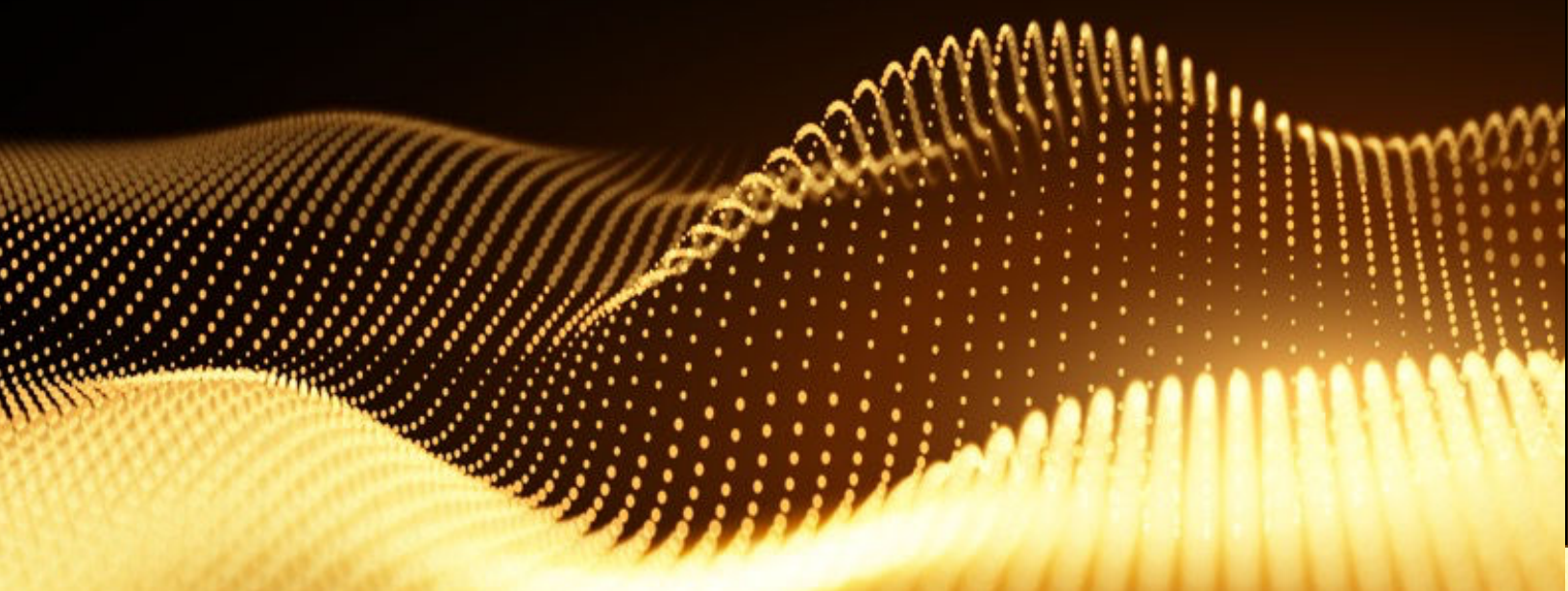
NOPALCYBER

ContractPodAi

NopalCyber Dynamic Application Security Testing/Vulnerability Assessment and Penetration Testing

Reassessment on CPAI's Clouduat2



Contents

1. Executive Summary

1.1 Synopsis

Based on CPAI's ask to revalidate/reassess the findings that were discovered during the last application security assessment/VAPT, NopalCyber has performed a re-assessment on https://clouduat2.contractpod.com to detect additional security vulnerabilities and revalidate the ones that were submitted earlier.

This report presents the results and findings of the proactive web application security assessment conducted on the cloud UAT application addresses of CPAI. This assessment, performed by NopalCyber, aimed to identify vulnerabilities and other security issues that might impact CPAI's cloud UAT application. The security assessment was carried out from NopalCyber's offices. Its purpose was to provide CPAI with an understanding of the risks and security posture of the cloud UAT application. The findings in this report are a snapshot of the conditions found during testing and should be considered for immediate action.

1.2 Scope

Target URL
https://clouduat2.contractpod.com

1.3 Key Findings

There are no Infra/Application Security Vulnerabilities/Findings reported as a part of our reassessment (DAST/VAPT) for https://clouduat2.contractpod.com. All the reported findings were fixed by CPAI team.

2 Dashboard

Target Data		Engagement Data	
Name	CPAI	Type	Reassessment AppSec VAPT
Type	Web Application	Methods	Automated & Manual
Platforms	URL	Dates	15 Days 7/3/2024 – 7/18/2024
Environment	Application security testing	Consultants	4

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

2.1 Methodology

NopalCyber's primary goal in conducting the assessment was to circumvent application security controls and then gain access to the systems and designated data an unauthorized user should not be able to obtain. Working within the defined parameters of the test, including time constraints, NopalCyber attempted to identify and exploit whatever application vulnerabilities were necessary to achieve the above-stated goals. In performing the test, NopalCyber may not have located and detailed all vulnerabilities inherent in the environment; rather, the testing was meant to ascertain the resiliency of the application to a determined attacker. Thus, the concentrated attack simulation was structured in such a way as to enable CPAI to accurately understand its current controls and how they could be circumvented during an actual attack. No attempts were made to disguise attacks, as this was not a stealth penetration attempt. It should be noted that actual attacks might not be as evident to system administrators. The noise generated by this engagement is not typical and should not be used as a comparison to judge actual penetration attempts by malicious individuals.

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

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

2.1.1 Reconnaissance

Reconnaissance starts with Internet search engines and information gathering about the organization. Next, public websites for information look-up and data mining, as well as public registries and authoritative bodies, are consulted, and specific

information is gathered and cataloged. Forceful interrogation of organizational Domain Name System (DNS) and DNS servers are probed for configuration concerns. Port scanning, fingerprinting, and network mapping techniques are utilized to build a system and network profile, and a complete target list is compiled from all the information gathered during the phase.

2.1.2 Vulnerability Identification

Each host and all associated listening services targeted for the test are probed singularly and in tandem with the other hosts to locate potential vulnerabilities. Using a vast working knowledge of exploit techniques, public information, and the results of private vulnerability research, NopalCyber consultants catalog all the possible attack vectors.

2.1.3 Vulnerability Exploitation

All vulnerabilities found are manually investigated and researched, and an attempt is made to exploit them. In exploiting vulnerabilities, NopalCyber has attempted to either gain unauthorized access to the target system or extract sensitive data. An exploit is considered successful if NopalCyber can achieve either of these objectives.

3 Finding Field Definitions

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

3.1.1 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.

3.1.2 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.

Rating	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 forapplication improvement, functional issues with the application, or conditions that could later lead to an exploitable finding.

3.1.3 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.

3.1.4 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.

<<< End of Report>>