

Federal Reserve Board of Governors

Course Description for e-Banking Hands-On (S&R Technology Lab)

Last Revised: September 2009

e-Banking Hands-On (S&R Technology Lab)

The Board of Governors of the Federal Reserve System is proud to offer technology-related courses developed and hosted by the S.T.R.E.A.M./Technology Lab at the Federal Reserve Bank of Chicago, Chicago, Illinois. For over nine years, the S.T.R.E.A.M./Technology Lab has pursued a unique approach to examiner technology training by combining lectures with hands-on exercises. The exercises reinforce concepts by allowing participants to input commands into software applications and observe how they work. The Technology Lab is outfitted with many applications and operating systems found in the financial industry.

Type of Participant Targeted

The e-Banking course is a 4-day course intended for examiners with IT examination responsibilities but who may not have had university training in information technology. At least one year of field examination experience is preferred.

Prerequisites

None required.

Course Overview

This course provides participants with an overview of the technologies and risks fundamental to transactional e-commerce. Topics include website information gathering, using SQL, common Web vulnerabilities, and vendor management of an outsourced e-Banking function. Hands-on exercises include evaluating a Web-site, vulnerability testing, and attacking a mock e-Banking Web-site. Mitigating controls such as web-application testing and the FFIEC's strong authentication guidance are also covered.

Course Objectives

After completing the course, the participant, at a minimum, will be able to demonstrate the following skills:

- Explain fundamental concepts behind modern e-commerce technologies
- Explain why e-commerce systems and technologies are important to examiners
- Describe the functionality and characteristics of component technologies, for example the Web Server (Apache and IIS are reviewed), the database (Microsoft SQL Server is used), and the presentation layer (Microsoft ASP)
- Explain the role e-commerce systems play in Internet banking and other banking activities
- List some of the fundamental risks and controls pertaining to the use of e-commerce technologies in banks
- Describe current tools used to automate the discovery of web-application weaknesses

Post-Course Intervention

Participants will learn the essential components that comprise an electronic banking Web-site. The separation of functionality into three or more tiers helps manage risk and response time, and participants will contrast the risks in each the presentation, business and database layers. Participants will be able to compare and contrast the functionality and features of both Apache and Microsoft's Internet Information Services (IIS).

Overview of e-Banking Curriculum

Subject	Approximate Class Hours
Introduction to e-Banking	1.0
Gathering Information about a Web-site	1.0
Searching the Web—Exercise	1.0
Functionally defining e-Banking	1.0
Using the SQL query language—Exercise	1.0
Phishing	1.0
Web Applications and Internet Information Services	2.0
Internet Information Services (IIS)—Exercise	1.0
Apache Web Server	1.0
Apache Web Server—Exercise	1.0
SQL Injection	1.0
SQL Injection—Case Study	1.0
Implementing e-Banking	1.0
Web Authentication	1.0
Strong Authentication—Demonstration	0.5
Vendor Management of e-Banking providers	1.0
Web Vulnerabilities	0.5
Evaluating the Vulnerabilities in an e-Banking site—Exercise	1.0
e-Banking Risks	2.0
Web-Application Testing—Demonstration	2.0
Vulnerability Testing	1.0
Examination Issues	1.0
Mobile Financial Services	1.0
Total Lecture & Exercise Hours	25.00 (*)

(*) Note: The total number of hours and topics may vary from class to class.

Learning Objectives

Examiners should be able to identify risks associated with the three tiers commonly used to describe the technical implementation of an e-Banking Web-site. Participants will also be able identify the risks associated with Microsoft's IIS and compare them to the Apache Web server. Hands-on exercises will provide participants with an understanding of the SQL query language, and how the presentation, business and database logic tiers can be compromised by attackers. Mitigating controls for these weaknesses will also be made familiar and reinforced using hands-on exercises and demonstrations. Finally, the participant will understand the importance of Web-application testing using an industry standard commercial testing tool.

By module, the following learning objectives will be accomplished:

Module	Learning Objectives
Introduction to e-Banking	<ul style="list-style-type: none"> • Foster a baseline understanding of key terms related to e-Banking
Gathering information about a Web-site	<ul style="list-style-type: none"> • Identify the means by which attackers can enumerate the technical characteristics of a Web-site • Recognize methods to hide certain key information from attackers
Searching the Web	<ul style="list-style-type: none"> • Identify the extent of publicly available information that can be found on the Internet about our Banks • Describe ways to reduce the amount of information that is available
Using SQL Query Language	<ul style="list-style-type: none"> • Hands-on exercise to learn how the structured query language works • Review key commands used to add, change or modify data in the database
Phishing	<ul style="list-style-type: none"> • Review the magnitude of threat posed by Phishing and other common exploits
Web Applications and Internet Information Services	<ul style="list-style-type: none"> • Hands-on exercise using IIS to understand how a web-server is implemented using Microsoft's Internet Information Services • Review the weaknesses of Basic Authentication
Apache Web Server	<ul style="list-style-type: none"> • Gain understanding of the basics of Apache Web Server functionality • Use a Web-Proxy to understand how Web-application proxies work
SQL Injection—Case Study	<ul style="list-style-type: none"> • Understand the technical operation and how SQL can be used to compromise a host • Review common configuration errors and mitigating controls
Web Authentication	<ul style="list-style-type: none"> • Review the FFIEC guidance on Strong Authentication • Demonstrate other transaction verification and authentication mechanisms that can be used by banks
Web-Application Testing	<ul style="list-style-type: none"> • Review current tools that are designed to automate the detection of vulnerabilities
Vulnerability Testing	<ul style="list-style-type: none"> • Identify other means of testing Web-applications
Mobile Banking	<ul style="list-style-type: none"> • Understand the mobile landscape, identify benefits and risks, and review fraud in payments • Review Risk management processes associated with payments

Class Size

The optimal class size for the e-Banking course offering is approximately 25 participants. To provide sufficient variety of interaction among class participants, the minimum class size should be 10 participants.

Instructors

e-Banking courses include one or more instructor(s) from the Federal Reserve System and may also include instructors from an external agency.