CASE STUDY

Briskinfosec secured Web Application for **One of The Prevalent Workforce Solution in Singapore**

INDUSTRY
Workforce Solution

STANDARDS
OWASP, PTES, SANS, NIST, OSSTMM

PRIMARY SECTOR
HR

LOCATION
Singapore

OFFERED SERVICE
Penetration Test, Security Assessment

TYPE OF SERVICES : **Web Application Security Assessment**
(for a Wrokforce Solution Company)

ABOUT CUSTOMER

Our Stakeholder is a unique HR Solutions Company who embarks on a journey to reinvent the way HR Technology and Services are delivered by providing high-value solutions that are client-focused, flexible and easily integrated across the global HR value chain. They have built that strong foundation and 25-year heritage with technology enhancements, highly skilled collaborative teams, and an end-to-end consultative approach that ensures full understanding of their business drivers, organizational goals, and HR service delivery environment to provide solutions that maximize return on investment.

ASSESSMENT SCOPE

Our Stakeholder provided us with an URL and IP address directly to perform security assessment for assessing and fixing the threats and vulnerabilities in the Web application and Network Devices (IP) of the Organization and to remove them. As a result of the security assessment, all the Stakeholder's applications and devices were free from vulnerabilities and threats that may compromise the application.

THE SOLUTION

Briskinfosec followed Open Web Application Security Project (OWASP Top10) unique framework and Penetration Testing Execution Standards (PTES) to identify all the hidden vulnerabilities. By using these frameworks, the security team completed the Web Application and Networks Security Assessment and Vulnerability fix

Key highlights of the Vulnerability fix are as below :

Serious issues related to Input validation and authorization, session management and cookies handling were identified. The identified vulnerabilities were fixed by the Development Team.

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.

We provided complete security assessment to their network devices based on the standards such as Penetration testing execution standards (PTES) and National Institute of standards and technology (NIST).

TECHNICAL SECURITY ASSESSMENT REPORT

By the completion of security assessment, we have identified a whopping quantity of more than 30 potential security vulnerabilities. The identified vulnerabilities were then documented by technical security assessment report along with proper POC, and also we shared the same through protected PDF.

ISSUE TRACKING SHEET

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

OWASP ASVS

(APPLICATION SECURITY VERIFICATION STANDARD) was shared.

FINAL BUG FIX REPORT

Docket of the entire engagement, the issues that are identified, the recommendations and remediation are made to mitigate the detected threats.

THE DELIVERABLE

The reports and remediation information provided were customized to match the Stakeholder's operational environment and development framework. The following reports were submitted to the customer: Key highlights of the Vulnerability fix are as below :

DAILY STATUS REPORT

This security assessment consumed around 1-2 weeks of time including retest. During the process of testing, issues were identified and we shared all the 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

THE CHALLENGES

During the assessment, we were provided with limited user privileges. With it, we faced complications like the inability to access the credentials of certain confidential contents, crashing of certain applications during security testing and the persistence of intermediary problems which caused denial of access to the destination. But with sheer grit, Briskinfosec triumphantly completed the security assessment

RISK BENEFITS

BriskInfosec alleviated the 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

Web Application and Networks vulnerability fix were 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 to be taken for remedying the various deficiencies in systems and processes. For remediation, we educated them about the various mandatory processes such as the monitoring of their web applications and scanning Networks 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. Also, we insisted on them that their day to day networks are 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