

Spis treści

O autorze	9
O redaktorze	11
Przedmowa	13
Rozdział 1. Zaczynamy	17
Wprowadzenie	17
Powszechnie używana terminologia	18
Wybór hostingu dostosowanego do potrzeb	19
Co to jest firma hostingowa?	19
Wybieranie firmy hostingowej	19
Pytania, jakie należy zadać przyszłemu dostawcy usług hostingowych	20
Pomieszczenia	20
O co zapytać dostawcę hostingu w kwestiach bezpieczeństwa?	21
Pytania dotyczące warunków w pomieszczeniach	21
Monitorowanie i ochrona lokalizacji	22
Instalowanie poprawek a bezpieczeństwo	22
Hosting współdzielony	23
Hosting dedykowany	25
Planowanie instalacji Joomla!	26
Jakemu celowi ma służyć Twoja witryna?	26
Jedenaście kroków do udanej architektury witryny	27
Pobieranie systemu Joomla!	29
Ustawienia	30
.htaccess	33
Uprawnienia	34
Zarządzanie użytkownikami	35
Typowe błędy	35
Ustanawianie parametrów bezpieczeństwa	38
Podsumowanie	45

Rozdział 2. Testowanie i rozwijanie witryny	47
Witaj w laboratorium!	48
Środowisko testowe	48
Jaki to ma związek z zabezpieczeniami?	49
Błędne koło aktualizowania	49
Tworzenie planu testów	52
Wykorzystanie środowiska testowego w planowaniu działań na wypadek awarii	54
Tworzenie dobrej dokumentacji	55
Korzystanie z systemu zarządzania tworzeniem oprogramowania	58
Raportowanie	60
Ravenswood Joomla! Server	62
Uruchamianie	63
Podsumowanie	64
Rozdział 3. Narzędzia	65
Wprowadzenie	65
Narzędzia, narzędzia i jeszcze raz narzędzia	66
HISA	66
Joomla! Tools Suite with Services	72
Jak zdrowie?	73
Nmap — narzędzie do mapowania sieci ze strony insecure.org	80
Wireshark	82
Metasploit — zestaw narzędzi do testów penetracyjnych	85
Nessus — skaner luk	87
Podsumowanie	89
Rozdział 4. Luki	91
Wprowadzenie	91
Instalowanie poprawek jest nieodzowne	93
Czym jest luka?	94
Luki związane z uszkodzeniem zawartości pamięci	95
Wstrzyknięcie kodu SQL	97
Ataki przez wstrzyknięcie poleceń	99
Dlaczego pojawiają się luki?	100
Co można zrobić, aby zapobiec lukom?	100
Odmowa dostępu	103
Niewłaściwe formatowanie zmiennych i niebezpiecznych danych wejściowych	103
Brak testów w zróżnicowanym środowisku	104
Testowanie w różnych wersjach baz SQL	104
Współdziałanie z rozszerzeniami niezależnych producentów	104
Użytkownicy końcowi	105
Socjotechnika	105
Nieregularne instalowanie poprawek i aktualizacji	106
Podsumowanie	107

Rozdział 5. Anatomia ataków	109
Wprowadzenie	110
Wstrzyknięcie kodu SQL	110
Testowanie odporności witryny na wstrzyknięcie kodu SQL	114
Kilka metod zapobiegania wstrzyknięciu kodu SQL	114
Metoda zapobiegania wstrzyknięciu kodu SQL zalecana przez PHP.NET	115
Ataki RFI	116
Najprostszy atak	118
Co możemy zrobić, żeby powstrzymać atak?	118
Zapobieganie atakom RFI	122
Podsumowanie	123
Rozdział 6. Jak to robią „zli chłopcy”?	125
Obecne regulacje prawne	126
Namierzanie celu	127
Poznawanie celu	128
Narzędzia do wykrywania luk	131
Nessus	131
Nikto — skaner luk o otwartym dostępie do kodu źródłowego	132
Acunetix	132
Nmap	133
Wireshark	134
Ping Sweep	134
Firewalk	134
Angry IP Scanner	135
Cyfrowe graffiti a prawdziwe ataki	137
Wyszukiwanie celów ataku	144
Co możesz zrobić?	144
Przeciwdziałanie	145
Co zrobić, jeśli firma hostingowa nie jest skłonna do współpracy?	146
Co zrobić, jeśli ktoś włamał się do mojej witryny i ją oszpecił?	146
Co zrobić, jeśli napastnik umieścił na serwerze rootkita?	147
Słowo na zakończenie	147
Podsumowanie	148
Rozdział 7. Pliki php.ini i .htaccess	149
Plik .htaccess	150
Zmniejszanie transferu danych	151
Wyłączanie sygnatury serwera	151
Zapobieganie dostępowi do pliku .htaccess	151
Zapobieganie dostępowi do jakiegokolwiek pliku	151
Zapobieganie dostępowi do plików różnych typów	152
Zapobieganie nieuprawnionemu przeglądaniu katalogów	152
Ukrywanie rozszerzeń skryptów	153
Ograniczanie dostępu do sieci LAN	153
Udostępnianie katalogów na podstawie adresu IP i (lub) domeny	153

