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 PRODUCT SECURITY THROUGH 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 e-commerce company offering online retail services and digital products sought to ensure the security of their latest product launch – an innovative mobile app designed to enhance customer shopping experiences. The company needed to evaluate the security posture of their product and identify vulnerabilities before releasing it to a large user base. With a commitment to data privacy, compliance, and trust, they wanted to ensure the product would withstand potential cyber-attacks and maintain user confidentiality.

Challenges Faced

Before undergoing Product Penetration Testing, the company recognized the following challenges:

- Exposure to cyber-attacks targeting user data, payment systems, and digital assets.
- Complex product architecture, which included third-party integrations and APIs.
- Lack of thorough security testing on mobile applications, leading to potential security flaws in app functionality.
- Data leakage risks, such as user credentials, payment information, and personal data being exposed.
- Integration issues between the mobile application and backend systems, increasing the chances of API misconfigurations and data interception.
- No external validation on the product's security controls and threat response capabilities.

Our Approach

To identify vulnerabilities and improve the product's overall security, we conducted comprehensive Product Penetration Testing. This testing focused on the app's functionality, its backend systems, and integrations to ensure robust protection against modern cyber threats.

COE SECURITY

©COE SECURITY LLC. ALL RIGHTS RESERVED.

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

We're Hiring!

Scoping & Threat Modeling

- We worked closely with the client to define:
- Scope of the engagement, covering mobile app security, backend systems, APIs, and third-party integrations.
- Security goals, focusing on data privacy, user authentication, payment security, and API integrity.
- Compliance considerations, ensuring the product met GDPR, PCI DSS, and other relevant regulations.
- Threat modeling to simulate real-world attack scenarios relevant to the e-commerce industry.

Security Testing Execution

• Mobile App Security – Evaluating storage, encryption, session management, and communication.
• API Security – Checking for insecure endpoints and authentication flaws.
• Authentication & Session Management – Ensuring MFA and session timeouts.
• Input Validation – Identifying XSS, SQL injection, and injection flaws.
• Business Logic – Testing user flow manipulation.
• Backend Security – Ensuring database and data storage security.
• Third-party Integration – Assessing external service vulnerabilities.
• Reverse Engineering – Analyzing hardcoded secrets and code issues.
• Ecosystem Penetration – Simulating multi-stage attacks across the app and infrastructure.

Findings & Risk Assessment

- Identified vulnerabilities, categorized by severity (Critical, High, Medium, Low) based on their potential business impact.
- Exploitable weaknesses in the mobile app, backend, and API that could lead to data breaches, unauthorized access, and loss of consumer trust.
- Proof-of-Concept (PoC) exploits, demonstrating how certain vulnerabilities could be leveraged by malicious actors.

COE SECURITY

©COE SECURITY LLC. ALL RIGHTS RESERVED.

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!

- Recommendations for remediation, including security patches, better data handling, and hardened access controls.
- Compliance risks, identifying areas where the product was not meeting regulatory standards such as GDPR or PCI DSS.

Remediation Support & Secure Hardware Development Best Practices

- Targeted employee awareness training, using real examples from the engagement.
- Phishing simulation exercises, ensuring employees could recognize future threats.
- Incident reporting improvements, encouraging employees to report suspicious interactions.
- Multi-factor authentication (MFA) enforcement, reducing the risk of credential-based attacks.
- Verification protocol enhancements, strengthening identity verification processes.
- Executive security training, helping C-suite members recognize BEC and deepfake scams.

Results

- Resolved critical vulnerabilities, reducing the risk of data breaches, financial fraud, and reputational damage.
- Enhanced the app's security posture, resulting in a safer user experience and increased customer trust.
- Achieved compliance with key regulations like GDPR and PCI DSS, ensuring customer data privacy and secure payment processing.
- Strengthened third-party integration security, minimizing external risks while maintaining seamless functionality.

COE SECURITY

©COE SECURITY LLC. ALL RIGHTS RESERVED.

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 conducting thorough Product Penetration Testing, we helped the company identify and remediate critical security vulnerabilities in their product before it reached customers. Our real-world attack simulations provided invaluable insights, allowing the company to proactively address security gaps and improve user protection.

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

©COE SECURITY LLC. ALL RIGHTS RESERVED.