Bezpieczeństwo aplikacji mobilnych (kod: Mobile Application Security)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Opis i cel szkolenia

Szkolenie zostało zaprojektowane, aby wyposażyć uczestników w kompleksową wiedzę i umiejętności z zakresu zabezpieczania aplikacji mobilnych. Program obejmuje zarówno podstawowe aspekty bezpieczeństwa, jak i zaawansowane techniki i narzędzia stosowane w praktyce (atakowanie i ochrona aplikacji mobilnych).

Na szkoleniu zostaną omówione kluczowe mechanizmy bezpieczeństwa dostępne w systemach iOS i Android, takie jak system uprawnień, Data Protection i Keychain, które są niezbędne do ochrony danych użytkowników. Uczestnicy dowiedzą się, jak skutecznie implementować te mechanizmy w swoich aplikacjach. **Część praktyczna szkolenia poświęcona będzie analizie i przełamywaniu zabezpieczeń systemowych**. Uczestnicy nauczą się, jak identyfikować i reagować na próby eskalacji uprawnień oraz jakie zagrożenia wiążą się z dostępem do danych użytkowników, takich jak SMS, e-mail czy dane GPS. Praktyczne ćwiczenia obejmą również analizę systemu plików oraz techniki przełamywania szyfrowania danych.

Szkolenie szczegółowo przedstawi metody bezpiecznego przechowywania danych, w tym loginów, haseł i kluczy kryptograficznych, oraz implementowania szyfrowania w aplikacjach mobilnych. Omówione zostaną także zagadnienia związane z bezpieczną komunikacją pomiędzy aplikacjami i ich komponentami, a także szyfrowaniem baz danych. W ramach szkolenia uczestnicy zapoznają się z zagrożeniami związanymi z transportem danych oraz z technikami implementacji bezpiecznych połączeń klient-serwer. Omówione zostaną mechanizmy szyfrowania SSL/TLS i wykorzystanie Public Key Infrastructure (PKI) w praktyce.

Szkolenie kończy się omówieniem specyficznych dla platform mechanizmów bezpieczeństwa oraz metod ataków, takich jak multitasking, input caching, CSRF, framing, clickjacking, identyfikacja urządzeń i użytkowników, tapjacking, oraz zarządzanie logami.

Czas trwania

3 dni

Program

1. Wprowadzenie do Platform Mobilnych: iOS i Android
   — Podstawy funkcjonowania systemów operacyjnych iOS i Android.
   — Porównanie kluczowych cech bezpieczeństwa obu platform.
2. Bezpieczeństwo z Perspektywy Użytkownika Urządzenia
   — Domyślnie dostępne sposoby zabezpieczeń urządzeń w systemach iOS i Android.
   — Wpływ domyślnych zabezpieczeń urządzeń na bezpieczeństwo aplikacji.
   — Mechanizmy usuwania danych (data wiping) i ich znaczenie dla użytkownika.
3. Mechanizmy Bezpieczeństwa Dostarczane Developerom przez Producentów Systemów
   — System uprawnień w Androidzie: jak działa i jak go implementować.
   — Data Protection i Keychain w iOS: zabezpieczanie danych użytkowników.
   — Praktyczne zastosowanie tych mechanizmów w aplikacjach mobilnych.
4. Przełamywanie Zabezpieczeń Systemów

- Eskalacja uprawnień w systemach mobilnych (jailbreak) i jej wpływ na bezpieczeństwo aplikacji.
- Analiza przypadków dostępu do danych użytkowników (SMS, e-mail, dane GPS).
- Techniki analizy systemu plików oraz przełamywania szyfrowania danych.

5. Bezpieczeństwo Danych
   - Zagrożenia związane z wykradaniem danych: studium przypadków.
   - Metody bezpiecznego przechowywania kluczowych danych (login, hasło, klucze, dane osobowe).
   - Implementowanie szyfrowania w aplikacjach mobilnych.
   - Zabezpieczanie aplikacji hasłem dostępowym.
   - Bezpieczna komunikacja pomiędzy aplikacjami i komponentami (Android: Activity, Service, Broadcast receiver, Content Resolver).
   - Szyfrowanie baz danych.
6. Bezpieczeństwo Komunikacji
   - Zagrożenia płynące z transportu danych i sposoby ich minimalizacji.
   - Poprawna, bezpieczna implementacja aplikacji klient-serwer.
   - Mechanizmy szyfrowania (SSL/TLS) i wykorzystanie PKI (Public Key Infrastructure).
7. Bezpieczeństwo Aplikacji
   - Analiza sposobów dystrybucji aplikacji i ryzyka z tym związane.
   - Analiza form binarnych aplikacji i ich dystrybucji (odex, Mach-O, ipa, apk).
   - Reverse Engineering aplikacji: narzędzia i techniki (Cycript, baksmali, apktool).
   - Metody utrudniania analizy kodu i modyfikacji działania aplikacji (blokowanie debuggerów, obfuskacja kodu, ASLR).
   - Wykrywanie środowisk z podwyższonymi uprawnieniami (jailbreak).
   - Narzędzia wspomagające analizę bezpieczeństwa aplikacji.
8. Istotne Mechanizmy Specyficzne dla Platform i Ataki z Nimi Związane
   - Multitasking i zarządzanie stanem aplikacji/GUI caching.
   - Wprowadzanie danych (input caching) i zagrożenia z tym związane.
   - Ataki na aplikacje webowe (CSRF, framing, clickjacking).
   - Identyfikacja urządzeń i użytkowników (UDID).
   - Bezpieczeństwo powiadomień push.
   - Tapjacking i zarządzanie logami.
9. Podsumowanie i Sesja Q&A;
   - Praktyczne ćwiczenia z zakresu bezpieczeństwa aplikacji mobilnych.
   - Sesja pytań i odpowiedzi, dyskusja nad najnowszymi zagrożeniami i technikami ochrony.

Przeznaczenie i wymagania

Celem szkolenia jest przekazanie uczestnikom niezbędnej wiedzy i praktycznych umiejętności, które pozwolą na skuteczne zabezpieczanie aplikacji mobilnych i ochronę danych użytkowników przed różnorodnymi zagrożeniami. Szkolenie jest skierowane zatem przede wszystkim do osób mających styczność z pracą aplikacjami mobilnymi - w szczególności, do programistów, testerów, specjalistów ds. bezpieczeństwa IT, administratorów, projektantów i architektów systemów mobilnych - oraz wszystkich zainteresowanych bezpieczeństwem aplikacji mobilnych.

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Lokalizacje

— Warszawa – ul. Jasna 14/16A
— Zdalnie – zajęcia realizowane poprzez platformę Zoom
— Kraków – ul. św. Filipa 23
— Katowice – ul. Stawowa 10
— Wrocław – ul. Rynek 35
— Gdańsk – ul. Toruńska 12
— Warsaw (English) – Jasna 14/16A
— Online (English) – your home, office or wherever you want
— na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Cena szkolenia

2790 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.