SIGMA – VAPT REPORT

Version 1.0

Assessed by:

<Enter Your Name>

Customer:

Justin Pineda

Date: <Insert Date>

All texts that are highlighted in yellow should be removed from the report. After finishing the VAPT report, save document as a password-protected PDF before sending to the customer. Share the password on a separate email.

Sigma- VAPT Report

Revision Changes

Version	Date	Changes	Last Modified by
1.0			

Sigma- VAPT Report

Table of Contents

Don’t forget to refresh the Table of Contents

Sigma- VAPT Report

Executive Summary

Guidelines for Writing the VAPT Executive Summary

The Executive Summary must be concise, non-technical, and focused on the business impact of the findings. It should be a maximum of one page and address the following mandatory elements:

1. Project Context and Scope

This section sets the stage by clearly defining what was tested and when.

Element	Description
Type of Test	State the specific type of engagement (e.g., External Network Penetration Test, Internal Application Security Test, Black Box Web Application VAPT).
Test Dates	Clearly state the start and end dates of the active testing phase (e.g., October 15, 2025, to October 26, 2025).
Duration	Specify the total engagement duration in working days or weeks (e.g., 10 days, 2 weeks).
Tools & Methodologies	Briefly mention the standards and primary tools used. *Do not list every single tool.* Focus on the approach (e.g., "The testing followed the OWASP Top 10 methodology, utilizing commercial tools like Burp Suite Professional and manual validation techniques.").
Scope of Assets	A high-level description of the assets tested (e.g., "The primary e-commerce application, version 2.1, and its underlying APIs.").

2. Summary of Findings

This must be a brief, high-level synopsis of the risk profile, **not** a list of vulnerabilities.

- **Risk Profile:** Summarize the overall security posture using key metrics.
    - *Example:* "The assessment identified **1 Critical** vulnerability, **3 High** severity vulnerabilities, and **5 Medium** severity items. The most severe flaw allows an unauthenticated attacker to bypass authorization controls."

- **Key Finding:** Clearly articulate the single most critical or impactful vulnerability in business terms.
    - *Example:* "The most significant risk identified is a failure in session management which, if exploited, could lead to a **full data breach** of customer PII."
- **Root Cause Theme:** Briefly touch on the overarching issue (e.g., "Most findings are rooted in unvalidated user input and outdated dependency usage.").

3. Overall Recommendation (Go/No-Go Decision)

This is the most important part for management. It must be a clear, unambiguous statement.

- **Current Status:** State the overall security disposition based on the identified risks.
    - *Example:* "**Recommendation: Postponed Deployment (No-Go)**"
- **Rationale:** Justify the recommendation in one or two sentences.
    - *Example:* "Due to the presence of a Critical vulnerability (Unauthorized Access) that severely compromises customer data integrity, the system is **not recommended** for live deployment until all Critical and High findings are verified as remediated."
- **Next Steps:** Provide immediate, clear direction for the remediation team.
    - *Example:* "Immediate action is required to patch the Critical flaw. A retest focusing on Critical and High items must be scheduled within 14 days."

Template Example Snippet:

*"This report details the findings of a **Black Box Web Application Penetration Test** conducted on the 'Project Phoenix' Customer Portal (V1.5) over a **10-day** period, from **November 1st to November 10th, 2025**. The engagement followed industry-standard methodologies, primarily utilizing the **OWASP Top 10** framework. The testing identified **1 Critical**, **4 High**, and **6 Medium** severity findings. The Critical finding—an unauthenticated remote code execution vulnerability—poses an unacceptable risk to organizational data integrity. **Overall Recommendation: No-Go for Production.** Deployment must be halted until the Critical and High findings are verified as fully remediated."*

Sigma- VAPT Report

INTRODUCTION

All sections/portions that are highlighted with green should be updated by the tester and remove the highlight after.

