Briskinfosec secured
Reviewed Source Code Of Largest Technology Innovator

INDUSTRY	STANDARDS	PRIMARY SECTOR
Technology Consultant	OWASP, SAST, SSDLC	Content Service Company

LOCATION	OFFERED SERVICE
APAC	Secure Source Code Review

TYPE OF SERVICES : **Secure Source Code Review**

ABOUT CUSTOMER

Our Stakeholder is one of the leading Content service providing company throughout the globe. They have more than 1500 employees in the organization. Their technology platform is synthesized with deep understanding of content workflows and data structures that prefers them to be the partner of choice for many leading information companies. They have been the pioneer all over the globe providing their highest ethical standards of service.

ASSESSMENT SCOPE

For fixing the bugs in the content of source codes, the Client wanted us to conduct a proactive, secure source code review. So, we followed the process of static analysis code review. It is the process of checking every programming language using a suitable tool accordingly. It was important that their Source Code is free from vulnerabilities that may compromise their Internal Codes.

THE SOLUTION

The security professionals of Briskinfosec completed the bug fixing in source code using standards like OWASP secure code review and SSDLC.

Key highlights of the bug fix are as below :

- Serious issues related to Injection attacks, Password disclosure and buffer overflow issues were identified. The identified bugs were then fixed by the Development Team.

- We completely secured the Source codes from OWASP common attack by hardening the default configuration.

- We performed vulnerability assessment by using both automation and manual methods for identifying the issues.

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

ISSUE TRACKING SHEET

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

FINAL BUG FIX REPORT

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

THE CHALLENGES

During testing, a lot of false positives were traced and identified. After identification, the false positives were subjected to infiltration for error rectification. Also, bugs in various Web applications persist due to improper codes. Like the phrase ("calm after storm"), with dedication and determination, Briskinfosec successfully reduced the Client's risk exposure where securing the Content service Bodies are taking an extremely strict approach to security.

THE DELIVERABLE

The reports and remediation information provided were customized 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 below :

DAILY STATUS REPORT

This security assessment consumed around eight days for Two million Lines of the code to detect the flawed codes. During the process of testing, improper codes were identified, and we shared all identified issues with corresponding recommendation Fix over mail on a daily basis. Our prospect looked at the given accurate 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.

TECHNICAL SECURITY ASSESSMENT REPORT

Complete security testing was carried out. All the detected issues and the proof of concept (POC) will be covered with detailed steps in a PDF format. All identified issues are highlighted with the Line number of each issue.

RISK BENEFITS

Briskinfosec declined various security risks by assessing the customer's infrastructure vulnerabilities and recommending solutions with proven methods to enhance security

COST SAVINGS

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

CUSTOMER SATISFACTION

Secure Source code review test 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 rectifying various errors in their codes. We have recommended using Secure SDLC process for limit source code vulnerabilities. For remediation, we also educated them about the various mandatory processes such as the monitoring of their 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 train the developers secure coding. We also worked closely with our Stakeholder to improve policies, procedures and employee awareness programmes for increasing security maturity.

BRISK INFOSEC

CYBER TRUST & ASSURANCE

BRISKINFOSEC

TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com