

**Name:** Bint e Fatima Niazi

**Date:** August 2025

**Contact:**

-Email: fatimabinte4@gmail.com

-LinkedIn: linkedin.com/in/bint-e-fatima-niazi

-GitHub: github.com/fatima-niazi

Project: Web Vulnerability Scanning using Nikto

# Introduction

On my cybersecurity learning journey, I explored Nikto — a powerful and fast web server scanner used for vulnerability assessment. The goal of this session was to scan both public and local web servers for misconfigurations, sensitive files, outdated software, and other vulnerabilities using Nikto.

# Objective

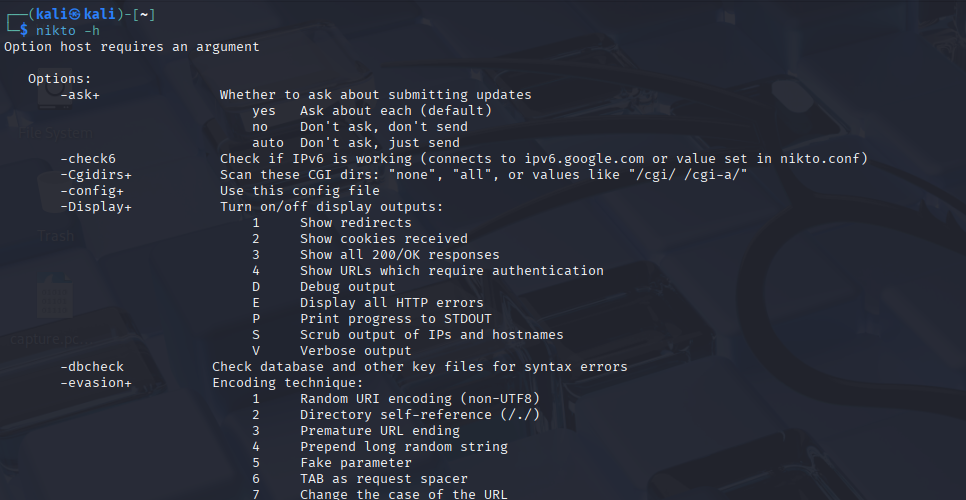
- Understand what Nikto is and how it helps in vulnerability scanning  
- Learn how to scan live and local web servers  
- Detect common misconfigurations, headers, and files  
- Use output for documentation and reporting

# Tools Used

- Kali Linux  
- Nikto (v2.5.0)  
- Python3 HTTP Server (for local testing)  
- Public target: testphp.vulnweb.com

# Step-by-Step Execution

**1. Verified Nikto installation:** nikto -h



**2. Ran Nikto on public test target:**  
 nikto -h <http://testphp.vulnweb.com>

A computer screen with white text

AI-generated content may be incorrect.

**3. Saved results to a file:**  
 nikto -h http://testphp.vulnweb.com -output nikto\_scan.txt

A computer screen shot of a program

AI-generated content may be incorrect.

**4. Applied tuning for specific scan types:**

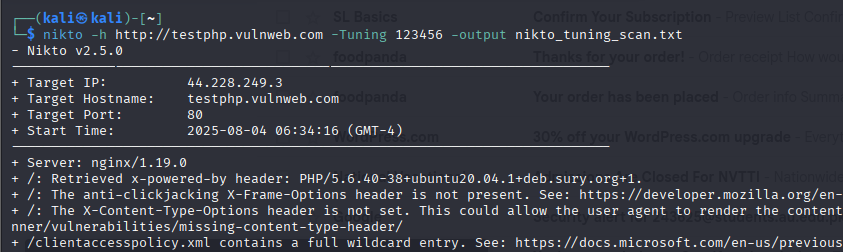
nikto -h <http://testphp.vulnweb.com> -Tuning 1

A screen shot of a computer screen

AI-generated content may be incorrect.

**5.** **Saved tuning results to a file:**

nikto -h <http://testphp.vulnweb.com> -Tuning 123456 -output nikto\_tuning\_scan.txt



**6. Ran local HTTP server:**  
 python3 -m http.server 8080

A screen shot of a computer

AI-generated content may be incorrect.

**7. Scanned local server:**  
 nikto -h 127.0.0.1 -p 8080

A screenshot of a computer program

AI-generated content may be incorrect.

**8. Applied tuning for specific scan types:**  
 nikto -h http://127.0.0.1 -p 8080 -Tuning 123

A screenshot of a computer program

AI-generated content may be incorrect.

# Output Analysis

Nikto returned results indicating:  
- Missing anti-clickjacking headers  
- Exposure of web server type and version  
- Availability of default and potentially dangerous files or directories  
- Basic information disclosure headers like X-Powered-By

# SOC Analyst Relevance

In a real SOC environment, these types of scans can trigger alerts or require monitoring. Analysts often look for repeated scanning behavior, exposure of default files, outdated software, or attempts to access administrative paths. Nikto is also used during vulnerability assessment and red teaming to identify publicly exposed attack surfaces.

# Conclusion

Using Nikto provides a quick and effective way to perform web reconnaissance and detect misconfigurations. It's a powerful tool for both red and blue teams to assess web server hygiene. The knowledge gained here strengthens web attack surface awareness for any SOC analyst or cybersecurity practitioner.