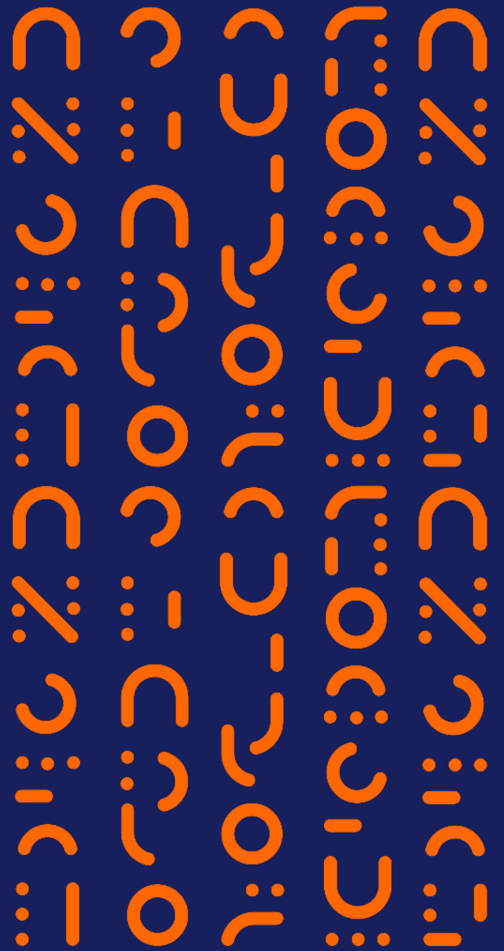
norbsoft

Czy Twoja aplikacja mobilna jest bezpieczna?



Top 10 zagrożeń

Sprawdź czy Twoja aplikacja mobilna jest bezpieczna na podstawie dobrych praktyk stosowanych w Norbsoft oraz listy Mobile Top 10 2024 opracowanej przez Fundację OWASP.

1. Postępowanie z hasłami
2. Zarządzanie zależnościami
3. Uwierzytelnianie i autoryzacja
4. Walidacja danych
5. Zabezpieczenie komunikacji
6. Ochrona prywatności
7. Zabezpieczenie plików aplikacji
8. Konfiguracja zabezpieczeń
9. Zabezpieczenie danych
10. Algorytmy kryptograficzne

Błędy w bezpieczeństwie aplikacji mobilnych mogą wiązać się z licznymi konsekwencjami, m.in.

- Nieautoryzowanym dostępem do funkcji lub danych
- Kradzieżą tożsamości lub informacji
- Konsekwencjami prawnymi
- Utratą własności intelektualnej
- Szkodami dla reputacji Twojej marki

norbsoft

1. Nieprawidłowe postępowanie z hasłami

- Hasła dostępu do Twoich usług nie powinny być umieszczane w kodzie aplikacji mobilnej, skąd atakujący może je odzyskać. Dotyczy to także wewnętrznych narzędzi biznesowych, których nie udostępniasz w Google Play czy Apple App Store - urządzenie może zostać zagubione lub skradzione.

- Hasła użytkownika powinny być przesyłane na serwer w sposób zapewniający ich poufność i integralność, np. z wykorzystaniem protokołu TLS i weryfikacji certyfikatu serwera

- Funkcja *Zapamiętaj mnie* nie powinna przechowywać hasła użytkownika na urządzeniu. Hasło powinno być wymienione w procesie logowania na token dostępowy, który można będzie zdalnie unieważnić.

  Zawsze weryfikuj i dokumentuj architekturę bezpieczeństwa Twojej aplikacji.

2. Nieprawidłowe zarządzanie zależnościami

- Większość aplikacji korzysta z przynajmniej jednej biblioteki open source. Atakujący może zmodyfikować kod takich bibliotek, umieszczając w nich malware, który w ten sposób może zostać dołączony do nowej wersji Twojej aplikacji i służyć do kradzieży danych użytkownika bądź wykonania nieautoryzowanych operacji na serwerze

- Zewnętrzne biblioteki mogą posiadać też własne błędy bezpieczeństwa

- Złośliwy kod może zostać wprowadzony także świadomie przez programistów

Korzystaj ze sprawdzonych bibliotek w ich najnowszych wersjach, przeprowadzaj regularne audyty kodu Twojej aplikacji, używaj narzędzi typu Dependency Check w swoich procesach CI/CD.

