

Penetration Testing on Web, Network and Cloud for a BFSI major

Client

Our Client is a leading player in the Banking, Financial and Insurance Services (BFSI) space (USA and worldwide).

Key Challenge

The Client was in the process of building a secure online insurance service provider. They contacted us for performing security testing across the various components of their services. The nature of the engagement was to conduct a multitier architecture web application security assessment that included:

1. AWS Cloud
2. Network
3. CMS
4. Umbraco
5. Amazon (AZ) Connect
6. Salesforce Marketing Cloud
7. Accenture Insight Platform
8. NFC
9. Matillion
10. Amazon Redshift

Solution

The information security experts from QA InfoTech's security testing team used a unique in-house developed methodology and an application driven framework, specific to BFSI. The team completed the Web Application Security Assessment and penetration testing against all the various components and reported multiple critical vulnerabilities.

Key highlights of the security assessment are outlined below:

1. Attack Surface Mapping of the entire application with every detail of the URLs, parameters, components and IPs that are being used in the application.
2. Test cases were created based on the BFSI application specific vulnerabilities such as Price tempering, Checksum related flaws, Security misconfiguration, payment integration flaw, Access control flaws etc. in conjunction with various sections that were mapped
3. Security testing conforming to OWASP top 10 and severe business logic vulnerabilities for web, cloud and network interface.
4. Automated scans using various commercial scanners
5. Test case verification by manually confirming each of the potential test cases identified above

Vulnerability correlation

QA InfoTech team educated the application owner about the risks and created a risk mitigation plan. The first cycle of the engagement involved identifying all the vulnerabilities in the client's website. Subsequently, the engineers leveraged the known vulnerabilities to further penetrate the client's application architecture and identify the true impact of the vulnerabilities.

The Deliverables

The reports and remediation information provided were customized to match the client's operational environment and development framework. The following reports were submitted:

- 1. Daily Execution Summary Report:** Details of the vulnerabilities identified during the day and progress of execution on a daily basis on Microsoft's VSTS vulnerability reporting and management tool.
- 2. Executive Presentation:** Overview of the entire engagement, the vulnerabilities discovered and the recommendations made to mitigate the threats identified on the client's websites
- 3. Detailed Technical Report:** Comprehensive information, proof of concept examples and detailed exploitation instructions of all the threats identified

Client Benefits

By conducting thorough penetration tests and identifying vulnerabilities, QA InfoTech reduced the client's risk exposure in an environment where Online Shopping Regulatory Bodies are taking an extremely strict approach to security. Additionally, we were able to bring in the following benefits-

1. Risk Benefits

The QA InfoTech security testing team minimized the security risks by assessing the customer's infrastructure and business solution specific vulnerabilities and recommended solutions with proven methods to enhance security. Some of the major vulnerabilities discovered were-

- SQL Injection
- Security Misconfiguration
- Insecure CORS
- Misconfigured S3 buckets
- Hard-coded sensitive credentials
- CSRF
- Cross Site Scripting
- Broken Authentication and Session Management
- Order Management Flaws
- Payment Integration Flaws

- Privilege Escalation
- Session Hijacking

2. Cost Savings

- QA InfoTech suggested cost-effective risk-mitigation measures based on the customer's business requirements that would ensure security and continuity of the business
- Reduced significant financial impact and disruption to the hard business deadlines

3. Compliance

The Client will be able to utilize the information gained from the engagement for compliance purposes.

About QA InfoTech

At QA InfoTech we specialize in providing independent offshore software testing and unbiased software quality assurance services to product companies, ranging from the Fortune 500 to start-ups. Established in 2003, with less than five testing experts, QA InfoTech has grown leaps and bounds with its three QA Centers of Excellence globally; located in the hub of IT activity in India in Noida and Bangalore and our affiliate QA InfoTech Inc. in Michigan, USA.

- 1000+ QA engineers and domain experts
- An ISO 9001:2008, CMMi Level 3, ISO 20000-1:2011 and ISO 27001:2005 compliant company
- Thought Leaders in E2E testing, specifically Test Automation, Performance Testing, Localization and Accessibility Testing

In 2017, QA InfoTech has been ranked in the top 100 places to work for in India. We are amongst the top 50 Best IT & ITeS Companies to Work For in 2012, 2014, 2015 & 16 in India.

"We assure the highest degree of Excellence and Accuracy in our engagements. Once you have placed your trust with us, rest assured we guarantee an elated peace of mind"

QA InfoTech Inc., Michigan, U.S.A.
32985 Hamilton Court East, Suite 121,
Farmington Hills, MI 48334 U.S.A

QA InfoTech Pvt. Ltd. Arkansas
Rain Tree Business Center, 900B South
Walton Blvd, Suite 1, Bentonville,
Arkansas, 72712

QA InfoTech Pvt. Ltd. (Head Office)
A-8, Sector 68
Noida, U.P, 201309, India

QA InfoTech Pvt. Ltd. Bengaluru
CoWrks, RMZ Ecoworld, Outer Ring Road,
Bellandur, Bengaluru,
Karnataka 560103, India

For More Details:

Contact Us: info@qainfotech.com | Visit Us: www.qainfotech.com