

Program szkolenia:

Bezpieczeństwo aplikacji iOS – naprawianie podatności

Informacje:

Nazwa:	Bezpieczeństwo aplikacji iOS – naprawianie podatności
Kod:	sec-ios
Kategoria:	Bezpieczeństwo
Odbiorcy:	developerzy, testerzy, architekci
Czas trwania:	1 dzień
Forma:	30% wykładów, 70% praktyki

Szkolenie jest przeznaczone dla osób uczestniczących w procesie wytwarzania aplikacji na platformę iOS. Jego celem jest przejście procesu wdrażania poprawek do aplikacji po otrzymaniu raportu z testów bezpieczeństwa. W trakcie szkolenia dowiesz się jak interpretować raport z testu penetracyjnego, jak odtworzyć wskazane podatności, jaki mają one faktyczny wpływ na ryzyko oraz jak zaimplementować poprawki

Zakres:

- Bezpieczeństwo systemu iOS
- Analiza raportu z testów bezpieczeństwa
- Bezpieczeństwo komunikacji pomiędzy aplikacją mobilną, a serwerem
- Bezpieczne przechowywanie danych wrażliwych na iOS
- Poprawna implementacja komunikacji międzyaplikacyjnej
- Wykrywanie jailbreaka
- Zabezpieczenia przed inżynierią wsteczną
- Bezpieczeństwo WebView
- Poprawna implementacji powyższych zagadnień

Forma

Szkolenie kładzie nacisk na aspekty praktyczne. Uczestnicy będą pracować na podatnej aplikacji na platformę iOS i na jej przykładzie będą implementowali poprawki do podatności zgłoszonych w omawianym raporcie z testów bezpieczeństwa. Dodatkowo, szkolenie przewiduje czas na dyskusje dotyczącą konkretnych problemów dotyczących bezpieczeństwa w aplikacjach rozwijanych przez uczestników. Uczestnicy będą mieli możliwość skonfrontować problemy, z którymi spotykają się na co dzień z wiedzą ekspercką.

Zalety szkolenia:

- Szkolenie jest prowadzone przez trenera zajmującego się faktycznie bezpieczeństwem iOSa, mającego własne badania w tym zakresie. Trener znajdował podatności także w oprogramowaniu Appa, za co został wyróżniony na stronie apple.com
- Szkolenie ma pomóc w efektywnym naprawianiu błędów bezpieczeństwa. Nie jest to kolejne szkolenie ofensywne, pozostawiające wiele wątpliwości dotyczących poprawnej implementacji omawianych zagadnień

BO·TT·EGA

IT minds

- Zajęcia zaczynają się od raportu z testów penetracyjnych. Trener przedstawi jak taki raport strawić i przedstawi metodykę odtworzenia przypadków testowych. Takie unikalne podejście pozwala skrócić czas spędzany na zrozumieniu jak podatności w aplikacjach mobilnych faktycznie działają

Szczegółowy program:

1. Wstęp do bezpieczeństwa systemu iOS

1.1. Krótka historia systemów Appli

1.2. Szyfrowanie dysku iPhonea

1.3. Sandboxing aplikacji

1.4. Jailbreaking

2. Raport z testów bezpieczeństwa – i co teraz?

2.1. Struktura raportu

2.2. Wycena ryzyka podatności

2.3. Opis podatności

2.4. Warunki wykorzystania

2.5. Przypadek testowy

3. Konfiguracja środowiska testowego

3.1. Konfiguracja sieciowa

3.2. Proxy HTTP/HTTPS

3.3. Konfiguracja macOS

3.4. Dostosowanie iPhonea do testów

4. Podatność 1 – Niebezpieczne przechowywanie danych na urządzeniu

4.1. Dyskusja na temat podatności

4.2. Odtworzenie przypadku testowego

4.3. Naprawa podatności

5. Podatność 2 – Brak sprawdzania certyfikatu SSL

5.1. Dyskusja na temat podatności

5.2. Odtworzenie przypadku testowego

5.3. Naprawa podatności

6. Podatność 3 – Nieprawidłowa walidacja danych w URL schemes

6.1. Dyskusja na temat podatności

6.2. Odtworzenie przypadku testowego

6.3. Naprawa podatności

7. Zalecenie – Wdrożenie mechanizmów utrudniających inżynierię wsteczną

7.1. Dyskusja na temat zalecenia

7.2. Odtworzenie przypadku testowego

7.3. Wdrożenie zalecenia

8. Podsumowanie