CONFIDENTIAL VAPT REPORT V1.0

Vulnerability Assessment & Penetration Testing Report

ZeroDay Shield conducted a comprehensive security assessment of ABC Technologies Inc.'s web application infrastructure between January 1-5, 2026. This controlled penetration testing exercise identified critical security weaknesses that require immediate attention to protect against potential cyber threats and ensure regulatory compliance.

Client	Assessment Period	Overall Risk Level
ABC Technologies Inc.	Jan 1-5, 2026	HIGH

This document contains confidential security information intended solely for ABC Technologies Inc. Unauthorized disclosure or distribution is strictly prohibited.

Sample Report

Executive Summary & Key Findings

Our comprehensive security assessment revealed multiple critical vulnerabilities that pose significant risks to ABC Technologies' digital infrastructure. The findings indicate that immediate action is required to prevent potential unauthorized access, data breaches, and business disruption.

9	2	3	5
Total Vulnerabilities	**Critical Issues**	**High-Risk Findings**	**Days of Testing**
Identified across the application	Requiring immediate remediation	Significant security concerns	Comprehensive assessment period

Business Impact Analysis

Customer Data at Risk

Unauthorized account access could compromise sensitive customer information, leading to privacy violations and loss of customer trust.

Regulatory Compliance

Current vulnerabilities may result in non-compliance with ISO 27001, GDPR, SOC 2, and potentially PCI DSS standards.

Financial & Reputational Damage

Security breaches could result in significant financial losses, legal penalties, and long-term damage to brand reputation.

> **Recommendation:** Immediate remediation of critical and high-risk vulnerabilities is strongly advised to prevent potential exploitation and protect business continuity.

Critical Vulnerabilities Discovered

Our penetration testing identified two critical security flaws that require immediate attention. These vulnerabilities could allow attackers to completely compromise user accounts and access sensitive data without authorization.

Account Takeover via Broken Authentication

Severity: CRITICAL WASP A07

Issue: Improper session handling allows attackers to reuse valid session tokens even after logout, enabling full account takeover.

Impact: Complete unauthorized access to user accounts, data manipulation, and fraudulent transactions.

Proof of Concept: Session tokens successfully reused after logout procedure completed.

- Implement proper session invalidation on logout
- Rotate session IDs after authentication events
- Apply secure cookie attributes (HttpOnly, Secure, SameSite)

Insecure Direct Object Reference (IDOR)

Severity: HIGH | OWASP A01

Issue: Application fails to properly validate user authorization, allowing attackers to access other users' data by manipulating request parameters.

Impact: Unauthorized access to sensitive customer data, privacy violations, and potential data exfiltration.

- Enforce server-side authorization checks
- Validate user ownership for all data objects
- Implement role-based access controls

Additional High & Medium Risk Issues

1

No Rate Limiting on Password Reset

Severity: Medium - Enables account enumeration and spam attacks. Implement rate limiting and CAPTCHA protection.

2

Cross-Site Scripting Vulnerabilities

Severity: High - Allows injection of malicious scripts. Implement input validation and output encoding.

3

Weak Password Policy

Severity: Medium - Increases brute-force attack success. Enforce stronger password requirements and multi-factor authentication.

Remediation Roadmap & Next Steps

Based on our comprehensive assessment using industry-standard methodologies including OWASP Top 10, PTES, and OSSTMM frameworks, we recommend a phased approach to remediation prioritized by severity and business impact.

Immediate Action

0-7 Days

Address all critical vulnerabilities including authentication flaws and access control issues

1

Short-Term Fixes

30 Days

2

Remediate high and medium severity findings, implement security controls and monitoring

Ongoing Security

Continuous

3

Establish periodic re-testing schedule, security training, and vulnerability management program

Testing Methodology & Tools

Security Standards Applied

- OWASP Web Security Testing Guide
- OWASP Top 10 (2021)
- PTES Framework
- OSSTMM Standards

Assessment Tools Used

- Burp Suite - Traffic analysis
- Nmap - Network discovery
- Nessus - Vulnerability scanning
- Manual validation & logic testing

Compliance Impact

Current vulnerabilities may affect compliance with ISO 27001, SOC 2, GDPR, and PCI DSS standards. Remediation will strengthen your security posture and ensure regulatory alignment.

ZDShield Support Services

Our team remains available for validation testing, ongoing security monitoring, and consultation to ensure successful remediation and continuous protection.

Prepared by ZeroDay Shield Security Operations Team

ZeroDay Shield Pvt. Ltd.

Website zdshield.com | Email: info@zdshield.com