## Project Guide: VAPT - testphp.vulnweb.com

### 1. Project Overview

This lab demonstrates a structured **Vulnerability Assessment and Penetration Test (VAPT)** against a controlled target, testphp.vulnweb.com. The project goal was to identify and document security flaws across the server infrastructure and the web application layer using a combination of automated and manual inspection techniques.

### Scope and Limitations

- **Scope:** External assessment targeting open ports and the HTTP web application layer.
- **Limitation:** Due to the nature of the target (minimal interactive input fields found), the assessment focused on configuration and component analysis, and **no active exploitation or destructive actions were performed.**

### Key Skills Demonstrated

- **Assessment Proficiency:** Skilled use of industry-standard tools (Nmap, Nikto, Burp Suite, Gobuster) for discovery and scanning.
- **Component Analysis:** Identifying outdated software (PHP 5.x) and linking it to specific, known **CVEs (Common Vulnerabilities and Exposures)**.
- **Risk Reporting:** Translating complex technical disclosures into clear, actionable risks for management.

### 2. Report Division and Purpose

This VAPT project includes a three-part deliverable set:

| **Report File** | **Target Audience** | **Primary Focus** |
|---|---|---|
| Formal_Report.md | Non-Technical Management | Summary of High-Risk Findings, Business Impact, and High-Level Remediation Strategy. |
| Technical_Report.md | Security Engineers / Developers | Detailed methodology, specific tool outputs, vulnerability URLs, and evidence log. |
| Project_Guide.md (This file) | Peers, Hiring Managers | Methodology breakdown, project scope, and demonstration of full VAPT lifecycle. |

### 3. Core Technical Finding

The primary critical finding was the clear **Component Disclosure** of an outdated PHP server version (PHP 5.x). This vulnerability, while passive, immediately subjects the environment to numerous public zero-day and patched exploits, confirming a critical need for patching.