Web Application Penetration Testing(WAPT) Project

Rules Of Engagement

Group 2:

Harshwardhan Raval

Nikita Jadav

Sanaz Dashti

Sarvani Vaddadi

Shikhant Saini

Varun Singh

Professor: Bipun Thapa

April 4, 2025

1 Introduction

1.1 Purpose

This Rules of Engagement (ROE) document details the agreement between CYBMOD and the client regarding the Web Application Penetration Testing (WebVAPT) engagement. Its main objectives are to define the scope of testing, establish clear communication channels, delineate responsibilities, and ensure ethical and legal compliance.

1.2 Scope of Testing

All client-owned web applications, domains, subdomains, APIs, and supporting infrastructure components explicitly authorized by the client (hereafter referred to as "in-scope assets") will be tested by CYBMOD. These tests aim to discover vulnerabilities such as those outlined in the OWASP Top Ten, server misconfigurations, and other common security flaws. The extent of testing may include white box, grey box, or black box approaches, depending on the client's requirements, provided such details are clearly agreed upon in writing.

1.3 Out of Scope

Any systems, applications, or services not explicitly stated within the engagement letter or authorized scope are considered out of scope. Testing on third-party services without explicit written consent from their respective owners is forbidden. Denial of Service (DoS) or distributed DoS stress tests will not be performed unless explicitly requested and authorized by the client in recognition of the potential service disruption and associated risks.

1.4 Assumptions and Limitations

It is assumed that the client has obtained all necessary approvals for testing and that systems have adequate backups to mitigate potential data loss. While CYBMOD will follow industry best practices, no penetration test can guarantee the detection of every vulnerability. Testing may inadvertently cause limited or temporary downtime, and the Client accepts this risk by engaging in this assessment.

2 Logistics

2.1 Personnel

Project Managers: Varun Singh and Sarvani Vaddadi
These individuals are responsible for coordinating all project-related activities on behalf of CYBMOD, including scheduling, resource allocation, and adherence to timelines.

Researcher: Sarvani Vaddadi
Sarvani Vaddadi will conduct in-depth research on relevant security methodologies, emerging threats, and best practices to inform CYBMOD's testing approach.

Presenter: Harshvardhan Raval
Harshvardhan Raval will deliver presentations and debriefs, ensuring both high-level summaries and technical details are communicated effectively to the Client.

Technical Writers: Nikita Jadav and Sanaz Dashti
Nikita Jadav and Sanaz Dashti will create and refine all documentation for CYBMOD, including interim updates and final reports, ensuring clarity and thoroughness in all written deliverables.

Course Coordinator: Shikhant Saini
Shikhant Saini will coordinate any educational and training-related activities associated with the project. This may include workshops or security awareness sessions delivered by CYBMOD.

Technical Leads: Harshvardhan Raval and Shikhant Saini
Harshvardhan Raval and Shikhant Saini will offer technical oversight throughout the engagement, validating findings and ensuring alignment with best practices under CYBMOD's methodology.

Client Contact: Bipun Thapa, CEO
Bipun Thapa is the primary contact and decision-maker for the Client. He will approve or amend the scope, oversee final acceptance of deliverables, and address high-level escalations.

2.2 Test Schedule and Sites

The project managers (Varun Singh and Sarvani Vaddadi) from CYBMOD will finalize and share a detailed test schedule with the client, outlining each phase—from reconnaissance to post-testing debriefs. Depending on organizational needs and potential operational impacts, certain testing phases may take place after business hours or during maintenance windows. If on-site assessments are required for internal networks or physical security tests, CYBMOD will coordinate logistics and ensure necessary access permissions are in place.

2.3 Testing Tools and Equipment

CYBMOD will utilize industry-standard tools such as Nmap, Nikto, OWASP ZAP, SQLMap, Burp Suite, and Metasploit. All hardware used for testing will be securely configured. If the client provides specialized credentials, tokens, or equipment, these items will be documented and managed securely throughout the engagement. CYBMOD follows strict operational security measures to protect both Client data and the integrity of the testing process.

3 Communication Strategy

3.1 General Communication

The primary mode of communication will be secure channels (e.g., encrypted email, VPN-based messaging) established by CYBMOD. Daily or weekly progress updates may be

provided by the project managers, depending on the engagement's complexity. Any significant findings will be communicated to the client as soon as they are verified by CYBMOD's team.

