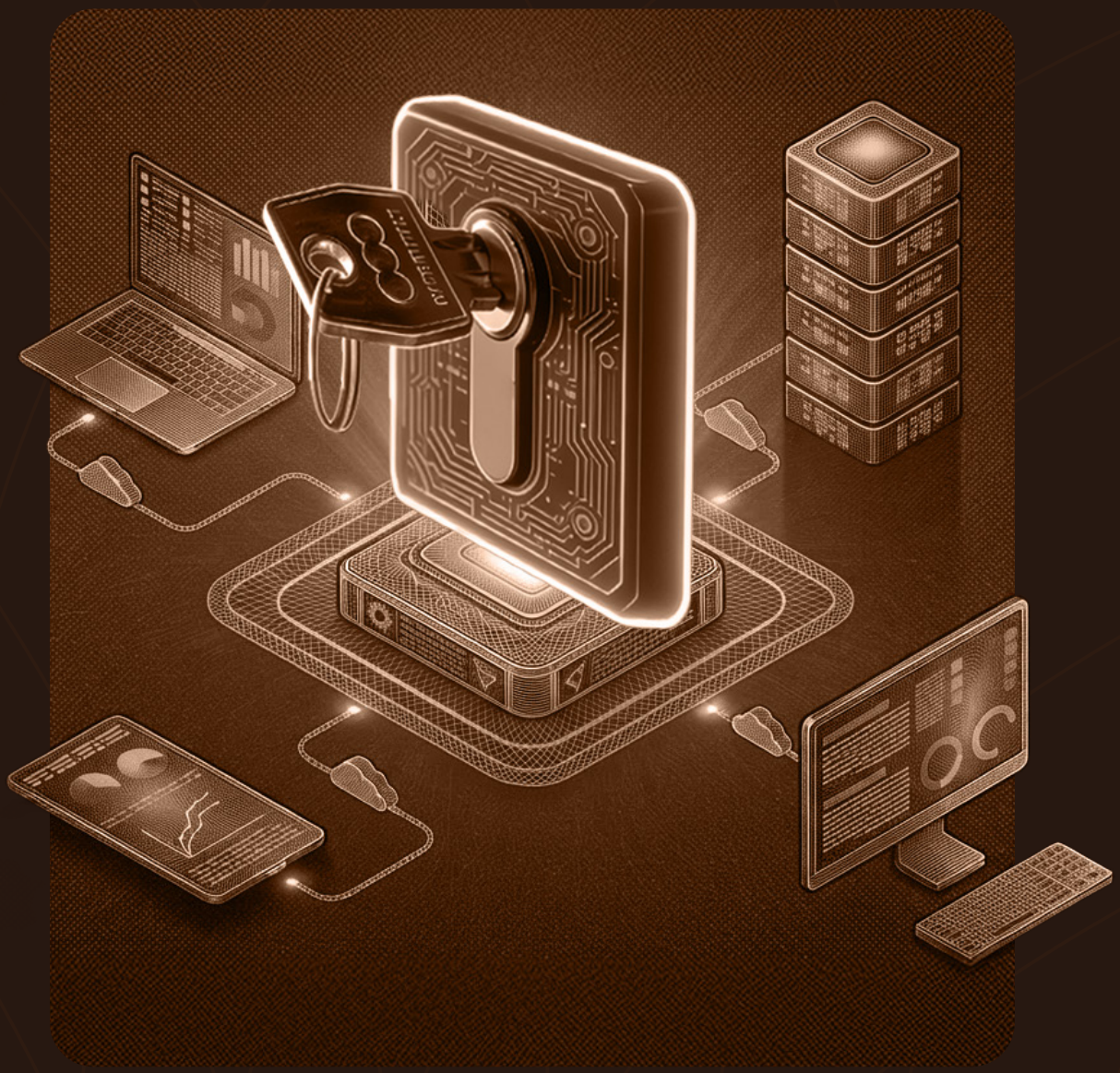
SISA



Customer Success Story

How SISA's Targeted Penetration Testing Secured the Maker-Checker Workflow for a Leading Financial Institution

About The Customer

The Client is a leading financial institution founded in 2004. Headquartered in the Emirate of Abu Dhabi, UAE, it operates an enterprise platform within a highly regulated environment targeted at consumer and commercial finance. With a portfolio of services that include Commercial & Retail Financing, Investment, Islamic Financing, Insurance and Brokerage, it helps both people and businesses with credit and wealth management. The company has built a strong awareness for its brand over the years and is well recognized as a niche player that provides innovative and value-adding solutions to its customers.

Business Challenge

During an internal security assessment performed by SISA, a critical Broken Access Control vulnerability (CVSS v3.1 Score 9.1) was identified within the core application logic governing the Client's dual-control "maker-checker" architecture. Under this framework, one set of user accounts is authorized to initiate requests (Makers), while a distinct tier of privileged accounts is required to review and authorize those actions (Checkers). While the platform successfully verified user identity at login, it failed to perform equivalent access control validations on the server side when individual functions were executed.

