

Index

A

- ``, 140
- access, 9–10
- access, 57
- Access administration pages, 173
- Access all views, 173
- access arguments, 54–56
 - hook_menu, 57
- access bypass, 20
- access callback, 54–56
 - hook_menu, 57
- Access content, 170
- Access site reports, 173
- access system, 89–97
- access user profiles, 10
- access-denied, 57, 58–59
 - HTTP, 58
- `$account->uid`, 55
- `action_as_another_user`, 60
- Add fields, 181
- Add filters, 181
- Admin Role module, 172
- Administer actions, 173
- Administer blocks, 173
- Administer content types, 173
- Administer files, 173
- Administer filters, 173
- Administer languages, 173
- Administer menu, 173
- Administer nodes, 171, 173
- Administer permissions, 173
- Administer search, 173

- Administer site configuration, 173
- Administer site-wide contact form, 173
- Administer taxonomy, 173
- Administer users, 173
- administer users permission, email address, 10
- Administer views, 173
- AJAX
 - CSRF, 18
 - passwords, 154
- anonymous role, 9
 - filters, 47
- AOL, OpenID, 43
- Apache, update, 23
- API, 49–51. *See also* Form API
 - Database, 144–145
 - filters, 74
 - security, 5–6, 50–51
 - SQL injection, 67
 - application programming interface. *See* API
- arbitrary file upload, 15–16
 - occurrences, 20
- architecture, 158–166
- `array(1)`, 55
- The Art of Deception* (Mitnick), 4, 26
- Atom, 205
- attack surface, 6, 38
 - modules, 40
- authenticated role, 9
 - filters, 47

- authentication, 6–7
 - weaknesses, 7–9
- authorization, 6, 9–10
 - bypass, 10
 - Vulnerable module, 9–10
 - weaknesses, 9–10
- automated security testing, 99–107

B

- `%b`, 64
- BASE, 47
- Basic settings, 181
- best practices
 - contributed modules, 38–40
 - filters, 86–88
 - templates, 86–88
- bilingual, 162–166
- binary data, escapes, 63
- blacklists, 12
- blobs. *See* binary data
- `<blockquote>`, 46
- blocks, 203
- blog, 54
- `_blog_post_exists()`, 56
- blogs
 - Drupal Planet, 39
 - page-request cycle, 13–14
- boundary validation, 13
 - XSS, 16
- `box.tpl.php`, 81
- branch, 208
- breadcrumb, 203–204

brute force attack, 7
 Login Security, 41
 build_id, 122
 business objects, 167–171

C

C programming, placeholder replacement system, 63
 callback, 208
 CAPTCHA bypass, 20
 Cascading Style Sheets (CSS), 86–87
 aggregation, 24
 CCK. *See* Content Construction Kit
 CCLite. *See* Creative Commons Lite module
 certificates, SSL, 5
 CHANGELOG.txt, 118–119
 check_markup, 74, 75, 85
 HTML, 77
 checkmarkup(\$tainted, \$filter==XYZ), 138–139
 check_plain(), 40, 53
 check_plain, 73, 132, 139
 HTML, 75–76
 sanitizing data, 88
 check_plain(\$tainted), 138
 check_url, 139
 theme_image, 141
 check_url
 (\$tainted_path), 140
 clean URL, 204
 Client, 169
 client, workflow, 177–184
 client_application, 168
 Code Red, 34
 code updates, 33–38
 test site, 36
 Coder module, 100–104
 Coder Tough Love module, 100
 Cohn, Mike, 148
 command execution, 12–16
 occurrences, 20
 SQL injection, 12
 command-line shell, 37–38, 112–115
 comment_edit, 143
 committer, 208
 Concurrent Version System (CVS), 36–37, 113, 209
 download, 155–156

