Vulnerability/Penetration Testing Report

For

Endel Pvt Ltd

By

LD Students

|  |  |
| --- | --- |
| **Document Type** | **Penetration Testing Report** |
| **Project Name** | Vulnerability Assessment and Penetration Testing |
| **Document Version** | 1.0 |
| **Testing Date** |  |
| **Report Date** |  |
| **Authored by** |  |
| **Reviewed by** |  |

**DOCUMENT DETAILS**

**Disclaimer:**

This report and any supplements are HIGHLY CONFIDENTIAL and may be protected by one or more legal privileges. It is intended solely for the use of the addressee identified in the report. This report is prepared based on the IT environment that prevailed in the approved period of assessment.

This report is not a guarantee or certification that all vulnerabilities have been discovered and reported in the findings. Subsequent reviews may report on previously unidentified findings or on new vulnerabilities. The samples screen shot should not be treated as the final vulnerabilities. Gaps which we have identified can also get replicated in any part of the Infrastructure. Client should ensure that Vulnerability Management Program should be adapted continuously rather than fixing just the issues identified within the areas which MQAS has highlighted.

Executive Summary

The testing took place over the period from / /. During this period the application was analysed and assessed using a combination of standard tools and utilities and the knowledge and experience of our technical team. Although at the time of this engagement, the application was not in production, we nonetheless stopped short of undertaking specific tests that would either a) evidently risk the integrity and stability of the systems, or b) actively exploit potential vulnerabilities.

Overall we believe that a reasonable level of security has been attained by the applications that were the target of this test, but due to there being a high and some medium and low risk issues, remedial action needs to be carried out prior to official launch of the product. Testing revealed elements that are well-protected against several well-known vulnerabilities.

Overall we believe that a reasonable level of security has been attained by the applications that were the target of this test, but due to there being a high and some medium and low risk issues, remedial action needs to be carried out prior to official launch of the product. Testing revealed elements that are well-protected against several well-known vulnerabilities.

Our penetration Test has identified High, Medium, and low risks

HIGH RISKS

The identified high risk vulnerability/recommendation is:

• BREACH attack

MEDIUM RISKS

The / no of risks / identified medium risk vulnerabilities/recommendations are:

• Application error message

• No anti-virus on file uploads

• TLS1/SSLv3 Renegotiation Vulnerability

LOW RISKS

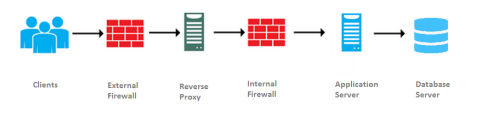
The / no of risks / identified low risk vulnerabilities/recommendations are:

We strongly recommend that Client Company does not disregard the findings encountered in this report. If these vulnerabilities/recommendations are dealt with and fixed, the organisation will find that the defence-in-depth posture of the system will improve substantially. We also recommend that in line with good security practice, Client Company conducts periodic re-testing to ensure that neither intentional nor inadvertent changes have compromised their systems, and that new vulnerabilities have not become a threat to them

System Overview:

DESCRIPTION

IP



Environment :

Goals

Primary goal of this penetration test is to validate that the appropriate security measures have been implemented by Client Company at the various layers of the portal to mitigate malicious activity occurring

Secondary Goals

• To achieve confidence in their customers that their secure information has been proactively tested by a 3rd party, and to attain an executive report stating that all risks have been mitigated.

**DESKTOP Penetration Test Report**

/ about application

/

The application is / / based, which is developed using the .net Framework and runs on Apache/Coyote

Security tools used

● Nmap

● Hydra

/

Other tools name

/