KRATIKAL
SECURE FOR SURE

HEALTHCARE
CASE STUDY

Industry

Healthcare

Client Background

One of the real-time patient engagements, a platform where patients may access transforming complex scheduling processes into easy, people-friendly experiences. They Integrate current system to provide a real time scheduling environment for the patients and the center staff.

Environment

- Operates in Multiple Locations.
- Trusted by some of the biggest firms of IT and healthcare.
- Globally Recognized Industry with several multi-specialty clinics.
- Pan-India Operations must be taken into consideration.

Business Challenges

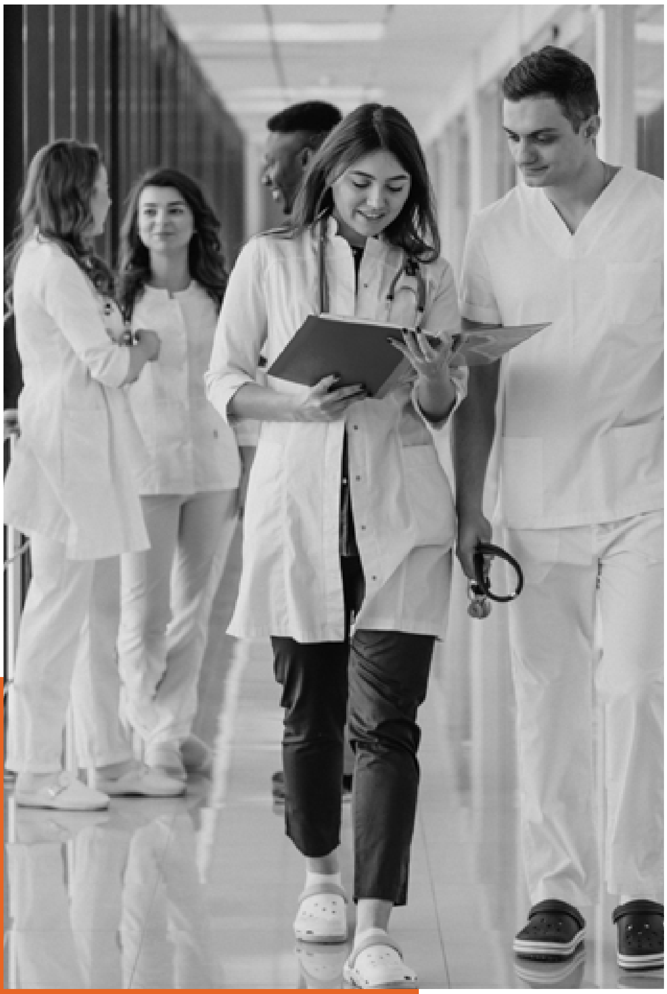
- Protecting the application from being abused to distribute malware.
- Design unique scripts for each device to guarantee that all test scenarios are covered.
- Find a good balance between security best practices and equipment operational issues.

Solution

The healthcare provider sought Kratikal's help in identifying technical and logical vulnerabilities that could jeopardize the operation of its network-connected IOT medical equipment. They also demanded concrete remedies to reduce the risks of exploiting those flaws.

Approach

- The tests were conducted in accordance with the best practices available in the industry, using the experience of Kratikal in Medical Device Security Testing and IOT device testing practices.
- Various hacks were attempted to test the medical devices, the consoles, and the network connection.
- The test was conducted as a Grey Box exercise.
- The tests were carried out in live environment, during times of no traffic on the machine.



Major Findings

- The application is vulnerable to SQL Injection, which is extremely risky when sensitive data is involved.
- Stored Cross Site Scripting (XSS)occurs when data collected from users is not adequately screened, allowing malicious code to run on the website.
- Blind XSS is when an attacker "blindly" deploys a series of malicious payloads on a website in the hopes of saving them in a permanent state and gaining access to them.
- An iframe Injection attack took place, in which iframe tags were placed into a page or other measures were taken to compromise the site visitors' computers.
- HTML injection occurs when a user has control over an input point and can inject arbitrary HTML code into a vulnerable web page.
- DIC can rapidly view or cancel RMI users' appointments by changing the Appointment ID in the request leading to a significant privacy risk to the platform's users.
- The application's logs may reveal sensitive information, which could lead to other attacks.
- The application is vulnerable to a Session Fixation attack, which allows an attacker to hijack a valid user session, compromising the program's confidentiality and integrity.
- CSS Injection is Possible in Application where Injecting code into the CSS context allows the attacker to run JavaScript and harvest sensitive data via CSS selectors.
- The application could be vulnerable to brute force attacks if it doesn't have a strong lockout mechanism, and a malicious user could gain access to sensitive data.
- An outdated version of Open SSL leading to vulnerable attack like Denial of Service, Information Disclosure.

Risks

- A SQL Injection attack can access, change, and execute sensitive database data.
- Data being sent from the device to the mobile interface could be snooped by the attacker.
- An attacker might also infect the machine with ransomware, viruses, or trojans, causing widespread network damage.
- The attacker could hijack the web and mobile interface of the devices.
- A breach of patient data could occur if secure authentication mechanisms are not implemented on IoT interfaces.
- Using the vulnerabilities, an attacker could steal confidential patient records from the systems.

Impact

- Attacker could exploit these vulnerabilities that could lead to life threatening condition for patients.
- Weak BLE and Wi Protocols posed a significant threat to data confidentiality and availability.
- Hijacking of the admin accounts of their application could lead to complete loss of service.
- The corporation could face a lot of financial losses, suffer lawsuits, and have its brand image ruined.
- The attacker might utilize the application's capability to redirect users to malicious websites and install malware such as ransomware on their computers and networks.
- Attacks against vital instruments, especially those dealing with nuclear medicine and radiology, could result in equipment failure in the best-case scenario and unrestrained radiation leakage in the hospital in the worst-case scenario.
- If a successful cyber-attack occurs, you may be locked out of your company's critical databases, with attackers demanding a large ransom to regain access.

Recommendations

- It is advised to constrain and sanitize input data by validating type, length, format, and range.
- “All input fields” must sanitize the input given to them before sending it to the server.
- To avoid loading any external website in the iframe, sanitize the user input before submission and add suitable HTTP Response Headers according to the application's requirements.
- It is advised to employ a per-user or per-person session to prevent attackers from directly targeting approved resources.
- It is recommended not to create logs of sensitive information like username, password, etc. of the users.
- It is advised that no sensitive information be made public, and those directory listings are restricted in the webserver setup.
- Before embedding user input in CSS blocks, make sure it's properly escaped, and use a whitelist to prevent arbitrary style files from loading.
- After 3 to 5 failed tries, the account should be locked out. Also, after being locked out, there should be a mechanism to reset the password, which might be self-unlocking after a period or requiring the intervention of the administrator.
- Vulnerabilities in the application are documented in detail was provided, along with an explanation of the problem, its origin, and how to fix it.
- It is recommended to not keep the files like setup.php publicly accessible.
- We recommend removing EXIF data from any new uploads as well as from existing uploads.

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.