CASE STUDY

"At COE Security, we build, operate, and transfer world-class security solutions, empowering businesses with resilience and trust."

Joseph Henderson

CASE STUDY

STRENGTHENING API SECURITY THROUGH COMPREHENSIVE PENETRATION TESTING

COE SECURITY LLC

USA | BRAZIL | UAE | INDIA

COE SECURITY

Measurable Impact Our Security in Numbers

- 1,500+ Global Engagements
- 95% Client Satisfaction
- 10+ Years of Cybersecurity Excellence
- 15K+ Critical Vulnerabilities Identified
- 1M+ Security Incidents Managed
- $350M+ Costs Saved
- $2.5B+ Transactions Secured
- 24/7/365 Threat Monitoring & Response
- Proactive Threat Hunting
- Cutting-Edge Security Technologies
- Dedicated Security Advisors
- Zero-Day Exploit Mitigation
- Incident Response Planning & Execution
- Security Awareness Training
- Customizable Security Solutions

Client Profile

A leading fintech company providing digital payment solutions relied heavily on its Application Programming Interface (API) ecosystem for seamless integration with banks, third-party vendors, and mobile applications. Given the sensitive nature of financial transactions, ensuring API security was critical to protect against cyber threats and regulatory non-compliance.

Challenges Faced

Before undergoing API Penetration Testing, the company identified several security concerns:

- Insecure authentication and authorization mechanisms, increasing the risk of account takeovers.
- Excessive data exposure, potentially leaking sensitive user and financial information.
- Broken object-level authorization (BOLA), allowing attackers to access or modify data they shouldn't.
- Rate-limiting and denial-of-service (DoS) vulnerabilities, making APIs susceptible to abuse.
- Injection vulnerabilities (SQLi, XML External Entity (XXE), and Server-Side Request Forgery (SSRF)), which could compromise backend systems.
- Compliance concerns with OWASP API Security Top 10, PCI DSS, GDPR, and ISO 27001.

Our Approach

To enhance API security, we conducted a comprehensive API Penetration Testing engagement, identifying vulnerabilities and providing remediation strategies.

Scoping & Threat Modeling

We're Hiring!

COE SECURITY

Compliance & Regulatory Mastery

- ISO 45001
- HIPAA & HITRUST
- NIST & NIST 800-171
- ISO 27001
- PCI DSS
- CMMC
- CIS Controls
- SOC 2
- CCPA & NYDFS
- EU CRA
- FedRAMP
- GDPR
- UK Cyber Essentials
- Essential Eight - Australia

Scoping & Threat Modeling

We worked with the client to define:

- Scope of testing, including RESTful APIs, GraphQL endpoints, SOAP services, and third-party integrations.
- Threat models specific to APIs, such as Broken Access Control, Injection Attacks, and Business Logic Flaws.
- Testing methodologies, including Black Box, Gray Box, and White Box testing.

Security Testing Execution

Security Testing Execution

Using industry-standard frameworks like OWASP API Security Top 10, NIST 800-53, and MITRE ATT&CK, we conducted rigorous API penetration testing, covering:

• Authentication & Authorization – Evaluating OAuth 2.0, JWT security, API keys, and token policies.

• BOLA & Broken Authentication – Identifying unauthorized data access and login vulnerabilities.

• Data Exposure & Rate Limiting – Detecting sensitive data leaks and DoS risks.

• Injection Attacks – Testing for SQLi, XXE, SSRF, and command injection.

• Endpoint & Business Logic Security – Assessing CORS, file uploads, logging, and logic flaws.

Findings & Risk Assessment

After completing the penetration test, we provided a detailed security report, including:

- Critical, High, Medium, and Low-risk vulnerabilities, with business impact analysis.
- Proof-of-Concept (PoC) exploits, demonstrating how attackers could exploit vulnerabilities.
- A prioritized remediation roadmap, helping the company fix vulnerabilities efficiently.

We're Hiring!

COE SECURITY

Our Cybersecurity Arsenal: Beyond Protection- We Build Resilience

- Application Penetration Testing (Thick/Thin)
- Mobile Application Penetration Testing
- API Penetration Testing
- Network Penetration Testing
- Operational Technology Security Testing
- Cloud Penetration Testing
- AI & LLM Security Audit and Pen Testing
- Red Teaming & Social Engineering Services
- Product & Hardware Penetration Testing
- IoT Security
- Security Operations Center Services (24/7)
- Custom Security Services

Remediation Support & Secure Coding Practices

To ensure the API ecosystem remained secure, we provided:

- Secure coding guidelines to prevent BOLA, BFLA, and injection attacks.
- Improved authentication mechanisms, including OAuth 2.0 hardening, token validation, and API key management.
- Implementation of rate limiting and throttling, preventing API abuse and DoS attacks.
- Enhanced logging and monitoring, enabling real-time API security event detection.
- Re-testing of critical vulnerabilities, ensuring proper remediation.

Compliance & Continuous Security

After implementing security fixes, the company achieved:

- Stronger API security posture, eliminating critical security flaws.
- Compliance readiness for PCI DSS, GDPR, ISO 27001, and OWASP standards.
- Secure API integrations, reducing the risk of data breaches and unauthorized access.
- Implementation of continuous security monitoring, ensuring long-term protection.

Results Achieved

Within six weeks, the company successfully:

- Eliminated critical security flaws, including SQLi, XSS, and Broken Access Control.
- Hardened authentication mechanisms, implementing MFA and secure session management.
- Implemented security best practices in development (SDLC), reducing future risks.
- Established a regular penetration testing cycle, ensuring continuous security improvements.

We're Hiring!

COE SECURITY

Industries We Protect with Cutting-Edge Security



- Financial Services
- Healthcare
- Retail
- E-commerce
- Government
- Cryptocurrency
- Blockchain Technology
- Automotive
- Transportation/Logistics
- Energy & Utilities
- Hospitality/Tourism
- Entertainment/Media
- Manufacturing
- Education
- Telecommunications
- HiTech & Information Technology

We're Hiring!

Need Application Penetration Testing?

If you're looking to secure your web applications, APIs, and cloud integrations, reach out to us today for a customized penetration testing engagement.

Conclusion

By leveraging our API Penetration Testing expertise, we helped the fintech company proactively identify vulnerabilities, enhance security controls, and achieve compliance with industry regulations. Our structured approach, from threat modeling to remediation, ensured the API ecosystem remained resilient against cyber threats.

COE Security LLC

COE Security is a leading cybersecurity services provider, offering comprehensive solutions to address the evolving threat landscape. We have a proven track record of helping organizations of all sizes mitigate risks, strengthen defenses, and recover from cyberattacks. Our team of experienced cybersecurity professionals possesses deep expertise in the latest technologies and best practices, enabling us to deliver tailored solutions that meet your unique security needs.

"Peace of mind in a world of cyber threats.
That's what we deliver."

Joseph Henderson

COE SECURITY