upload, 155–156
 confirm_form, 134
 Contact module, 161
 Content Construction Kit (CCK), 83–85, 147
 Content module, 161
 Content Translation module, 161
 content_format, 85
 contrib, 204
 contributed modules, 19
 best practices, 38–40
 email, 35
 RSS, 35
 vulnerabilities, 112–123
 contributor, 208–209
 /cookie-monster, 128
 cookies, JavaScript, 120–123
 core, vulnerabilities, 112–123
 core contributor, 209
 core modules, 19
 crackingdrupal.com, 202
 Create page content, 171
 Create translation content, 171
 Creative Commons Lite module (CCLite), 114–116
 cron, 204
 cron.php, 204
 cross-site request forgery (CSRF), 17–18
 AJAX, 18
 Filtered HTML, 46
 occurrences, 20
 tokens, 17
 Userpoints, 117–119
 cross-site scripting (XSS), 12, 16–17, 19, 200
 boundary validation, 16
 db_query, 130
 DOM, 16
 Filtered HTML, 46
 filters, 77
 HTML, 46
 occurrences, 20
 reflected, 16
 Security Scanner, 103–104
 stored, 16
 t(), 102, 130
 Talk module, 119–123
 Vulnerable module, 16
 Crypto-Gram, 201
 CSRF. *See* cross-site request forgery
 /csrf-diable, 128
 CSS. *See* Cascading Style Sheets

.css, 118
 CSS/HTML markup, 80
 \$current_user, 60
 CVS. *See* Concurrent Version System
 cvs checkout, 157
 cvs up, 37
 cvs update, 157
 Cygwin tool, 114

D

%d, 64
 #DANGEROUS_SKIP_CHECK, 72
 Database API, 144–145
 databases
 installation, 151
 Least Privilege, 25–26
 Date module, 161
 db_escape_table
 (\$table_name), 145
 db_ewrite_sql, 130–131
 db_placeholders, 65
 db_query(), 40
 db_query, 63–67
 improper use, 65–66
 SQL injection, 66, 102
 XSS, 130
 db_query("SELECT name FROM {user} WHERE mail=%s, "\$tainted), 144
 db_query_range, 65
 db_query_range(), 144–145
 db_result, 66
 db_rewrite_sql, 90–92
 Deelstra, Heine, 122, 200–201
 default_nodes_main, 71
 default.settings.php, 150, 156
 Defense in Depth, 23–24
 SQL injection, 26
 Delete any translation content, 171
 Delete own page content, 171
 Delete own translation content, 171
 Delete revisions, 171
 denial of service attacks, 23
 designer, 80
 Devel module, 82
 Devel Node Access, 95
 development terms, 208–211
 dictionary attack, 7

diff, 37
 distributed denial of service
 attack, 23
 DIV, 47
 div, 81
 DOM, XSS, 16
 domain, 158–159
 domain names, login form, 43
 double escape, 76
 download, CVS, 155–156
 downloading, 150
 Drupal Handbook
 Documentation, 149
 Drupal Planet, blogs, 39
 DRUPAL-6, 37
 drupal_access_denied, 59
 drupal_access_denied(),
 143–144
 Drupalcamp, 205
 Drupalcon, 205
 drupal_get_form, 73
 drupal_get_token
 (\$string), 142
 drupal.org/handbook/cvs, 37
 drupal.org/projet/
 issues/drupal, 37
 drupal.org/projet/
 update_status, 35
 drupal.org/projet/
 usage, 39
 drupal.org/security, 34
 drupal.org/security/
 rss.xml, 34
 drupal_set_message, 102
 drupal_set_title, 75, 120,
 123
 drupal_valid_token, 142
 Druplicon, 204
 drush -l d6.example.com
 pm update, 38
 drush module, 37–38
 Due date, 169

E

Edit any translation content,
 171
 Edit field_translation_client,
 170
 Edit field_translation_date_
 due, 170
 Edit field_translation_status,
 170
 Edit field_translation_
 translator, 170

Edit own page content, 171
 Edit own translation content,
 171
 , 46
 email, contributed modules, 35
 email address
 administer users permission,
 10
 hash, 14
 username, 10
 EMBED, 47
 <embed>, 46
 enabled, 205
 English, 162–166, 179
 escape
 binary data, 63
 double, 76
 slash, 14
 SQL, 13
 strings, 63
 example.com/
 CHANGELOG.txt, 118

