CyberSapiens
THE CYBER SECURITY EXPERTS

FinWhiz

Case Study
Mobile Application VAPT

MOBILE APPLICATION VAPT

Securing a FinTech Android, iOS & Web Application Ecosystem

Customer : FinTech

Industry : Technology

Services : Technology

How a Complete VAPT Assessment Helped Improve Security for a Growing FinTech Platform

In today's digital world, fintech applications are used for managing financial activities, onboarding users, verifying accounts, uploading documents, and accessing important services directly from mobile phones.

A growing fintech company approached our security team to perform a complete Mobile Application VAPT (Vulnerability Assessment and Penetration Testing) for its:

- Android application
- iOS application
- Backend APIs
- Supporting web application

THE GOAL OF THE ASSESSMENT WAS SIMPLE:

- Identify security risks
- Improve applicatin security
- Strengthen API protection
- Secure authentication workflows
- Help the development team build a safer platform before scaling further

To maintain confidentiality, the company name and sensitive technical details have been generalized in this case study.

ABOUT THE APPLICATION

The client was building a fintech ecosystem focused on helping women improve their financial understanding, money management habits, and long-term financial independence.

The platform consisted of:

- Android mobile application
- iOS mobile application
- Backend API
- Supporting web application

The primary purpose of the mobile application was to provide women with:

- Financial guidance
- Personal finance tracking
- Financial insights
- Goal tracking
- Net worth and income visibility
- Insurance tracking
- Secure document vault features
- Learning resources and community support

The application aimed to simplify financial management for women by avoiding complicated financial jargon and instead providing easy-to-understand financial insights and tools.

The platform also focused on creating a supportive community where women could learn from shared experiences, podcasts, strategies, and financial education content.

Understanding the Web Application

The web application was mainly designed as a marketing and onboarding platform.

Its primary purpose was to:

- Introduce this platform
- Explain the mission behind the application
- Highlight women-focused financial challenges
- Allow users to register their interest before launch
- Help build an early user community

Compared to the mobile applications, the web application had limited functionality and mostly static content.

The website mainly contained:

- Application introduction pages
- Register interest forms
- About us section
- Financial awareness messaging
- Community and learning information

Since the web platform had a relatively small attack surface and limited dynamic functionality.

The main focus of the security assessment remained on the Android and iOS mobile applications along with the backend APIs, where the majority of user interaction and financial functionality existed.

Scope of the Security Testing

The assessment covered:

Mobile Application Security Testing

- Android Application VAPT
- iOS Application VAPT
- Runtime Security Testing
- Secure Storage Validation

API Security Testing

- Authentication testing
- Authorization testing
- Session validation
- Business logic testing
- Rate limit testing

Web Application Security Testing

- Input validation testing
- Rate limiting checks
- Basic security hardening review

Advanced Security Testing

- Dynamic testing
- Network interception testing
- SSL/TLS validation testing
- Runtime analysis

CREATING A PROPER VAPT TRACKING PROCESS

Before testing started, a dedicated VAPT tracker was created to manage:

- Vulnerability updates
- Severity levels
- Remediation timelines
- Retesting activities
- Developer coordination
- Client communication

This helped maintain proper communication between the security team and the client throughout the project.

The tracking process also made it easier to prioritize critical findings first while continuously monitoring medium and low-risk issues.

STATIC ANALYSIS OF ANDROID AND IOS APPLICATIONS

The engagement started with static analysis of both mobile applications.

During this phase, the applications were reviewed for:

- Application hardening
- Sensitive data exposure
- Backup configurations
- Local storage security
- Runtime protection mechanisms
- Reverse engineering protection

Most of the findings during static testing were lower-risk security hardening issues and configuration-related weaknesses.

Although these issues were not immediately critical, they highlighted the need for stronger secure coding and application protection practices.

DYNAMIC TESTING REVEALED DEEPER SECURITY RISKS

Once the engagement moved into dynamic testing, more serious security issues were identified.

By testing live application workflows and backend APIs, the assessment revealed weaknesses in:

- Backend validation
- Authorization handling
- Authentication workflows
- Session management
- API request validation

The testing showed that some functionalities relied too much on client-side trust instead of strict server-side validation.

This created situations where attackers could potentially manipulate requests or abuse insecure workflows.

This phase proved very important because many impactful risks were not visible during static analysis alone.

API SECURITY TESTING

API Security Testing was one of the most important parts of the engagement.

Since the mobile applications communicated heavily with backend APIs, proper validation and access control became critical.

The APIs were tested for:

- Access control validation
- Authentication handling
- Session security
- Authorization enforcement
- Business logic security
- Rate limiting protections

The organization was guided on implementing stronger backend validation and layered API security controls.

RUNTIME ANALYSIS AND NETWORK INTERCEPTION TESTING

Advanced runtime analysis and HTTPS interception testing were also performed. This helped evaluate how securely the applications communicated with backend servers and how resistant the apps were against runtime manipulation techniques.

The testing highlighted the importance of:

- SSL/TLS validation
- ·Runtime protection
- Authentication workflows
- Anti-tampering mechanism
- Secure certificate validation
- Protection against instrumentation frameworks

The client was advised to implement multiple layers of runtime security instead of depending on a single protection mechanism.

WEB APPLICATION SECURITY TESTING

The organization also had a supporting web application.

Compared to the mobile applications, the web platform had a smaller attack surface and mostly static functionality.

During the assessment, only a few lower-risk issues were identified, mainly related to:

- Missing request throttling
- Limited rate limiting protections

The client was guided on:

- Which issues should be fixed before launch?
- Which security improvements could be planned after launch?
- How to prioritize remediation activities based on risk severity

This helped the development team balance security improvements with project timelines.

