Security Strategies in Web Applications and Social Networking

Lesson 15

Web Application Security Organizations, Education, Training, and Certification

Learning Objective

- Explain the responsibilities and interests of various national and international security organizations.

Key Concepts

- Purpose of the Web Application Security Consortium (WASC)
- Purpose of the Open Web Application Security Project (OWASP)
- Non-vendor certificates and programs
- Qualifications applicable to students' areas of interest

Department of Homeland Security (DHS)

- National Cyber Security Division (NCSD)
- National Infrastructure Advisory Council
- Critical Infrastructure Partnership Advisory Council
- U.S. Secret Service

FLETC

NCSD/US-CERT

- United States Computer Emergency Response Team (US-CERT) National Infrastructure Advisory Council
- Operational arm of the NCSD
- Helps to investigate and stop online attacks and restore services
- Provides a public threat and vulnerability alert service
    - National Cyber Alert System

CERT®/CC

- Computer Emergency Response Team Coordination Center (CERT®/CC)
- Conducts research and training for the computer security incident response team (CSIRT) community
- Is a major sponsor of the international Forum of Incident Response and Security Teams (FIRST)

Common Vulnerabilities and Exposures (CVE) List

- A collaboration with a number of software and security vendors
- CVE-Compatible accreditation for testing products
- What Is a CVE Identifier?

MITRE

CVE-YYYY-nnnn

CMTIP

CVE number—This is in the form of CVE-YYYY-nnnn, for example, CVE-2010-1868.
Identifier status—Either “candidate” or “entry.” Before 2005, candidates were identified with a “CAN” label rather than a “CVE” prefix.
Description—This is a brief, standardized description of the vulnerability. In the case of 2010-1868, the description is “The (1) sqlite_single_query and (2) sqlite_array_query functions in ext/sqlite/sqlite.c in PHP 5.2 through 5.2.13 and 5.3 through 5.3.2 allow context-dependent attackers to execute arbitrary code by calling these functions with an empty SQL query, which triggers access of uninitialized memory.”
References—These may be to the discoverer’s announcement, the vendor’s security bulletin, or third-party reports such as the Open Source Vulnerability Database at http://osvdb.org.
Additional—Candidates may also have information on the stages of the CVE process, and any votes from the CVE Editorial Board. This also includes a comment field.

CVE Identifier

- CVE Identifier number (i.e., "CVE-1999-0067")
- Indication of “candidate” or “entry” status
- Brief description of the security vulnerability or exposure
- Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID)

National Institute of Standards and Technology (NIST)

- Federal agency within the U.S. Department of Commerce
- National Vulnerability Database
- Computer Security Resource Center (CSRC)
- Federal Information Processing Standards (FIPS)
- Special Publications (SPs)

(ISC)^2 Certifications

- Systems Security Certified Practitioner (SSCP)
- Certified Information Systems Security Professional (CISSP)
- Certified Authorization Professional (CAP)
- Certified Secure Software Lifecycle Professional (CSSLP)

WASC

- Web Application Security Consortium (WASC)
- Compiles best practices in securing Web application
- Projects:
  - Web-Hacking Incident Database
  - Distributed open proxy honeypots
  - (Web) Threat Classification

OWASP

- Open Web Application Security Project (OWASP)
- Focuses on educating application developers on security risks
- OWASP Top 10 List
- WebScarab, AntiSamy, Enterprise Security API (ESAPI), WebGoat
- Open Software Assurance Maturity Model (OpenSAMM)
- OWASP Guides

Summary

- Responsibilities and interests of various national and international security organizations
- Purpose of the Web Application Security Consortium (WASC)
- Purpose of the Open Web Application Security Project (OWASP)
- Non-vendor certificates and programs
- Qualifications applicable to students' areas of interest

OPTIONAL SLIDES

International Organization for Standardization (ISO)

- Publishes many standards, such as:
  - International Standard Book Number (ISBN)
  - Open Systems Interconnection (OSI) reference model

World Wide Web Consortium (W3C)

- The main international standards organization for the World Wide Web
- Has developed or endorsed include the following:
  - Cascading Style Sheets (CSS)
  - Common Gateway Interface (CGI)
  - Hypertext Markup Language (HTML)
  - Simple Object Access Protocol (SOAP)
  - Web Services Description Language (WSDL)
  - Extensible Markup Language (XML)

Vendor-Neutral Certifications

- Covers concepts and topics that are general in nature
- Does not focus on a specific product or product line

Certification Essentials

- An official statement that validates a person has satisfied specific requirements:
  - Possessing a certain level of experience
  - Completing a course of study
  - Passing an examination
- Does *not* guarantee that a person is good at a specific job