ZUCI SYSTEMS

Holistic upgrade of the Security Posture for a Technology Fast 500 Fintech institution

CASE STUDY

PENETRATION TESTING FOR FINANCIAL SUCCESS

US-based leading provider of tech-enabled credit products & services for underbanked consumers upgrades its security posture with the help of security penetration testing

PROBLEM STATEMENT

The client is the leading provider of tech-enabled credit products and services for underbanked consumers. Their Chicago based team of technologists developed a next-generation approach to lending, and they were working to envision a world where every individual has opportunities to achieve financial success without being held back by a three-digit credit score.

The client soon realized that in order to become a financial tool for everyone, they must be secure. It is with this ‘security first’ ambition in mind they turned to Zuci to discover security gaps in their suite of loan and credit services.

HOW ZUCI HELPED

Test engineers at Zuci worked closely with the client to identify the vulnerable business use cases

Performed a feasibility study on commercial and open-source penetration testing tools

Carried out broad & targeted scans to identify potential areas of exposure and services that may act as entry points

Devised security best practices checklist

Tech Stack

BURPSUITE

NMAP

KALI LINUX

Nessus 7 Professional

SOLUTION

- Thorough implementation of the following industry-standard penetration testing methods at both web and API levels
  - OWASP: Open Web Application Security Project (OWASP) Testing Guide
  - OWASP: OWASP API Security Top 10 – 2019
  - PTES: The Penetration Testing Execution Standard (PTES)
- Identified all security vulnerabilities using relevant risk rating mechanism
- Ranked each vulnerability based on the severity, loss potential, and likelihood of exploitation
- Recommended solutions for issues which are prone to creating immediate consequences

BUSINESS OUTCOME

- Improved application's overall security posture using the security best practices
- Mitigated each vulnerability with relevant CVE identifiers mapping (Common Vulnerabilities and Exposures)

Vulnerabilities	Risk Level	Ease of Exploit	CVE
Insecure Direct Object Reference (IDOR) to view User Information	Critical	Trivial	CWE-639
Unrestricted access to Spring Boot Actuator Endpoints	High	Moderate	CVE-200
Log Poisoning via HTTP header injection	Medium	Trivial	CWE-113
Password reset token leakage via referrer	Medium	Trivial	–
Missing 'X-Frame-Options' Header (Clickjacking)	Medium	Trivial	CVE-2016-9168

With Security Pentest, address all the security gaps in your application and improve your security posture holistically.

Learn How

Headquarters – Chicago, U.S.
+1 (331) 903 – 5007

Office – Chennai, India
+91 (44) 49525020

www.zucisystems.com

sales@zucisystems.com

ZUCI SYSTEMS