This flaw allowed a low-privileged Maker user to intercept application traffic and manipulate JSON Web Tokens (JWT) during the workflow phase. By substituting authentication tokens, a Maker could effectively authorize their own privilege escalation requests. If exploited by an insider threat or an attacker utilizing a compromised low-privilege account, this vulnerability completely bypassed the institution's dual-control mechanisms. Such an unauthorized privilege escalation could lead to fraudulent transactions, compromised audit logs, and severe non-compliance with industry regulations (such as SOX or PCI-DSS), resulting in hefty financial and reputational liability.

SISA's Solution

To thoroughly evaluate the application's logical boundaries, SISA executed a structured penetration testing methodology aimed at assessing the resilience of role-based access controls (RBAC) against token manipulation.

SISA's Structured Penetration Testing Methodology Contextualized to the Case Environment

01 Request Initiation & Capture

SISA accessed the application using valid Maker credentials, submitted a request to elevate the account's role to a Checker, and extracted the active Maker JWT authentication token from the communication session.

02 Proxy Traffic Interception

The testing team routed application traffic through a local proxy tool (Burp Suite), enabling the real-time capture and modification of outbound HTTP/HTTPS requests before they reached the server backend.

03 Token Substitution Manipulation

SISA authenticated with a separate Checker account to locate the pending role-elevation request. Upon clicking the "Approve" function, the outbound request was paused via the proxy, and the valid Checker JWT was replaced entirely with the low-privileged Maker JWT.

04 Exploitation Verification

The server accepted and processed the modified request without verifying the context of the user token, successfully updating the Maker's role to Checker and demonstrating that a user could unilaterally approve their own privilege level.

Key Security Gaps Uncovered

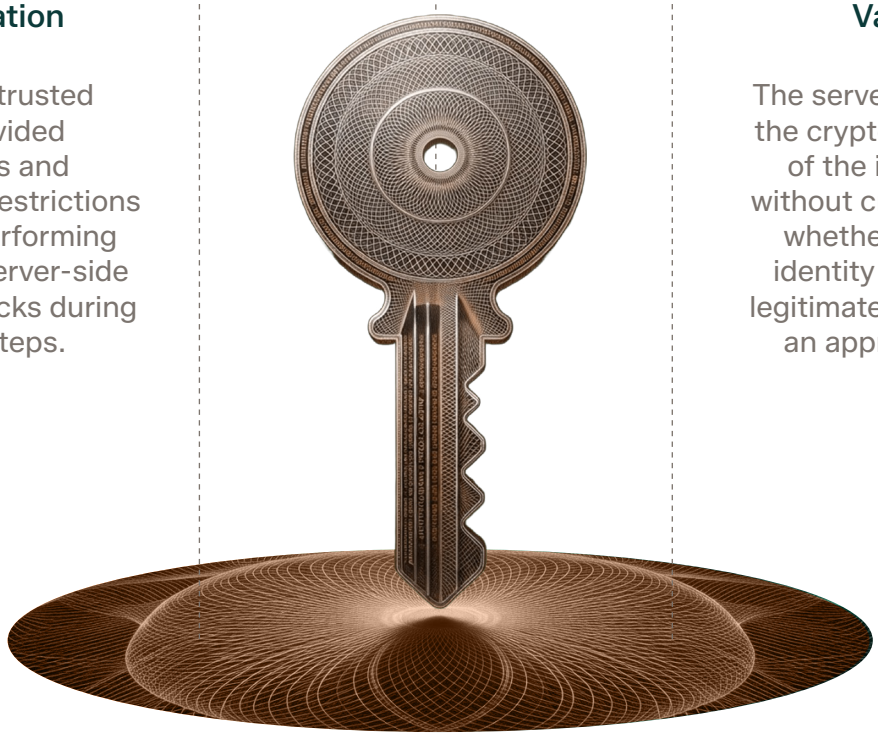
SISA's penetration test revealed that while the application properly confirmed who a user was, it failed to securely govern what that user was authorized to do on the server side. The core vulnerabilities that chained together to permit this compromise included:

Missing Request Ownership Controls

The application lacked backend business logic to verify that the user ID approving a transaction was distinct from the user ID who originally created it.

Reliance on Client-Side Authorization

The system trusted client-provided parameters and interface-level restrictions rather than performing independent server-side permission checks during approval steps.



Contextless Token Validation

The server blindly verified the cryptographic validity of the incoming JWT without cross-referencing whether that specific identity possessed the legitimate right to execute an approval function.

Remediation Measures

To restore absolute integrity to the dual-control environment, SISA delivered an immediate, prioritized remediation strategy combining server-side structural logic fixes and comprehensive monitoring.

SISA's 5-Step Remediation Plan

STEP 01

Immediate Server-Side Authorization Enforcement

SISA directed the Client to implement robust server-side validation filters across all administrative and approval endpoints. This included ensuring the backend server explicitly checks that the incoming session identity inherently possesses Checker role privileges prior to executing any transaction state change.

STEP 02

Implementation of Request Ownership Checks

The database architecture was updated to tie the creator's unique identifier to each pending request. Code-level rules were instituted to mandate that if the approver's user ID (extracted securely from the server-validated token) matches the request creator's ID, the transaction is immediately blocked and rejected.