F

%f, 64
 failed logins, Login Security,
 41
 FAPI. *See* Form API
 feed, 205
 field_client_email, 171
 field_translation_client, 169
 field_translation_due_date,
 169
 field_translation_status, 169
 field_translation_text, 169
 field_translation_translator,
 169
 file overwrite, 20
 file_create_url
 (\$name_of_file), 141
 files, 24
 Filter module, security, 56
 filter_access, 56
 filters, 205
 anonymous role, 47
 API, 74
 authenticated role, 47
 best practices, 86–88
 HTML, 16, 46, 77, 205
 PHP, 47–48
 roles, 47
 t(), 50
 text, 137–139
 URL, 205

XSS, 77
 filter_xss, 74, 84
 filter_xss_admin(), 40
 filter_xss_admin, 74, 75,
 77
 filter_xss_admin
 (\$tainted), 139
 fingerprinting, 120
 foo.module, 86
 foo_process, 86
 Form API (FAPI), 17, 70–74
 sanitizing data, 73–74
 semantic protection, 71–73
 FRAMESET, 47
 FreeBSD, 22
 FTP, 150
 Full HTML, 46, 77
 function, password, 15
 "function theme_*", 82
 functionality, 205

G

GET, 18
 Ghilardi, Dario Battista, 102
 gid, 94
 GNU/Linux, 22
 Google Code University, 200
 grant_view, 95
 Green, Doug, 100
 Grendel-Scan, 105–107
 grep, 113–115
 groups.drupal.org, 201

H

<h1>, 77
 H1 tags, 205
 <h2>, 46
 ha.ckers.org, 201
 hacking core, 36
 handbook, security team,
 198–199
 handlers, 209
 submit, 51
 validation, 51
 Hansen, Robert, 201
 hash
 email address, 14
 password, 14
 hax0rs lab, 3
 HEAD/Dev, 209
 heine.familiedeelstra.com,
 200–201
 hook_cron, 204

hook_disable, 93, 97
hook_enable, 97
hook_file_download, 97
hook_form_alter, 51
hook_menu, 54, 113, 129
 access arguments, 57
 access callback, 57
 _hookname, 83
hook_node_access
 _records, 97
hook_nodeapi, 51, 209
hook_node_grants, 9, 97
hook_perm(), 52–53
hooks, 51, 209
href, 70
.htaccess, 41, 155
HTML, 12, 71, 73
 check_markup, 77
 check_plain, 75–76
 filters, 16, 46, 77, 205
 HTTP, 14
 input formats, 45–48
 XSS, 46
HTML corrector, 205
HTTP
 access-denied, 58
 HTML, 14
 Internet, 10
 HTTP POST, 122
 HTTP response splitting, 20
 http:BL:http://drupal.org/
 project/httpbl module, 44
 HTTPS, 11

I

IBM DB2, 22
IFRAME, 47
Illegal choice warning screen,
 73
IMG, 47
includes/theme.inc, 80
INPUT, 47
input format, 205
 HTML, 45–48
installation, 147–196
 databases, 151
 workflow, 148–149
Installation Wizard, 151–155
IN-style query, 65
insufficient authentication, 7
 /insufficient-
 authentication,
 128–129
internal diagnostic utilities, 27

Internationalization, 101
Internet, HTTP, 10
 "inurl:", 15
 "inurl:node," 115
IP address, Login Security, 41
issues, 209

J

jargon, 203–206
Java, PHP, 22
JavaScript, 16
 cookies, 120–123
 Password Strength, 42
 Vulnerable module, 16
jQuery, 12
 .js, 12, 118

