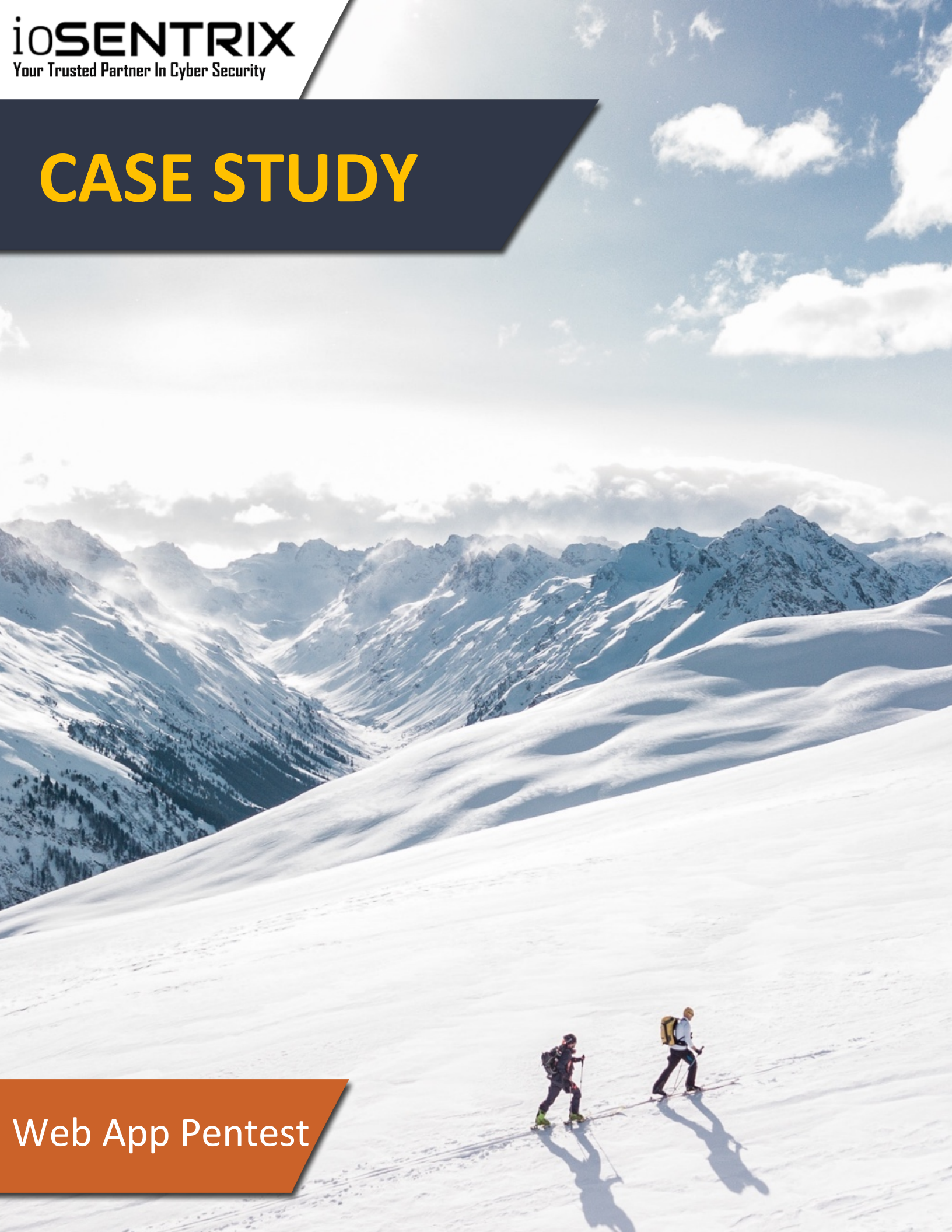# ioSENTRIX
Your Trusted Partner In Cyber Security

CASE STUDY

Web App Pentest

# Background

A large financial service provider engaged ioSENTRIX to perform the overall assessment of the web application, including the primary web and database servers. The application was used to handle financials for both medium and large corporations. The target web application was hosted on a secure web server which was protected by a web application firewall and closely monitored.

The Challenge

The Client's main business objective was to provide its corporate customers with a safe and secure online portal to manage their financials. It was immensely crucial for the Client to ensure that the web application was not prone to technical bugs or design flaws while simultaneously providing a smooth experience to its customers. Furthermore, as the in-house team had developed the web application, our Client wanted assurance from an outside perspective that the web application and the underlying servers were handling the customer data and storage as per the latest standards.

