Briskinfosec secured

Largest Marketing Cloud Application

INDUSTRY	STANDARDS	PRIMARY SECTOR
Marketing Service	OWASP, PTES, ISO27001, ITIL, ASVS	Commercial Marketing

LOCATION	OFFERED SERVICE
APAC	Penetration Test

TYPE OF SERVICES : **Cloud Application Marketing Services**

ABOUT CUSTOMER

Our Stakeholder is one of the leading Commercial Marketing agents throughout the globe. They are one of the mightiest forces which drive higher sales and market share for consumer goods manufacturers and retailers around the world. They are the nation's leading agency for food and non-food manufacturers, distributors and other operators across all away-from-home meal channels. More than 12000+ employees are working in the Organization. They are also the sales and marketing powerhouse behind the most recognised brands and a proven resource for top retailers all across the U.S. and Canada providing flexible solutions backed by talent, technology, reach and relationships. They have been the pioneer all over the globe providing their highest ethical standards of service.

ASSESSMENT SCOPE

To fix the vulnerabilities in the cloud application, the Stakeholder wanted us to conduct a proactive Cloud application security testing. As the given application was an internal web application, the testing will be done by SAAS (security as a Service). The IP's of the application was given, and the ultimate goal was to ensure that the cloud application is free from vulnerabilities that may compromise the application.

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 by using frameworks.

Key highlights of the vulnerability fix are as below :

- Serious issues related to Input validation and authorisation, session management and cookies handling were identified, and the Development Team fixed the identified bugs.

- Platform level vulnerabilities were identified in the cloud application safeguarding the Source code of the application.

- We completely secured the cloud application from most common attacks by hardening the default configuration.

- We performed vulnerability assessment by both automation and manual method of identifying the issues.

- We provided the complete bug fixing document as a reference to your development team.

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 a XLS format.

FINAL BUG FIX REPORT

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

OWASP ASVS

Application security test was executed with the respective of OWASP ASVS (APPLICATION SECURITY VERIFICATION STANDARD) and Issue mapping sheet was shared along with security assessment report.

CHALLENGES

During vulnerability assessment, there were many challenges faced by our technical team. The challenges are cited below :

- Since the application was hosted in cloud, we couldn't directly access the application.
- We had to procure permission from 3rd party groups as they were also a part of it.

THE DELIVERABLE

The reports and remediation information provided were customised to match the Stakeholder'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

During the process of security testing, issues in cloud application 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.

- We had to get then their authentication and approval for the measurement of not being a stranger accessing their applications but trusted and officially hired security team from Briskinfosec.
- Only after this, we had to proceed with the security testing process.
- One IP address was mentioned for testing. Only with that IP, our team was allowed to access the cloud applications.
- If we used other area's for testing which isn't customised under that mentioned IP, then it becomes a breach against ethical service.

Because of this, too much of time was consumed to scan every part of testing process.
But with perseverance and sheer grit, Briskinfosec completed the vulnerability assessment and reduced the vulnerabilities.

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

Cloud-based Web-Application security testing was conducted with minimum interruption and damage across other customer systems to identify security vulnerabilities, impacts, and potential risks.

SUPPORT

We offering 1year support with periodic security assessment review to keep customer stay and secure.

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 necessary procedures such as the monitoring of their cloud applications daily and most significantly emphasising them about the need to tighten their security to cult Quality. We also insisted them to implement Web Application Firewall (WAF) for hardening their firewall and making it stronger. We then advised them to enhance log monitoring for security purposes. Also, we insisted them that their day to day networks to get segregated from the system storing sensitive personal information. Finally, we worked closely with our Stakeholder to improve 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