Week 1 Assignment Report

Securing Node.js Web Applications

Naveed Qadir

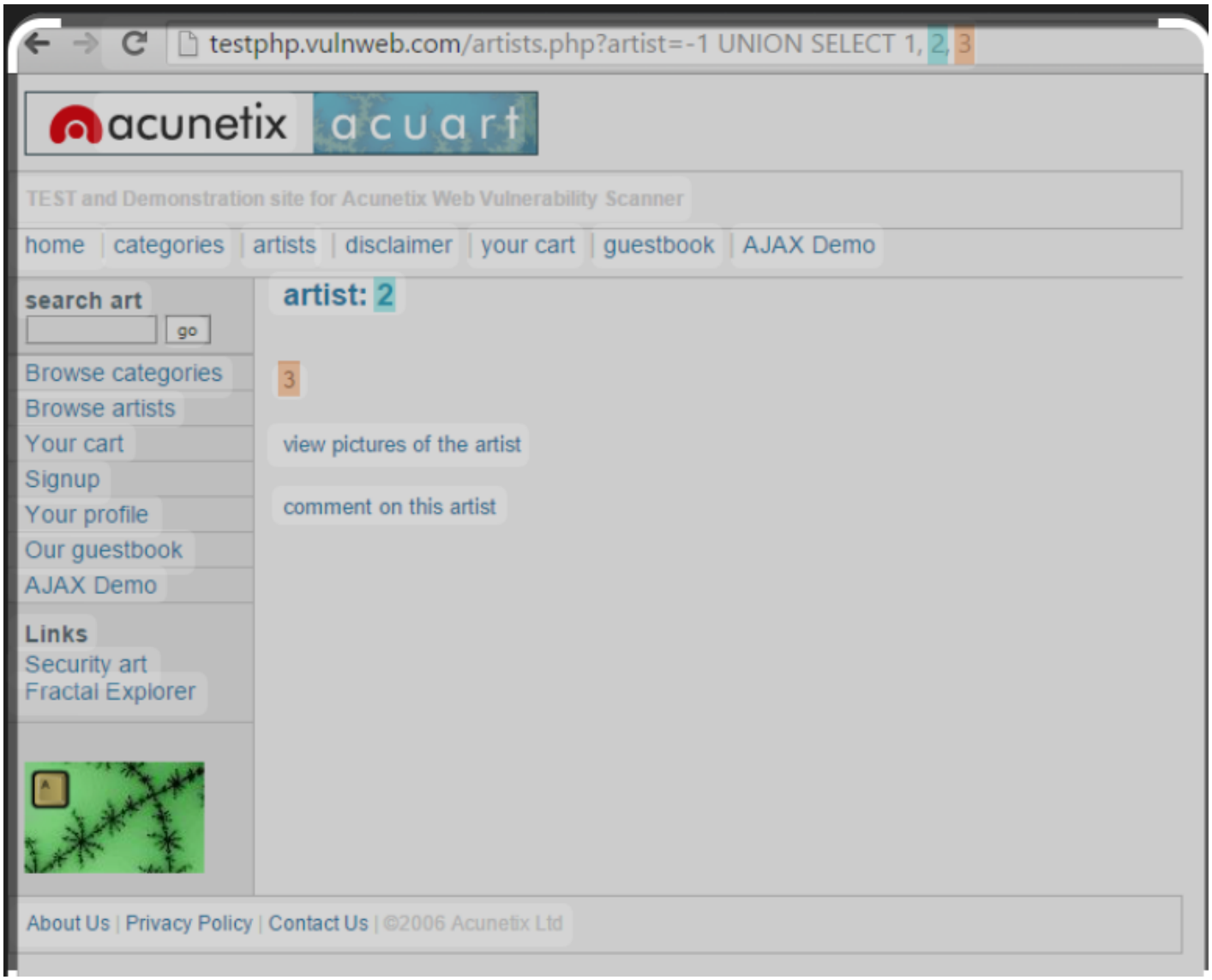
May 16, 2025

Introduction

- Started hands-on security testing with http://testphp.vulnweb.com/

- Used Kali Linux and OWASP ZAP

- Goal: Set up environment & explore vulnerabilities



Objectives

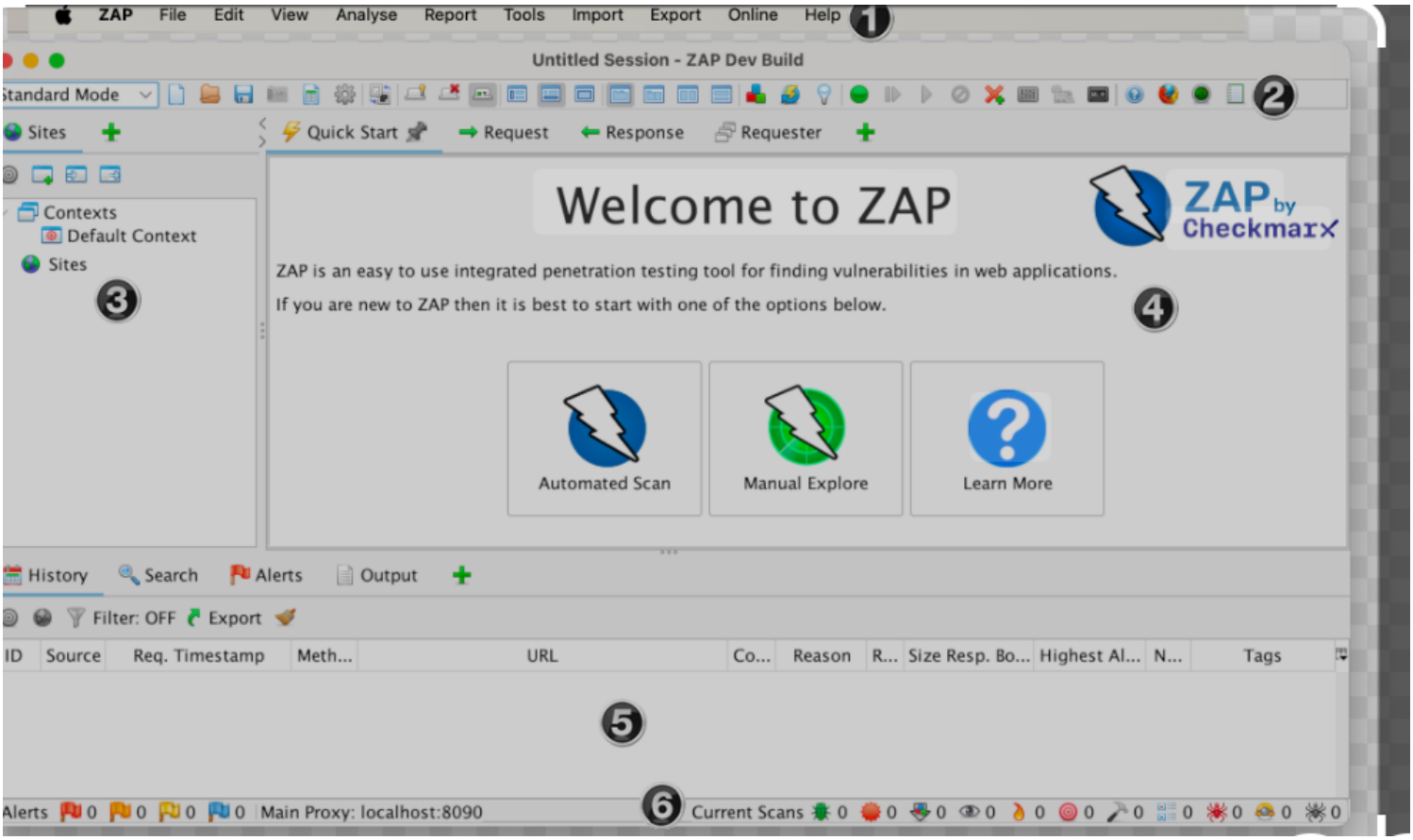
- Setup Kali Linux testing environment
- Use OWASP ZAP for scanning
- Explore the vulnerable website
- Identify possible vulnerabilities safely

Tools & Technologies

- Kali Linux (Pen testing OS)
- OWASP ZAP (Security scanner)
- Vulnerable site: testphp.vulnweb.com
- Firefox browser (configured with ZAP proxy)

What I Did

- Set up Kali Linux on VirtualBox
- Accessed vulnerable web app via Firefox
- Configured browser proxy with OWASP ZAP
- Crawled the website using ZAP spider
- Ran active scan to detect vulnerabilities



Knowledge Gained

- How to set up pen-testing lab with Kali Linux & ZAP
- Using automated tools to find website weaknesses
- Common vulnerabilities: XSS, directory listing, HTTP methods
- Importance of input validation and server config

Challenges Faced

- Configuring browser proxy with ZAP was tricky at first
- Understanding scan results and prioritizing issues
- Learning about HTTP security headers took extra time

Solutions & Recommendations

- Fix reflected XSS by sanitizing user input (e.g., htmlspecialchars() in PHP)
- Disable unnecessary HTTP methods except GET and POST
- Turn off directory listing (Options -Indexes)
- Add security headers (X-Frame-Options, Content-Security-Policy)
- Validate all user inputs on client and server sides