Executive Summary Validation Report
Neptune Mutual Application
for

CYRAAC Services Private Limited
(The Pavilion, #175 & 176, 5th Floor, Bannerghatta Main Road, Dollars Colony, Phase 4, J. P. Nagar, Bengaluru – 560076)

Application Vulnerability Assessment and Penetration Testing

Report Created By	Report Created For
CyRAAC Services Private Limited [CyRAACS]	Chain Commit Limited

---

Confidential Information

The following report contains company confidential information. Do not distribute, email, fax, or transfer via any electronic mechanism unless it has been approved by the recipient company's security policy. All copies and backups of this document should be saved on protected storage always. Do not share any of the information contained within this report with anyone unless they are authorized to view the information. The specific IP addresses / Domain were identified by Client. Our subsequent test work, study of issues in detail and developing action plans are directed towards the issues identified. Consequently, this report may not necessarily comment on all the weaknesses perceived as important by the Client and / or Client management.

Table of Contents

1. Introduction

About Engagement

Engagement Start Date	07-Oct-22
Engagement End Date/ Report release date	15-Oct-22
Engagement Start Date (Validation Assessment)	30-Oct-22
Engagement End Date/ Report release date (Validation Assessment)	03-Nov-22
Location	Bangalore

2. Engagement Scope

The project scope covered Vulnerability Assessment and Penetration Testing for the Web Application of **Chain Commit Limited.** The vulnerability information details after the validation round of application security testing for **Neptune Mutual** is as given below:

2.1 Component Details

Application Name/URL	https://test.neptunemutual.com/
Type of Testing	Grey Box
Testing approach	External
Reference/Standards	OWASP Top 10 and other web application vulnerabilities

2.2 Vulnerability Information

Issues	**Vulnerability Information – Initial Assessment**				
	Critical	**High**	**Medium**	**Low**	**Total**
Total	0	0	1	0	1

Issues	**Vulnerability Information – Validation Assessment**				
	Critical	**High**	**Medium**	**Low**	**Total**
Total	0	0	0	0	0

3. Report Analysis

The issues identified and proposed action plans in this report are based on testing conducted by CyRAACS VAPT team. CyRAACS has made specific efforts to verify the accuracy and authenticity of the information gathered only in those cases where it was felt necessary.

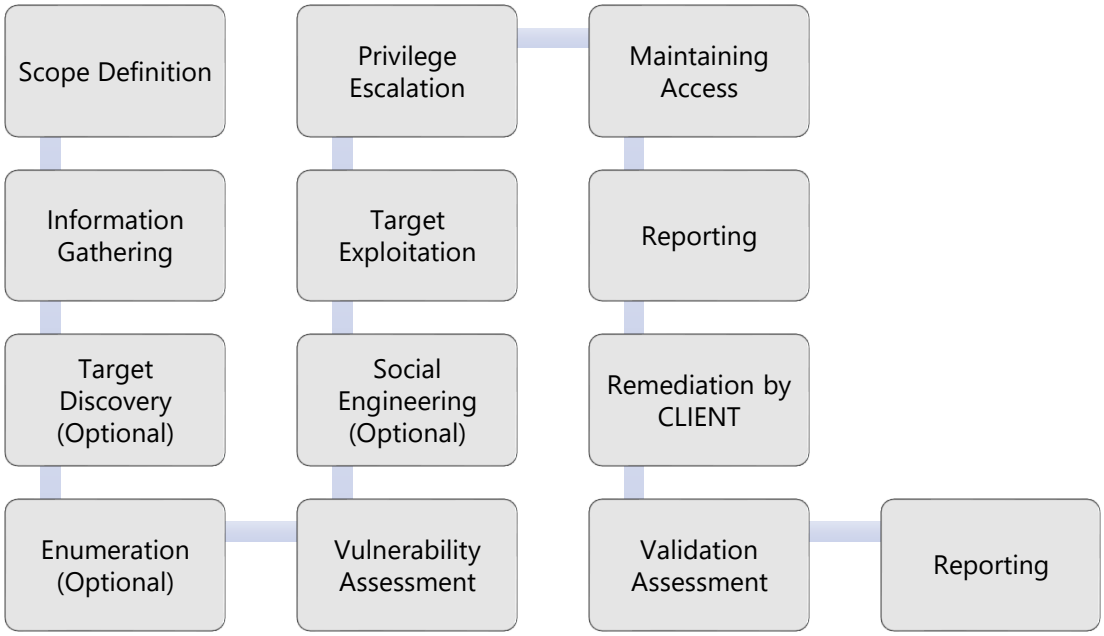
The identification of the issues in the report is primarily based on the tests carried out during the limited time for conducting such an exercise. The vulnerabilities reported in this report are valid as of Date **03-Nov-2022.** Any vulnerability, which may have been discovered after this or any exploit, been made available after the above stated date, does not come under the purview of this report.

Any configuration changes or software/hardware updates made on hosts/machines on the application covered in this test after the date mentioned herein may impact the security posture either positively or negatively and hence invalidates the claims & observations in this report. Whenever there is an update on the application, we recommend that you conduct penetration test to ensure that your security posture is compliant with your security policies.

CyRAACS has identified **NO** Vulnerabilities in **Neptune Mutual** during Validation Assessment.

4. Methodology

The entire assessment was done in phases. The Web Application under test was analyzed for security lapses. The steps depicted below gives us a broad idea on the methodology, the flow chart below gives us a clear flow of how the assessment was conducted.



