ТЕСТУВАННЯ НА ПРОНИКНЕННЯ МОБІЛЬНОГО ЗАСТОСУНКУ

Служба кібербезпеки BDO в Україні на базі ImmuniWeb®

Чому важливо захищати свій мобільний застосунок?

→ Оскільки незахищені застосунки можуть принести своїм користувачам великі фінансові та репутаційні втрати

Отже, якщо у вашої компанії або бізнесу є...

1. Мобільний застосунок невеликого розміру та складності*
2. з однією або двома кінцевими точками (наприклад, API або веб-сервіси) і одна роль користувача

**однак в разі потреби у нас є рішення для кожного розміру та складності*

... тоді найкращим рішенням буде

- **ВИЯВИТИ** Топ-10 недоліків OWASP Mobile у вашому мобільному застосунку iOS або Android і знайти Топ-25 вразливостей SANS у кінцевих точках
- **ПЕРЕВІРИТИ,** чи відповідають механізми конфіденційності, відповідності та шифрування ваших мобільних застосунків найкращим практикам галузі

Як ми надаємо повну оцінку безпеки вашого мобільного застосунка?

→ Через виконання передового технологічного тестування на проникнення

Що це і як це працює?

Завдяки передовим рішенням від ImmuniWeb® MobileSuite ми використовуємо технологію Машинного навчання для прискорення й покращення тестування на проникнення мобільного застосунку. Кожен тест на проникнення забезпечений договірною угодою про рівень обслуговування без хибних спрацьовувань і гарантією повернення грошей, якщо є навіть одне хибне спрацьовування.

BDO DIGITAL

ТЕСТУВАННЯ НА ПРОНИКНЕННЯ МОБІЛЬНОГО ЗАСТОСУНКУ

Методи тестування наступні:

- Керівництво з тестування мобільної безпеки OWASP (MSTG)
- NIST SP 800-115 Технічний посібник з тестування і оцінки інформаційної безпеки
- Інформаційний додаток PCI DSS: Інструкція з тестування на проникнення
- Матриці MITRE ATT&CK® для мобільних пристроїв і підприємств
- Посібник з тестування на проникнення FedRAMP
- Як провести аудит GDPR від ISACA

Які переваги отримує ваш мобільний застосунок від використання нашої служби?

→ Після завершення повної технічної перевірки на вразливості ви отримуєте подальше безкоштовне тестування

Що ви отримуєте при гарантованих результатах?

1. Виявлені вразливості бізнес-логіки та обходу аутентифікації
2. Експорт даних про вразливості з інтерактивної інформаційної панелі в PDF або безпосередньо в SIEM або систему відстеження помилок для швидшого усунення
3. Необмежену кількість перевірок після проведення тесту на проникнення, аби розробники програмного забезпечення могли легко перевірити, чи всі результати були належним чином виправлені

Використані стандарти звітності:

- Стандарт перевірки безпеки застосунків OWASP (ASVS v4.0.2)
- Сумісна система ідентифікації вразливостей (CVE)
- Сумісний загальний перелік вразливостей та проблем у коді (CWE)
- Загальна система оцінки вразливостей (CVSS v3.1)

Цікаво?
Зв'яжіться з нами:

АНДРІЙ БОРЕНКОВ
Директор BDO Consulting

aborenkov@bdo.ua
+380 50 380 96 01

ImmuniWeb® AI for Application Security

BDO в Україні
www.bdo.ua
info@bdo.ua

BDO DIGITAL