indium
Make Technology Work

VAPT: Preventing unapproved access to Premium Features

QA Services

Success Story

www.indiumsoftware.com

Status Quo

The client is a software provider offering solutions for E-reading, Information Consumptions and Document visualization. The solution is a productivity application creating digital PDF experiences, making it easy to connect facts across sources and preserve context. The app works on iPad, allows working with multiple documents at a time, and finds best use cases for users in Law, analyzing technical documents, contracts, RFPs etc.

The application is free to download and provides premium features in paid model. The major case for QA here is users trying to exploit the premium walls of the application and gain access to advanced features. The platform required to go through a vulnerability assessment to identify the weak links in premium access. The premium users need to hold their privileges without sharing the key / license to unauthorized users.

Business Requirements

- Identify and report all the security loopholes for a user/hacker to find access to premium account features.
- Verify the vulnerabilities of reverse engineering/ decompiling the app code that may lead to taking advantage of unauthorized features.
- 360-degree security tests (VAPT), report defects and impending business impact.

Solutions

- Implemented an optimized QA strategy that uses automated assessment (using open-source tools) and manual methods (as a Hacker) to penetrate and identify defects.
- Vulnerability assessments on thick client for Enterprise and Consumer versions of the platform.
- Static Analysis to identify interesting files, performed injection attacks, reverse engineering attacks (license key forgery attacks, memory analysis and binary analysis).

  o Verified windows search and load algorithm exploits that might lead to tampering the code of application.

  o Validated hardcoded sensitive credentials / data, keys, comments, and hidden functions.
- Dynamic Analysis

  o Performed Man-in-Middle Attacks using manual enumeration method

  o Analysed API calls (request & response)
- Manual enumeration for identification of defects and used CLI tools.
- Identified two critical vulnerabilities under the category of Sensitive Data Exposure and Insecure Communication.
- Highlights of recommended defect fixes

  o API to use more secure Http methods and transport level encryptions to secure communication

  o Configurations of server address, handling of API/App error responses by removing sensitive information

Domain

IT Services, Productivity App

Tools

Wireshark, Burpsuite, Postman, CFF Explorer, Process Monitor Filter, Immunity Debugger, Kali Linux-Command/Shell interface tools, VM

Services

Security Testing

Key Highlights

- Reported security loopholes in exploiting access to premium account features underlining the test coverage standards of OWASP
- Static and dynamic analysis of vulnerabilities; manual enumeration of security gaps.
- Detailed reports of the defects with affected URLs, Screenshots and Logs, and remediation methods.

Business Impact

- QA approach underlined with OWASP Top 10 and SANS 25/CWE Security Standards to ensure complete coverage of scenarios.
- Defined processes led to extensive coverage, inclusive QA methods like false positive analysis, binary analysis etc.
- Potential vertical privilege escalation methods were covered preventing recreation of malicious versions.
- Identified critical vulnerabilities and informed the development/product team of the security risks and corrective measures. The reported defects are fixed and closed with zero loopholes.
- The app reveals stable revenue over three quarters from the QA and zero reviews on the store regarding security issues.
- Reproduced and provided detailed reports of the defects with aspects of affected URLs, Screenshots and Logs, and remediation methods provided by SME at Indium.

INDIA

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

USA

Cupertino | Princeton
Toll-free: 1 888 207 5969

UK

London

SINGAPORE

+65 9630 7959

General Inquiries
info@indiumsoftware.com

Sales Inquiries
sales@indiumsoftware.com