K

Kudwien, Daniel F., 100

L

l(), 40
l, 69–70
l(\$sanitized_html,
 \$tainted_path,
 array('html' => TRUE)),
 141
l(\$tainted_title,
 \$tainted_path), 139
LAMP (Linux, Apache,
 MySQL, PHP), 22
language, bilingual, 162–166
Least Privilege
 databases, 25–26
 permissions, 25
"LIMIT 0, 10," 64
line break converter, 205
LINK, 47
links, tokens, 18
Linux, update, 23
Linux, Apache, MySQL, PHP.
 See LAMP
Locale module, 161
localization system, 50
 t(), 67
logging sensitive data, 20
login form, 7
 domain names, 43
 OpenID, 43
Login Security, 41
Login Security module, 41

/log-in-sql-injection,
 128
Logout, 174, 178, 185

M

Mac OS X, 22
mail header injection, 20
Mailhandler module, 65
Malformed UTF-8, 200
Manage Fields, 167–168
MD5. See Message-Digest
 algorithm 5
menu, 128
menus, 206
 security, 57
Message-Digest algorithm 5
 (MD5), 14
 password, 15
META, 47
Mitnick, Kevin, 4, 26
module_invoke, 53
modules, 209–210. See also
 specific modules
 attack surface, 40
 enabling, 161–162
 installing, 161–162
 new, 41
 passwords, 42–43
 security, 6
 security team, 198
 SQL injection, 10
 uploads, 16
 users, 11–12
modules_d6, 113
Mueller, John Paul, 21
Multilingual Support, 164, 169
My account, 174, 178, 185
myopenid.com, 43
MySQL, 22
my_text_field, 86

N

-n flag, 113
Négyesi, Károly, 102, 200
Nester, David, 99
New translation, 178, 185
nid, 94
no mixed-mode, SSL, 45
node, 206
Node module, 170
node_access, 90–97, 131
node_access_example.
 module, 93

node_access_rebuild, 93
 nodeapi, 96
 node_build_content, 85
 node-list, security, 131–133
 /node-list, 128
 node_load, 86

O

OBJECT, 47
 Official Release, 36
 Open Web Application
 Security Project (OWASP),
 199–200
 OpenID, 42, 161
 login form, 43
 OpenID Support module, 43
 #options, 74
 \$options, 69
 Oracle, 22
 overrides, 51, 210
 OWASP. *See* Open Web
 Application Security
 Project

P

PAC. *See*
 Presentation-Abstraction
 Control
 page-request cycle, blogs,
 13–14
 pager_query, 64
 PASS_THROUGH, 123
 password(s), 7
 AJAX, 154
 changing, 26
 function, 15
 hash, 14
 Login Security, 41
 MD5, 15
 modules, 42–43
 server, 28
 vendors, 26–27
 Password Checker, 42
 Password Policy module, 42
 Password Strength module, 42
 patches, 210
 path alias, 206
 Path module, 66, 69
 penetration test, 99–100
 permissions, 9–10, 206
 Administer, 173
 Least Privilege, 25
 mistakes, 56–61

overloading, 58
 users, 10, 12, 45, 142–144
 Persistent Login module, 41
 PHP, 16, 22
 filters, 47–48
 Java, 22
 upload, 24
 XHTML, 86
 PHP Filter module, 161
 phpass. *See* Secure Password
 Hashes module
 phpBB, 3, 4
 PHPIDS. *See* PHP-Intrusion
 Detection System
 php.ini, 41
 PHP-Intrusion Detection
 System (PHPIDS), 40, 44
 PhpMyAdmin, 151
 PHP.net, 199
 PHPTemplate, 210
 phptemplate_box, 81
 physical access, servers, 28
 piggybackers, 26
 placeholder replacement
 system, C programming, 63
 .po, 163
 POST, 17
 PostgreSQL, 22
 Power, Stella, 100
 preprocess, 83
 Presentation-Abstraction
 Control (PAC), 79
 printf(), 64
 private key, 17
 Private module, 89, 93
 private_author, 95
 private_file_download,
 96
 private_form_alter, 96
 private.install, 93
 private_install, 96
 private_link, 96
 private_node_access_
 records, 96
 private_nodeapi, 96
 private_perm, 95
 private_theme, 96
 privilege escalation, 12, 20
 Profile module, 161, 206
 profile_browse, 59
 profiles, 210
 Project Usage Overview, 39
 pseudo markup, 46

