Software Security

- Security in Computing, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies
- The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws, Dafydd Stuttard

	Security in Computing
	Introduction
	What is Computer Security? – Topics 2
	Threats – Topics 5
	Harm – Topics 2
	Vulnerabilities
	Controls
	Conclusion
	What’s Next?
	Exercises
	Toolbox: Authentication, Access Control, and Cryptography
	Authentication – Topics 7
	Access Control – Topics 4
	Cryptography – Topics 10
	Exercises
	Programs and Programming
	Unintentional (Nonmalicious) Programming Oversights – Topics 10
	Malicious Code – Malware – Topics 2
	Countermeasures – Topics 5
	Exercises
	The Web- User Side
	Browser Attacks – Topics 2
	Web Attacks Targeting Users – Topics 3
	Obtaining User or Website Data – Topics 3
	Email Attacks – Topics 5
	Exercises
	Operating Systems
	Security in Operating Systems – Topics 5
	Security in the Design of Operating Systems – Topics 9
	Rootkit – Topics 6
	Conclusion
	Exercises
	Networks
	Network Concepts – Topics3
	Part-1: War on Network: Network Security Attacks
	Threats to Network Communication – Topics 5
	Wireless Network security – Topics 4
	Denial of Service – Topics 10
	Distributed Denial-of-Service Attacks – Topics 4
	Part-2: Strategic Defenses: Security Countermeasures
	Cryptography in Network Security – Topics 6
	Firewalls – Topics 8
	Intrusion Detection and Prevention Systems – Topics 6
	Network Management – Topics 2
	Conclusion

	Exercises
	Databases
	Introduction to Databases – Topics 3
	Security Requirements of Databases – Topics 7
	Reliability and Integrity – Topics 5
	Database Disclosure – Topics 3
	Modification – Topics | Security Versus Precision
	Data Mining and Big Data – Topics 2
	Conclusion
	Exercises
	Cloud Computing
	Cloud Computing Concepts – Topics 2
	Moving to the Cloud – Topics 4
	Cloud Security Tools and Techniques – Topics 3
	Cloud Identity Management – Topics 3
	Securing IaaS | Public IaaS Versus Private Network Security
	Conclusion – Topics 2
	Exercises
	Privacy
	Privacy Concepts – Topics 2
	Privacy Principles and Policies – Topics 8
	Authentication and Privacy – Topics 2
	Data Mining – Topics 2
	Privacy on the Web – Topics 7
	Email Security – Topics 6
	Privacy Impacts of Emerging Technologies – Topics 5
	Where the Field is Headed
	Conclusion
	Exercises
	Management and Incidents
	Security Planning – Topics 4
	Business Continuity Planning – Topics 3
	Handling Incidents – Topics 2
	Risk Analysis – Topics 3
	Dealing with Disaster – Topics 6
	Conclusion
	Exercises
	Legal Issues and Ethics
	Protecting Programs and Data – Topics 4
	Information and the Law – Topics 4
	Rights of Employees and Employers – Topics 2
	Redress for Software Failures – Topics 2
	Computer Crime – Topics 8
	Ethical Issues in Computer Security – Topics 3
	Incident Analysis with Ethics – Topics 9
	Conclusion of Computer Ethics
	Conclusion
	Exercises
	Details of Cryptography
	Cryptology – Topics 5
	Symmetric Encryption Algorithms – Topics 3

	Asymmetric Encryption with RSA – Topics 2
	Message Digests – Topics 3
	Digital Signatures – Topics 3
	Quantum Cryptography – Topics 4
	Conclusion
	Emerging Topics
	The Internet of Things – Topics 3
	Economics – Topics 3
	Electronic Voting – Topics 3
	Cyber Warfare – Topics 3
	Conclusion
	The Web Application Hacker's Handbook
	Introduction
	Web Application (In)security
	The Evolution of Web Applications – Topics 2
	Web Application Security – Topics 5
	Summary
	Core Defense Mechanisms
	Handling User Access – Topics 3
	Handing User Input – Topics 4
	Handling Attackers – Topics 4
	Managing the Application
	Summary
	Questions
	Web Application Technologies
	The HTTP Protocol – Topics 11
	Web Functionality – Topics 3
	Encoding Schemes – Topics 6
	Next Steps
	Questions
	Mapping the Application
	Enumerating Content and Functionality – Topics 5
	Analyzing he Application – Topics 4
	Summary
	Questions
	Bypassing Client-Side Controls
	Transmitting Data Via the Client – Topics 6
	Capturing User Data: HTML Forms – Topics 3
	Capturing User Data: Browser Extensions – Topics 6
	Handling Client-Side Data Securely – Topics 3
	Summary
	Questions
	Attacking Authentication
	Authentication Technologies
	Design Flaws in Authentication Mechanisms – Topics 13
	Implementation Flaws in Authentication – Topics 3
	Securing Authentication – Topics 8
	Summary
	Attacking Session Management
	The Need for State – Topics 1
	Weaknesses in Token Generation – Topics 3

