CASE STUDY

Briskinfosec secured

Top Software Development Company's Website

INDUSTRY
Software Development

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

PRIMARY SECTOR
Software

LOCATION
Middle East

OFFERED SERVICE
Penetration Test

TYPE OF SERVICES : **Website Security Assessment**

ABOUT CUSTOMER

Our stakeholder offers Strategic IT consulting and Managed Solutions to Technology companies.They have transformed over the years from a plain contract staffing service provider into a leader in Consulting for myriad technologies ranging from application development using Open Source, Microsoft, Java and Mainframe technologies to state of the art SMAC technologies. They have been the pioneer all over Globe providing the highest ethical standards of service. They operate across eight major cities in India apart from the overseas operations. Their scale of capabilities, offerings and customer engagements in the IT & ITES domain differentiates them from other companies in the consulting and recruitment vertical.

ASSESSMENT SCOPE

To find the vulnerabilities in the Website, Stakeholder wanted us to conduct a proactive website Penetration test to find any loopholes in Website for hackers to gain access. So, an URL was given directly for scanning vulnerabilities. The kind of testing executed was Black Box Testing, testing without credentials. Most importantly, the ultimate goal was to make the website free from any vulnerability that may compromise their site.

THE SOLUTION

Briskinfosec followed standards like Open Web Application Security Project (OWASP) TOP 10 and Application Security Verification Standards (ASVS) to identify all exposed vulnerabilities in the Website. BriskInfosec's security team completely tested the Website

Key highlights of the bug fix are as below :

- Serious issues related to Input validation, Injection attacks, Sensitive Data Exposure and Clickjacking attacks were identified. The Development team then fixed the identified bugs.

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

- 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.

- OWASP ASVS (APPLICATION SECURITY VERIFICATION STANDARD) was also shared without failing.

TECHNICAL SECURITY ASSESSMENT REPORT

Complete security testing was carried. All the detected issues and the proof of concept (POC) will be covered with detailed steps in a PDF format.

ISSUE TRACKING SHEET

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

OWASP ASVS

(APPLICATION SECURITY VERIFICATION STANDARD) was shared.

THE CHALLENGE

During Vulnerability Assesment, a stunning number of functional issues were identified because of which there were many restrictions and disruptions during testing. Due to this inconvenience, we were unable to access certain credentials with restricted user privilege experienced by our security team. However, with dexterous perseverance, Brisk Infosec reduced the Stakeholder risks of their site being visible to breaches.

THE DELIVERABLE

The reports 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 bug fix are as below :

DAILY STATUS REPORT

This website security assessment consumed around 1-2 weeks of time including retest. During the process of website 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.

RISK BENEFITS

Brisk Infosec 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

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

CONCLUSION

We educated our Stakeholder on the measures to be taken for remedying the various flaws in their systems and processes. For remediation, we educated them about the mandatory processes such as the monitoring of their website daily 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.

BRISK INFOSEC

CYBER TRUST & ASSURANCE

BRISKINFOSEC

TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com