

YOUR LOGO

# SECURITY AUDIT REPORT FOR MY BUSINESS

Testing Date(s): Jan 23, 2024 to Jan 31, 2024

Report Date: Jan 31, 2024

CLIENT  
LOGO

ATTENTION: This document contains information from SecurityScan. Ltd. that is confidential and privileged. The information is intended for private use of the client. By accepting this document you agree to keep the contents in confidence and not copy, disclose, or distribute this without written request to and written confirmation from SecurityScan. If you are not the intended recipient, be aware that any disclosure, copying, or distribution of the contents of this document is prohibited. August, 10 , 2024

## Document Information

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into

Title	Details
COMPLETED ON:	August 11, 2024
REPORT TYPE:	MANUAL SCAN
VALIDITY:	30 DAYS

## Document History

Contrary to popular belief, Lorem Ipsum is not simply random text. It has roots in a piece of classical Latin literature from 45 BC, making it over 2000 years old.

Richard McClintock, a Latin professor at Hampden-Sydney College in Virginia, looked up one of the more obscure Latin words, consectetur, from a Lorem Ipsum passage, and going through the cites of the word in classical literature, discovered the undoubtable source.

Lorem Ipsum comes from sections 1.10.32 and 1.10.33 of "de Finibus Bonorum et Malorum" (The Extremes of Good and Evil) by Cicero, written in 45 BC.

This book is a treatise on the theory of ethics, very popular during the Renaissance. The first line of Lorem Ipsum, "Lorem ipsum dolor sit amet..", comes from a line in section 1.10.32.

The standard chunk of Lorem Ipsum used since the 1500s is reproduced below for those interested. Sections 1.10.32 and 1.10.33 from "de Finibus Bonorum et Malorum" by Cicero are also reproduced in their exact original form, accompanied by English versions from the 1914 translation by H. Rackham.

Title	Details	Details	Title	Details	Details
COMPLETED ON:	August 11, 2024	August 11, 2024	COMPLETED ON:	August 11, 2024	August 11, 2024
REPORT TYPE:	MANUAL SCAN	MANUAL SCAN	REPORT TYPE:	MANUAL SCAN	MANUAL SCAN
VALIDITY:	30 DAYS	30 DAYS	VALIDITY:	30 DAYS	30 DAYS

# Table of Content

1. Executive Summary
1.1 Scope of Testing
1.2 Graphical Summary
1.3 List of Vulnerabilities

2. Discovered Vulnerabilities Details
2.1 xyz
2.2 xyz

3. List of Tests Performed
3.1 OWASP Top 10
3.2 SANS 25 Software Errors/Tests
3.3 Other Test Cases
3.4 Server-Level Test Cases
3.5 Test Cases for Windows
3.6 Test Cases for Android / iOS
3.7 Test Cases for Cloud (AWS, Azure, GCP, and Other)
3.8 Test Cases for Blockchain

# 1. Executive Summary

Third party Vulnerability assessment and Penetration testing are indispensable tools when used in conjunction with a vulnerability management program. They help identify vulnerabilities and misconfigurations of websites, applications, and information technology infrastructures with Internet-facing Internet Protocol (IP) addresses.

It is a best practice to perform third party Security testing at least annually or whenever there is a major change in the Client's IT infra and/or application scope.

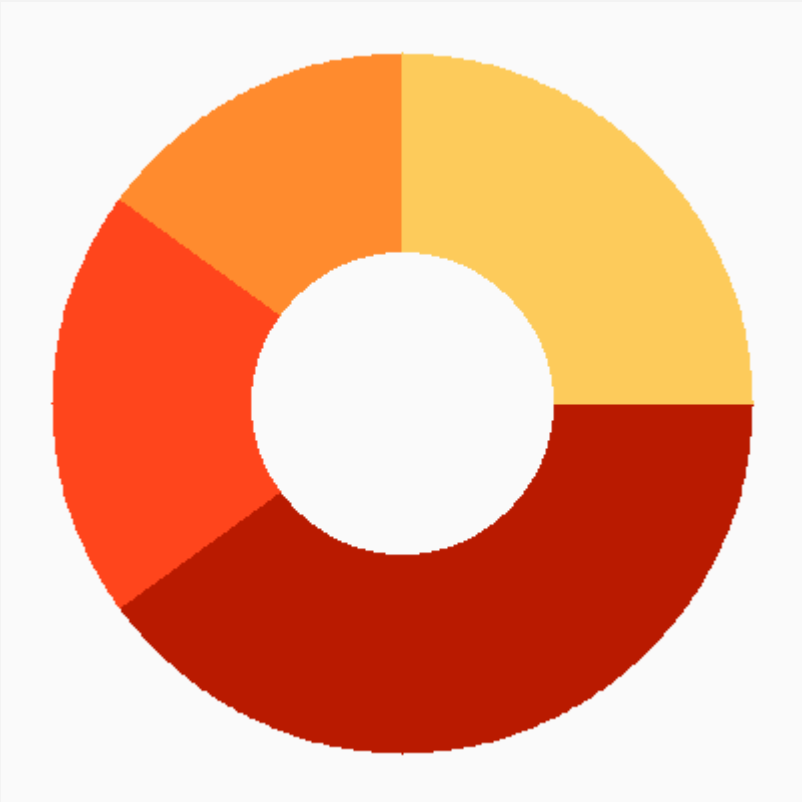
## Scope of Testing

The following was the scope covered under the security audit:

- Application 1: (URL 1)
- Application 2: (URL 2)
- Confidential 3

## Testing Dates

The Testing activities were performed between **28th April 2023 and 19th May 2023**.



