Szkolenie: Compendium CE
Bezpieczeństwo aplikacji WWW

DOSTĘPNE TERMINY

2025-05-29 | 2 dni | Kraków / Wirtualna sala
2025-06-12 | 2 dni | Warszawa / Wirtualna sala

Cel szkolenia:

Celem szkolenia jest podniesienie wiedzy dotyczącej **bezpiecznego tworzenia aplikacji internetowych**. W trakcie szkolenia przedstawione zostaną zarówno współczesne techniki ataków na aplikacje i jak metody skutecznej przed nimi obrony. Największy nacisk zostanie położony na tzw. **aplikacje internetowe**, czyli aplikacje, dla których interfejsem jest przeglądarka WWW.

Po ukończeniu szkolenia, uczestnicy powinni być znacznie bardziej świadomi zagrożeń, na jakie mogą być narażone tworzone przez nich aplikacje oraz znać praktyki pisania bezpiecznego kodu.

Szkolenie adresowane do:

- kierowników projektów,
- projektantów,
- inżynierów jakości kodu,
- programistów tworzących aplikacje webowe,
- administratorów bezpieczeństwa IT.

Plan szkolenia:

- Skala zagrożeń dla współczesnych aplikacji webowych
- Wpływ architektury aplikacji na bezpieczeństwo
  - od stron statycznych do dynamicznych
  - architektury oparte o CGI i SSI
  - architektury oparta o języki skryptowe (PHP, ASP, JSP i inne)
  - zaawansowane modele aplikacji webowych (ASP.NET, J2EE - Tomcat, Oracle AS, JBoss, WebSphere, WebLogic i inne)
  - współpraca aplikacji z bazą danych
  - interfejsy zewnętrzne aplikacji webowej
- Wpływ na bezpieczeństwo przeniesienia logiki z serwera do klienta

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- języki interpretowane po stronie klienta (JavaScript, VBScript, ECMAScript)
- architektura RIA (Rich Internet Applications) - Adobe Flex
- applety Java
- aplikacje klasyczne pobierające dane przez HTTP ("rich clients")
- komunikacja z serwerem - XML-RPC, SOAP

- Ograniczenia aplikacji po stronie klienta i ich nadużycia
  - przeglądarka WWW jako środowisko uruchamiania aplikacji
  - wyłamywanie się z ograniczeń środowiska ("sandbox")
  - wykorzystywanie dziur w przeglądarce
  - naruszenie zasady "same-origin policy" - atak "DNS Rebinding"
- Aplikacja webowa w ogólnym modelu bezpieczeństwa
  - wpływ aplikacji na całościowe bezpieczeństwo systemu
  - wpływ innych komponentów na bezpieczeństwo aplikacji
  - bezpieczeństwo bazy danych
  - ochrona i rozliczalność operacji na bazach danych
  - pozaprogramistyczne środki ochrony (systemy IDS/IPS)
- Typowe ataki na aplikacje webowe
  - zagrożenia związane z architekturą aplikacji
  - trywialne zagrożenia
  - konsekwencje braku obsługi błędów manipulacje parametrami
  - techniki podsłuchu i modyfikowania transmisji
  - penetracja niepublicznych zasobów serwera ("path traversal", "Google hacking")
  - wstrzykiwanie kodu ("code injection")
  - przejmowanie serwera przez "PHP shell"
  - wstrzykiwanie komend systemowych
- Ataki na bazę danych
  - obsługa błędów w komunikacji z bazą danych
  - ataki "SQL injection" jako konsekwencja błędów projektowych i programistycznych
  - konsekwencje prawne nieautoryzowanego dostępu do bazy danych (dane osobowe itd)
  - ataki na bazę pomimo zabezpieczeń ("blind SQL injection")
  - bezpieczeństwo i wydajność w komunikacji z bazą (techniki "stored procedure", "prepared statement")
  - separacja uprawnień w bazie danych jako mechanizm bezpieczeństwa
  - cechy charakterystyczne środowisk Oracle, Microsoft SQL, MySQL i PostgreSQL
- Ataki na sesje
  - rola sesji w aplikacji webowej

