1.	Record Nr.	UNINA9910789334203321
	Autore	Canavan Tom
	Titolo	CMS security handbook [[electronic resource]] : the comprehensive guide for WordPress, Joomla!, Drupal, and Plone / / Tom Canavan
	Pubbl/distr/stampa	Indianapolis, Ind., : Wiley Pub., c2011
	ISBN	1-283-39776-5 9786613397768 1-118-09174-4
	Edizione	[1st edition]
	Descrizione fisica	1 online resource (434 p.)
	Disciplina	005.8
	Soggetti	Computer networks - Security measures Data protection Web sites - Security measures
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Note generali	Includes index.
	Nota di contenuto	CMS Security Handbook; Contents; Introduction; Chapter 1 Introduction to CMS Security and Operations; Target Acquired; Operational Considerations; Educating Your Employees and End Users; Raising Security Awareness; Training on Information Security Policies; Providing a Standard Protocol for Threat Reporting; Ensuring E-mail Security; Applying Patches and Updates; Being Aware and Staying Safe; Looking at Your Site Through the Eyes of a Hacker; Steps to Gaining Access to Your Site; Researching; Googling Away; Using Google Hacking Tools (Dorks); Footprinting; Using NMAP for Nefarious Means Using TracerouteFinding Subdomains; Enumeration; Attacking and Owning the Site; Wiping Out Their Tracks; Examples of Threats; Social Engineering; Calling into Your Office; Sending in a Trusted Friend; Using USB Keys; Indiscriminate Browsing or Instant Messaging; External Media; Vendors or External Clients/Customers as the Threat; Reviewing Your Perimeter; Using Virus Protection; Banning Passwords on Desks; Enforcing a Password Complexity and Change Policy; Policing Open Wireless; Tools for Wireless Detection; How Will You Respond to an Incident?; Does Your Plan Exist?; Is the Plan Up to Date? Where Are Your Backup Tapes, Disks, and USBs?Summary; Chapter 2

Choosing the Right Hosting Company; Types of Hosting Available; Shared Hosting; Virtual Private Server (VPS); Dedicated Server; Cloud Hosting; Security of Data in a Cloud; Selecting the Right Hosting Option; Budget Considerations; Determining the Appropriate Server Size; Case 1: Light Website Traffic (Shared Hosting); Case 2: Medium Website Traffic (VPS); Case 3: Heavy Website Traffic; Using Backups; What to Look for in Web Host Security; Physical Security; Glass Windows; Flooding; Signs; People

Dumpster Diving and Social EngineeringBreach Response; Terrorists; Access to Equipment; Water Detection; Fire Suppression; Emergency Procedures; Disaster Recovery and Business Continuity; Cyber Security; Firewalls and Intrusion Detection; Log File Auditing; Spam, Virus Scanning, and Prevention; Patching for Weaknesses; VoIP; Web Servers; Environmental Support; Network Redundancy; Electrical Service; Technical Support; Emergency Planning for the Host; Location of the Host's Data Center; Processes; Backups; Offsite Procedures; Accepting Credit Cards on Your Website; Understanding PCI

PCI TerminologyBecoming PCI Certified; Installing an SSL Certificate; Testing by ASV; Choosing a Shopping Cart; Storing Data Securely; PCI Vulnerability Management Plan; Avoiding Common ASV Testing Pitfalls; After Certification; Domain Name System Servers; Understanding DNS; Threats to DNS; DNS (Name Server) Failure; Zone Transfers; Lack of Patching DNS Servers; DNS Poisoning; Hosting Your Own Website Server; Getting Ready; Making Your Shopping List; Choosing an Operating System; Ensuring Security; Patching; Summary; Chapter 3 Preventing Problems Before They Start

Choosing an Appropriate CMS for Your Needs

Sommario/riassunto

Provides information on maintaining security for websites built on open source Content Management Systems.