	Weaknesses in Session Token Handling – Topics 6
	Securing Session Management – Topics 3
	Summary
	Questions
	Attacking Access Controls
	Common Vulnerabilities – Topics 6
	Attacking Access Controls – Topics 6
	Securing Access Controls – Topics 1
	Summary
	Questions
	Attacking Data Stores
	Injecting into Interpreted Contexts – Topics 1
	Injecting into SQL – Topics 14
	Injecting into NoSQL – Topics 1
	Injecting into XPath – Topics 5
	Injecting into LDAP – Topics 3
	Summary
	Questions
	Attacking Back-End Components
	Injecting OS Commands – Topics 7
	Manipulating File Paths – Topics 2
	Injecting into XML Interpreters – Topics 4
	Injecting into Back-end HTTP Requests – Topics 2
	Injecting into Mail Services – Topics 4
	Summary
	Questions
	Attacking Application Logic
	The Nature of Logic Flaws
	Real-World Logic Flaws – Topics 12
	Avoiding Logic Flaws
	Summary
	Questions
	Attacking Users: Cross-Site Scripting
	Varieties of XSS – Topics 3
	XSS Attacks in Action – Topics 3
	Finding and Exploiting XSS Vulnerabilities – Topics 3
	Preventing XSS Attacks – Topics 2
	Summary
	Questions
	Attacking Users: Other Techniques
	Inducing User Actions – Topics 2
	Capturing Data Cross-Domain – Topics 3
	The Same-Origin Policy Revisited – Topics 3
	Other Client-Side Injection Attacks – Topics 5
	Local Privacy Attacks – Topics 9
	Attacking ActiveX Controls – Topics 2
	Attacking the Browser – Topics 10
	Summary
	Questions
	Automating Customized Attacks
	Users for Customized Automation

	Enumerating Valid Identifiers – Topics 4
	Harvesting Useful Data
	Fuzzing for Common Vulnerabilities
	Putting It All Together: Burp Intruder
	Barriers to Automation – Topics 2
	Summary
	Questions
	Exploiting Information Disclosure
	Exploiting Error Messages – Topics 6
	Gathering Published Information
	Using Inference
	Preventing Information Leakage – Topics 3
	Summary
	Questions
	Attacking Native Compiled Applications
	Buffer Overflow Vulnerabilities – Topics 4
	Integer Vulnerabilities – Topics 3
	Format String Vulnerabilities – Topics 1
	Summary
	Questions
	Attacking Application Architecture
	Tiered Architectures – Topics 2
	Shared Hosting and Application Service Providers – Topics 4
	Summary
	Questions
	Attacking the Application Server
	Vulnerable Server Configuration – Topics 7
	Vulnerable Server Software – Topics 5
	Web Application Firewalls
	Summary
	Finding Vulnerabilities in Source Code
	Approaches to Code Review – Topics 2
	Signatures of Common Vulnerabilities – Topics 10
	PHP – Topics 4
	JavaScript
	Database Code Components – Topics 2
	Tools for Code Browsing
	Summary
	Questions
	A Web Application Hacker’s Toolkit
	Web Browsers – Topics 3
	Integrated Testing Suites – Topics 3
	Standalone Vulnerability Scanners – Topics 5
	Other Tools – Topics 4
	Summary
	A Web Application Hacker’s Methodology
	General Guidelines
	Map the Application’s Content – Topics 6
	Analyze the Application – Topics 4
	Test Client-Side Controls – Topics 3
	Test the Authentication Mechanism – Topics 14

	Test the Session Management Mechanism – Topics 10
	Test Access Controls – Topics 4
	Test for Input-Based Vulnerabilities – Topics 7
	Test for Function-Specific Input Vulnerabilities – Topics 7
	Test for Logic Flaws – Topics 5
	Test for Shared Hosting Vulnerabilities – Topics 2
	Test for Application Server Vulnerabilities – Topics 7
	Miscellaneous Checks – Topics 4
	Follow Up Any Information Leakage