

Remediation and Fixes for vulnerabilities based on VAPT reports



About client

Our client is a leading non-banking financial institution (NBFC) that utilizes a mobile application for its agents.

This application is critical for day-to-day operations, enabling agents to manage collections and report data in real-time.





Client challenges

The client proactively wanted to avoid challenges in safeguarding sensitive financial information and ensuring compliance for their mobile application. Hence they went through regular third-party Vulnerability Assessment and Penetration Testing (VAPT) which threw up a significant number of vulnerabilities. The client found it challenging to fix all of them considering the varied technologies used for the application. Subsequently, Qruize was tasked with addressing and resolving the vulnerabilities identified in the VAPT report.

Qruize Solution


The initial step in addressing vulnerabilities are to analyze and segregate the VAPT report. Qruize assembled a skilled development team to come up with solutions for the segregated vulnerabilities. A detailed plan was drawn up by combining similar fixes and identifying the responsible client teams for easy collaboration. This strategic planning minimized the interaction time for testing or deploying various solutions, thereby saving significant cycle time. The team's efficient communication facilitated swift decision-making among client teams, and regular reviews with client teams resulted in completing the fixes in a quick turn around time.





The entire remediation process was managed from start to finish –analyzing vulnerabilities, segregating them, identifying relevant client teams, implementing fixes, regular reviews and documenting the remediation report. This allowed our client to focus on strategic initiatives rather than operational concerns. By dividing the tasks among our skilled team and linking with corresponding client team members, we ensured vulnerabilities are addressed in a single run, delivering reliable,secured solutions in quick time and in cost-effective manner.


Results

- All identified vulnerabilities, which spanned across critical, medium, and low severity levels were fixed.
 - To ensure the effectiveness of the implemented solutions, they were tested using industry-standard VAPT tools.
 - Following the implementation of the fixes, the application underwent a final assessment by the third-party vendor, and all issues were resolved in a single run.
- 



Conclusion

Through the execution of the remediation process for Vulnerability Assessment and Penetration Testing (VAPT) reports, the security posture of the client's mobile collection app has been significantly improved. The critical vulnerabilities were effectively mitigated, which in turn reduced the risk of data breaches and unauthorized access. This enhancement in security has fostered greater trust among clients and stakeholders, while also increasing operational efficiency by ensuring uninterrupted and reliable service delivery.



About Qruize

Qruize is a leading deep technology firm headquartered at California, with over a decade of experience in driving digital transformation for global businesses. Our expertise spans around software architecture consulting, technology strategy, cloud infrastructure and talent solutions. We are committed to empowering organizations through innovative technology solutions and strategic innovation.

For more details mail us on info@qruize.com



© 2024 Qruize Inc



<https://www.qruize.com/>

Qruize
Delivering Technology