R

README.txt, 119
 realm, 94
 ReCrawl, 103
 reflected XSS, 16
 region, 206
 Register as a client!, 174, 178,
 185
 Register as a translator!, 174,
 178, 185
 registration, workflow,
 172–177
 team leader, 186–187
 Remember Me, 41
 REST, 12, 22
 Revert revisions, 171
 roles, 9, 206
 creating, 160–161
 filters, 47
 RSA key fob, 8
 RSA SecurID, 8
 RSS, 34, 205
 contributed modules, 35
 translator workflow, 188

S

%s, 64
 SA-2008– 049, 104
 Sadmin, 34
 safe, 85
 safe data handling, 13
 safe tags, 47
 safety, themes, 79–88
 safety for all, 205
 salt, 42–43
 Salt module, 42–43
 sanitizing data, 12–13, 28–29,
 63–67
 check_plain, 88
 FAPI, 73–74
 sanity for themers, 205–206
 SantyWorm, 3, 34
 scalability, 132
 Schneier, Bruce, 201
Schneier on Security (Schneier),
 201
 schneier.com, 201
 scope, 158–159
 SCRIPT, 47
 Secure Password Hashes
 module (phpass), 43
 security
 API, 5–6, 50–51
 balance, 5

- security (*continued*)
 - Filter module, 56
 - menus, 57
 - modules, 6
 - node-list, 131–133
 - resources, 199–202
 - user search, 130–131
 - Security Checks, 101
 - Security Complete* (Mueller), 21
 - security scan, 40
 - Security Scanner, 102–104, 201
 - XSS, 103–104
 - security team, 197–199
 - handbook, 198–199
 - modules, 198
 - Select different theme, 173
 - self-signed certificates, 5
 - semantic protection, FAPI, 71–73
 - servers
 - passwords, 28
 - physical access, 28
 - session fixation, 20
 - session ID, 11, 17
 - WiFi, 11
 - session impersonation, 20
 - sessions, 6
 - weaknesses, 10–12
 - session_save, 130
 - session_save_session, 60–61
 - session_save_session (TRUE|FALSE), 142–143
 - /session-switcher, 128
 - settings.php, 24–25, 41, 150
 - shoulder surfers, 26
 - show-me-the-data, 130
 - /show-me-the-data, 128
 - Single Login module, 41
 - single quote, SQL, 14
 - ./sites/all/modules, 161
 - sites/all/modules, 195
 - .sites/default, 156
 - slash escape, SQL, 14
 - snippets, 210
 - SOAP, 12
 - social engineers, 26, 119
 - telephone numbers, 27
 - Spanish, 162–166, 179
 - special characters, username, 14
 - SQL. *See* Structured Query Language
 - SQL injection, 5
 - API, 67
 - command execution, 12
 - db_query, 66, 102
 - Defense in Depth, 26
 - modules, 10
 - occurrences, 20
 - t(), 130
 - Vulnerable module, 14–15
 - SQL Server, 22
 - SQL Slammer, 34
 - SQL Standards, 101
 - SQLite, 22
 - SSL
 - certificates, 5
 - no mixed-mode, 45
 - stacks, 22–23
 - Status, 169
 - stored, XSS, 16
 - \$string, 65
 - strings, escapes, 63
 - strip_tags, 84
 - , 46
 - Structured Query Language (SQL), 210. *See also* SQL injection
 - escape, 13
 - single quote, 14
 - slash escape, 14
 - STYLE, 47
 - submit handlers, 51
 - Sutton, Willie, 112
 - system path, 206–207
- T**
- t(), 40, 50
 - filters, 50
 - localization system, 67
 - SQL injection, 130
 - XSS, 102, 130
 - t('String@cleaned, 'array('@cleaned'=>\$stainted)'), 137–138
 - TABLE, 47
 - tag, 207
 - Talk module, 104
 - XSS, 119–123
 - Tamper Data, 72
 - taxonomy, 207
 - TD, 47
 - team leader
 - registration workflow, 186–187
 - translation workflow, 187–188
 - workflow, 184–188
 - teaser, 207
 - telephone numbers, social engineers, 27
 - temp, 24
 - template.php, 81, 85
 - templates, 210
 - best practices, 86–88
 - themes, 80
 - variables, 82–83
 - terms, 207
 - test site, code updates, 36
 - Text, 169
 - text filtering, 137–139
 - them(), 80–81
 - theme(), 51
 - theme_*, 82
 - Theme Developer module, 82
 - theme_box, 80–81, 83
 - theme_form_name, 82
 - theme_image, 141
 - check_url, 141
 - theme_menu_item, 80
 - theme_private_node_link, 96
 - themer, 80
 - themes, 210–211
 - safety, 79–88
 - templates, 80
 - theming, 211
 - third-party modules, 9
 - title, 69
 - tokens
 - CSRF, 17
 - links, 18
 - tpl.php, 82
 - TR, 47
 - Translate interface, 173
 - Translation, 162
 - Translation Studio, 147, 164–166, 189–190, 195
 - translation workflow, team leader, 187–188
 - translation_client, 167
 - Translator, 169
 - translator, workflow, 188–195
 - RSS, 188
 - Translator Application, 169
 - Trigger module, 162
- U**
- uid, 56
 - \$uid, 64

