Briskinfosec secured API's of **Largest Wealth Management Industry**

INDUSTRY	STANDARDS	PRIMARY SECTOR
Wealth Management	OWASP, PTES, SANS, NIST, ISO27001, PCIDSS.	Financial Sector

LOCATION	OFFERED SERVICE
Worldwide	API Security Assessment

TYPE OF SERVICES : **API (Application Program Interface) Security Assessment**

ABOUT CUSTOMER

Our Stakeholder is one of the leading Insurance service company throughout the globe. They are a potential leader in Wealth Management system WMS. They maintain a vast mutual fund dealer system using EWMS. There are more than 1000+ employees in the organisation. Through sheer perseverance, they have grown as one of the dignified software firms in the financial service sector throughout the Globe.

ASSESSMENT SCOPE

Our Stakeholder provided us with the web application to be tested directly with login credentials to carry out grey box security assessment. Our primary goal is to successfully perform a complete Security Assessment VA/PT on their Application Program Interface (API) endpoints of web application flowing between client and server. The Client wanted us to conduct a complete grey-box API Penetration test and then fix the bugs for their internal and external web applications which were done by using the API endpoints. The client has also provided us with the API documentation for proactive testing.

THE SOLUTION

By using our BriskInfosec's team of security engineers, API security test was completed using the OWASP and SANS Standards.

Key highlights of the API security test are as below :

- Serious issues related to API testing like Input validation, Injection attacks and API based vulnerabilities were identified and then fixed which was given to the development team.

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

- We performed vulnerability assessment by the usage of both automation and manual scanning tools for identification of the issues.

- Proxy-based tools like Burp Suite Pro, Fiddler and OWASP ZAP proxy tools are used for effective security assessment.

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

TECHNICAL SECURITY ASSESSMENT REPORT

At the end of the security assessment, we have identified 35 potential security vulnerabilities and then documented technical security assessment report with proper POC, and also we shared the same over protected PDF.

ISSUE TRACKING SHEET

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

REASSESSMENT REPORT

Overview of the entire engagement we have conducted retest on fixed issues and captured open issues which exist on the application.

CHALLENGES

By conducting a complete API security test, we faced some unforeseen difficulties due to the complexity of the API endpoints workflow of the financial application. Due to this, the assessment process consumed much time for thoroughly testing every endpoint. However, with sheer grit, BriskInfosec triumphantly reduced the risks of sensitive user data through the usage of secure API's.

THE DELIVERABLE

Briskinfosec security assessment report 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 API security test are cited below :

RISK BENEFITS

BriskInfosec reduced security risks by assessing the customer's infrastructure vulnerabilities and recommended solutions with proven methods for enhancing security

COST SAVINGS

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

CUSTOMER SATISFACTION

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

SUPPORT

We are offering 1year support with a periodic security assessment.

CONCLUSION

We advised the Stakeholder on the measures they should take for rectifying the various vulnerabilities in Web applications and API endpoints. While building the API or web services, the organisation should also implement a secure SDLC process from the initial operation of API implementations. We have educated in-house developers about the different mandatory methods, Best practices such as the monitoring of their web applications daily, about the encryption of Data 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. We also worked closely with our Stakeholder to improve policies, procedures and employee awareness programs for increasing security maturity.

BRISK INFOSEC
BAN RISK IN INFORMATION BY SECURITY KINGS

BRISKINFOSEC
TECHNOLOGY AND CONSULTING PVT LTD

+91-8608634123
044 - 43524537

contact@briskinfosec.com
www.briskinfosec.com