CASE STUDY

Aspire's Vulnerability Assessment and Penetrative Testing solution fixed Application security issues for a leading FinTech player

aspire SYSTEMS

attention. always.

Challenges:

- *Application lacked a security evaluation*
- *No clarity on vulnerability of application to security attacks*

Solution:

- *Application was screened for vulnerabilities from OWASP's security risks check list*
- *Checks were performed with automated scanner and manual penetration test*
- *Application was re-tested after remediation to ensure all reported vulnerabilities fixed*

About The Customer

Our customer offers a scalable web-based solution that incorporates an Insurance-Tech ecosystem to manage the full lifecycle of their client's (re)insurance operations. The customer's application is an all-encompassing software covering client management, underwriting, claims, accounting, reporting and retroceding to optimize their client's business for efficiency.

The Need

Our customer had the following business needs to:

- Uncover potential security gaps and vulnerabilities in the application
- Provide solid security protection

The Challenges

Meanwhile, they faced the following business challenges:

- Lack of security evaluation of the application
- Faced uncertainty on the type and depth of vulnerability of the application to security attacks

Benefits:

- *Achieved the cyber security compliance objectives*
- *Reduced the exploitation risks of application*
- *Identified and plugged the data leaks found*
- *Uncovered the Security issues*

Aspire's Solution in Detail

Aspire's Performance testing experts understood the customer's needs and challenges and came up with a quick and comprehensive Vulnerability Assessment and Penetrative Testing (VAPT) solution. The security assessments were standardized in line with globally recognized Open Web Application Security Project (OWASP)'s Top 10 vulnerabilities and SANS-25 software errors.

- A series of non-intrusive tests were performed to gather information and perform technical reconnaissance
- Appropriate tools were selected and a series of deep-dive tests were performed on the application portal
- Comprehensive checks were done through automated scanner followed by manual penetration tests
- The application was screened for all the vulnerabilities from OWASP's security risks check list
- A detailed audit and test report with problems detected and recommendations on remediation was given to the customer
- An additional round of re-testing was performed to ensure all the reported vulnerabilities were fixed

Technology Snapshot

- Burp Suite Professional
- Kali Linux Tool Sets
- Custom Scripts
- Burp Add-ons

Benefits

- Security issues of Critical, High and Medium intensity were uncovered through a well-crafted approach
- Data leaks were found and fixed by deploying appropriate vulnerability remediation
- The risk of application being exploited was reduced which made the application robust
- The objectives of cyber security compliance were achieved

Aspire Systems is a global technology services firm serving as a trusted technology partner for our customers. We work with some of the world's most innovative enterprises and independent software vendors, helping them leverage technology and outsourcing in our specific areas of expertise. Our core philosophy of "Attention. Always." communicates our belief in lavishing care and attention on our customer and employees.

For more info contact: info@aspiresys.com or visit www.aspiresys.com

USA
+ 1 630 368 0970

SINGAPORE
+65 3163 3050

INDIA
+91 44 6740 4000

UK
+44 203 170 6115

NETHERLANDS
+ 31 (0)30 800 92 16

POLAND
+48 58 732 77 71

MEXICO
+52 222 980 0115