Scope of Assessment:	<IP addresses and domains> DVWA Application WebGoat Application BWAPP Application
Exclusions:	<What are not included>
Inclusive Dates of Assessment:	
User Accounts:	
Assessors:	
Contact #:	
E-mail Address:	
Customer Contact:	Justin David Pineda
Designation:	CISO
E-mail Address:	justinp@pinedacybersecurity.com

METHODOLOGY

Web Application VAPT Methodology (Sigma VAPT Standard)

This engagement utilized a comprehensive, five-phased approach based on industry best practices (e.g., OWASP Testing Guide, PTES), ensuring thorough coverage of both technical vulnerabilities and business logic flaws.

Phase 1: Planning and Scoping (Define the Rules of Engagement)

This initial phase focuses on defining the project's boundaries and goals.

1. **Scope Finalization:** Confirming the list of in-scope assets (URLs, IP ranges, APIs) and clearly identifying all exclusions.
2. **Credential Setup:** Provisioning necessary accounts for authenticated testing (if required for the engagement type).
3. **Rules of Engagement (ROE):** Establishing communication channels, incident handling procedures, and clear limits on destructive testing.

Phase 2: Information Gathering and Reconnaissance

The objective is to gather deep technical and functional knowledge about the target application.

1. **Passive Reconnaissance:** Identifying technologies, frameworks, infrastructure details, and potential sensitive data exposure (e.g., public code repositories, exposed endpoints).
2. **Application Mapping:** Mapping the entire application structure, including all visible and hidden directories, pages, parameters, and application state transitions.
3. **Client-Side Analysis:** Inspecting JavaScript files, cookies, headers, and local storage to understand client-side logic and identify potential weaknesses.

Phase 3: Vulnerability Analysis and Manual Testing

This phase involves systematic analysis and exploitation attempts across all identified attack surfaces.

1. **Automated Scanning:** Utilizing commercial-grade scanning tools to quickly identify low-hanging and easily discoverable technical vulnerabilities.
2. **Manual Penetration Testing:** Deep-dive manual testing focused on high-impact categories, including:
    - **Injection Flaws (SQL, Command, LDAP)**
    - **Authentication and Authorization Bypass**
    - **Session Management Weaknesses**
    - **Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF)**
    - **Security Misconfigurations**
    - **Outdated Components and Libraries**
3. **Business Logic Testing:** Testing specific, non-technical flows unique to the application (e.g., abusing shopping cart discounts, manipulating loan application data, unauthorized access between user accounts).
4. **Proof-of-Concept (PoC) Generation:** Developing non-destructive PoC exploits to validate the actual risk and impact of key findings.

Phase 4: Reporting, Risk Rating, and Communication

All findings are documented, rated, and presented to the client.

1. **Risk Rating:** Assigning a severity rating (Critical, High, Medium, Low, Informational) based on a matrix considering Likelihood and Business Impact.
2. **Remediation Guidance:** Providing detailed, specific, and actionable advice for fixing each vulnerability, including code examples and best practice references.
3. **Presentation:** Delivering a final report that includes the Executive Summary, detailed findings, and the overall Go/No-Go recommendation.

Phase 5: Retest and Closure

Post-remediation activity to confirm the application's security posture has improved.

1. **Remediation Verification:** Conducting a focused retest of all Critical and High severity findings reported in the initial assessment to verify successful patch deployment.
2. **Final Sign-Off:** Issuing a final summary letter confirming which issues have been fixed and formally closing the engagement.

Defect Levels

VAPT Defect Severity Levels and Risk Rating

Vulnerabilities are rated based on a combination of technical likelihood of exploitation and the potential business impact. This matrix defines the risk levels used throughout this report.

