Technical requirements -- Testing for Bypassing Authentication -- Getting ready -- How to do it... -- How it works... -- Testing for Credentials Transported over an Encrypted Channel -- Getting ready -- How to do it... -- How it works... -- Testing for Default Credentials -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Testing Directory Traversal File Include -- Getting ready -- How to do it... -- How it works... -- See also -- Testing for Privilege Escalation and Bypassing Authorization Schema -- Getting ready -- How to do it... -- How it works... -- Testing for Insecure Direct Object References -- Getting ready -- How to do it... -- How it works... -- There's more... -- Chapter 5: Testing of Session Management -- Technical requirements -- Mutillidae setup -- Testing for cookie attributes -- Getting ready -- How to do it... -- How it works... -- Testing for cross-site request forgery (CSRF) -- Getting ready -- How to do it... -- How it works... -- Testing for logout functionality -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Testing for session hijacking -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Chapter 6: Validating (Data) Inputs - Part 1 -- Technical requirements -- Testing for reflected XSS -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Testing for HTTP verb tampering -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Testing for HTTP Parameter Pollution (HPP) -- Getting ready -- How to do it... -- How it works... -- See also -- Testing for SQL Injection -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Chapter 7: Validating (Data) Inputs - Part 2 -- Technical requirements -- Testing for code injection -- Getting ready -- How to do it... -- How it works... -- Testing for command injection -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Testing for server-side template injection -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Testing for server-side request forgery -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Chapter 8: Business Logic Testing -- Technical requirements -- Test ability to forge requests -- Getting ready -- How to do it... -- How it works... -- See also -- Test for process timing -- Getting ready -- How to do it... -- How it works... -- See also -- Testing for the circumvention of workflows -- Getting ready -- How to do it... -- How it works... -- See also -- Testing upload of unexpected file types with a malicious payload -- Getting ready -- How to do it... -- How it works... -- See also -- Chapter 9: Client-Side Testing -- Technical requirements -- Testing for DOM-based cross-site scripting -- Getting ready -- How to do it... -- How it works... -- There's more... -- Testing for JavaScript execution -- Getting ready -- How to do it... -- How it works... -- There's more... -- Testing for HTML injection -- Getting ready -- How to do it... -- How it works... -- There's more... -- Testing for client-side URL redirect -- Getting ready -- How to do it... -- How it works... -- There's more... -- Testing cross-origin resource sharing -- Getting ready -- How to do it... -- How it works... -- There's more... -- Testing WebSockets -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Chapter 10: Advanced Attack Techniques

-- Technical requirements Performing XXE attacks -- Getting ready -- How to do it... -- How it works... -- Working with JSON Web Tokens -- Getting ready -- How to do it... -- How it works... -- There's more... -- Performing Java deserialization attacks -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Password brute-force via password change -- Getting ready -- How to do it... -- How it works... -- See also -- Web cache poisoning -- Getting ready -- How to do it... -- How it works... -- See also -- Chapter 11: Advanced Adventures with ZAP -- Technical requirements -- How to use the ZAP GUI local API to scan a target -- Getting ready -- How to do it... -- How it works... -- How to use the ZAP API via Docker -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Utilizing ZAP DAST testing with Jenkins -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Installing, configuring, and running the ZAP GUI OAST server -- Getting ready -- How to do it... -- How it works... -- There's more... -- See also -- Index -- About Packt -- Other Books You May Enjoy

**ISBN:** 1-80181-015-X

**Materia:** Penetration testing (Computer security) Web applications- Testing

**Autores:** Torres, Nestor N., author Almoailu, Ahmed, author

**Enlace a formato físico adicional:** Print version Soper, Ryan. Zed Attack Proxy Cookbook Birmingham : Packt Publishing, Limited,c2023

---

## Baratz Innovación Documental

- Gran Vía, 59 28013 Madrid
- (+34) 91 456 03 60
- informa@baratz.es