

Segurança em PHP

**Desenvolva programas PHP com alto nível de segurança
e aprenda como manter os servidores web livres de ameaças**

Márcio Pessoa

Sumário

Agradecimentos	11
Sobre o autor	12
Prefácio	13
Software livre	15
Convenções tipográficas	16
Capítulo 1 ▪ Conceitos gerais.....	17
1.1 Segurança.....	17
1.2 Usabilidade <i>versus</i> segurança.....	19
1.3 Postura de defesa.....	20
1.4 Desempenho	20
1.5 Usuários ilegítimos	21
1.6 Filtro de dados	22
1.7 Manipulação de erros.....	22
1.8 Limitador de acessos	23
Capítulo 2 ▪ Segurança na internet	24
2.1 Desafios de segurança na web	24
2.2 Introdução ao HTTPS	25
Capítulo 3 ▪ Servidor web	28
3.1 Introdução ao servidor web.....	28
3.1.1 Usuário do servidor web	29
3.1.2 Estrutura de diretórios	30
3.2 Configuração do servidor web	30
3.2.1 Indexes	31
3.2.2 FollowSymLinks	31
3.2.3 Includes	31
3.2.4 ServerTokens	32
3.3 Restrições de acesso.....	34
3.3.1 Restrição por hosts	35
3.3.2 Restrição por autenticação.....	36
3.4 Proteção adicional	41
3.4.1 Rate limit	41
3.4.2 Controle de banda	41

Capítulo 4 • Boas práticas em PHP	43
4.1 Estrutura de um projeto	43
4.1.1 Protegendo informações confidenciais do sistema	44
4.1.2 Estrutura de diretórios.....	45
4.2 Configuração do PHP	46
4.2.1 register_globals	46
4.2.2 display_errors	49
4.2.3 log_errors.....	49
4.2.4 error_reporting.....	50
4.2.5 error_log.....	51
4.2.6 disable_functions	51
4.2.7 disable_classes	51
4.2.8 expose_php	52
4.2.9 upload_max_filesize	53
4.2.10 include_path.....	53
4.2.11 Outras diretrizes	53
4.3 Gerenciamento de erros	54
4.3.1 Alteração das mensagens de erros padrão	54
4.3.2 Configuração de um servidor compartilhado	56
Capítulo 5 • Formulários	58
5.1 Trabalhando com variáveis.....	58
5.1.1 Registrando variáveis	59
5.1.2 Tipos de dados	61
5.1.3 Filtro de dados	63
5.2 Ataques pelos formulários	64
5.2.1 Abuso no envio de e-mails (spam)	65
5.2.2 Cross-Site Scripting (XSS)	68
5.2.3 Ataques por upload de arquivo	70
5.2.4 CAPTCHA	72
5.2.5 CAPTCHA inverso	73
Capítulo 6 • Includes.....	74
6.1 Inibindo a exposição do código-fonte	74
6.2 Escondendo nomes de arquivos.....	77
6.3 Evitando injeção de código.....	79
6.3.1 White list	80
6.3.2 Black list.....	84
6.3.3 Ofuscamento de URL.....	85
Capítulo 7 • Sessões.....	86
7.1 Alguns conceitos sobre sessões	86
7.2 Cookies	88

7.2.1 Funcionamento	88
7.2.2 A problemática dos cookies	89
7.3 Dados de sessão expostos	90
7.4 Roubo de sessões.....	91
7.4.1 Fixação de sessões	91
7.5 Autenticação	94
Capítulo 8 ▪ Criptografia	96
8.1 HTTPS	96
8.1.1 Sobrecarga do HTTPS.....	96
8.1.2 Configuração do HTTPS.....	98
8.2 Scripts criptográficos.....	100
8.2.1 Armazenando senhas	101
8.3 Criptografando e descriptografando dados	102
Capítulo 9 ▪ SQL.....	105
9.1 Exposição dos dados de acesso.....	105
9.2 SQL injection	107
Capítulo 10 ▪ Reagindo às ameaças.....	111
10.1 Vírus	111
10.1.1 Instalação da biblioteca php-clamavlib.....	112
10.1.2 cl_info.....	113
10.1.3 cl_scanfile	113
10.1.4 cl_setlimits	114
10.1.5 cl_scanfile_ex	114
10.1.6 cl_pretcode	115
10.1.7 clam_scan_file	115
10.1.8 clam_get_version	115
10.1.9 Testando o php-clamavlib	116
10.1.10 Escaneando arquivos	117
10.2 Resposta a incidentes.....	117
10.2.1 O que fazer?	118
10.2.2 Como fazer?.....	118
10.3 Violação de propriedade intelectual	119
Apêndice A ▪ Notas sobre desempenho	121
A.1 Temporizador	122
A.2 Cuidados com temporizadores	125
Apêndice B ▪ Monitoração	126
B.1 Logs	126
B.2 Estatísticas de acesso	127
B.2.1 Webalizer.....	127
B.2.2 AWStats	128

B.3 Gerenciamento do sistema	128
B.3.1 SNMP.....	129
B.3.2 MRTG	130
B.3.3 Nagios	134
Apêndice C ■ phpMyAdmin	135
C.1 Criptografia.....	135
C.2 Métodos de autenticação	136
C.2.1 http.....	136
C.2.2 cookie	136
C.2.3 signon	137
C.2.4 config	137
Apêndice D ■ Funções que devem ser usadas com cautela	138
Apêndice E ■ Glossário	141
Referências bibliográficas.....	149
Índice remissivo	150