NOPALCYBER

LeAh

NopalCyber Reassessment of Dynamic Application Security Testing of Leah Copilot

For CPAI

Report – Version 1.0

Thursday 5th Dec 2024

1 Contents

2 Executive Summary

Based on CPAI's ask to revalidate/reassess the findings that were discovered during the last application security assessment/DAST, NopalCyber has performed a re-assessment on https://pentest-sandbox.leahcopilot.com/ to detect additional security vulnerabilities and revalidate the ones that were submitted earlier.

This report presents the results and findings of Graybox Dynamic web application security reassessment conducted on **Leah copilot** application of "ContractPodAi." This reassessment, performed by NopalCyber, aimed to identify vulnerabilities and other security issues that might impact **Leah copilot** application. The security reassessment was carried out from the NopalCyber office. Its purpose was to provide ContractPodAi with an understanding of the risks and security posture of **Leah's copilot**. The findings in this report are a snapshot of the conditions found during testing and should be considered for immediate action.

2.1 Scope

Target URL
https://pentest-sandbox.leahcopilot.com/

2.2 Key Findings

There are no Application Security Vulnerabilities/Findings reported as a part of our reassessment (DAST/VAPT) for https://pentest-sandbox.leahcopilot.com/. All the reported findings were fixed by the CPAI team.

3 Dashboard

Target Data		Engagement Data	
Name	CPAI	Type	Reassessment DAST
Type	Graybox DAST	Methods	Automated & Manual
Platforms	Application	Dates	12/05/2025

External VAPT findings				
Critical	High	Medium	Low	Informational
0	0	0	0	0

4 Methodology

NopalCyber conducted a reassessment to test the security controls of the system, network, and applications. The goal was to gain unauthorized access to sensitive data. Operated within defined parameters, including time constraints, and attempted to identify and exploit vulnerabilities. It's important to note that the test may not have uncovered all vulnerabilities, but it was designed to evaluate the network's resilience to determined attackers. The simulation was meant to help ContractPodAi understand its current controls and how they could be bypassed during a real attack. It's important to emphasize that this was not a stealth

penetration attempt, and the noise generated during the reassessment is not representative of typical attacks.

The test process itself can be broken into three major phases:

- Reconnaissance (Information Gathering)
- Vulnerability Identification
- Vulnerability Exploitation

Reconnaissance

Reconnaissance begins with using internet search engines to gather information about the organization. Then, public websites, registries, and authoritative bodies are consulted to gather specific information. The Domain Name System (DNS) and DNS servers of the organization are examined for configuration concerns. Techniques such as port scanning, fingerprinting, and network mapping are used to create a profile of the system and network. Finally, a comprehensive target list is compiled using all the information gathered during this phase.

Vulnerability Identification

During the test, each host and its associated listening services are individually and collectively examined to identify potential vulnerabilities. Our team of offensive security experts use extensive knowledge of exploit techniques, public information, and the findings of private vulnerability research to catalogue all possible attack vectors.

Vulnerability Exploitation

All vulnerabilities are manually investigated and researched to attempt exploitation. NopalCyber seeks to gain unauthorized access to the target system or extract sensitive data when exploiting vulnerabilities. An exploit is considered successful if NopalCyber achieves either of these objectives.

5 Finding Field Definitions

The following sections describe the risk rating and category assigned to issues NopalCyber identified.

Risk Scale

NopalCyber uses a composite risk score that takes into account the severity of the risk, the application's exposure and user population, the technical difficulty of exploitation, and other factors. The risk rating is NopalCyber's recommended prioritization for addressing findings. Every organization has a different risk sensitivity, so to some extent, these Recommendations are more relative than absolute guidelines.

Overall Risk

Overall risk reflects NopalCyber's estimation of the risk that a finding poses to the target system(s). It takes into account the impact of the finding, the difficulty of exploitation, and any other relevant factors.

Risk	Description
Critical	Implies an immediate, easily accessible threat of total compromise.
High	Implies an immediate threat of system compromise, or an easily accessible threat of large-scale breach.
Medium	A difficult-to-exploit threat of large-scale breach or easy compromise of a small portion of the application.
Low	Implies a relatively minor threat to the application.
Informational	There is no immediate threat to the application. May provide suggestions for application improvement, functional issues with the application, or conditions that could later lead to an exploitable finding.

Impact

Impact reflects successful exploitation's effects upon the target system or systems. It considers potential

losses of confidentiality, integrity, and availability, as well as potential reputational losses.

Rating	Description
High	Attackers can read or modify all data in a system, execute arbitrary code on the system or escalate their privileges to the superuser level.
Medium	Attackers can read or modify some unauthorized data on a system, deny access to that system, or gain significant internal technical information.
Low	Attackers can gain small amounts of unauthorized information or slightly degrade system performance. It may have a negative public perception of security.

Exploitability

Exploitability reflects the ease with which attackers may exploit a finding. It considers the level of access required, availability of exploitation information, requirements relating to social engineering, race conditions, brute forcing, etc., and other impediments to exploitation.

Rating	Description
High	Attackers can unilaterally exploit the finding without special permissions or significant roadblocks.
Medium	Attackers would need to leverage a third party, gain non-public information, exploit a race condition, already have privileged access, or otherwise overcome moderate hurdles to exploit the finding.

Low	Exploitation requires implausible social engineering, a difficult race condition, guessing difficult-to-guess data, or is otherwise unlikely.

Category

NopalCyber categories findings based on the security area to which they belong. This will help ContractPodAi to identify gaps in secure development, development, patching, etc.

Category Name	Description
Access Control	Related to authorization of users and assessment of rights
Auditing and logging	Related to auditing of actions or logging of problems.
Authentication	Related to the identification of users
Configuration	Related to the security configuration of servers, devices, or software
Cryptography	Related to mathematical protections for data.
Data Exposure	Related to unintended exposure of sensitive information.
Data Validation	Related to improper reliance on the structure or values of data.
Denial of Service	Related to causing system failure.
Error Reporting	Related to the reporting of error conditions in a secure fashion.
Patching	Related to keeping software up to date.
Session Management	Related to the identification of authenticated users.
Timing	Related to race conditions, locking, or order of operations.

<<< End of Report>>