Severity Level	Description	Business Impact
Critical	Vulnerabilities that allow an unauthenticated or authenticated attacker to gain unauthorized access to critical data, perform arbitrary code execution, or compromise the entire system. Exploitation is typically straightforward and requires low skill.	**Immediate and Catastrophic:** Financial loss, regulatory fines, severe reputational damage, complete system compromise, and potential service outage. Requires immediate remediation (within 24-48 hours).
High	Vulnerabilities that lead to significant access to sensitive information, unauthorized modification of user data, or elevation of privileges for a limited set of users. Exploitation may require moderate skill or specific conditions.	**Serious:** Significant financial or reputational damage, breach of customer PII, compliance violations, or limited denial of service (DoS). Must be remediated urgently (within 7-14 days).
Medium	Vulnerabilities that could potentially lead to minor information leakage, minor privilege	**Moderate:** Limited exposure of non-critical data, minor user experience degradation,

	escalation, or impact a limited number of users. Exploitation requires the attacker to overcome moderate hurdles.	potential for account hijacking of low-privilege users. Should be addressed as part of the normal development cycle (within 30-60 days).
Low	Vulnerabilities that pose minimal direct risk to the application or data. These are typically best practice recommendations, configuration issues, or minor information disclosure that do not directly facilitate a more serious attack.	**Minimal:** Minor operational inconvenience, marginal risk to business objectives, or improvements to defensive posture. Recommended for future security hardening efforts.

Security Assessment Results

Critical (0)	
High (0)	
Medium (0)	
Low (0)	

Note:

- The results only show a single instance of the defect. It is the responsibility of the internal IT Team to ensure that all instances of the defect are fixed.

Sigma- VAPT Report

Defective Findings

Defect # 1- Fail Open Authentication Scheme

Defect #	1
Defect Name:	Fail Open Authentication Scheme
Severity	Critical
Status (Open / Closed)	Open
Tool Used	Burp Suite (Proxy)
Description	The application allows “Password” field to be removed. It can successfully login an account using only a Username.
Application Name	WebGoat
URL	http://127.0.0.1/WebGoat/attack?Screen=39&menu=1000
Proof of Concept (PoC)	1. Go to http://127.0.0.1/WebGoat/attack?Screen=39&menu=1000 2. Input a valid username (e.g. webgoat) 3. Open BurpSuite and turn Intercept On 4. Do not input any password. Click login

Original request

Pretty Raw Hex

```
12 Upgrade-Insecure-Requests: 1
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/146.0.0.0
   Safari/537.36
14 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/
   avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
   ange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer:
   http://127.0.0.1/WebGoat/attack?Screen=39&menu=1000&Restart=
   39
20 Accept-Encoding: gzip, deflate, br
21 Cookie: JSESSIONID=8A4ED07D386A73D642AB7A7C2F9FB214
22 Connection: keep-alive
23
24 Username=webgoat&Password=&SUBMIT=Login
```

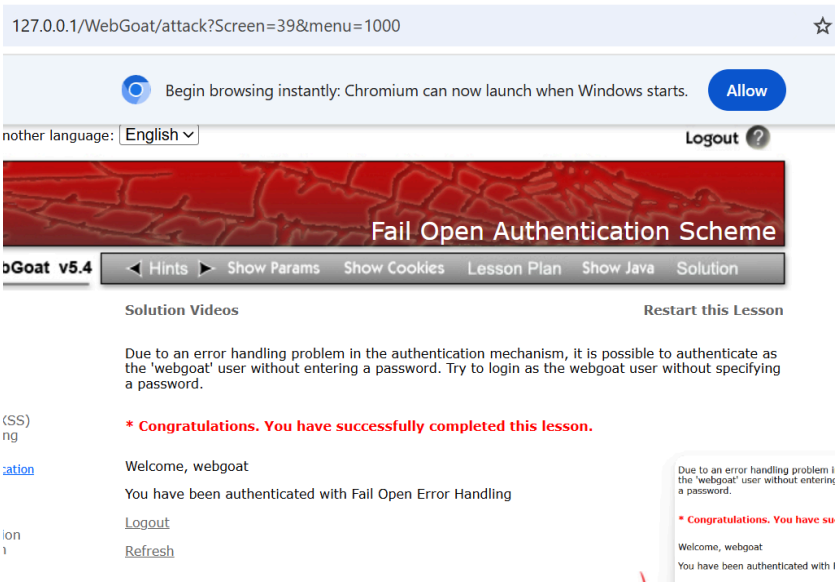
5. In BurpSuite, remove the parameter password and click Forward.

