CASE STUDY

Briskinfosec secured Database for The Largest Financial Company In Asia

INDUSTRY
Trade Industry

STANDARDS
PTES, SANS, NIST, ISO27001

PRIMARY SECTOR
Financial Company

LOCATION
Asia

OFFERED SERVICE
Database Security Assessment

TYPE OF SERVICES : **Database Security Assessment**
(for a Trading leader)

ABOUT CUSTOMER

Our stakeholder provides an artificial intelligence (AI) platform that matches corporate executives with the institutional investors who are most likely to buy or sell their stock in the next 90 days. Simultaneously, they offer all users data discovery technologies to efficiently prepare for all types of corporate-investor access events. They are a financial technology company combining machine learning analytics with workflow optimization software to make access events such as non-deal roadshows (NDRs) and broker conferences, more efficient and actionable. They also offer services to the entire capital market, including corporates, investors and brokers.

ASSESSMENT SCOPE

To find the vulnerabilities in the Database, our Stakeholder wanted us to conduct a proactive Penetration test to find any loopholes in Database for hackers to gain access. So, an URL was given directly for scanning vulnerabilities. The kind of testing executed was Grey Box Testing, a testing with credentials provided. The Database which we scanned was My SQL Database type. Most importantly, our ultimate goal was to make the Database secure from any vulnerability that may compromise their data's.

THE SOLUTION

Briskinfosec followed standards like Open Web Application Security Project (OWASP) TOP 10 and My SQL guidelines for identifying all the exposed vulnerabilities in the Database. BriskInfosec's security team thoroughly tested the Database. Post-testing, we have cited the key highlights.

Key highlights of the vulnerability fix are as below :

- Serious issues related to Input validation, Injection attacks, Sensitive Data Exposure and Clickjacking attacks were identified. The identified issues were then fixed by the Development team.
- We completely secured the Database from common threats by hardening the default configuration.
- Privilege escalation was found.
- We figured out default configuration related vulnerabilities.
- The detected vulnerabilities were of both critical and high severities.
- We performed vulnerability assessment by both automation and manual method of identifying the issues.
- We provided the complete vulnerability fixing document as a reference to your development team.

THE DELIVERABLE

The reports and remediation information provided were customized to match the Stakeholder's operational environment and development framework. The Data's were also consolidated and then given. The following reports were submitted to the customer.

Key highlights of the bug fix are as below :

DAILY STATUS REPORT

This Database security assessment consumed around 1-2 weeks of time including retest. During the process of Database security testing, issues were identified and we shared all identified issues with corresponding recommendation Fix over mail on a daily basis. Our prospect looked at the given valid report (XLS) and started working the fix right from Day 1 as they need not work laboriously on the last day when the entire report is given by the security team thus making their final assessment report easier for preparation.

ISSUE TRACKING SHEET

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

WORKFLOW REPORT

Every process was carried out by the entire team without ignorance of anything.

FINAL BUG FIX REPORT

Overview of the entire engagement, the issues identified and the recommendations made to mitigate the same.

THE CHALLENGE

During Database security Assessment, issues were identified because of which there disruptions during testing. Due to this inconvenience, we were unable to access certain credentials with restricted user privilege experienced by our security team. As Database assessment is very new, it was also an opportunity for us to explore and procure more wisdom in that area which consumed more time but most importantly aided in broadening our Horizons. However, with an untiring perseverance and a "Never Give Up" attitude, BriskInfosec successfully reduced the Stakeholder risks of their Database becoming amicable to breaches.

RISK BENEFITS

BriskInfosec diminished security risks by assessing the customer's infrastructure vulnerabilities and recommended solutions with proven methods to enhance security.

COST SAVINGS

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

CUSTOMER SATISFACTION

Database security assessment 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 educated our Stakeholder on the measures to be taken for remedying the various flaws in their Database. For remediation, we educated them about the mandatory processes such as the monitoring of their database daily, educating the need to remove the unwanted testing database, insisting on disabling the default user and most significantly emphasizing them about the need to tighten their security to cult Quality. Also, we insisted them that their day to day networks to be segregated from the network storing sensitive personal information. We also worked closely with our Stakeholder to improve their policies, procedures and employee awareness programmes to increase their security maturity.

BRISKINFOSEC

TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com