Penetration Testing 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
CyRAAC Services Private Limited [CyRAACS]

Report Created For
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

Details of Vulnerabilities

INFORMATIONAL

1. Slowloris DOS Vulnerable

Summary:
It was observed that the application is vulnerable to Slowloris which affects the target web server only, with almost no side effects on other services and ports.

Risk:
Slowloris attack which is DDoS attack software that enables a single computer to take down a web server.

Impact:
With minimum bandwidth requirement, it aims to use up server resources with requests that seem slower than normal but otherwise mimic regular traffic.

Reference:
OWASP: A5 - Security Misconfiguration
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
https://owasp.org/www-pdf-archive/Owasp_KS_slowDoS.pdf

Advisory:
https://cwe.mitre.org/data/definitions/400.html

POC(s):

From the screenshot below, it can be observed that the application is vulnerable to Slowloris DOS attack.

Remediation:

Increase server availability - Increasing the maximum number of clients the server will allow at any one time will increase the number of connections the attacker must make before they can overload the server. Realistically, an attacker may scale the number of attacks to overcome server capacity regardless of increases. Rate limit incoming requests - Restricting access based on certain usage factors will help mitigate a Slowloris attack. Techniques such as limiting the maximum number of connections a single IP address is allowed to make, restricting slow transfer speeds, and limiting the maximum time a client is allowed to stay connected are all approaches for limiting the effectiveness of low and slow attacks.

Vulnerable URL(s):

https://test.neptunemutual.com/