

CONTENTS IN DETAIL

INTRODUCTION

xiii

1

THE FAQs OF LIFE—THE SCRIPTS EVERY PHP PROGRAMMER WANTS (OR NEEDS) TO KNOW 1

#1: Including Another File as a Part of Your Script	2
What Can Go Wrong?	3
#2: Highlighting Alternate Row Colors in a Table	4
Hacking the Script	5
#3: Creating Previous/Next Links	7
Using the Script	10
#4: Printing the Contents of an Array	11
#5: Turning an Array into a Nonarray Variable That Can Be Restored Later	12
What Can Go Wrong?	12
#6: Sorting Multidimensional Arrays	13
Hacking the Script	14
#7: Templating Your Site with Smarty	14
Installing Smarty	14
A Brief Smarty Tutorial	15
What Can Go Wrong?	16
Hacking the Script	17

2

CONFIGURING PHP 19

Configuration Settings and the php.ini File	20
Locating Your php.ini File	20
#8: Revealing All of PHP's Settings	21
#9: Reading an Individual Setting	21
#10: Error Reporting	22
Common Error Messages	23
#11: Suppressing All Error Messages	24
#12: Extending the Run Time of a Script	24
What Can Go Wrong?	25
#13: Preventing Users from Uploading Large Files	25
#14: Turning Off Registered Global Variables	25
#15: Enabling Magic Quotes	26
What Can Go Wrong?	26
#16: Restricting the Files that PHP Can Access	26
What Can Go Wrong?	27
#17: Shutting Down Specific Functions	27
#18: Adding Extensions to PHP	27
Adding PHP Extensions	28
Installing Extensions with a Web-Based Control Panel	29
What Can Go Wrong?	32

3	PHP SECURITY	33
	Recommended Security Configuration Options	35
	#19: SQL Injection Attacks	35
	#20: Preventing Basic XSS Attacks	37
	#21: Using SafeHTML	38
	What Can Go Wrong?	39
	#22: Protecting Data with a One-Way Hash	40
	Hacking the Script	41
	#23: Encrypting Data with Mcrypt	41
	Hacking the Script	43
	#24: Generating Random Passwords	43
	Using the Script	44
4	WORKING WITH FORMS	45
	Security Measures: Forms Are Not Trustworthy	45
	Verification Strategies	46
	Using \$_POST, \$_GET, \$_REQUEST, and \$_FILES to Access Form Data	47
	#25: Fetching Form Variables Consistently and Safely	47
	#26: Trimming Excess Whitespace	47
	#27: Importing Form Variables into an Array	48
	#28: Making Sure a Response Is One of a Set of Given Values	51
	Hacking the Script	51
	#29: Using Multiple Submit Buttons	52
	#30: Validating a Credit Card	52
	Using the Script	54
	Hacking the Script	55
	#31: Double-Checking a Credit Card's Expiration Date	55
	Using the Script	56
	#32: Checking Valid Email Addresses	56
	#33: Checking American Phone Numbers	57
5	WORKING WITH TEXT AND HTML	59
	#34: Extracting Part of a String	59
	Hacking the Script	61
	#35: Making a String Uppercase, Lowercase, or Capitalized	62
	What Can Go Wrong?	62
	#36: Finding Substrings	63
	What Can Go Wrong?	64
	#37: Replacing Substrings	64
	What Can Go Wrong?	65
	#38: Finding and Fixing Misspelled Words with pspell	65
	Working with the Default Dictionary	66
	Adding a Custom Dictionary to pspell	68
	What Can Go Wrong?	69

#39: Regular Expressions	69
Regular Expression Basics	69
Special Character Sequences	70
Pattern Repeaters	71
Grouping	71
Character Classes	71
Putting It All Together	72
Matching and Extracting with Regular Expressions	72
Replacing Substrings with Regular Expressions	74
#40: Rearranging a Table	75
#41: Creating a Screen Scraper	75
Hacking the Script	77
#42: Converting Plaintext into HTML-Ready Markup	77
#43: Automatically Hyperlinking URLs	80
#44: Stripping HTML Tags from Strings	80

6

WORKING WITH DATES

81

How Unix Time Works	81
#45: Getting the Current Timestamp	82
#46: Getting the Timestamp of a Date in the Past or Future	83
Creating Timestamps from a String	83
Creating Timestamps from Date Values	84
#47: Formatting Dates and Times	85
#48: Calculating the Day of the Week from a Given Date	88
#49: Finding the Difference Between Two Dates	88
Using the Script	89
Hacking the Script	90
MySQL Date Formats	90

7

WORKING WITH FILES

91

File Permissions	91
Permissions with an FTP Program	92
The Command Line	93
What Can Go Wrong?	93
#50: Placing a File's Contents into a Variable	93
Hacking the Script	95
What Can Go Wrong?	95
#51: Creating and Writing to a File	96
#52: Checking to See If a File Exists	96
#53: Deleting Files	97
#54: Uploading Images to a Directory	97
Using the Script	101
What Can Go Wrong?	101
Hacking the Script	101
#55: Reading a Comma-Separated File	101

8	USER AND SESSION TRACKING	103
	Using Cookies and Sessions to Track User Data	104
	Cookies	104
	Sessions	104
	#56: Creating a “Welcome Back, <i>Username!</i> ” Message with Cookies	105
	What Can Go Wrong?	106
	#57: Using Sessions to Temporarily Store Data	107
	What Can Go Wrong?	109
	#58: Checking to See If a User’s Browser Accepts Cookies	109
	#59: Redirecting Users to Different Pages	110
	#60: Forcing a User to Use SSL-Encrypted Pages	111
	#61: Extracting Client Information	111
	#62: Session Timeouts	115
	#63: A Simple Login System	116
9	WORKING WITH EMAIL	119
	#64: Using PHPMailer to Send Mail	120
	Installing PHPMailer	120
	Using the Script	121
	Adding Attachments	122
	What Can Go Wrong?	123
	#65: Using Email to Verify User Accounts	124
10	WORKING WITH IMAGES	129
	#66: Creating a CAPTCHA (Security) Image	129
	#67: Creating Thumbnail Images	136
11	USING cURL TO INTERACT WITH WEB SERVICES	141
	#68: Connecting to Other Websites	142
	#69: Using Cookies	144
	#70: Transforming XML into a Usable Form	144
	#71: Using Mapping Web Services	146
	#72: Using PHP and SOAP to Request Data from Amazon.com	149
	#73: Building a Web Service	151

12	
INTERMEDIATE PROJECTS	155
#74: A User Poll	156
Creating a Ballot Form	157
Processing the Ballot	159
Getting Poll Results	160
Hacking the Script	162
#75: Electronic Greeting Cards	162
Choosing a Card	164
Sending the Card	165
Viewing the Card	169
Hacking the Script	171
#76: A Blogging System	171
Creating Blog Entries	172
Displaying an Entry	174
Adding Comments	178
Creating a Blog Index	178
Hacking the Script	181
 APPENDIX	 183
 INDEX	 185