

# CASE STUDY

**HITACHI**  
Inspire the Next

## PENETRATION TESTING AND VULNERABILITY ASSESSMENTS FOR THE BANKING INDUSTRY

Hitachi Systems Security Inc.'s technical security audits will provide you with the answers and recommendations you need to improve your security posture and protect your organization's most valuable assets. Technical security audits detect the vulnerabilities that can be used by unauthorized users and uncover the weaknesses of your organization's security processes. They are carried by our certified security consultants (ethical hackers) who simulate attacks by using the same techniques as a malicious attacker. The objective of such an audit is to evaluate if your organization's informational structure can be easily accessed without authorization or not.

### QUICK FACTS

**Industry:** Financial Services

**Company Type:** Privately Held Bank

**Location:** Offices in 5 Countries

**Number of Employees:** 2,500+

#### Needs & Requirements:

- Improve security posture to better protect corporate IT assets against vulnerabilities and intrusions
- Identify and implement remediation measures for corporate vulnerabilities
- Report findings to executive team

### THE CHALLENGE

Within their yearly security strategic plan, custodians of information security wanted to assess their bank's main website application in order to know potential vulnerabilities that could be exploited by external hackers or competitors.

### THE SOLUTION

During an external penetration or intrusion test, automated and manual attacks are simulated in order to determine the permeability of the web application.

### DELIVERABLES

The final result of the penetration test was a detailed report that included all the findings of the test as well as the countermeasures and recommendations to secure the customer's IT infrastructure. The report documented the following elements:

- The security level of the servers as perceived by an attacker.
- The security breaches, vulnerabilities, as well as countermeasures and corrective actions to be applied.
- All testing activities and raw scan data are also provided alongside the final deliverable as report appendixes and supporting documents.

All serious vulnerabilities that were discovered in the course of this evaluation were sent to the customer as an interim report.

## MAIN BENEFITS



Gain a better understanding of potential corporate vulnerabilities that may be visible from the Internet.



Augmented protection of the account holders' confidential data.



Improve its defence against technological vulnerabilities that can lead to intrusions, fraud and service interruption.



Obtain specific advices on how to lower risks in the web application.

## SERVICES PROVIDED

A team of Hitachi Systems Security Inc.'s Senior Cyber Security Experts collaborated on this engagement:

### **In-Depth Web Application Vulnerability Assessment**

The web application vulnerability assessment evaluated the security of the connection requests to the databases, dynamic forms, users' sessions, authentication and authorizations management of the application. This assessment also verified if this application could resist hostile attacks without revealing too much information on the hosting environment and if identified vulnerabilities could lead to further intrusion and exploitation.

### **External Intrusion Test**

The external infrastructure and network penetration test checked the ease for an intruder to access the company information system through external assets directly reachable from the Internet.

### **Hitachi Systems Security Inc.**

955 boul. Michèle-Bohec, Suite 244, Blainville (Québec) J7C 5J6 Canada  
Tel: +1 450-430-8166 Fax: +1 450-430-1858  
[www.hitachi-systems-security.com](http://www.hitachi-systems-security.com)