SECURITY MEETINGS AND CLIENT GUIDANCE

Apart from identifying issues, the engagement also focused on helping the client understand how stronger security controls could be implemented.

Multiple technical meetings were conducted with the application owner and development teams.

The discussions covered:

- Secure API architecture
- Authentication security
- Layered security implementation
- Runtime protection strategies
- Session management improvements
- API abuse prevention

Each recommendation was explained step-by-step so the development team could clearly understand:

- Why the issue happened
- What risk it created
- How it could be fixed securely
- Which fixes should be prioritized first?

This collaborative approach improved security awareness across the organization.

OPERATIONAL CHALLENGES DURING THE ENGAGEMENT

Like many real-world enterprise projects, the engagement also faced a few operational challenges.

1 TestFlight Access Removal During iOS Testing

Like many real-world enterprise projects, the engagement also faced a few operational challenges.

This delayed certain validation and retesting activities until access was restored later.

Once access was re-enabled, testing resumed successfully.

2 Delays in Remediation Due to Development Dependencies

Several findings required backend-level changes from the client's development team.

Because some fixes impacted:

- Authentication workflows
- Backend validation logic
- API authorization handling
- Session management mechanisms

The remediation process took additional time.

Continuous follow-ups and retesting support were maintained throughout the project to ensure fixes were implemented properly.

REPORTING AND RETESTING PROCESS

A detailed Mobile Application VAPT report was shared with the client containing:

- Technical observations
- Business impact explanations
- Remediation guidance
- Retesting updates
- Secure implementation recommendations

After fixes were implemented, retesting was performed to validate whether the identified risks were properly addressed.

ACHIEVING A SUCCESSFUL SECURITY OUTCOME

Despite operational interruptions and remediation delays, the project achieved a successful outcome through strong collaboration between the security and development teams.

The engagement helped the organization build a stronger security foundation for scaling its fintech ecosystem securely.

By the end of the engagement:

- Mobile application security was significantly improved
- API validation mechanisms became stronger
- Runtime security awareness increased
- Secure development practices improved
- Security coordination became more structured
- Additional security layers were planned for future releases

WHY MOBILE APPLICATION VAPT IS IMPORTANT

Modern fintech applications handle sensitive user and financial data.

Without proper security testing, organizations may face risks such as:

- Unauthorized access
- API abuse
- Account compromise
- Data exposure
- Session hijacking
- Financial fraud
- Reputation damage

Performing regular:

- Android Application VAPT
- iOS Application VAPT
- API Security Testing
- Web Application Security Testing
- Runtime Security Assessments

helps organizations identify and fix security risks before attackers exploit them.

CONCLUSION

This Mobile Application VAPT case study shows how proper security testing across Android, iOS, APIs, runtime environments, and web applications can help fintech organizations strengthen their cybersecurity posture.

The engagement combined:

- Static analysis
- Dynamic testing
- API security testing
- Runtime analysis
- Network interception testing
- Security consultation
- Continuous remediation support

To help the organization improve long-term application security.

Most importantly, the project highlighted that successful security is not achieved only through finding vulnerabilities, it is achieved through:

- Collaboration
- Proper remediation planning
- Secure development practices
- Continuous security validation
- Layered security implementation

As fintech ecosystems continue growing, proactive Mobile Application VAPT and API Security Testing remain essential for protecting users, financial data, and business trust.

Looking for Mobile Application VAPT Services?

If your organization manages:

- Android applications
- iOS applications
- APIs
- FinTech platforms
- Web applications
- Customer onboarding systems

then performing regular security assessments is extremely important.

A proper Mobile Application VAPT helps organizations:

- Identify security risks early
- Protect sensitive customer information
- Strengthen authentication security
- Prevent unauthorized access
- Improve API protection
- Reduce business security risks

Security should always be treated as a continuous process, especially for applications handling financial and sensitive user data.

FINAL THOUGHTS

This case study highlights how a complete Mobile Application VAPT engagement helped strengthen the security posture of a growing fintech ecosystem.

- Android Application Security Testing
- iOS Application VAPT
- API Security Testing
- Runtime Analysis
- Security Consultation
- Business impact explanations
- Continuous Retesting

the organization was able to improve its application security and build a stronger foundation for future growth.

Cybersecurity is not only about finding vulnerabilities.

It is about:

- Understanding risks
- Building secure systems
- Improving development practices
- Implementing layered defenses
- Continuously validating security controls

As mobile and fintech ecosystems continue evolving, proactive VAPT assessments remain essential for protecting users, business operations, and digital trust.

devini Goonetilleke Founder

I am a FinTech founder. I engaged Claude Pinto and his team from CyberSapiens to help me with Vulnerability and Penetration Testing (VAPT) for my FinWhiz Platform. They were not only extremely professional but very accommodating. They worked within our budget and timeframes. They understood our priorities and delivered to them. They provided practical advice for our situation. They also provided development teams with clear solutions which sped implementation. We are proud to partner with CyberSapiens as long-term partners and have no hesitation in recommending them to other founders and businesses.

★ ★ ★ ★ ★

CyberSapiens

CyberSapiens unites our country's most trusted experts in delivering an unparallel, comprehensive end-to-end portfolio of complex and challenging threat environment.cyber security services across Australia and India , Canada, USA.

Contact us to find out how CyberSapiens can boost the cyber security skills of your entire organization.

Call Us
1300 507 668

Email Us
sales@cybersapiens.co

Our Location
Lvl 1 206 Lorimer St, Port Melbourne, Australia

CyberSapiens
THE CYBER SECURITY EXPERTS