



Client Overview

- An Established Digital Technology Solutions provider primarily into Telecommunications, Media and IoT



Business Requirements

- The application is a simple and effective mobile e-Wallet offering a dynamic platform for both consumers and merchants
- Test the POS Terminal of the application
- Client required to conduct Vulnerability Tests on the mobile application (Android and iOS versions)
- Test the Merchant portal and Admin Portal for Vulnerabilities
- Test Hosting and DB Configurations, API Calls



Our Solutions

- Conducted application vulnerability tests based on OWASP Top 10 Vulnerability List, using tools and Regression
- Tested the locally accessible Mobile App (different OS Versions)
- Tested the POS Terminal installed on a locally accessible mobile android device
- Tested Merchant Portal, Admin Portal
- Validated the API Calls using URLs for known vulnerabilities
- DB Configuration Assessment based on CIS (DB Access Remotely Accessible)
- Host Configuration Assessment based on CIS (Host Access Remotely Accessible)



Tools

- Zap, Burp Suite, Vega and Manual Python Scripts to evaluate SQL injection errors

Engagement

- 1 Test Lead Security Testing
1 Test Engineer Security Testing
30 Day Engagement including First Cycle of VAPT Testing, interim for Defect Fixing and Regression Tests



Business Impact

- Detected 4 vulnerabilities of moderate impact including Broken Authentication and Session Management, Cross Site Request Forgery; Low impact defect on Sensitive Data Exposure in Web Application
- Detected 4 vulnerabilities of moderate impact including Insecure Authentication and Insecure Authorization; Low impact defect on Insecure Data Storage in Mobile Application



INDIA

Chennai | Bengaluru | Mumbai
Toll-free: 1800-123-1191

USA

Cupertino | Princeton
Toll-free: +1-888-207-5969

UK

London

SINGAPORE

+65 9630 7959