## Graphical Summary

The below graphical representations from Astra's VAPT dashboard will provide you an overall summary of the security audit scan results, including:

- Vulnerabilities discovered
- Severity
- Respective CVSS Score
- Other vulnerability details such as its impact, detailed PoC, steps to reproduce, affected URLs/network parameters, and recommended fixes

## Issues Type

## Table Summary

#	Vulnerability	Severity	CVSS	Score	Status
1	SQL Injection	High	7.8	Critical	Open
2	Cross-Site Scripting	Medium	6.4	High	Closed
3	Buffer Overflow	Critical	9.0	Critical	In Progress
4	Broken Authentication	High	7.5	High	Open
5	Insecure Direct Object References	Medium	6.0	Medium	Closed
6	Security Misconfiguration	High	7.3	High	Open
7	Insufficient Logging & Monitoring	Low	5.2	Medium	In Progress

Vulnerability Severity	No. of Vulnerabilities Found
Critical	1
High	3
Medium	2
Low	1
Recommendations	0

## 2. Technical Details Of Vulnerabilities

### 1. Vulnerability

#### Missing API Security Headers

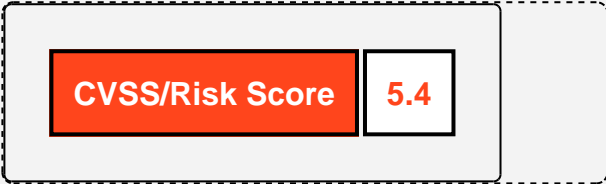
Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book. It has survived not only five centuries, but also the leap into electronic typesetting, remaining essentially unchanged.

Severity	Status
Medium	Unsolved

#### Impact

- Missing Content-Type header means that this website could be at risk of MIME-sniffing attacks.
- Missing Strict Transport Security header means that the application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption and use the application as a platform for attacks against its users.

#### Score



#### Affected URL:

Sitewide

#### Details of Vulnerability:

We were able to detect that the following API security headers are missing:

- Content Security Policy
- Strict Transport Security
- X-Content-Type-Options

A Content Security Policy (CSP) is an important standard by the W3C aimed at preventing a broad range of content injection attacks such as cross-site scripting (XSS), data injection attacks, and passive sniffing attacks. It is a declarative policy that informs the user agent what are valid sources to load resources from.

# Proof of Concept

Image Placeholder

## Suggested Fixes:

The recommended Configuration for API Endpoint is:

In Content-Security-Policy: default-src 'none'; frame-ancestors 'none' \nStrict-Transport-Security: max-age=63072000;\nX-Content-Type-Options: nosniff\n

## Additional References:

<https://www.example.com/reference>

<https://test.com/reference>



# Testing Methodology

We follow the NIST Special Publication 800-115, SANS, and OWASP Top 10 standards. Automated and Manual Testing was conducted using both Burp Suite, Kali Linux, Nmap, Nikto, and OWASP ZAP in addition to home-grown tools/scripts.

- The testing covers various security controls/methods in use.
- The testing verifies that security controls/methods are operational and effective.
- The testing verifies that security controls/methods have protective security measures.

For Vulnerability assessment and Penetration testing, we have adopted the following approach:

- Vulnerability identification using automated and manual techniques.
- Vulnerability identification involved the following:
  - Customized tool policy settings to perform "non-intrusive" and "non-destructive" vulnerability scanning.
  - List of scoped assets, servers IP addresses were configured in the tool.
  - Conducted brute-force testing for the identified vulnerabilities.
  - Identified and removed false positives from the test output.
  - The non-intrusive and non-destructive approaches were followed throughout the testing by using manual methods and safe tools.
  - Produced Proof-of-Concept (PoC) for the identified vulnerabilities.
  - Assigned severity ratings to the identified vulnerabilities.
  - Provided recommendations for fixing the identified vulnerabilities.

Manual Penetration testing of the running system was performed for Data Collection and to launch simulated attacks.

# Risk Levels

Discovering vulnerabilities is important, but being able to estimate the associated risk to the business is just as important. Risk Rating is assessing the risk involved and classifying them based on the impact.

Risk Level	Description
Critical	Very high risk of security controls being compromised with system-wide effect on multiple customers and a high degree of financial or reputational risks.
High	High risk of security controls being compromised with limited effect in individual system components or individual customers that may result in sensitive data access by unauthorized persons.
Medium	Medium risk of security controls being compromised that may cause data loss by unauthorized persons.
Low	Low risk of security controls being compromised that does not affect the system directly but can be used with another vulnerability.
Info	Observations that pose no security risk but potential areas for improvement or useful information for the support employee.

Re-evaluation of Information Security on a regular basis is vital to ensure that the safeguards employed continue to offer the appropriate level of protection.

## List of VAPT Tests

3. List of Tests Performed
3.1 OWASP Top 10
3.2 SANS 25 Software Errors/Tests
3.3 Other Test Cases
3.4 Server-Level Test Cases
3.5 Test Cases for Windows
3.6 Test Cases for Android / iOS
3.7 Test Cases for Cloud (AWS, Azure, GCP, and Other)
3.8 Test Cases for Blockchain

YOUR LOGO

# Efficient Security Assessments

Contact Us