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- konsekwencje kradzieży, zgadnięcia lub podsłuchania sesji
- narzucenie sesji - ataki "session ?xation", "session adoption"
- kradzież sesji za pomocą "cross-site scripting" (XSS)
- nieautoryzowane operacje w aplikacji - ataki "cross-site request forgery" (CSRF)
- jak poprawnie zarządzać sesją?
- mechanizmy bezpieczeństwa sesji zapewniane przez środowiska do budowy aplikacji
- błędy podczas tworzenia własnych implementacji zarządzania sesją
- kiedy szyfrować połączenie - ochrona przed podsłuchaniem sesji

- Filtrowanie danych
  - filtrowanie danych w aplikacji webowej jako mechanizm bezpieczeństwa
  - poziomy filtrowania danych
  - filtrowanie danych wchodzących
  - filtrowanie danych wychodzących
  - techniki filtrowania danych w językach PHP i innych
  - wykrywanie włamań w aplikacjach webowych - PHP IDS
- Ochrona przed spamem
  - zagrozenie ze strony automatów spammerskich
  - nieetyczne działania SEO ("Search Engine Optimization")
  - ochrona za pomocą "testów człowieczeństwa" (CAPTCHA)
  - błędy i słabości systemów CAPTCHA
  - zalecenia dla ochrony przed spammerami
  - "czarne listy" w aplikacjach webowych - http:bl
- Jak poprawnie korzystać z SSL
  - funkcje bezpieczeństwa protokołu SSL
  - specyfika architektury SSL i X.509
  - ochrona zapewniana przez SSL i certyfikaty X.509
  - błędy popełniane podczas konfiguracji serwerów SSL
- Podsumowanie zasad najlepszej praktyki dla aplikacji webowych.

Wymagania:

Podstawowa wiedza z zakresu architektur aplikacji, sposobu działania serwisów WWW oraz protokołu HTTP.

Poziom trudności

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Certyfikaty:

Uczestnicy szkolenia "**WWW: atakowanie i ochrona webaplikacji**" otrzymują **certyfikat** wystawiony imiennie oraz na firmę, sygnowany przez **Compendium Centrum Edukacyjne**.

Prowadzący:

Wykładowca Compendium Centrum Edukacyjnego.

Informacje dodatkowe:

- **Każdy z uczestników tego szkolenia jest zobowiązany do podpisania oświadczenia (bezpośrednio przed jego rozpoczęciem), że zdobytą wiedzę będzie wykorzystywał w sposób etyczny i zgodny z obowiązującym prawem, wyłącznie w celu podnoszenia poziomu bezpieczeństwa sieci, systemów i zasobów, których on lub jego pracodawca jest właścicielem.**

- Punkty CPE (CISSP) za udział w szkoleniu:

  Uczestnicy tego szkolenia, którzy posiadają aktualną **certyfikację System Security Certified Practitioner** (**SSCP**) lub **Certified Information Systems Security Professional** (**CISSP**) mogą zdobyć jeden punkt Continuing Professional Education (CPE) za każdą godzinę szkolenia (1 CPE za pełną godzinę edukacyjną, co daje 6 CPE za standardowy dzień szkolenia w Compendium CE - ale nie więcej niż 8 CPE dziennie). W celu przyznania punktów CPE członkowie (ISC) 2 muszą samodzielnie zgłosić udział w naszym szkoleniu do (ISC)2 i muszą zachować dowód udziału (certyfikat uczestnictwa w szkoleniu) w przypadku konieczności potwierdzenia tego faktu w (ISC)2. Więcej informacji pod adresem https://www.isc2.org/ (dostęp tylko dla członków (ISC)2).

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001