3. Niewystarczające uwierzytelnianie i autoryzacja

Uwierzytelnianie - czy użytkownik jest tym, za kogo się podaje
Autoryzacja - czy ma prawo dostępu do konkretnych danych i operacji

- Jeśli aplikacja zapewnia dostęp do różnych zestawów funkcji w zależności od uprawnień użytkownika, serwer powinien przeprowadzać kontrolę dostępu do każdego zasobu, tak by poprawnie zalogowany użytkownik nie mógł korzystać z API, które nie jest dla niego przeznaczone.

- Pamiętaj, że jeśli Twoja aplikacja pozwala na logowanie i pracę offline i jednocześnie korzysta np. z kilkucyfrowych kodów PIN, atakujący może uzyskać łatwy dostęp do danych przechowywanych lokalnie.

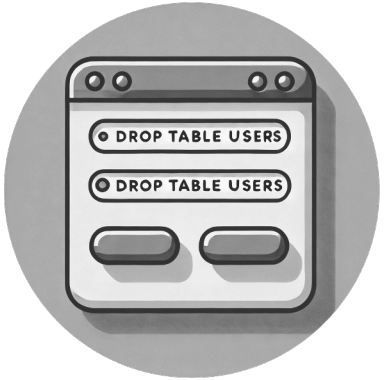
- Jeśli Twoja aplikacja korzysta z lokalnego uwierzytelniania biometrycznego (FaceID/TouchID), użyj systemowego mechanizmu (KeyChain/KeyStore) do przechowywania niezbędnych poufnych tokenów czy kluczy szyfrujących, nie polegaj jedynie na informacji z systemu, że użytkownik został uwierzytelniony

4. Brak wystarczającej walidacji danych

- Niezależnie od lokalnej walidacji danych przez samą aplikację mobilną, wszelkie dane otrzymywane z niej przez serwer muszą być poddane ponownej weryfikacji - atakujący może użyć Twojego API z pominięciem aplikacji mobilnej

- Jeśli aplikacja mobilna pozwala na dodawanie załączników, załóż, że mogą być one złośliwie spreparowane (obrazy, archiwa ZIP, dokumenty PDF mogą wykorzystywać luki w oprogramowaniu, które je dekoduje na Twoim serwerze)

- Jeśli prezentujesz w aplikacji zdjęcia lub bogato sformatowaną treść HTML powstającą na bazie danych wprowadzonych przez Twoich użytkowników, przefiltruj ją pod kątem potencjalnego złośliwego kodu, który mógłby wykonać się w przeglądarce osadzonej wewnątrz aplikacji mobilnej



5. Niezabezpieczona komunikacja

- Upewnij się w aplikacji mobilnej, że serwer API przedstawia się przy pomocy ważnego certyfikatu wystawionego przez urząd certyfikacji (CA) uznawany przez systemy Android i iOS - nie korzystaj z certyfikatów self-signed na środowiskach produkcyjnych

- Nie wysyłaj poufnych danych (kluczy, tokenów) przy pomocy powiadomień push

- Upewnij się, że tokeny otrzymywane od innych aplikacji (np. przeglądarki internetowej) nie mogą zostać podsłuchane przez złośliwe oprogramowanie na urządzeniu. Np. jeśli Twój proces logowania korzysta z OAuth 2.0 Authorization Code Flow, zabezpiecz go przez Proof Key for Code Exchange (PKCE) - RFC 7636

6. Niewystarczająca ochrona prywatności

- Upewnij się, że w logach nie są wysyłane nadmiarowe informacje, w tym dane osobowe (np. w ramach crashy aplikacji do Firebase Crashlytics czy Sentry, lub w parametrach zapytań skąd mogą trafić do logów serwera HTTP)
- Dane osobowe nie mogą także trafiać do zewnętrznych systemów analitycznych jak Google Analytics
- Jeśli Twoja aplikacja pozwala na utworzenie kopii zapasowej danych w ramach funkcji udostępnianych przez system operacyjny, upewnij się, że do kopii tej trafią tylko niezbędne informacje

7. Niewystarczające zabezpieczenie plików aplikacji

- Aplikacje mobilne dystrybuowane są przez sklepy, głównie Google Play i Apple App Store. Każdy może uzyskać dostęp do ich plików binarnych, np. pobranych bezpośrednio z urządzenia, a następnie spróbować opublikować (szczególnie w sklepach alternatywnych) kopię zawierającą złośliwy kod.