Request

Pretty Raw Hex

```
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: http://127.0.0.1/WebGoat/attack?Screen=39
20 Accept-Encoding: gzip, deflate, br
21 Cookie: JSESSIONID=8A4ED07D386A73D642AB7A7C2F9FB21
22 Connection: keep-alive
23
24 Username=webgoat&SUBMIT=Login
```

6. The application will allow you to login successfully.

	
Recommendation	The application must ensure that both username and password are validated correctly before a successful login.
Assessor	Justin Pineda

NMAP Results

These instructions cover the essential steps for utilizing Nmap to identify network services, open ports, and version information, providing the foundation for deeper vulnerability analysis.

1. Basic Host Discovery and Open Ports (Quick Scan)

The goal of this initial scan is to quickly determine which hosts are live and which TCP ports are open. This is used to define the initial attack surface.

Command	Description	Purpose
nmap -sS <target_ip_range>	**TCP SYN Scan (Stealth Scan)**	The standard, fast, and default scan. It does not complete the three-way handshake, making it less intrusive and quicker than a full connect scan.
nmap -Pn <target_ip>	**Treat Host as Online**	Use if the target appears down. It skips the host discovery phase (ping) and attempts the port scan directly.
nmap -F <target_ip>	**Fast Scan**	Scans only the 100 most common ports. Useful for quick checks before a full, comprehensive scan.

2. Complete Port Scan (Full Range and UDP)

A full port scan ensures no services running on non-standard ports are missed. UDP scanning is essential for services like DNS, SNMP, and DHCP.

Command	Description	Purpose
nmap -p- <target_ip>	**Full TCP Port Scan**	Scans all 65,535 TCP ports. This scan takes significantly longer but is mandatory for a comprehensive VAPT.

nmap -sU <target_ip>	**UDP Scan**	Scans for open UDP ports. Because UDP is stateless, this scan is much slower and less reliable, but critical for finding services that rely solely on UDP.
nmap -sS -sU -p 1-65535,U:161,53 <target_ip>	**Combined Comprehensive Scan**	A comprehensive scan combining SYN and UDP, focusing on all TCP ports and key UDP ports.

3. Service and Version Enumeration (-sV)

Once open ports are identified, this step determines the exact application and version running on each port. This is vital for cross-referencing public vulnerability databases (CVEs).

Command	Description	Purpose
nmap -sV <target_ip>	**Service and Version Detection**	Attempts to determine the service name and version number running on open ports.
nmap -A <target_ip>	**Aggressive Scan**	Enables OS detection (-O), version detection (-sV), script scanning (-sC), and traceroute. This is a very noisy but highly informative scan.
nmap -sC -sV <target_ip>	**Default Scripts and Version**	Runs the default set of Nmap Scripting Engine (NSE) scripts (-sC) alongside version detection (-sV) to check for common vulnerabilities and perform deeper enumeration.

4. Output Management (Mandatory)

Always save the scan results in multiple formats for reporting and analysis.

Command	Description	Purpose
nmap -oA <filename_prefix> <target>	**All Formats Output**	Saves the scan results in normal, XML, and Grepable formats using the specified prefix (e.g., nmap_results.nmap, nmap_results.xml, etc.).

CVE-MITRE

Cross reference whether NMAP scan findings have a corresponding CVE.

Directory Paths Dicovered

Crawl the applications assigned and past all the directories here.

Sigma- VAPT Report

Defect Findings

Defect #	1
Defect Name:	Cross-Site Scripting (Reflected)
Severity	
Status (Open / Closed)	
Tool Used	
Description	
Application Name	DVWA - Low
URL	
Proof of Concept (PoC)	
Recommendation	
Assessor	

Defect #	2
Defect Name:	Cross-Site Scripting (Stored)
Severity	
Status (Open / Closed)	
Tool Used	
Description	
Application Name	DVWA - Low
URL	
Proof of Concept (PoC)	
Recommendation	
Assessor	