

ТЕСТУВАННЯ ВЕБ-ЗАСТОСУНКУ НА ПРОНИКНЕННЯ

Служба кібербезпеки BDO в Україні на базі ImmuniWeb®

Чому важливо підтримувати оновлення безпеки веб-застосунку?

→ Сьогодні це не формальність, а найкраща практика, необхідна для конкуренції на світовому ринку

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

... тоді найкращим рішенням буде

- 1** Один веб-застосунок невеликого розміру і складності*
- 2** Розташований в одному або двох дочірніх доменах з однією роллю користувача

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

- ▶ **ВИЯВИТИ** 25 найпопулярніших вразливостей по методології OWASP, перелік PCI DSS 6.5 і 25 найпопулярніших вразливостей SANS у ваших веб-застосунках, API RESTful та мікросервісах.
- ▶ **ЗНАЙТИ** можливості підвищення привілеїв, обходу аутентифікації та вразливості бізнес-логіки.

Як ми надаємо повну оцінку безпеки вашого веб-застосунку?

→ Через виконання сучасного високотехнологічного тестування на проникнення

Що це і як це працює?

Використовуючи передові рішення від [ImmuniWeb® On-Demand](#) ми поєднуємо автоматизований AI з ручним тестуванням логіки програми. Послуга надається з договірною угодою про рівень обслуговування без хибних спрацьовувань і гарантією повернення грошей, якщо є навіть одне хибне спрацьовування.



Методи тестування наступні:

- ▶ Керівництво з тестування веб-безпеки OWASP (WSTG)
- ▶ NIST SP 800-115 Технічний посібник з тестування і оцінки інформаційної безпеки
- ▶ Інформаційний додаток PCI DSS: Інструкція з тестування на проникнення
- ▶ Матриця MITRE ATT&CK® для підприємства
- ▶ Посібник з тестування на проникнення FedRAMP
- ▶ Як провести аудит GDPR від ISACA

Які переваги отримує ваш веб-застосунок від використання нашого сервісу?

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

Що ви отримуєте при гарантованих результатах?



Багатоцільову панель інструментів зі структурованими висновками



Інтеграцію DevSecOps для експорту даних безпосередньо у ваші системи відстеження



Необмежену кількість оцінок вразливості після пентесту безкоштовно; отже розробники програмного забезпечення можуть легко перевірити, чи правильно виправлено рекомендації пентесту.

Використані стандарти звітності:

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

Зацікавлені?

Зв'яжіться з нами:



АНДРІЙ БОРЕНКОВ

Директор BDO Consulting

✉ aborenkov@bdo.ua

☎ +380 50 380 96 01



BDO в Україні

🌐 www.bdo.ua
✉ info@bdo.ua

ТОВ «БДО», українське товариство з обмеженою відповідальністю, є членом BDO International Limited, британського товариства з відповідальністю, обмеженою гарантіями його членів, а також входить до складу міжнародної мережі незалежних фірм-членів BDO. BDO – це бренд мережі BDO і кожної фірми-члена BDO.