Blokowanie dostępu i zezwalanie na dostęp do domeny na podstawie przedziału adresów IP	154
Blokowanie hotlinkingu i zwracanie materiałów zastępczych	154
Blokowanie robotów, programów typu site ripper, przeglądarek offline i innych „szkodników”	155
Pliki, katalogi i inne elementy chronione hasłem	157
Aktywowanie trybu SSL za pomocą pliku .htaccess	160
Automatyczne ustawianie uprawnień do plików różnych typów	160
Ograniczanie wielkości plików w celu ochrony witryny przed atakami przez odmowę usługi (DoS)	161
Niestandardowe strony błędów	161
Udostępnianie uniwersalnej strony błędu	162
Zapobieganie dostępowi w określonych godzinach	162
Przekierowywanie żądań z danym łańcuchem znaków pod określony adres	162
Wyłączanie ustawienia magic_quotes_gpc na serwerach z obsługą PHP	163
Plik php.ini	164
Czym jest plik php.ini?	164
Jak przebiega odczytywanie pliku php.ini?	164
Podsumowanie	166
Rozdział 8. Pliki dziennika	167
Czym dokładnie są pliki dziennika?	168
Nauka czytania logów	169
A co z tym?	170
Kody stanu w HTTP 1.1	172
Analizowanie plików dziennika	175
Łańcuchy znaków z nazwą agenta	176
Blokowanie przedziałów adresów IP z danego kraju	177
Skąd pochodzi napastnik?	177
Konserwowanie plików dziennika	178
Etapy konserwowania plików dziennika	179
Narzędzia do przeglądania plików dziennika	180
BSQ-SiteStats	180
JoomlaWatch	181
AWStats	181
Podsumowanie	182
Rozdział 9. SSL w witrynach opartych na Joomla!	183
Czym jest technologia SSL (TLS)?	184
Używanie SSL do nawiązywania zabezpieczonych sesji	185
Certyfikaty autentyczności	186
Uzyskiwanie certyfikatów	187
Procedura wdrażania SSL	188
SSL w systemie Joomla!	188
Kwestie związane z wydajnością	190
Inne zasoby	191
Podsumowanie	191

Rozdział 10. Zarządzanie incydentami	193
Tworzenie polityki reagowania na incydenty	194
Tworzenie procedur na podstawie polityki reagowania na incydenty	197
Obsługa incyduentu	199
Komunikacja z zewnętrznymi jednostkami na temat incydentów	199
Określanie struktury zespołu	203
Podsumowanie	203
Dodatek A Podręcznik zabezpieczeń	205
Spis treści podręcznika zabezpieczeń	205
Informacje ogólne	206
Przygotowywanie pakietu narzędzi	206
Narzędzia do tworzenia kopii zapasowej	207
Lista kontrolna z obszaru pomocy	207
Codzienne operacje	209
Podstawowa lista kontrolna z obszaru bezpieczeństwa	209
Narzędzia	210
Nmap	210
Telnet	212
FTP	212
Skanowanie pod kątem wirusów	212
JCheck	212
Zestaw narzędzi dla systemu Joomla!	213
Narzędzia dla użytkowników Firefoksa	213
Porty	214
Pliki dziennika	216
Kody stanu serwera Apache	216
Format CLF	218
Informacje o kraju — kody domen najwyższego poziomu	219
Lista krytycznych ustawień	227
Plik .htaccess	227
Plik php.ini	230
Ogólne informacje na temat serwera Apache	231
Lista portów	232
Podsumowanie	236
Skorowidz	237