1. Record Nr. UNINA9910456752803321

Autore	Connelly Olly
Titolo	WordPress 3 ultimate security [[electronic resource]] : protect your WordPress site and its network / / Olly Connelly
Pubbl/distr/stampa	Birmingham, U.K., : Packt Open Source, 2011
ISBN	1-283-34924-8 9786613349248 1-84951-211-6
Descrizione fisica	1 online resource (408 p.)
Collana	Community experience distilled
Disciplina	006.7 006.752
Soggetti	Computer networks - Security measures World Wide Web - Security measures Data protection Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Copyright; Credits; About the Author; About the Reviewers; www.PacktPub.com; Table of Contents; Preface; Chapter 1: So What's the Risk?; Calculated risk; An overview of our risk; Meet the hackers; White hat; Black hat; Botnets; Cybercriminals; Hacktivists; Scrapers; Script kiddies; Spammers; Misfits; Grey hat; Hackers and crackers; Physically hacked off; Social engineering; Phone calls; Walk-ins; Enticing URLs; Phishing; Social networking (and so on); Protecting against social engineering; Weighing up Windows, Linux, and Mac OS X; The deny-by-default permission model The open source advantageSystem security summary; Malwares dissected; Blended threats; Crimeware; Data loggers; At loggerheads with the loggers; Hoax virus; Rootkits; Spyware; Trojan horses; Viruses; Worms; Zero day; World wide worry; Old browser (and other app) versions; Unencrypted traffic; Dodgy sites, social engineering, and phish food; Infected public PCs; Sniffing out problems with wireless; Wireless hotspots; Evil twins; Ground zero; Overall risk to the site and server; Physical server vulnerabilities; Open ports with vulnerable

services; Access and authentication issues
Buffer overflow attacksIntercepting data with man-in-the-middle attacks; Cracking authentication with password attacks; The many dangers of cross-site scripting (XSS); Assorted threats with cross-site request forgery (CSRF); Accessible round-up; Lazy site and server administration; Vulnerable versions; Redundant files; Privilege escalation and jailbreak opportunities; Unchecked information leak; Content theft, SEO pillaging, and spam defacement; Scraping and media hotlinking; Damn spam, rants, and heart attacks; Summary; Chapter 2: Hack or Be Hacked; Introducing the hacker's methodology ReconnaissanceScanning; Gain access; Secure access; Cover tracks; Ethical hacking vs. doing time; The reconnaissance phase; What to look for; How to look for it; Google hacking; More on Google hacking; Scouting-assistive applications; Hacking Google hacking with SiteDigger; WHOIS whacking; Demystifying DNS; Resolving a web address; Domain name security; The scanning phase; Mapping out the network; Nmap: the Network Mapper; Secondary scanners; Scanning for server vulnerabilities; Nessus; OpenVAS; GFI Languard; Qualys; NeXpose and Metasploit; Scanning for web vulnerabilities; Wikto; Paros Proxy
HackerTargetAlternative tools; Hack packs; Summary; Chapter 3: Securing the Local Box; Breaking Windows: considering alternatives; Windows security services; Security or Action Center; Windows Firewall; Windows Update; Internet Options; Windows Defender; User Account Control; Configuring UAC in Vista; Configuring UAC in Windows 7; Disabling UAC at the registry (Vista and 7); UAC problems with Vista Home and Premium; Proactive about anti-malware; The reactionary old guard: detection; Regular antivirus scanners; The proactive new guard: prevention; The almost perfect anti-malware solution
Comodo Internet Security (CIS)

Sommario/riassunto

Protect your WordPress site and its network