> **2019 VERIZON DBIR**
>
> *62% of the breaches and 39% of incidents occur at the web application layer.*
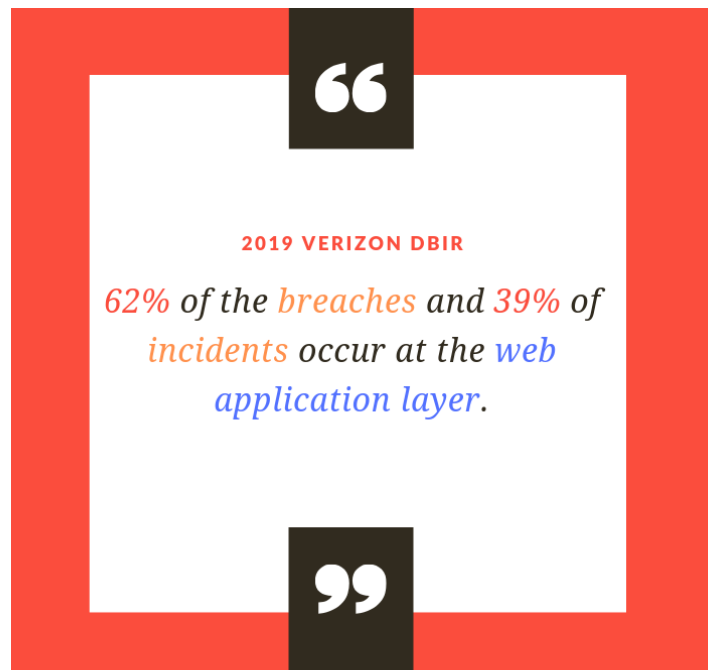
The Solution

By using ioSENTRIX's unique in-house developed security testing methodology, the penetration testers completed the Web Application Security Assessment.

Some of the key highlights of the security assessment were:

1) Our testers created a functional Mapping of the entire website with every detail on the URLs, parameters that are passed.
2) Test cases were created by the testers based on the various sections that were mapped.
3) Manual and automated scans using various open-source and in-house developed techniques were performed.
4) The testers manually verified each of the potential test cases identified.
5) Our testers created a correlation for each of the identified vulnerabilities for better impact analysis.
6) The testers highlighted the business impacts resulting from the technical impacts of the vulnerabilities.

Once the first cycle of the engagement was completed and vulnerabilities were identified in the Client's web application, the testers leveraged the known vulnerabilities to penetrate the Client's application architecture further and identify the true effect of the vulnerabilities found.

The Deliverables

The reports and remediation information provided were specifically tailored to enhance the Client's remediation process.

The following reports were submitted to the customer:

EXECUTIVE REPORT — **TECHNICAL REPORT** — **EXCEL TRACKER**

Executive Report: This report outlines the entire engagement, the vulnerabilities discovered, and the recommendations made against the identified threats. The report informed the client on their security vulnerabilities, so they know which software and hardware improvements to consider or which recommendations and policies would improve the overall security.

Technical Report: Detailed comprehensive information including, proof of concept examples and detailed instructions of all the identified threats were delivered. An analysis of the business impact of each identified vulnerability was also listed in this version of the report.

Excel Tracker: This is a simple and comprehensive vulnerability tracker aimed at helping the IT asset owner keep track of the vulnerabilities, remediation status, action items, etc.

The Benefits

By conducting thorough security tests and identifying vulnerabilities, ioSENTRIX provided the Client with a business continuity audit by reducing the Client's risk exposure in a climate where financial applications are the major target for rivals.

Additionally, the Client gained the following benefits:

Risk Benefits: ioSENTRIX assisted in maximizing the client's overall security standing of the web application and its underlying servers via security assessment and providing the recommended solutions with proven methods to enhance security.

Cost Savings: ioSENTRIX suggested lucrative risk-mitigation measures based on the customer's business necessities that would ensure security and potential expansion of the business.

Customer Satisfaction: Web Application Security Assessment was conducted with the slightest interruption and damage across customer systems to identify security vulnerabilities, impacts and potential risks.

Compliance: As an added bonus, the Client was able to exploit the information gained from this Web Application Security Assessment to easily gain industry certifications to provide an enhanced level of service to its customers.

Risk Benefits

Compliance

Cost Savings

Customer Satisfaction

About ioSENTRIX:

ioSENTRIX LLC is a Security Consulting firm. We provide a wide range of security consulting services to our clients worldwide. Our list of clients spans the fortune 500, large enterprises to small start-ups, financial institutions, and several high-tech companies.

We are an innovative consulting company offering a full range of cyber security services to businesses of all sizes, tailored to meet any budget requirements. We help our clients by identifying, mitigating and preventing vulnerabilities in their software, infrastructure, and cloud.

We offer a comprehensive vulnerability assessment that includes design-review, threat model, penetration test, code review, and open source software security. We've got the necessary tools and the expertise to secure your business so you can focus on growing it.

Learn more about our services at **https://www.iosentrix.com.**

ioSENTRIX LLC.

150 S. Sterling Blvd, Suite 543	**Sales:**	1 (888) 958-0554
Sterling Virginia 20164 (USA)	**Email:**	sales@iosentrix.com