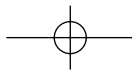
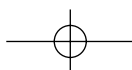


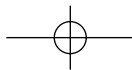
Contents

Introduction		xiv
Part I	Anatomy of Vulnerabilities	1
Chapter 1	That Horrible Sinking Feeling	3
	Avoiding That Sinking Feeling	4
	It's Up to You	4
	What Is Web Application Security?	5
	Security Is a Balance	5
	Common Ways Drupal Gets Cracked	5
	Authentication, Authorization, and Sessions	6
	Command Execution: SQL Injection and Friends	12
	Cross-Site Scripting	16
	Cross-Site Request Forgery	17
	The Big Scary World	19
	The Most Common Vulnerabilities	19
	Summary	20
Chapter 2	Security Principles and Vulnerabilities outside Drupal	21
	Server and Network Vulnerabilities	22
	Weaknesses across the Stack	22
	Denial of Service—Generic and Specific	23
	Defense in Depth	23

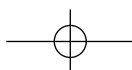


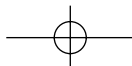
	Web Server File System Permissions	24
	Least Privilege—Minimum Permissions for the Task	25
	Least Privilege for Database Accounts	25
	Social and Physical Vulnerabilities	26
	The Vendor Password Please?	26
	This Is IT; Can I Help?	27
	Let's Get Physical	28
	Sanitizing a Typical Drupal Database	28
	Summary	29
Part II	Protecting against Vulnerabilities	31
Chapter 3	Protecting Your Site with Configuration	33
	Stay Current with Code Updates	33
	Staying Informed about Code Updates	34
	Updating Your Site's Code	36
	Know Your Attack Surface	38
	Best Practices for Contributed Modules	38
	Performing a Quick Security Scan	40
	Using Extra Security Modules	40
	Login and Session-Related Modules	41
	Password-Related Modules	42
	Visitor Analysis	44
	Smart Configuration of Core	45
	User Permissions	45
	Input Formats and Filters	45
	Summary	48
Chapter 4	Drupal's User and Permissions System	49
	Using the API	49
	What Are Hooks, Form Handlers, and Overrides?	51
	Defining Permissions: hook_perm	52
	Checking Permission: user_access and Friends	53
	Menu Callback Permissions	54
	Input Format Access: filter_access	56
	Common Mistakes with Users and Permissions	57
	Insufficient or Incorrect Menu Access	57
	Overloading a Permission	58
	Access Definitely Denied	58



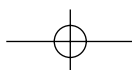


	Acting as Another User—and Getting Stuck	59
	Summary	61
Chapter 5	Dangerous Input, Cleaning Output	63
	Database Sanitizing: db_query and Friends	63
	Queries for Drupal 6.x and Earlier	64
	Improper Use of db_query	65
	Queries for Drupal 7.x and Newer	66
	Translation and Sanitizing: t	67
	Improper Use of t	68
	Linking to Content: l and url	69
	The Form API	70
	Semantic Protection: Invalid Form Data	71
	Form API: Sanitizing Options and Labels	73
	Filtering Content: check_plain, check_markup, filter_xss_admin	74
	Escaping Everything: check_plain	75
	Filtering HTML-Formatted Code: check_markup	77
	Basic Filtering for Admins: filter_xss_admin	77
	Summary	78
Chapter 6	Safety in the Theme	79
	Quick Introduction to Theming in Drupal	79
	Overridable Templates and Functions	80
	Providing Variables for Templates	82
	Common Mistakes	83
	Printing Raw Node Data	83
	Best Practice: Filter Data Prior to Using Templates	86
	Summary	88
Chapter 7	The Drupal Access System	89
	Respecting the Access System	90
	Modifying Queries for Access: db_rewrite_sql	90
	Testing Access for a Single Node: node_access	92
	Case Study: Private Module	93
	Node Access Storage Explained	93
	Summary	97
Chapter 8	Automated Security Testing	99
	Test Drupal with Drupal: Coder Module	100



**xii Contents**

	More Testing Drupal with Drupal Security Scanner	102
	Testing Drupal with Grendel-Scan	105
	Summary	107
Part III	Weaknesses in the Wild	109
Chapter 9	Finding, Exploiting, and Avoiding Vulnerabilities	111
	Strategies to Crack Drupal	112
	Searching Core and Contrib for Vulnerabilities	112
	Using Grep to Search for Common Mistakes	112
	Finding Sites Vulnerable to the Stock Weakness	115
	Finding Vulnerabilities by Happenstance	116
	Exploiting the Talk Module XSS Vulnerability	120
	How to Report Vulnerabilities	123
	Summary	124
Chapter 10	Un-Cracking Drupal	127
	Step 1: Secure the Menu	128
	Step 2: Secure the User Search	130
	Step 3: Secure the Node List	131
	Step 4: Disable Users Safely	133
	Drupal Un-cracked	134
Part IV	Appendixes	135
Appendix A	Function Reference	137
	Text-Filtering Functions	137
	Link and URL Building Functions	139
	Users and Permissions	142
	Database Interaction	144
Appendix B	Installing and Using Drupal 6 Fresh out of the Box	147
	Step 1: Installing Drupal—Easier Than Ever Before	149
	Downloading Drupal	150
	Unzipping and Preparing Files for Upload	150
	Uploading Files	150
	Creating the Database and User for the Drupal Installation	151
	Running the Drupal Installation Wizard	151
	Alternate Method: Managing Drupal with CVS	155



Updating Drupal Core and Running the Update Script	156
Step 2: Designing and Building the Architecture	158
Application Scope and Domain	158
Creating Roles and Users	160
Installing and Enabling Modules	161
Making the Site Bilingual	162
Step 3: Creating the Business Objects	167
Step 4: Creating the Workflows	172
Implementing the Registration Workflow	172
Implementing the Client’s Workflow	177
Implementing the Translator Team Leader’s Workflow	184
Implementing the Translator’s Workflow	188
Installing the Vulnerable.module	195
Summary	196
Appendix C Leveraging Community Resources	197
Resources from the Drupal Security Team	197
General Security Resources	199
PHP.net	199
OWASP	199
Google Code University	200
Heine Deelstra	200
Groups.Drupal.org	201
Robert Hansen—rsnake	201
Bruce Schneier	201
CrackingDrupal.com	202
Summary	202
Glossary	203
Index	213