KRATIKAL
SECURE FOR SURE

E-COMMERCE

CASE STUDY

Industry

E-Commerce

Client Background

A well-known internet marketplace for B2B transactions. This company specializes in bringing Indian manufacturers and purchasers together. The company is well-known for being the country's largest online marketplace. Clients can place orders and sell products through the organization's web site (as per demand).

Environment

- One Mobile Application
- One Web Application
- 35 Million + Buyers
- 3 Million + Suppliers
- 43 Million + Products

Business Challenges

- Evaluate the company's mobile and web applications for vulnerabilities.
- Protecting the data of over 3 million suppliers and the user behavior of over 35 million buyers.
- Prevent access to and changes to supplier product and listing data.

Solution

The organization approached Kratikal's security testing department to uncover technical and logical vulnerabilities in their application, as well as to get advice for limiting the risks that could emerge from exploiting those vulnerabilities.

Approach

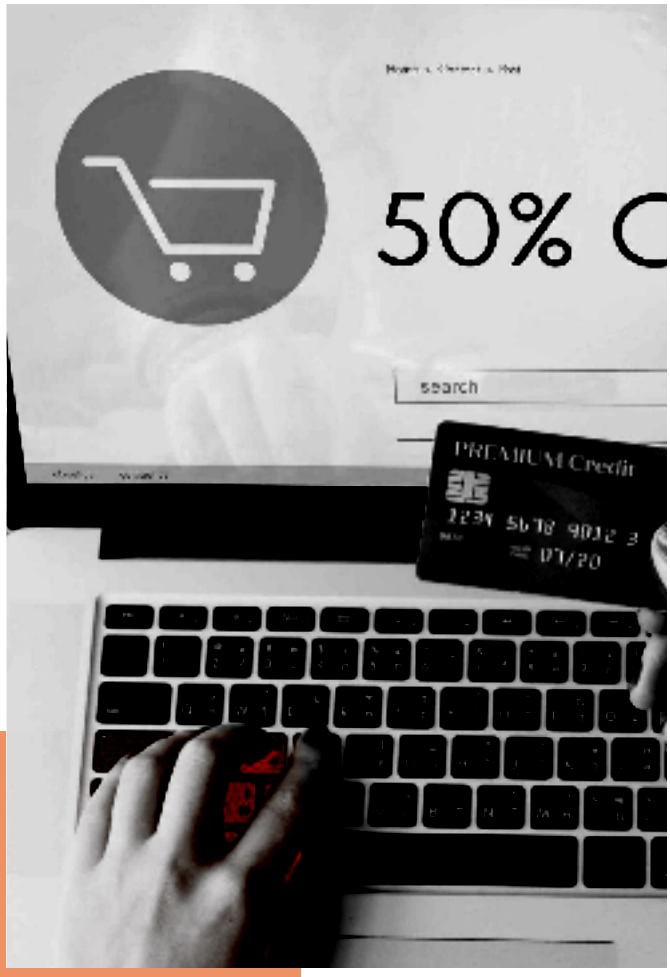
- The experiment was conducted in a simulated environment.
- The test was carried out in a black box environment, with several hacking techniques used to test the application's infrastructure.
- The tests were carried out in compliance with industry best practices, such as the Open Web Application Security Project (OWASP).

Major Findings

- The attackers were determined to be able to replicate the full data base associated with a user's account.
- They can access the supplier's profile information and retrieve all of the information about a certain source, in addition to tampering with the application's database.
- It was revealed that the administrators' login URL could be retrieved via Google Search.
- It was determined that the administrator login page's username and password fields were weak and readily cracked by attackers.

Risks

- If the attackers are successful in exploiting the program and gaining access to the database linked with it, they can abuse the credentials they have obtained.
- Retrieve supplier-related information, it can be tampered for example, they could change the legitimate supplier's contact details and fool the customers, causing harm to both the customers and the suppliers.
- Weak validations on the administrator page, if exploited, could allow the attackers to perform unauthorized actions and make any changes to both the sellers and the buyers.



Impact

- Because the company had a big client base and was widely used, any damage to the program would directly affect all the clients' personal information and businesses.
- The corporation could lose a lot of money, suffer lawsuits, and have its brand image ruined.
- The potential losses from the vulnerabilities, based on rough estimates, totaled USD 1 million.
- All clients who had enrolled in the portal, totaling over 3 million individuals, were impacted.

Recommendations

- In terms of the application, we fixed many critical issues in authentication and authorization processes.
- We recommended significant changes to the database and application server architecture of the application.
- Detailed documentation of the vulnerabilities detected in the web application was provided, outlining the problem, its origin, and solution.
- We advised the organization on advanced controls and cryptographic techniques for database security and server design.

Kratikal Privacy Commitment

Kratikal is dedicated to safeguarding your company from advanced threats, such as data leakage. For this reason, we do not reveal the names of our case study participants.

+91 9289192210
sales@kratikal.com
www.kratikal.com
A-130, 2nd Floor, Sector 63, Noida,
Uttar Pradesh, India-201307