3.2 Client Contact Details

For technical and logistical matters, direct communication will occur between the Project Managers (Varun Singh, Sarvani Vaddadi) and the client's designated technical counterparts. High-level or strategic decisions will be escalated to Bipun Thapa. If emergency support is needed (such as a critical vulnerability requiring immediate attention), the project managers will contact Bipun Thapa or any other emergency contact the client designates.

3.3 Incident Handling and Response

Critical vulnerabilities discovered by CYBMOD during testing will be reported immediately. The client and CYBMOD's Technical Leads will collaborate to decide on immediate measures such as isolating affected systems or deploying patches. Detailed logs will be maintained to document the nature of the incident, the steps taken for mitigation, and any potential follow-up actions.

4 Sensitive Data Handling

4.1 Data Collection, Storage, and Transmission

All data gathered by CYBMOD during testing—such as credentials, vulnerability scans, or network details—will be encrypted at rest and in transit. Access to this data is restricted to authorized CYBMOD personnel involved in the engagement. The Technical Leads will oversee its secure storage and ensure minimal exposure to third parties.

4.2 Data Minimization and Retention

CYBMOD will collect only the data necessary to confirm vulnerabilities and assess their impact. Upon conclusion of the engagement and delivery of the final report, this data will be either destroyed or returned to the Client based on the agreed-upon retention schedule (commonly 30–60 days).

4.3 Employee and Customer Data Testing Logistics

When testing functions involving personal or sensitive data, CYBMOD will endeavor to avoid collecting more information than is essential. If demonstrating data leakage requires evidence, only the minimal sample necessary to confirm the risk will be taken. Should live customer or employee data be used, appropriate safeguards will be deployed to ensure compliance with relevant regulations.

5 Testing Execution

5.1 Nontechnical Test Components

Should the Client opt in, CYBMOD may incorporate social engineering techniques (such as phishing or phone-based intrusion attempts) to evaluate personnel security awareness. Additionally, CYBMOD can perform a review of the Client's security policies, training programs, and incident response procedures, with assistance from the Course Coordinator if required.

5.2 Technical Test Components

CYBMOD will use automated scanning tools and manual techniques to identify vulnerabilities within the authorized scope. Exploitation attempts will be cautiously performed to verify identified weaknesses without causing undue disruption. The Client will be notified in advance of high-risk exploits that may affect system stability, allowing the Client to make informed decisions on how to proceed.

6 Legal and Ethical Considerations

All testing activities undertaken by CYBMOD will comply with relevant laws, regulations, and industry standards. Written authorization from the Client is required before any testing begins. Findings are protected under a nondisclosure agreement (NDA), and CYBMOD adheres to a strict professional code of ethics, limiting all actions to those explicitly authorized within this ROE or any mutually agreed-upon amendments.

7 Reporting

7.1 Final Report

Upon completion, CYBMOD's Technical Writers (Nikita Jadav and Sanaz Dashti) will compile a comprehensive final report. This will include: An executive summary highlighting key risks and recommendations. Detailed technical analysis of discovered vulnerabilities, mapped to CVSS or CWE categories. Remediation or mitigation strategies tailored to the Client's environment. An overview of the testing tools and methodologies used by CYBMOD. The Presenter (Harshvardhan Raval) will deliver a formal presentation to the Client, ensuring a thorough understanding of the results and the proposed remediation steps.

7.2 Post-Engagement Deliverables

Within an agreed timeframe following the engagement, CYBMOD may provide additional services such as re-testing of critical vulnerabilities, consulting on patch strategies, or facilitating security training. If compliance-related or proof-of-testing documentation is required (for audits or regulatory bodies), CYBMOD will furnish these as part of the final deliverables or upon separate request.

8 Engagement Terms & Conditions

Payment Terms: The Client agrees to the financial arrangements outlined in the contract with CYBMOD, covering the scope of work, additional services, and any change requests.

Liability Limitations: Both CYBMOD and the Client acknowledge that penetration testing carries some inherent risk of service disruption. CYBMOD's liability is limited as stated in the contract and any associated legal agreements.

Termination Clause: Either party may terminate the agreement under conditions specified in the master services contract or if there is a material breach of these terms.

Governing Law and Dispute Resolution: Any disputes arising from this engagement will be addressed under the jurisdiction and legal framework designated in the signed agreement between CYBMOD and the Client.

By accepting and signing this document, both CYBMOD and the Client confirm their understanding and agreement to all points detailed herein. Amendments must be documented in writing and signed by authorized representatives from both parties to ensure continued clarity and mutual consent.