STEP 03

Hardening Session & State Management

SISA advised transitioning toward server-side session management rather than relying exclusively on stateless client tokens for critical workflow authorization boundaries. State transitions (e.g., pending $\rightarrow$ approved) were re-written to be strictly atomic to prevent race conditions or unexpected manipulation.

STEP 04

Enriching Compliance & Integrity Audit Logs

Comprehensive logging was enabled across all privilege-sensitive endpoints for recording the user ID, role, exact timestamp, request ID, and the final authorization outcome. Real-time system alerts were established to instantly flag any anomalous self-approval attempts or invalid role elevation requests.

STEP 05

Post-Remediation Validation & Automated Testing

Following full deployment of the patches, SISA performed thorough validation testing to guarantee the specific token substitution bypass was entirely neutralized. Automated security regression tests were subsequently integrated into the development pipeline to inspect all parallel approval systems for hidden authorization flaws.

Business Impact

By identifying and closing this critical Broken Access Control gap, SISA helped the Client secure their core workflows and preserve the foundational trust of their identity management framework.

Significantly Reduced Business Risk

The assessment gave the Client definitive visibility into a structural logic flaw, eliminating vulnerabilities before they could be exploited for internal fraud or privilege manipulation.

Strengthened Security of Critical Services

Validating authorization directly on the server backend comprehensively protected the platform's core identity layer, internal user permissions, and sensitive approval workflows.

Prevention of Financial and Reputational Damage

By neutralizing an exploit vector capable of circumventing dual-control rules, the Client drastically minimized exposure to unauthorized data manipulation, fraudulent system modifications, and public fallout.

Improved Operational Continuity

By preventing unauthorized privilege changes, the Client ensured that user roles, approval workflows, and transaction processes remained consistent, controlled, and protected from manipulation.

Enhanced Governance and Audit Readiness

Eliminating self-approval capabilities strengthened separation of duties, reduced control gaps, and improved alignment with financial governance and audit requirements.

Greater Trust in Internal Controls

The remediation reinforced confidence that critical access and approval mechanisms were operating as intended, supporting stronger stakeholder trust in the Client's security posture.

About SISA

SISA is a global leader in cybersecurity for the payment ecosystem, operating at the intersection of AI, cybersecurity, and payments. Trusted by leading brands and financial institutions across 40+ countries, SISA secures over 1,000 organizations by helping them anticipate threats, strengthen resilience, and protect critical payment infrastructure. Powered by real-world breach intelligence, SISA enables organizations to stay ahead of evolving cyber risks. Follow SISA on LinkedIn for the latest insights on cybersecurity, payment security innovation, and emerging technologies.

Portfolio of Forensics-driven Cybersecurity Solutions

SISA Cybersecurity Advisory

Regulatory & Privacy Advisory

- Data Privacy (GDPR, HIPAA,DPDP)
- Central Bank Mandates
- Privacy Program/Fractional DPO

Risk & Exposure Advisory

- Risk Assessment
- Cyber Risk Quantification/Board Advisory
- Cyber Insurance Readiness Advisory

Strategic Leadership Advisory

- Security Posture & Maturity Assessment
- Security Roadmap & Transformation Blueprint
- AI Governance & Model Risk Advisory

SISA One

Unified Platform for Compliance, Security and Privacy

ProACT

Agentic SOC

- AI-Powered cyber-defence
- Security Orchestration, Automation and Response (SOAR)
- File Integrity Monitoring (FIM)
- Breach and Attack Simulation

Pulse

Continuous Compliance

- Continuous Compliance monitoring
- Evidence Automation
- Risk Assessment
- Third Party Risk Management

Radar

Data Protection & Governance

- Discovery (Structured and Unstructured)
- Classification
- Consent Management

Prism

AI Security and Governance

- AI Discovery
- AI Red Teaming
- GenAI App PT
- AI Agent PT
- AI BOM
- Secure Fine tuning
- AI Observability
- AI Governance

SISA Services

Expert-led services

Compliance

- PCI DSS Compliance
- PCI PIN
- PCI 3D Secure (3DS)
- PCI P2PE Compliance
- PCI S3/S-SLC
- PCI CP
- PCI SAQ
- SWIFT
- MPoC
- SOC2 Compliance

DFIR/Sappers

- Forensic Resilience Assurance
- Payment Forensics Investigation
- Compromise Assessment
- Cloud Forensics
- Forensic Retainer

Offensive Security

- Application Security
- Infrastructure & Network Security
- Cloud & Container Security
- Adversary-Led Ransomware Simulation
- Red Teaming
- Hardware/IoT Security

Data Protection

- Data Privacy (GDPR, HIPAA, DPDP)
- NIST
- HITRUST
- Risk Assessment
- CSA STAR
- Central Bank Mandates
- Quantum Security

SISA Institute

Capability Building & Certification

Payment Data Security Programs

- CPISI
- CPISI - Hybrid
- CPISI - Advanced
- CPISI - D

Quantum Security

- CQSP

AI Security

- CSPAI

Certified Payment Privacy Professional (CP3)

SISA is a global cybersecurity leader for the payments ecosystem

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia www.sisa.ai | contact@sisa.ai