BO·TT·EGA
IT minds

Program szkolenia:

Bezpieczeństwo aplikacji Android – naprawianie podatności

Informacje:

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

Szkolenie jest przeznaczone dla osób uczestniczących w procesie wytwarzania aplikacji na platformę Android. 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 Android
- Analiza raportu z testów bezpieczeństwa
- Bezpieczeństwo komunikacji pomiędzy aplikacją mobilną, a serwerem
- Bezpieczne przechowywanie danych wrażliwych na Androidzie
- Poprawna identyfikacja instancji aplikacji
- Wykrywanie roota
- 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 Android i na jej przykładzie będą implementowali poprawki do podatności zgłoszonych w omawianym raporcie z testów bezpieczeństwa. Dodatkowo, szkolenie przewiduje czas na dyskusję 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 Androida i mającego własne badania w tym zakresie
- Szkolenie ma pomóc w efektywnym naprawianiu błędów bezpieczeństwa. Nie jest to kolejne szkolenie ofensywne pozostawiające wiele wątpliwości dotyczących poprawnej implementacji omawianych zagadnień
- Zajęcia zaczynają się od analizy raportu z testów penetracyjnych. Trener przedstawi jak zinterpretować taki raport oraz przedstawi metodykę odtworzenia przypadków testowych. Takie unikalne podejście pozwoli uczestnikom skrócić czas potrzebny do zrozumienia jak podatności w aplikacjach mobilnych faktycznie działają

BO·TT·EGA
IT minds

Szczegółowy program:

1. Wstęp do bezpieczeństwa systemu Android

- 1.1. Krótka historia Androida
- 1.2. Struktura uprawnień
- 1.3. Rooting

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. Dostosowanie Androida oraz stacji roboczej 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 konfiguracja WebView

BOTTEGA IT minds