# VAPT Case Study

For

# E-commerce Industry Client

## Client Profile:

A major e-commerce platform with millions of active users. a multi-billion-dollar transnational company— is a leading retail conglomerate in the fashion and lifestyle industry. Caters to millions of customers through its extensive network of over 2,200 stores and over 85 brands across 14 countries. Cemented its position as one of the best retail companies in Dubai & United Arab Emirates (UAE) and has extended its operations across the GCC and beyond.

## Challenges Faced by the Client:

- Protecting customer data and payment information.

- Ensuring the security of web and mobile applications.

- Preventing downtime caused by cyber-attacks.

## Solutions Provided by IBN:

- Web Application Testing: Conducted VAPT on the e-commerce platform to identify and fix security vulnerabilities.
- 24x7 Support in cloud: Implemented complex cloud infrastructure and providing continuous monitoring and support for their cloud infra.

- Methodology Used:



- Key Findings

  - Broken Access Control

  - Cross-site request forgery / CSRF, XSRF, one-click attack, session riding.

  - Cross-Domain Misconfiguration.

  - Vulnerable JS Library.

  - Absence of Anti-CSRF Tokens.

## Vulnerabilities by Severity
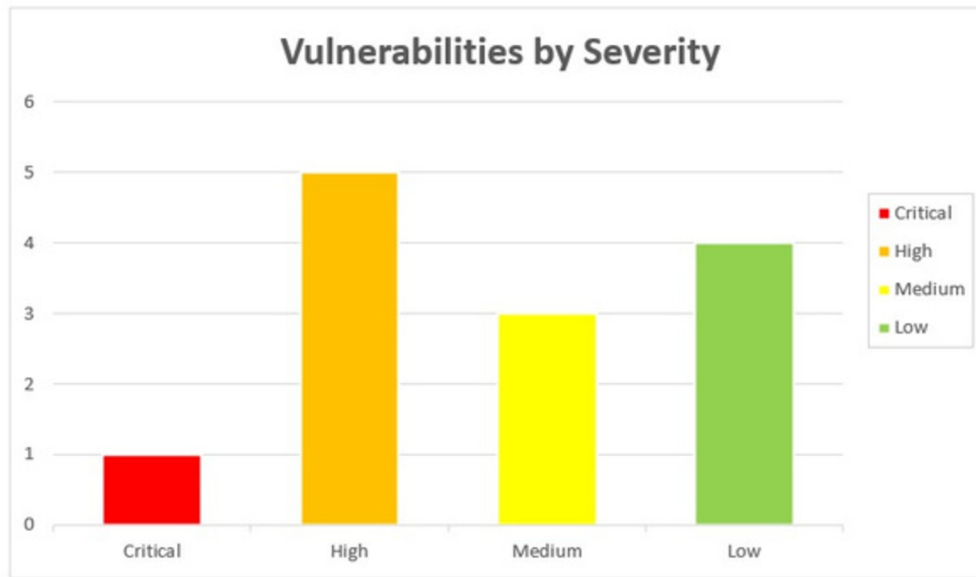


- Technology / Tools Used
    - OWASP Top 10 Standard
    - Nikto
    - BurpSuite
    - Kali Linux
    - Nmap
    - Metasploit
    - DirBuster
    - Custom scripts

- Recommendations and Remediation
    - Continuous Inspection and Testing
    - Limiting CORS Usage
    - Implementation of Role-based Access Control
    - Enable Permission-Based Access Control
    - Enforce Mandatory access control through out the applications, system, IT Infra.

## Benefits Observed from the Client:

- Improved security of customer data and payment information.

- Enhanced reliability and security of web and mobile applications.

Reduced risk of downtime, ensuring a smooth shopping experience for users.