

Wstęp (9)

Część I Planowanie bezpiecznej strony WWW (15)

Rozdział 1. Polityka bezpieczeństwa (17)

- Funkcjonalność, koszt, bezpieczeństwo (18)
 - o Bezpieczeństwo nie jest tanie (18)
 - o Bezpieczeństwo jest przeciwieństwem funkcjonalności (19)
 - o Dlaczego bezpieczeństwo jest najważniejsze? (20)
- Bezpieczeństwo = prostota + bezbłądność (21)
 - o Program powinien być jak najprostszy (21)
 - o Program powinien mieć jak najmniej błędów (22)
- Zagrożenia (22)
 - o Przyczyny ataku (22)
 - o Kto jest naszym wrogiem (24)
 - o Słabe punkty (25)
- Klasyfikacja zagrożeń - model STRIDE (28)
 - o S Spoofing identity (fałszowanie tożsamości) (29)
 - o T Tampering with data (modyfikowanie danych) (29)
 - o R Repudiability (zaprzeczalność) (29)
 - o I Information disclosure (ujawnienie danych) (29)
 - o D Denial of Service (odmowa obsługi) (30)
 - o E Elevation of Privilege (poszerzenie uprawnień) (30)
- SD3 - dobra strategia programowania (30)
 - o Security by design (31)
 - o Security by deployment (31)
 - o Security by default (31)
- Zabezpieczanie nie polega na ukrywaniu (32)
 - o Dezinformacja jako technika obrony (32)
- Dogłębna obrona (32)
 - o Strategia wielu warstw (33)

Rozdział 2. Projekt aplikacji WWW (37)

- Programowanie Voodoo (38)
- Analiza zagrożeń (39)
 - o Określenie dóbr (40)
 - o Wyznaczenie granic bezpieczeństwa (40)
 - o Zdefiniowanie przepływu danych (40)
 - o Zidentyfikowanie punktów dostępowych (41)
 - o Określenie uprzywilejowanego kodu (42)
 - o Diagram ataku (43)
- Określenie priorytetów (43)
- Dokumentacja (44)
 - o Narzędzia (44)
- Ocena zagrożeń (49)
 - o Ochrona dóbr (51)
 - o Typy dóbr (51)
 - o Wycena dóbr (52)
 - o Ocena ryzyka utraty dóbr (52)
- Zarządzanie ryzykiem (54)

- o Akceptacja ryzyka (54)
 - o Minimalizacja ryzyka (54)
- Uczenie się na błędach (55)
- Dobre praktyki programowania (56)
 - o Modułowa struktura programu (56)
 - o Dogłębna obrona (57)
 - o Sprawdzanie danych wejściowych (57)
 - o Zasada minimalnych uprawnień (57)
 - o Zabezpieczanie przez zaciemnianie (58)
 - o Zabezpieczenia bazujące na rolach (58)
 - o Bezpieczna domyślna konfiguracja (58)
 - o Obsługa wyjątków (59)
 - o Korzystanie ze sprawdzonych systemów kryptograficznych (59)
 - o Nieprzechowywanie poufnych danych (59)
 - o Niekorzystanie z wyskakujących okien (60)
 - o Testowanie (60)

Część II Tworzenie bezpiecznej strony WWW (61)

Rozdział 3. Sprawdzanie poprawności danych (63)

- Źródła danych (63)
 - o URL (63)
 - o Metoda POST (66)
 - o Cookies (69)
 - o Nagłówki HTTP (71)
 - o Niestandardowe rozszerzenia (72)
 - o SOAP i XML (72)
- Zagrożenia (73)
 - o Ukryte dane (73)
 - o Przepelnienie bufora (75)
 - o Iniekcja kodu (Cross-site scripting) (75)
 - o Ataki na formę kanoniczną (77)
 - o Identyfikatory sesji (79)
 - o Dostęp do zasobów systemu (80)
 - o Upload plików (81)
- Walidacja po stronie klienta (81)
 - o Skrypty Java (82)
- Walidacja po stronie serwera (83)
- Wyrażenia regularne (84)

Rozdział 4. Uwierzytelnianie (87)

- Dostęp anonimowy (87)
- Metody uwierzytelniania (88)
 - o Uwierzytelnianie na poziomie serwera WWW (88)
 - o Uwierzytelnianie na poziomie formularzy (89)
- Hasła (90)
 - o Wymaganie bezpiecznych haseł (91)
 - o Sygnatury (93)
 - o Automatyczne generowanie haseł (94)

Rozdział 5. Autoryzacja (95)

- Model zaufanych podsystemów (95)
- Przedstawianie i delegowanie uprawnień (96)
 - Przedstawianie (96)
 - Delegowanie (97)
- Uwierzytelnianie i autoryzacja przez serwer WWW (97)
 - Blokowanie klientów (97)
 - Uwierzytelnienie i autoryzacja klientów (99)
- Konfiguracja aplikacji (102)

