CASE STUDY

INFRASTRUCTURE

Client Background

The client has a B2B background. Their work primarily focuses on developing luxury residential and commercial properties, with a strong emphasis on quality and customer satisfaction. One of the company's most notable projects is a massive master-planned community in Dubai, which features a mix of residential, commercial, and recreational spaces. The project is designed to provide a unique living experience, with a focus on sustainability and community engagement. The company also has a significant presence in the education sector, having partnered with a prominent university to establish a new campus.

Business Challenges

- Assess the Client Web App
- Assess the Web Application Flaw, Employee portal
- Assess the user’s privilege

Environment

- 3 Web App
- 2 IP Machines

Solution

The organization approached Kratikal. Kratikal's security testing experts comprehensively assessed the organization's application to identify technical and logical vulnerabilities. The goal was to uncover weaknesses that could potentially be exploited by malicious actors, and guide on mitigating the associated risks.

Risk

- The attacker can hijack user sessions, and cookies or install malware on the user’s device
- The attacker can do credential theft by injecting fake forms
- An attacker can inject malicious HTML code to modify existing data, such as changing the content of a form or altering the appearance of a webpage

Major Findings

- The attacker injected malicious code into the webpage
- The web app form was vulnerable to HTML injection attacks
- The web app was vulnerable to iframe injection attacks

Our Approach

- We started with threat modeling to check every attack vector.
- Our security analyst is an external user where no special privileges were assigned to the tester.
- Our security analyst tested the application using up-to-date attack techniques to audit the web app based on OWASP & SANS 25 standards.

Impact

- The company has big clients and daily active users any attack on the web app can impact their employee privacy and personal data
- The organization's employee and PII data could have been leaked online or stolen by the attackers
- The organization can face defacement because an attacker can inject malicious HTML code into the website's content.

Recommendations

- Kratikal's security team reported and worked with the developer team to fix multiple server-side validation issues to prevent any unauthorized change to requests going from the client side
- Our security team also guided the client to fix the injection vulnerability by ensuring that all user input including data form, and URL parameters are getting encoded before rendering in HTML or all user inputs are getting escaped.
- We also guided them to implement a Content Security Policy that restricts sources from loading from third-party sites.

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
B-70, Second Floor, Sector-67, Noida(UP), India-201301