A USA-BASED HEALTHCARE TECHNOLOGY ORGANIZATION STAYS AHEAD OF CYBER THREATS WITH CONSISTENT SYSTEM'S EXPERTISE

Web & Mobile API Collection Security Testing | Case Study

ABOUT THE CLIENT

The client provides a social networking and wellness platform for healthcare employers to improve the mental and emotional well-being of their staff. It helps organizational leadership unlock insights on mental health trends & drivers of burnout on a departmental level so that they support their staff better.

BUSINESS REQUIREMENT

The Client required us to carry out a detailed Vulnerability Assessment and Penetration testing of the API Collection used in their application to examine its security posture.

AUTOMATED TESTING UTILITIES

- ☑ BurpSuite Pro
- ☑ Postman
- ☑ TestSSL

50% Faster Results

40% Lesser Costs

Enhanced API security with OWASP Top 10, NIST & SANS 25 Standards

ENHANCED TESTING METHODOLOGIES COVERED

- Rigorous testing methodologies are employed to safeguard the confidentiality and integrity of patients' health records, ensuring compliance with data privacy regulations such as HIPAA.
- Focus areas include identifying vulnerabilities related to unauthorized access, insecure data transmission, and inadequate encryption protocols to mitigate potential breaches of sensitive health information.

IDENTIFIED SECURITY FLAWS

1. Thorough API-specific functionality testing is conducted to evaluate the security posture of critical endpoints.
2. Specific tests encompass OTP verification mechanisms, examination of upload and download functionalities for vulnerabilities, and validation of access controls to prevent unauthorized access to sensitive data.
3. Systematic analysis reveals weaknesses in access control mechanisms, including Broken Object Property Level Authorization and Broken Object Level Authorization.
4. Unrestricted Resource Consumption issues are addressed to prevent resource depletion attacks and ensure the availability and reliability of the system under varying loads.