Document Details

Title	Application Server(Contact Center) VAPT report.
Description	This document provides detail summary of vulnerabilities identified in the application server
Version	2.0
Author	Suraj Pawar, Soumen Jana, Kush Janani
Classification	Internal
Review Date	Sept 14th 2022
Reviewer	Moosa Meeran
Publish Date	Sept 16th 2022
Owner	Information Security Manager

Rescan

Sr No	Retested By	Date	Reviewed By

Exotel Techcom Pvt. Ltd.

Application Server VAPT Report

1. Introduction

This report document hereby describes the proceedings and results of a Grey Box security assessment conducted against **Application Server Portal**. The report hereby lists the findings and corresponding best practice mitigation actions and recommendations.

2. Objective

The objective of the assessment was to assess the state of security and uncover vulnerabilities in **Application Server Portal** and provide with a final security assessment report comprising vulnerabilities, remediation strategy and recommendation guidelines to help mitigate the identified vulnerabilities and risks during the activity.

3. Scope

This section defines the scope and boundaries of the project.

Application Name	Application Server
URL	https://vapt.ameyo.net:8443/app/
Version	ameyo-server-4.13.454.20221005-R_59437-linux-gtk.x86_64

3.1. Assessment Attribute(s)

Parameter	Value
Starting Vector	External
Target Criticality	Critical
Assessment Nature	Cautious & Calculated
Assessment Conspicuity	Clear
Proof of Concept(s)	Attached wherever possible and applicable.
Penetration Tester	Kush Janani, Soumen Jana, Suraj Pawar
Date	13-09-22
Version	2.0
Pentesting Duration	8 hours

3.2. Risk Calculation and Classification

Following is the risk classification:

Info	Low	Medium	High	Critical
No direct threat to host/ individual user accounts. Sensitive information can be revealed to the adversary.	Vulnerabilities may not have public exploit (code) available or cannot be exploited in the wild. Vulnerability observed may not have a high rate of occurrence. Patch workaround released by vendor.	Vulnerabilities may not have public exploit (code) available or cannot be exploited in the wild. Patch/ workaround not yet released by vendor.	Vulnerabilities which can be exploited publicly, workaround or fix/ patch available by vendor.	Vulnerabilities which can be exploited publicly, workaround or fix/ patch may not be available by vendor.

Table 1: Risk Rating

Summary

Outlined it is a Grey Box Application Security assessment for **Application Server Portal**.

https://vapt.ameyo.net:8443/app/

Following section illustrates **Detailed** Technical information about identified vulnerabilities.

Total: 13 Vulnerabilities

Round 1

High	Medium	Low	Exception	Total

0	4	9	0	13

3.3. Vulnerability Table

Sr. No	Vulnerability Name	Severity	CVSS	Status	InfoSec Comments
1	Sensitive Data Exposure	Low	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	OPEN	
2	Content Security Policy (CSP not set properly)	Low	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	OPEN	
3	Using Components with known Vulnerabilities	Medium	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	OPEN	
4	Weak Password Complexity	Low	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	OPEN	
5	Broken Access Control on Download Recordings	Medium	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	OPEN	
6	Weak SSL Ciphers	Medium	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	OPEN	
7	OCSP Stapling not enabled	Low	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	OPEN	
8	Strict transport security not enforced	Low	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	OPEN	
9	LUCKY13	Low	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	OPEN	

10	Vulnerable to Breach Attack	Low	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	OPEN	
11	Captcha Bypass	Low	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	OPEN	
12	Account Blocked Temporarily	Low	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	OPEN	
13	Cross site scripting(XSS)	Medium	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	OPEN	