CASE STUDY

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

FINANCIAL SERVICES

APPLICATION 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

We're Hiring!

Client Profile

A leading financial services company providing online banking and digital payment solutions needed to ensure its web and mobile applications were secure from cyber threats. Given the nature of their business, the company handled sensitive customer financial data, making security a top priority.

Challenges Faced

Before undergoing Application Penetration Testing (App Pentesting), the company identified several concerns:

- Potential vulnerabilities in their web and mobile applications that could lead to data breaches.
- Lack of proactive security testing, exposing the company to risks such as SQL injection, XSS, and authentication bypass attacks.
- Compliane concerns with regulatory frameworks such as PCI DSS, GDPR, and NIST that required regular security testing.
- Growing cyber threats targeting financial institutions, including credential stuffing and API abuse.

Our Approach

To strengthen the company's application security, we conducted a comprehensive penetration testing engagement, identifying vulnerabilities and providing remediation strategies.

Scoping & Threat Modeling

Before starting the penetration test, we worked closely with the client to:

- Define the scope of testing (web and mobile applications, APIs, authentication mechanisms, and third-party integrations).
- Identify threat models specific to financial applications, such as unauthorized transactions and account takeovers.
- Determine testing methodologies (Black Box, Gray Box, and White Box testing).

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

Security Testing Execution

Leveraging industry-standard frameworks like OWASP Top 10 and NIST SP 800-115, we conducted a comprehensive application penetration test, covering:

- Recon & Intelligence Gathering – Mapping application structure, identifying exposed endpoints, and assessing attack vectors.
- Automated & Manual Testing – Using Burp Suite, OWASP ZAP, and Kali Linux to uncover and validate vulnerabilities.
- Authentication & Authorization – Detecting weak authentication, privilege escalation, and session mismanagement.
- API Security – Identifying BOLA, IDOR, and rate-limiting flaws.
- Injection & Input Validation – Testing for SQLi, XSS, and command injection.
- Business Logic Flaws – Analyzing transaction workflows for exploitation risks.
- Mobile App Security – Evaluating data storage, reverse engineering threats, and insecure API calls.

Findings & Risk Assessment

Following the penetration test, we compiled a detailed report highlighting:

- Critical, High, Medium, and Low-risk vulnerabilities along with their potential business impact.
- Proof-of-Concept (PoC) exploits demonstrating how attackers could exploit weaknesses.
- A prioritized remediation roadmap to help 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

We're Hiring!

Remediation Support & Re-Testing

To ensure all security flaws were mitigated, we provided:

- Hands-on remediation guidance, helping developers patch vulnerabilities securely.
- Secure coding best practices to prevent recurring security issues.
- Re-testing of critical vulnerabilities to validate that all fixes were effective.

Compliance & Continuous Security

After completing the penetration test, the company achieved:

- Stronger security posture with proactive vulnerability detection and remediation.
- Compliance readiness for PCI DSS, GDPR, and other regulatory standards.
- Reduced risk of financial fraud and data breaches, safeguarding customer information.
- Enhanced trust and reputation, reassuring customers and stakeholders of their commitment to security.

Results Achieved

Within six weeks, the company successfully:

- Eliminated critical vulnerabilities, including authentication bypass and insecure API endpoints.
- Strengthened its web and mobile applications against cyber threats.
- Integrated security best practices into its software development lifecycle (SDLC).
- Established a regular penetration testing cycle, ensuring ongoing security improvements.

Need Application Penetration Testing?

If you're looking to secure your applications and identify vulnerabilities before attackers do, reach out to us today for a customized penetration testing engagement.

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!

Conclusion

By leveraging our Application Penetration Testing expertise, we helped the financial services company proactively identify vulnerabilities, enhance security controls, and achieve compliance with industry regulations. Our structured approach, from threat modeling to remediation, ensured the company was well-prepared 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