- Discovery [Scope definition, Information gathering (Optional), target discovery (Optional)]
- Assessment (Enumeration, Vulnerability Assessment)
- Exploitation (Target Exploitation, Privilege Escalation, Maintaining Access)
- Results analysis (Reporting)
- Validation Assessment

Phase 1: Discovery

The first step relates to information gathering, which is comprised of profiling the target as per:

1. Information gathering – Gathering the required pre-requisite details to initiate the assessment on the application(s) under scope.
2. Testing environment setup – Provision of test accounts and sample data for application(s) under scope.
3. Threat modelling for the application under scope – Assessing the application from a Black hat's perspective to list the possible threats inside the application considering the functionalities and access roles provided within the application(s) under scope.

Phase 2: Assessment

Assessing the application by performing automated scans and manually testing the application as per the test cases mentioned in section 8. Removal of false positive(s) if any.

- **Tools used for Assessment:** Burp Suite Professional, OWASP scanners, Nmap, Nessus.

Phase 3: Exploitation

Using least privileges to leverage greater access rights. The vulnerabilities identified in phase 2 are further exploited to check the extent and coverage of each vulnerability throughout the application.

Phase 4: Result Analysis (Reporting)

On completion, reports (Executive Summary and Technical report) detailing the activities performed, list of security loopholes, and recommendations (were possible) is sent to the business owners.

Phase 5: Validation Assessment

Post remediation of the vulnerabilities identified during the initial round of testing, the second round of assessment is conducted for the application(s) under the scope to confirm and validate the remediated vulnerabilities.

5. Key Observations

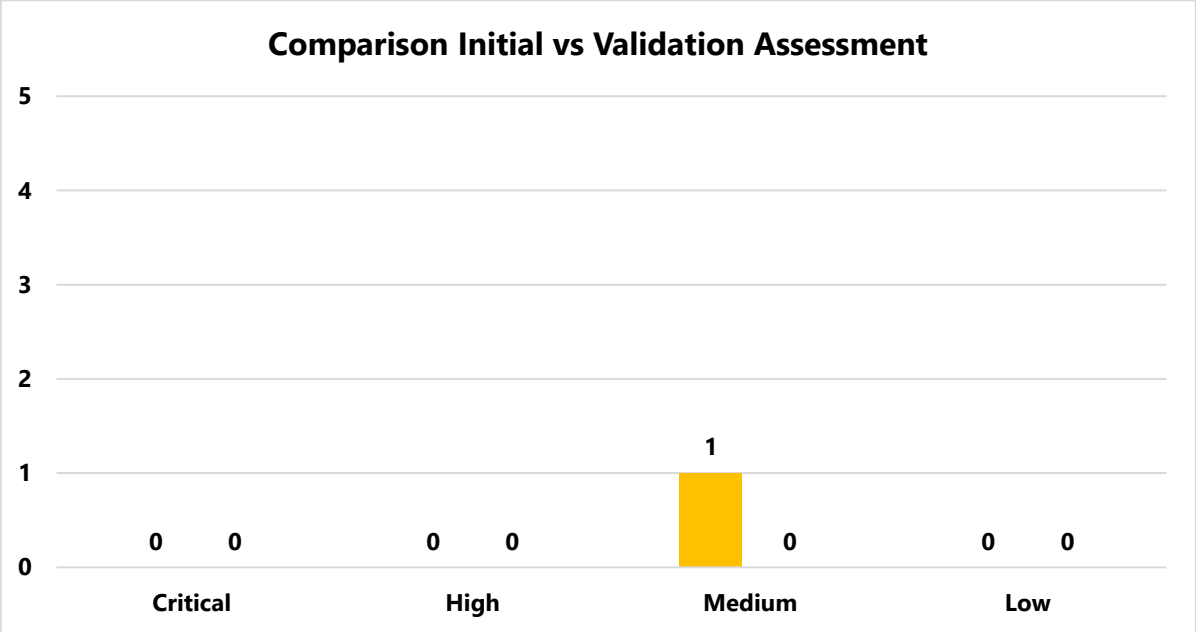
No CRITICAL or HIGH Vulnerabilities were identified during the Validation Assessment.

6. Vulnerability Information

No CRITICAL or HIGH Vulnerabilities were identified during the Validation Assessment.

7. Vulnerability Information

7.1 Graphical Representation



Vulnerability count by Risk Severity

7.2 Table of Vulnerability

The below table details the various severities of vulnerabilities identified as an outcome of the engagement.

Vulnerabilities Summary at Glance – Initial Assessment

Medium Severity Vulnerabilities (1)

Vulnerability	Vulnerable URL(s)
Insecure Direct Object Reference	https://api2.neptunemutual.com/subgraph/fuji

Vulnerabilities Summary at Glance – Validation Assessment

No issues were identified

8. Test Cases (OWASP Top 10)

Test Scenarios	Result
Broken Access Control	Passed
Cryptographic Failures	Passed
Injection	Passed
Insecure Design	Passed
Security Misconfiguration	Passed
Vulnerable and Outdated Components	Passed
Identification and Authentication Failures	Passed
Software and Data Integrity Failures	Passed
Security Logging and Monitoring Failures	Passed
Server-Side Request Forgery	Passed

Business Use Cases Provided:

Vulnerability Name	Business Use Case
Insecure Direct Object Reference	In Blockchain application, sensitive information such as transaction id, account address are transparent in nature. In this case, if attacker has user's account address, they can view all the user transactions on public blockchain explorers.

Disclaimer:

The testing is conducted based on applicable OWASP standards and industry best practices. As the discovery and identification of vulnerabilities are dynamic in nature, hence they represent a point in time scenario which can vary based on the information provided during the testing period. Hence any vulnerability which may not have been discovered due to non-availability of complete and accurate information / data may be treated as scope exclusion.