1. Record Nr. UNINA9910453182703321

Autore	Pauli Joshua J
Titolo	The basics of web hacking [[electronic resource]] : tools and techniques to attack the Web / / Josh Pauli ; Scott White, technical editor
Pubbl/distr/stampa	Amsterdam, : Syngress, an imprint of Elsevier, 2013
ISBN	0-12-416659-8
Edizione	[1st edition]
Descrizione fisica	1 online resource (160 p.)
Collana	The basics The basics of web hacking
Altri autori (Persone)	WhiteScott
Disciplina	005.8
Soggetti	Web sites - Security measures Web applications - Security measures Computer networks - Security measures Penetration testing (Computer security) Computer hackers Computer crimes - Prevention Electronic books.
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	Front Cover; The Basics of Web Hacking: Tools and Techniques to Attack the Web; Copyright; Dedication; Acknowledgments; Honey Bear; Lizard; Baby Bird; Family and Friends; Security Community; Scott White-Technical Reviewer; Syngress Team; My Vices; Biography; Foreword; Introduction; About this Book; A Hands-on Approach; What's in this Book?; A Quick Disclaimer; Contents; Chapter 1: The Basics of Web Hacking; Introduction; What Is a Web Application?; What You Need to Know About Web Servers; What You Need to Know About HTTP; HTTP Cycles; Noteworthy HTTP Headers; Noteworthy HTTP Status Codes The Basics of Web Hacking: Our ApproachOur Targets; Our Tools; Web Apps Touch Every Part of IT; Existing Methodologies; The Open-Source Security Testing Methodology Manual (OSSTM); Penetration Testing Execution Standard (PTES); Making Sense of Existing Methodologies; Most Common Web Vulnerabilities; Injection; Cross-site Scripting (XSS); Broken Authentication and Session Management; Cross-site Request Forgery; Security Misconfiguration; Setting Up a Test Environment; Target Web Application; Installing the Target Web Application;

Configuring the Target Web Application; DVWA Install Script
Chapter 2: Web Server HackingIntroduction; Reconnaissance; Learning About the Web Server; The Robots.txt File; Port Scanning; Nmap; Updating Nmap; Running Nmap; Nmap Scripting Engine (NSE); Vulnerability Scanning; Nessus; Installing Nessus; Configuring Nessus; Running Nessus; Reviewing Nessus Results; Nikto; Exploitation; Basics of Metasploit; Search; Use; Show Payloads; Set Payload; Show Options; Set Option; Exploit; Maintaining Access; Chapter 3: Web Application Recon and Scanning; Introduction; Web Application Recon; Basics of a Web Proxy; Burp Suite; Configuring Burp Proxy
Spidering with BurpAutomated Spidering; Manual Spidering; Running Burp Spider; Web Application Scanning; What a Scanner Will Find; What a Scanner Won't Find; Scanning with ZED Attack Proxy (ZAP); Configuring ZAP; Running ZAP; Reviewing ZAP Results; ZAP Brute Force; Scanning with Burp Scanner; Configuring Burp Scanner; Running Burp Scanner; Reviewing Burp Scanner Results; Chapter 4: Web Application Exploitation with Injection; Introduction; SQL Injection Vulnerabilities; SQL Interpreter; SQL for Hackers; SQL Injection Attacks; Finding the Vulnerability; Bypassing Authentication
Extracting Additional InformationHarvesting Password Hashes; Offline Password Cracking; sqlmap; Operating System Command Injection Vulnerabilities; O/S Command Injection for Hackers; Operating System Command Injection Attacks; Web Shells; Chapter 5: Web Application Exploitation with Broken Authentication and Path Traversal; Introduction; Authentication and Session Vulnerabilities; Path Traversal Vulnerabilities; Brute Force Authentication Attacks; Intercepting the Authentication Attempt; Configuring Burp Intruder; Intruder Payloads; Running Intruder; Session Attacks; Cracking Cookies
Burp Sequencer

Sommario/riassunto

The Basics of Web Hacking introduces you to a tool-driven process to identify the most widespread vulnerabilities in Web applications. No prior experience is needed. Web apps are a ""path of least resistance"" that can be exploited to cause the most damage to a system, with the lowest hurdles to overcome. This is a perfect storm for beginning hackers. The process set forth in this book introduces not only the theory and practical information related to these vulnerabilities, but also the detailed configuration and usage of widely available tools necessary to exploit these vulnerabili