ДЕРЕВО РІШЕНЬ

Оберіть пентест під ризики вашого бізнесу

Без потрібних доступів пентестер може не знайти проблеми за сторінкою входу.

ЩО ВСЕРЕДИНІ

- [ ] Оберіть один із трьох форматів
- [ ] Підготуйте акаунти й потрібні матеріали
- [ ] Надішліть готовий запит виконавцю

Для: Власники бізнесу, CTO та технічні керівники

🖨️ Остання сторінка для друку

Veiltrack

Незалежне тестування безпеки

Ситуація

Компанія замовляє перевірку особистого кабінету. Пентестер отримує адресу сайту, але не має акаунтів. Він може не перевірити, чи бачать клієнти чужі рахунки.

Пентест, це практична перевірка системи на вразливості. Формат визначає, яку інформацію та доступи отримує пентестер.

Для більшості бізнес-застосунків починайте з grey box: надайте тестові акаунти різних користувачів. Так пентестер зможе перевірити функції після входу.

01 / 05

Назвіть ризик, який хочете перевірити

Прочитайте завдання. Чи зрозуміло, що перевіряють: зовнішній доступ, чужі дані, права користувачів або помилки в коді?

> У завданні написано лише «перевірити сайт на вразливості».

→ **Назвіть конкретний ризик і виберіть формат за схемою.**

02 / 05

Перелічіть системи та функції для перевірки

Звірте завдання із застосунком. Чи включили кабінет, платежі, адміністративні сторінки та обмін даними між програмами?

> У завданні є лише адреса головної сторінки.

→ **Додайте потрібні адреси й функції. Узгодьте перелік із виконавцем.**

03 / 05

Створіть окремі тестові акаунти

Увійдіть у кожен акаунт. Перевірте, що два клієнти мають різні тестові дані й доступні потрібні ролі.

> Є лише один клієнтський акаунт. Порівняти доступ між клієнтами неможливо.

→ **Створіть відсутні акаунти. Перевірте вхід і тестові дані.**

04 / 05

Запишіть, хто що може робити

Прочитайте опис прав. Чи зрозуміло, хто бачить рахунки, змінює платежі та керує іншими користувачами?

> Ніхто не знає, хто може бачити чужі рахунки.

→ **Запишіть дозволені дії для кожної ролі. Передайте опис виконавцю.**

ДЕРЕВО РІШЕНЬ

05 / 05

Передайте матеріали та погодьте правила

ЯК МАЄ БУТИ

Виконавець отримав потрібні матеріали. Сторони погодили межі перевірки, заборони, контакти та передавання доступів.

ЯК ПЕРЕВІРИТИ

Звірте матеріали із завданням. Чи визначили заборонені дії, контакт відповідального та безпечний спосіб передавання доступів?

ОЗНАКА ПРОБЛЕМИ

Виконавець не знає обмежень або не має контакту відповідального.

ЩО ЗРОБИТИ

Узгодьте обмеження й контакт.
Передайте доступи безпечним способом.

ДЕРЕВО РІШЕНЬ

РІШЕННЯ

Що саме потрібно перевірити?

Що сторонній бачить без входу
Оберіть black box. Пентестер перевірить погоджені зовнішні адреси без наданих акаунтів.

Чи можна побачити чужі дані або обійти права
Оберіть grey box. Дайте два незалежні клієнтські акаунти й акаунти інших потрібних ролей.

Чи є помилки в коді платежів, входу або прав
Оберіть white box. Дайте код і опис будови системи. Перевірте також працюючий застосунок.

ДЕРЕВО РІШЕНЬ

ГОТОВА ФРАЗА

Готовий запит виконавцю

«Хочемо перевірити [застосунок] на [ризик]. Пропонуємо [формат]. Перевіряємо [функції]. Надамо [тестові акаунти, опис прав або код]. Підкажіть, чого бракує та які правила погодити.»

ЧОГО НЕ РОБИТИ

Не надсилайте робочі паролі чи дані клієнтів звичайним листом.

VEILTRACK

Незалежне тестування безпеки

ДЛЯ ДРУКУ · ПАМ’ЯТКА КОМАНДІ

Який пентест обрати та що підготувати

Роздрукуйте й роздайте відділу. 30 днів тримайте перед очима й позначайте день, коли діяли за пам’яткою. Коли це стане звичкою, аркуш можна зняти.

Перед замовленням пентесту або зміною його обсягу:

- [ ] Називаю ризик і вибираю формат.
- [ ] Записую адреси та функції для перевірки.
- [ ] Готую два клієнтські акаунти й інші ролі.
- [ ] Записую, хто що може бачити й змінювати.
- [ ] Погоджую правила й передаю потрібні матеріали.

30 ДНІВ ДО ЗВИЧКИ: ПОЗНАЧТЕ ДЕНЬ

	Пн	Вт	Ср	Чт	Пт
ТИЖДЕНЬ 1	☐	☐	☐	☐	☐
ТИЖДЕНЬ 2	☐	☐	☐	☐	☐
ТИЖДЕНЬ 3	☐	☐	☐	☐	☐
ТИЖДЕНЬ 4	☐	☐	☐	☐	☐

Ім’я, відділ: _____ Старт: _____

Питання щодо безпеки? Напишіть нам



Vlad Kraevsky
засновник Veiltrack

WEB
veiltrack.io

EMAIL
vlad@veiltrack.io