KRATIKAL
SECURE FOR SURE

CONSUMER INTERNET CASE STUDY

Industry

Consumer Internet

Client Background

A lifestyle fashion brand launched in 2012 that makes a creative, trendy influence via innovation, honesty, and mindfulness. With a workforce of 400 people and over 8 million products sold, we've come a long way. The product line is current and new, with sales exceeding 1 lakh each item. A direct-to-consumer business strategy enables high-quality clothing to be produced at a low cost.

Environment

- More than 400 members.
- Vertically Integrated, Manufacturer of their own products.
- Direct-to-customer model cuts out the middleman wherever possible.
- High Quality fashion at affordable Prices.

Business Challenges

- Minimize environmental impact while increasing social impact.
- It was difficult to integrate everything from rain harvesting to suitable packaging to employee perks.
- Preventing the application from being exposed to security vulnerabilities.

Solution

The organization approached Kratikal's Managed Security Services division to investigate potential technical and logical vulnerabilities in their Web Application Penetration testing. To devise risk mitigation strategies based on successful exploits of these flaws.

Approach

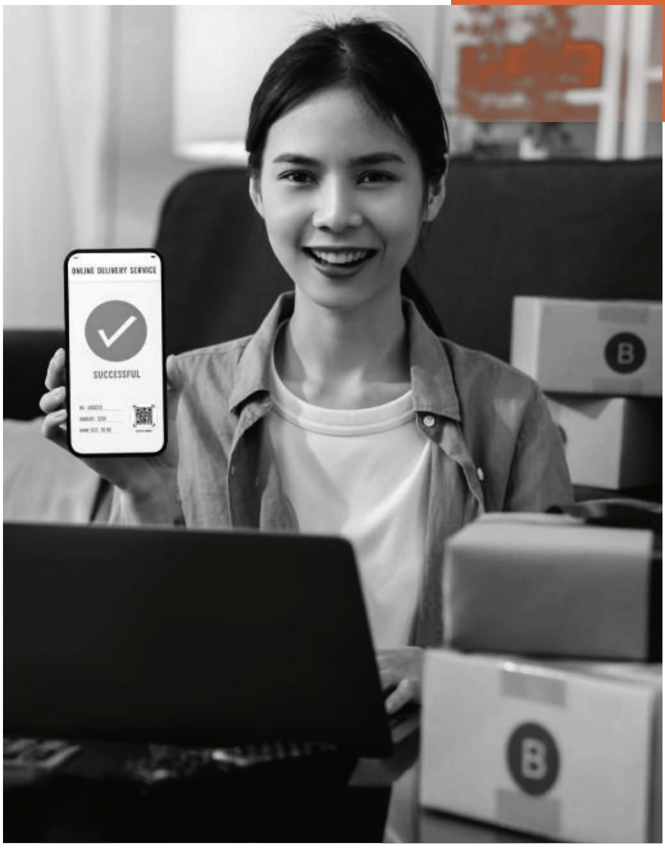
- The test was conducted with best practices industries like OWASP WSTG 4.1 and SANS25.
- The assessment was evaluated in a Grey Box Approach.
- The goal was to determine the impact of a security breach, vulnerability of confidentiality, Integrity, and Availability of protected data.
- Various manual scripts were executed to test their web application.

Major Findings

- The user input was not properly sanitized, and the output was not encoded, resulting in HTML injection.
- There is a Weak Lockout Mechanism, which makes the application vulnerable to brute force attacks.
- A weak password policy was put in place, making the password guessable and brute-force crack able.
- Password change procedure is insecure due to old password bypass, where the password can be changed without knowing the previous password.
- Exit information was not being removed, affecting the whole customer base, and infringing on the privacy of users who upload images to the web application, as well as sharing critical information.
- One of the results was that the password reset link does not expire after being used, allowing unauthorized access to the users' resources.
- Cookie that does not use HTTP Cross-Site Scripting (XSS) is a vulnerability in which an attacker's script code attempts to read the contents of a cookie and exfiltrate the data obtained.
- If the HSTS Header is missing, an attacker will be able to change a valid user's network traffic and bypass the application's SSL/ TLS encryption.
- On the target web application, admin login panels have been discovered. Here an attacker may use the Brute-Force or Dictionary Attack to obtain access to on this functionality.
- Refer Header Policy was not implemented which leads to cross domain referrer leakage.

Risks

- Disclosure of a user's session cookies, which might be used to impersonate the victim or, more broadly, allow the attacker to alter the page content that the victims see.
- The application may be vulnerable to brute force assaults if it has a strong lockout mechanism.
- Users are routed to other malicious websites that are utilized in Phishing and other types of attacks.
- Without knowing the old password, any unauthorized user can get access to the account and change the password.
- The user's privacy is jeopardized because the attacker has access to the details of the other team members.



Impact

- Leaking sensitive client data from their application about their clients and users can result in enormous fines under a variety of compliances and local cyber laws in the countries where they work.
- One may be locked out of your company's critical databases if a successful cyber-attack occurs, with attackers demanding a huge ransom to recover access.
- The attacker might leverage the application's capacity to lead users to fraudulent websites and install malware such as ransomware on their computers and networks.
- A significant impact leading to financial losses, lawsuits, and a tarnished brand image for the company.

Recommendations

- Before transferring the data to the server, it is advised that all input fields sanitize the data.
- After 3 to 5 failed tries, the account should be locked out.
- A mechanism to reset the password, which might be self-unlocking after a period or requiring the intervention of the administrator to be implemented.
- It is suggested that you implement a strong password policy that only accepts passwords with at least 8 characters and at least three of the four-character sets.
- Validating the client-side request and current password is highly recommended.
- To avoid data loss and account takeovers, we advised them to change their application flows.
- The application's vulnerabilities were documented in detail, with explanations of the issue, its cause, and how to fix it.

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