CASE STUDY

Briskinfosec secured

IOT Solutions for A Leading Manufacturing Sector

INDUSTRY
Information Management Company

STANDARDS
OWASP, PTES, SANS, NIST, ISO27001, PCI-DSS

PRIMARY SECTOR
Manufacturing Sector

LOCATION
Worldwide

OFFERED SERVICE
IOT Security Assessment

TYPE OF SERVICES : **IOT Security Assessment**
(Internet Of Things)

ABOUT CUSTOMER

Our Stakeholders in the IOT domain face privacy issues, most of the time being unaware of the situation. As such, IOT devices have come under increasing levels of scrutiny in recent months over poor security controls and numerous vulnerabilities.

ASSESSMENT SCOPE

IOT testing consist of two types of testing static and dynamic testing. Static testing is the most frequently implemented process. But static testing is not intended or designed to find vulnerabilities that exist in the 'off the shelf' components such as processors and memory into which the application will be installed.

Dynamic testing, on the other hand, is capable of exposing both code weaknesses and any underlying defects or vulnerabilities introduced by hardware and which may not be visible to static analysis. Also, dynamic testing often turns out to be a more pragmatic way of testing the IOT devices and plays a pivotal role in finding out vulnerabilities that are created when new code is used on old processors. As such, manufacturers who purchase hardware and software from others must do dynamic testing to ensure the items are secure.

THE SOLUTION

By using our Briskinfosec's team of security engineers, IOT security test was completed using the IOT Security Standards

Key highlights of the IOT security test are as below :

- Serious issues related to IoT testing like Input validation, Injection attacks, IoT based vulnerabilities, Hardware based vulnerabilities were identified and then fixed which was given to the development team.

- We completely secured the web application of IoT endpoints from OWASP common attack by hardening the default application configuration.

- We performed vulnerability assessment by the usage of both automation and manual scanning tools for identification of the issues in IoT application and Hardware based.

- Proxy-based tools like Burp Suite Pro, Fiddler and Networking tools are used for effective security assessment.

- We provided the complete bug fixing document as a reference to the client's development team.

TECHNICAL SECURITY ASSESSMENT REPORT

End of security assessment we have identified 35 potential security vulnerabilities and documented technical security assessment report with proper POC and share the same over protected PDF.

ISSUE TRACKING SHEET

All the identified issues were captured and will the be subjected for the retest review in an XLS format.

FINAL BUG FIX REPORT

Overview of the entire engagement we have conducted retest on fixed issues and captured open issues which exist on the application.

CHALLENGES

By conducting a complete IOT security test, we faced some unforeseen difficulties due to the complexity of the IOT endpoints workflow of the organization's application. Due to this, the assessment process consumed much time for thoroughly testing every endpoint. However, with sheer grit, BriskinfoSec triumphantly reduced the risks of sensitive user data through the usage of secure IOT's

THE DELIVERABLE

Briskinfosec security assessment report and remediation information provided were customised to match the Client's operational environment and development framework. The following reports were submitted to the customer.

Key highlights of the IOT security test are cited below :

DAILY STATUS REPORT

This security assessment consumed around 1-2 weeks of time including retest. We have shared all identified issues with corresponding recommended FIX over mail on a daily basis. Our prospect look at these valid report (XLS) and start working the fix from DAY 1 as they no need to wait for final security assessment report to work on the same.

RISK BENEFITS

Briskinfosec reduced security risks by assessing the customer's infrastructure vulnerabilities and recommended solutions with proven methods for enhancing IOT security.

COST SAVINGS

Briskinfosec suggested cost-effective measures based on the customer's business requirements that ensure security and continuity of their business.

CUSTOMER SATISFACTION

IOT security testing was conducted with minimum interruption and damage across customer systems to identify security vulnerabilities, impacts, and potential risks.

SUPPORT

We provide 1year support with periodic security assessment.

CONCLUSION

We advised the Stakeholder on the measures they should take for rectifying the various vulnerabilities in Web applications and IOT endpoints. To improve IoT manufacturing process, we have educated in-house developers about the different mandatory methods, Best practices such as the monitoring of their web applications daily, about the encryption of Data's that are to be sent to other distant places and most significantly emphasizing them about the need to properly train the developers with quality training. We also worked closely with our Stakeholder to improve policies, procedures and employee awareness programs for increasing security maturity.

BRISKINFOSEC

TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com