PRAKTYCZNY MATERIAŁ DLA FIRM

CHECKLISTA PRZED PENTESTEM

27 decyzji, które skracają przygotowanie, ograniczają ryzyko operacyjne i zwiększają wartość raportu.

DLA KOGO	CO DOSTAJESZ
CTO, właściciele produktów, software house'y i zespoły IT	Zakres, zgody, dostępy, zasady bezpieczeństwa i plan naprawy

AI kwalifikuje zakres. Pentester weryfikuje każdą raportowaną podatność.

Najpierw ustal, po co robisz pentest

Najdroższy pentest to taki, który kończy się raportem bez właściciela, terminu i decyzji. Zacznij od celu biznesowego, a dopiero potem dobieraj zakres techniczny.

1. Cel i priorytety

- ☐ 01 Zapisaliśmy jeden główny cel testu, na przykład ochrona danych klientów, gotowość przed wdrożeniem albo wymaganie audytowe.
- ☐ 02 Wskazaliśmy krytyczne procesy biznesowe: logowanie, płatności, panel administratora, eksport danych i integracje.
- ☐ 03 Ustaliliśmy kryterium sukcesu: co musi zostać potwierdzone, aby test był dla firmy wartościowy.
- ☐ 04 Wyznaczyliśmy właściciela biznesowego i technicznego, którzy odbiorą wyniki i podejmą decyzje.

2. Zakres i autoryzacja

- ☐ 05 Mamy dokładną listę domen, hostów, aplikacji, API i środowisk objętych testem.
- ☐ 06 Opisaliśmy elementy wyłączone z zakresu, w tym systemy dostawców oraz dane, których nie wolno modyfikować.
- ☐ 07 Właściciel każdego celu potwierdził prawo do testowania i podpisze pisemną autoryzację przed rozpoczęciem.
- ☐ 08 Ustaliliśmy dozwolone techniki oraz zakaz testów destrukcyjnych, DoS i socjotechniki, jeśli nie są osobno zatwierdzone.
- ☐ 09 Ustaliliśmy okno testowe, strefę czasową, procedurę przerwania i kontakt alarmowy dostępny podczas testu.

ZASADA	Brak pisemnej zgody oznacza brak testu. Sama znajomość adresu systemu nie jest autoryzacją.

Przygotuj środowisko, nie niespodzianki

Pentester powinien od pierwszej godziny testować bezpieczeństwo, a nie szukać właściciela konta, naprawiać niedziałający VPN albo zgadywać role użytkowników.

3. Środowisko i dostęp

- [ ] 10 Przygotowaliśmy konta testowe dla każdej istotnej roli, bez używania prawdziwych danych klientów.
- [ ] 11 Sprawdziliśmy logowanie, MFA, VPN, allowlistę IP i dostęp do dokumentacji przed rozpoczęciem okna testowego.
- [ ] 12 Przekazaliśmy diagram architektury, listę integracji i opis przepływów danych w zakresie potrzebnym do testu.
- [ ] 13 Podaliśmy liczbę unikalnych ekranów, endpointów API, ról i krytycznych scenariuszy, aby uniknąć błędnej wyceny.
- [ ] 14 Ustaliliśmy bezpieczny kanał przekazania haseł i tokenów. Nie wysyłamy ich zwykłym formularzem ani w otwartym e-mailu.

4. Bezpieczeństwo operacyjne

- [ ] 15 Mamy aktualny backup i potwierdzony proces odtworzenia danych dla środowiska objętego testem.
- [ ] 16 Monitoring i logowanie zdarzeń działają, a zespół wie, jak odróżnić ruch testowy od rzeczywistego incydentu.
- [ ] 17 Ustaliliśmy sposób natychmiastowego zgłoszenia podatności krytycznej, bez czekania na raport końcowy.
- [ ] 18 Zespół utrzymaniowy zna termin testu i wie, kto może podjąć decyzję o jego zatrzymaniu.

Minimum dla aplikacji webowej

Role użytkowników, lista ekranów, krytyczne procesy, domeny, konto administratora i konto zwykłego użytkownika.

Minimum dla API

Specyfikacja lub kolekcja, sposób autoryzacji, role, przykładowe identyfikatory obiektów i limity wywołań.

Raport ma uruchamiać naprawę

Ustal format wyniku jeszcze przed testem. Raport powinien łączyć dowód techniczny z wpływem biznesowym i jasną kolejnością działań.

5. Raport, naprawa i retest

- [ ] 19 Uzgodniliśmy skalę ryzyka oraz elementy każdego znaleziska: opis, dowód, wpływ, priorytet i zalecenie naprawcze.
- [ ] 20 Raport zawiera podsumowanie zarządcze i część techniczną możliwą do przekazania zespołowi deweloperskiemu.
- [ ] 21 Każde znalezisko ma właściciela oraz planowany termin naprawy zgodny z poziomem ryzyka.
- [ ] 22 Retest jest zaplanowany po wdrożeniu poprawek, a wynik potwierdzi status każdej zgłoszonej podatności.

6. Czy zakres kwalifikuje się do wyniku w 24h?

- [ ] 23 Zakres obejmuje jedną aplikację webową lub jedno API o ograniczonej liczbie ekranów, endpointów i ról.
- [ ] 24 Dostępy, dokumentacja i pisemna autoryzacja są gotowe przed rozpoczęciem testu.
- [ ] 25 Nie oczekujemy testów destrukcyjnych, rozbudowanej infrastruktury, wielu środowisk ani dużej liczby integracji.
- [ ] 26 Zespół odpowiada szybko na pytania dotyczące logiki biznesowej i potrafi odblokować dostęp bez opóźnień.
- [ ] 27 Rozumiemy, że większy zakres może otrzymać wynik wstępny w 24 godziny, a pełny raport w potwierdzonym terminie.

Szybka karta zakresu

Typ celu	[ ] Web [ ] API [ ] Mobile [ ] Infrastruktura
Środowisko	[ ] Produkcyjne [ ] Testowe [ ] Inne: _____
Role	Liczba: _____ Najwyższa rola: _____
Termin	Start: _____ Oczekiwany raport: _____
Kontakt alarmowy	Imię: _____ Telefon: _____

Masz zakres? Odpowiedź dostaniesz w 60 sekund.

Wypełnij krótką kwalifikację. AI przygotuje orientacyjne widełki, a człowiek potwierdzi finalny zakres, termin i warunki testu.

BEZPŁATNA WYCENA

pentest24.pl

Bez zobowiązań. NDA przed testem. Jeden retest w cenie.

Jak korzystać z checklisty

1. Wypełnij wewnętrznie

Przejdź listę z właścicielem produktu i zespołem technicznym przed rozmową z wykonawcą.

2. Dołącz do zakresu

Przekaż uzupełnioną kartę jako punkt startowy do wyceny i zasad testu.

3. Wróć po raporcie

Sprawdź właścicieli napraw, terminy i gotowość do retestu.

Punkty kontrolne są zgodne z typowymi zasadami przygotowania testów opisanymi w OWASP Web Security Testing Guide, PTES i NIST SP 800-115. Ostateczny zakres zawsze wymaga indywidualnej oceny i pisemnej autoryzacji.