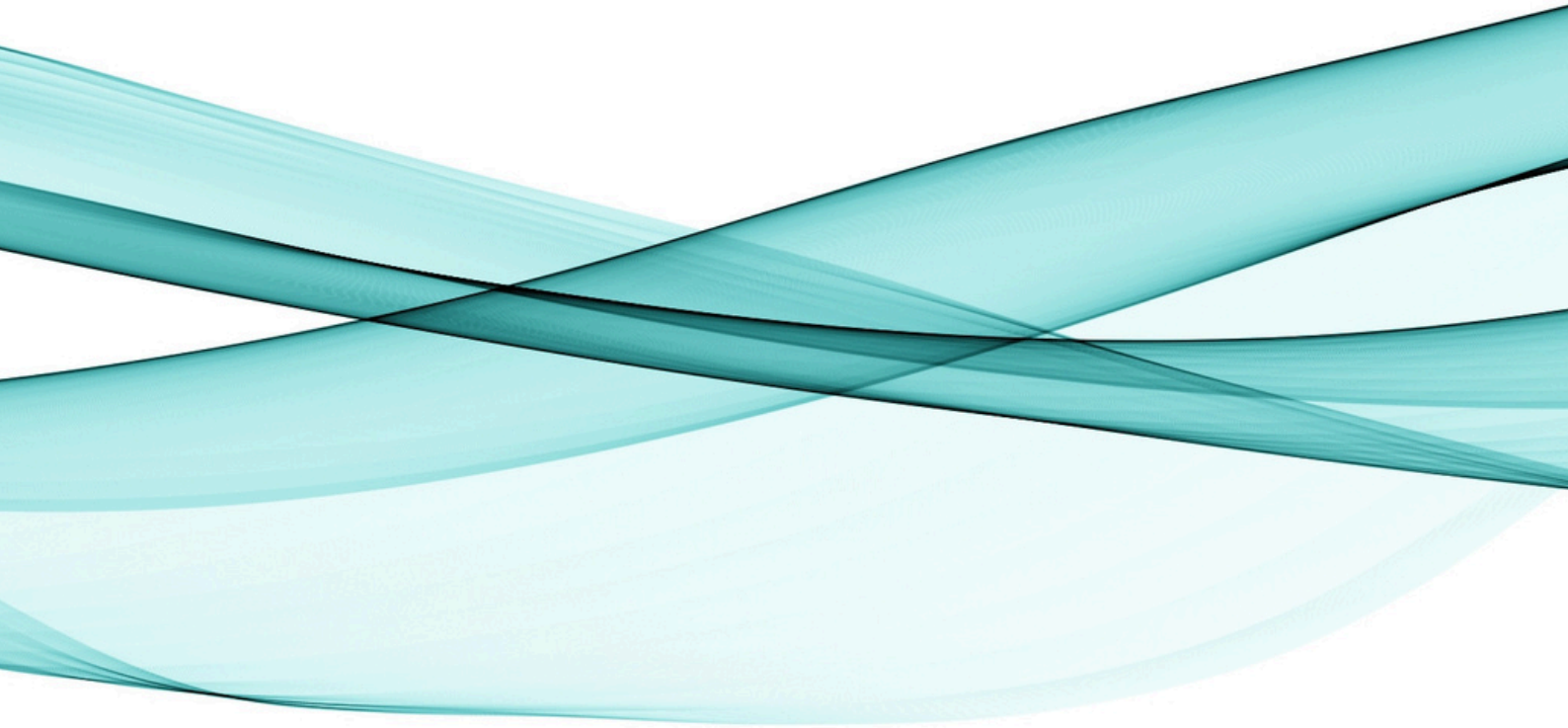




SECURIFY

EDGE UP YOUR SECURITY

White-Label Cybersecurity Report



White-Label Cybersecurity Case Study (USA)

This report outlines how Securify successfully delivered white-label penetration testing and vulnerability assessment services for a USA-based organization under a confidential partnership model. The engagement was completed within the agreed timeline, while exceeding client expectations through additional value-added services.

Scope of Work

- Web Application Penetration Testing
- Network Vulnerability Assessment
- Cloud Security Review
- API Security Testing
- Compliance-Aligned Reporting

Execution Approach

The project followed a structured methodology including reconnaissance, vulnerability scanning, manual exploitation, and post-exploitation validation. All activities were performed in alignment with industry standards such as OWASP and NIST.

Evidence Highlights

- Identified multiple critical and high-risk vulnerabilities
- Demonstrated real-world exploitation scenarios
- Provided proof-of-concept screenshots and logs
- Validated remediation fixes through retesting

Risk Severity Overview

Severity	findings
Critical	2
High	5
Medium	9
Low	6

Outcome & Client Satisfaction

Securify completed the engagement within the defined timeline and delivered comprehensive reporting aligned with client branding. Additional advisory support and remediation guidance were provided, resulting in improved security posture and high client satisfaction.

Conclusion

This engagement highlights Securify's ability to deliver high-quality white-label cybersecurity services for USA-based clients, ensuring trust, compliance readiness, and long-term partnership value.