- Możesz wprowadzić zabezpieczenia, które utrudniają takie działania - np. weryfikacja integralności i zaciemnianie kodu komercyjnymi narzędziami typu DexGuard, iXGuard, Verimatrix Code Shield

- Jeśli aplikacja wykorzystuje cenne dla Ciebie algorytmy czy modele AI, powinny być one zaimplementowane po stronie serwera, gdyż mogą zostać odtworzone na podstawie kodu binarnego pobranego na urządzenie.

- Podobnie, jeśli korzystasz z zewnętrznych API, które opłacasz za zużycie - umieszczenie ich kluczy dostępowych w kodzie aplikacji mobilnej narazi Cię na dodatkowe koszty, gdy ktoś zacznie korzystać z nich bezpośrednio.

8. Błędy w konfiguracji zabezpieczeń

- Upewnij się, że elementy aplikacji, które wspomagały procesy testowania nie są dostępne w produkcyjnej wersji aplikacji (np. tryb debugowania, logi, testowe dane logowania, adresy serwerów testowych) a środowiska testowe, dokumentacja nie są publicznie dostępne bez żadnych zabezpieczeń (blokada na adresy IP, VPN, itp.)

- Jeśli Twoja aplikacja udostępnia swoje pliki innym (np. podgląd pliku PDF w aplikacji Acrobat Reader) powinna udostępniać te pliki tylko w zakresie i czasie niezbędnym na wykonanie danej funkcji

- Jeśli potrzebujesz uprawnienia dostępu do np. aparatu, lokalizacji czy kontaktów, pozyskaj je dopiero gdy użytkownik chce skorzystać z danej funkcji

- Nie pozwalaj produkcyjnej aplikacji na komunikowanie się ze światem przy pomocy nieszyfrowanych protokołów, nie akceptuj certyfikatów self-signed nawet jeśli korzystasz z nich w wersjach testowych swojej aplikacji

9. Słabe zabezpieczenie danych

- Upewnij się, że klucze sesji, tokeny i hasła nie trafią do logów aplikacji
- Jeśli Twoja aplikacja przechowuje poufne dane w cache, upewnij się, że będą one usuwane z uwzględnieniem ich określonego cyklu życia
- Monitoruj i aktualizuj biblioteki zewnętrzne, które wykorzystywane są do parsowania i przechowywania danych w Twojej aplikacji

10. Słabe algorytmy kryptograficzne

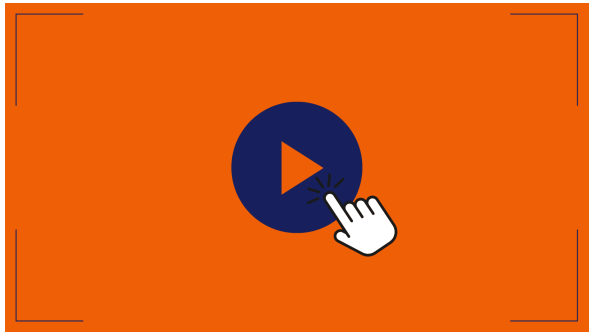
- Nie implementuj algorytmów kryptograficznych samodzielnie, korzystaj ze sprawdzonych rozwiązań zapewniających poufność i integralność danych
- Upewnij się, że wybrane przez Ciebie algorytmy kryptograficzne (szyfrujące, hashujące) odpowiadają obecnym standardom i nie zawierają znanych luk a klucze mają wystarczającą długość
- Przechowuj poufne tokeny i klucze w dedykowanych magazynach dostarczanych przez systemy operacyjne - KeyChain (iOS) i KeyStore (Android)

Kim jesteśmy?

Działająca od 2003 roku firma Norbsoft jest wiodącą spółką zajmującą się tworzeniem aplikacji mobilnych, zatrudniającą wysoko wykwalifikowanych specjalistów z doświadczeniem w zakresie strategii, projektowania i rozwoju doświadczeń użytkowników.

Skupiamy się przede wszystkim na produkcji użytecznych, wygodnych i bezpiecznych rozwiązań, z których my i nasi klienci możemy być dumni.

Zapewniamy także doradztwo oferując "Prognozę wartości" i "Mobilną transparentność".



www.norbsoft.com

norbsoft

Bądźmy w kontakcie

Tomasz Witt
Prezes Zarządu

tomasz.witt@norbsoft.com

+48 511 000 666

www.norbsoft.com