Uniform Resource Locator (URL), 6, 207
 building functions, 139–142
 clean, 204
 filter, 205
 Vulnerable module, 18

UNION, 14, 15

Unix, 22

unzipping, 150

update script, 156–158

Update Status module, 34–35, 198

update.php, 38

UPGRADE.txt, 36

upload, 150–151
 CVS, 155–156
 modules, 16
 PHP, 24

Upload module, 162

URL. *See* Uniform Resource Locator

url, 69–70

url (\$stainted_path), 140

Use PHP for block visibility, 173

Use PHP input for field settings, 173

\$user, 60–61

user(s), 207
 creating, 160–161
 disabling, 133–134
 mistakes, 56–61
 modules, 11–12
 permissions, 10, 12, 45, 142–144

user 1, 8–9

user ID, Vulnerable module, 7–8

user search, security, 130–131
User Stories Applied (Cohn), 148

user_access(), 53–54

user_access, 95, 113

user_access('permission name'), 143

user_access system, 56

user.admin.in, 53

\$user_data, 70, 74

\$user_data2, 70

/user-form-data, 128

username, 7
 email address, 10
 special characters, 14

%user-name, 40

user-picture.tpl.php, 88

Userpoints, CSRF, 117–119

users:0, 55

\$user_search, 69

%user_uid_optional, 55

user_user_operations_block, 134

UTF-7, 200

V

validation handlers, 51

variables, templates, 82–83

\$variables, 83

vendors
 password, 26–27
 virtual private network, 26

View Description, 180

View Name, 180

View revisions, 171

View Tag, 180

View translations, 185

View Type, 180

Views module, 147, 162

virtual private network, vendors, 26

visitor analysis, 44

vocabulary, 207–208

vulnerability analysis tool, 99–100

/vulnerable, 18

Vulnerable module, 6, 73
 authorization, 9–10
 installing, 195–196

JavaScript, 16

SQL injection, 14–15

URL, 18
 user ID, 7–8
 XSS, 16

vulnerable_node_list, 91

W

website security, 5

weight, 208

where, 95

whitelist, 12

WiFi, session ID, 11

Wikis, 119

workflow
 client, 177–184
 creating, 172–196
 installation, 148–149
 registration, 172–177
 team leader, 186–187
 team leader, 184–188
 translator, 188–195
 RSS, 188

X

XHTML, 82
 PHP, 86

XMLRPC, 12

XSS. *See* cross-site scripting

Y

Yahoo!, OpenID, 43
 "yourmodule," 51

Z

zero indexed, 55