Rozdział 6. Pliki (105)

- Rozmieszczenie aplikacji (106)
- Kontrola dostępu do plików i folderów (106)
 - Linux/Unix (106)
 - Windows (111)
- Interpretowanie plików PHP (114)

Rozdział 7. Serwery baz danych (115)

- Konfiguracja serwera (115)
 - PostgreSQL (116)
- Model bezpieczeństwa serwerów baz danych (119)
 - Użytkownicy (120)
 - Uprawnienia (120)
- Połączenie z bazą (122)
 - PostgreSQL (122)
- Iniekcja SQL (128)
 - Atak (129)
 - Obrona (132)

Rozdział 8. Ochrona danych (135)

- Ujawnianie poufnych danych (135)
 - Komunikaty błędów (136)
 - Komunikaty systemowe (136)
 - Przechowywane w bazie dane (136)
 - Pliki źródłowe (136)
- Kryptologia (137)
 - Podstawowe pojęcia (137)
 - Funkcje mieszania (143)
 - Szyfrowanie blokowe i strumieniowe (146)
 - Szyfrowanie symetryczne (151)
 - Szyfrowanie asymetryczne (152)
 - Systemy hybrydowe - PGP (GPG) (157)
- Certyfikaty (158)
 - Zawartość certyfikatu (158)
 - Wystawianie (158)
 - Cykl życia certyfikatu (159)

- o Sprawdzanie poprawności (160)
- SSL (161)
 - o Konfiguracja serwera WWW (163)
- IPSec (167)

Rozdział 9. PHP (169)

- Konfiguracja środowiska (169)
 - o Zmienne globalne (170)
 - o Izolowanie skryptów PHP (174)
- Reguły pisania bezpiecznego kodu (176)
 - o Zasada minimalnych uprawnień (177)
 - o Kontrola typów danych (177)
 - o Obsługa wyjątków (179)
- Usługi sieciowe (Web Services) (182)

Część III Uruchamianie bezpiecznej strony WWW (187)

Rozdział 10. Serwer WWW (189)

- Apache (httpd) (189)
 - o Instalacja w systemach Linux (190)
 - o Instalacja w systemach Microsoft Windows (192)
 - o Konfiguracja serwera do współpracy z PHP (192)
 - o Apache a bezpieczeństwo aplikacji WWW (194)
 - o Podsumowanie (198)
- Internet Information Server (199)
 - o Instalacja (199)
 - o Konfiguracja (201)
 - o IIS a bezpieczeństwo aplikacji WWW (205)

Rozdział 11. Aplikacja (215)

- Przygotowanie plików do publikacji (215)
- Dostosowanie aplikacji do środowiska (217)
- Kopie zapasowe (221)

Rozdział 12. Testowanie (223)

- Testowanie a uruchamianie (223)
- Typy błędów (224)
- Dlaczego testowanie jest tak ważne? (224)
- Narzędzia (225)
 - o Komunikaty błędów (225)
 - o Narzędzia dodatkowe (227)
- Poprawność kodu HTML i XHTML (229)
- Metoda niezmienników (231)
- Biblioteka błędów (233)

Rozdział 13. Zapory sieciowe (235)

- Instalacja (235)
- Konfiguracja (236)
 - o Całkowita blokada ruchu sieciowego (237)
 - o Blokada pakietów przychodzących (238)
 - o Blokada pakietów wychodzących (239)
 - o Zdalny dostęp (239)
 - o Udostępnianie wybranych usług (240)
 - o Blokada żądań echa (ping) (240)
 - o Zapis i odtworzenie ustawień (241)
- Podsumowanie (241)

Rozdział 14. Audyt bezpieczeństwa (243)

- Specyfika testów bezpieczeństwa (243)
 - o Testy otwarte (243)
 - o Testy zamknięte (244)
 - o Analiza zidentyfikowanych zagrożeń (244)
- Narzędzia (244)
 - o Nessus (245)
 - o Retina (247)
 - o Nikto (248)
 - o AppScan (249)
 - o N-Stealth (250)
 - o Sleuth (252)
 - o RATS (252)
- Analiza typowych zagrożeń (254)
 - o Powszechnie znane luki w bezpieczeństwie (254)
 - o Zagrożenie związane z poufnymi danymi użytkowników (255)
 - o Zagrożenie związane z danymi sesji (258)
 - o Zagrożenie związane z ujawnieniem danych (260)
 - o Zagrożenia związane z wykonaniem wrogiego kodu (262)

Dodatki (265)

Dodatek A Zaciemnianie kodu PHP (267)

- POBS (267)
 - o Instalacja (268)
 - o Konfiguracja (268)
 - o Test (269)
 - o Więcej opcji konfiguracyjnych (272)

Dodatek B Kompilacja skryptów PHP (273)

- Zend Encoder (273)
 - o Instalacja (274)
 - o Konfiguracja (274)
 - o Test (274)
 - o Inne możliwości (276)

Skorowidz (279)