1. Record Nr. UNINA9910777901703321

Autore	Canavan Tom
Titolo	Joomla! web security [[electronic resource]] : secure your Joomla! website from common security threats with this easy-to-use guide / / Tom Canavan
Pubbl/distr/stampa	Birmingham, U.K., : Packt Pub., c2008
ISBN	1-281-85616-9 9786611856168 1-84719-489-3
Descrizione fisica	1 online resource (264 p.)
Collana	From technologies to solutions
Disciplina	005.8
Soggetti	Web sites - Security measures Computer networks - Security measures Web sites - Authoring programs Web site development
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover; Table of Contents; Preface; Chapter 1: Let's Get Started; Introduction; Common Terminology; Hosting-Selection and Unique Needs; What Is a Host?; Choosing a Host; Questions to Ask a Prospective Host; Facilities; Things to Ask Your Host about Facility Security; Environmental Questions about the Facility; Site Monitoring and Protection; Patching and Security; Shared Hosting; Dedicated Hosting; Architecting for a Successful Site; What Is the Purpose of Your Site?; Eleven Steps to Successful Site Architecture; Downloading Joomla!; Settings; .htaccess; Permissions; User Management Common Trip UpsFailure to Check Vulnerability List First; Register Globals, Again; Permissions; Poor Documentation; Got Backups?; Setting Up Security Metrics; Summary; Chapter 2: Test and Development; Welcome to the Laboratory!; Test and Development Environment; What Does This Have to Do with Security?; The Evil Hamster Wheel of Upgrades; Determine the Need for Upgrade; Developing Your Test Plan; Essential Parameters for a Successful Test; Using Your Test and Development Site for Disaster Planning; Updating

Your Disaster Recovery Documentation

Make DR Testing a Part of Your Upgrade/Rollout CycleCrafting Good Documentation; Using a Software Development Management System; Tour of Lighthouse from Artifact Software; Reporting; Using the Ravenswood Joomla! Server; Roll-out; Summary; Chapter 3: Tools; Introduction; Tools, Tools, and More Tools; HISA; Installation Check; Web-Server Environment; Required Settings for Joomla!; Recommended Settings; Joomla Tools Suite with Services; How's Our Health?; NMAP-Network Mapping Tool from insecure.org; Wireshark; Metasploit-The Penetration Testers Tool Set; Nessus Vulnerability Scanner
Why You Need NessusSummary; Chapter 4: Vulnerabilities; Introduction; Importance of Patching is Paramount; What is a Vulnerability?; Memory Corruption Vulnerabilities; SQL Injections; Command Injection Attacks; Attack Example; Why do Vulnerabilities Exist?; What Can be Done to Prevent Vulnerabilities?; Developers; Poor Testing and Planning; Forbidden; Improper Variable Sanitization and Dangerous Inputs; Not Testing in a Broad Enough Environment; Testing for Various Versions of SQL; Interactions with Other Third-Party Extensions; End Users; Social Engineering; Poor Patching and Updating SummaryChapter 5: Anatomy of Attacks; Introduction; SQL Injections; Testing for SQL Injections; A Few Methods to Prevent SQL Injections; And According to PHP.NET; Remote File Includes; The Most Basic Attempt; What Can We Do to Stop This?; Preventing RFI Attacks; Summary; Chapter 6: How the Bad Guys Do It; Laws on the Books; Acquiring Target; Sizing up the Target; Vulnerability Tools; Nessus; Nikto: An Open-Source Vulnerability Scanner; Acunetix; NMAP; Wireshark; Ping Sweep; Firewalk; Angry IP Scanner; Digital Graffiti versus Real Attacks; Finding Targets to Attack; What Do I Do Then? Countermeasures

Sommario/riassunto

Secure your Joomla! website from common security threats with this easy-to-use guide