Yethi
Innovation for quality

CASE STUDY

Yethi Enables Secure Omnichannel Banking Transformation for a Leading European Bank

The Client

A leading Malta-based bank embarked on a large-scale omnichannel banking transformation to modernize its digital banking ecosystem across web and mobile channels. The initiative focused on delivering secure, seamless, and compliant customer experiences while integrating multiple core banking and payment systems.

The Scope of Work

- Security assessment of Open Banking Web Flow, OSB APIs, Saltedge APIs, and DRM Data Remediation platform
- Validation aligned to OWASP Web and API Top 10 frameworks
- End-to-end security testing across omnichannel banking applications and APIs using manual and automated approaches
- Coverage across key security areas including authentication, authorization, session management, input validation, cryptography, and business logic
- Execution of vulnerability assessments using tools such as Postman, OWASP ZAP, Burp Suite, and Acunetix
- Threat profiling and testing across Information Gathering, Configuration Management, Identity Management, Session Management, Error Handling, Cryptography, Business Logic, and Client/Server-side controls
- Validation of API security including parameter tampering, injection, fuzzing, and HTTP method handling
- Defect management with severity-based classification (High, Medium, Low) and structured reporting

Company & Asset Size

Employees: ~ 2200+

Branches: ~ 40+

Net Income: ~ $15B

Application Involved

Redhat, Apache HTTP Server, Java-based Applications, Salt-Edge, DRM System & Open Banking API

Business Impact

- Enabled secure interactions across web and API layers with improved protection against identified vulnerabilities
- Strengthened API security by addressing authentication and authorization gaps to support Open Banking requirements
- Reduced risk of data breaches and unauthorized access across interconnected systems
- Strengthened protection against vulnerabilities such as XSS, CSRF, injection, SSRF, and clickjacking
- Delivered a hardened security posture aligned with OWASP standards
- Improved system resilience through secure configuration, session management, and encryption practices
- Enhanced customer trust by ensuring secure, reliable, and compliant digital banking experiences

The Challenge

01 Exposure to critical vulnerabilities such as broken authentication in APIs and improper input validation across systems, missing security headers, and insufficient rate limiting in APIs

02 Inconsistent implementation of security controls across web, API, and remediation platforms

03 Lack of standardized input validation, increasing risk of injection, XSS, and parameter tampering attacks

04 Missing security headers and weak session management practices impacting application hardening

05 Absence of rate limiting controls, exposing APIs to brute force and abuse scenarios

06 Configuration-level information leakage (e.g.version disclosure via headers) revealing technology stack details

07 Presence of outdated components and certificate issues (e.g., expired TLS/SSL certificates, outdated JavaScript libraries)

08 Complexity in securing interconnected Open Banking architecture including third-party integrations (Saltedge)

09 Ensuring compliance with evolving security standards while maintaining system stability and availability

The Solution

- Performed comprehensive threat modeling aligned to OWASP Web and API security guidelines
- Executed end-to-end security assessments across web, API, and application layers covering authentication, authorization, session management, and input validation
- Identified and remediated critical vulnerabilities including broken API authentication and improper input validation
- Strengthened input validation across web and API layers using whitelist-based controls to mitigate injection and XSS risks
- Addressed missing security headers including HSTS, X-Frame-Options, and X-Content-Type-Options identified during the API security assessment
- Performed security testing for Open Banking Web-to-Web customer journeys including consent creation and payment initiation workflows
- Identified vulnerabilities including broken authentication, improper input validation, missing HTTP security headers, session fingerprinting, and insufficient rate limiting
- Enhanced session security with HTTP Only cookies, Secure flags, session timeout controls, and protection against session fixation and hijacking
- Enabled rate limiting and traffic throttling to mitigate brute force and denial-of-service risks
- Eliminated information leakage by disabling unnecessary headers such as X-Powered-By and securing configurations
- Upgraded outdated libraries and resolved TLS/SSL certificate validity issues to ensure secure communication
- Validated strong cryptographic controls including secure HTTPS enforcement and TLS configurations
- Ensured secure API behavior through strict validation of HTTP methods, endpoint access control, and input handling
- Verified robust third-party API security (Saltedge) with certificate-based authentication, strict validation, and no identified vulnerabilities

Conclusion

This security testing initiative played a critical role in ensuring that the bank's omnichannel transformation across APIs, digital banking applications, and open banking ecosystems. By validating real-world attack scenarios across web applications, APIs, and third-party integrations—including authentication flows, data exchange mechanisms, and backend processing systems—the bank was able to proactively identify and mitigate vulnerabilities prior to production rollout.

This engagement highlights how security testing must be tightly integrated into digital transformation programs. It enabled the bank to deliver secure, compliant, and resilient services while maintaining data confidentiality, system integrity, and regulatory adherence across a highly integrated banking ecosystem.

About Yethi

Leading Banks rely on the Yethi Consulting Assurance expertise for business success with their financial applications. Yethi Consulting Pvt Ltd, is the leading provider of Quality Assurance and Testing Automation solutions to the Global Banking and Financial services Industry for their applications reliability and business success. With over a decade of operations, Yethi Consulting brings deep domain and industry expertise along with an inbuilt library of **over 1 million Test cases for over 250 Financial Applications.**

Today, Yethi Consulting through a combination of products, services and solutions, has delivered **over 750+ projects for 130+ Customers, across 30+ countries.**

Yethi Consulting has been awarded with the IBS intelligence Leadership club in their Annual sales league Table 2023 as the 'Best in Quality Assurance and Testing platforms'.

Learn more on **www.yethi.in**

Contact Us

www.yethi.in

India | UAE | USA | Africa