

Wzór zakresu testu penetracyjnego

Formularz do wypełnienia przed wysłaniem zapytania ofertowego · wersja 1.0, sierpień 2026

Po co ten dokument. Wykonawcy wyceniają testy na podstawie pracochłonności, a tę wyznacza zakres. Zapytanie „proszę o wycenę testów penetracyjnych” prowadzi do wyceny opartej na domysłach — albo do serii telefonów. Wypełniony formularz pozwala porównać oferty, które faktycznie dotyczą tego samego. Możesz go wysłać do dowolnego wykonawcy, także innego niż Pentestica.

1. Podstawowe informacje

Pole	Wartość
Nazwa organizacji	
Osoba kontaktowa i rola	
Oczekiwany termin realizacji	
Czy test wynika z regulacji	NIS2 / DORA (TLPT) / ISO 27001 / PCI DSS / potrzeba biznesowa
Czy wymagane NDA przed rozmową	tak / nie

2. Cel testu

Jedno-dwa zdania: co ma zostać potwierdzone albo obalone. Dobry cel brzmi „sprawdzić, czy da się uzyskać dostęp do danych innego klienta”, a nie „przetestować aplikację”.

3. Zakres techniczny

3.1. Aplikacje webowe i API

Element	Wartość
Liczba aplikacji	
Adresy (produkcja / staging)	
Liczba ról uwierzytelnienia	bez logowania / 1 / 2-3 / 4 i więcej
Rodzaj API	REST / GraphQL / SOAP / brak
Liczba endpointów (przybliżona)	
Czy jest dokumentacja API	tak / nie

3.2. Infrastruktura i sieć

Element	Wartość
Liczba publicznych adresów IP	
Liczba hostów w sieci wewnętrznej	<25 / 25-100 / 100-500 / >500
Active Directory w zakresie	tak / nie
Segmentacja sieci do weryfikacji	tak / nie
Środowisko chmurowe	AWS / Azure / GCP / brak

3.3. Wyłączenia

Systemy, adresy i działania **wyłączone** z zakresu. To pole ratuje przed najczęstszym nieporozumieniem w projektach testowych.

4. Model testu

Parametr	Opcje
Poziom wiedzy testera	black box / grey box / white box

Konta testowe	zapewniamy / tester zakłada sam / nie dotyczy
Środowisko	produkcja / kopia produkcji / staging
Kto wie o teście	cały zespół IT / wąska grupa / tylko zarząd
Socjotechnika i phishing	w zakresie / poza zakresem
Testy DoS	w zakresie / poza zakresem

5. Zasady bezpieczeństwa testu

- Okna czasowe, w których testy są dozwolone:
- Dopuszczalny wpływ na produkcję:
- Osoba do kontaktu awaryjnego (24/7):
- Procedura przerwania testu:
- Kanał zgłaszania krytycznych znalezisk w trakcie:

6. Produkty końcowe

Element	Wymagany
Raport techniczny z krokami odtworzenia	tak / nie
Raport zarządczy (podsumowanie dla decydentów)	tak / nie
Ocena ryzyka według CVSS	tak / nie
Rekomendacje naprawcze z priorytetami	tak / nie
Retest po wdrożeniu poprawek	tak / nie
Prezentacja wyników dla zespołu	tak / nie
Raport w języku angielskim	tak / nie

7. Wymagania wobec wykonawcy

Warto zapytać wprost — odpowiedzi bardzo różnicują oferty:

- Jakie certyfikaty mają osoby, które faktycznie wykonają test (nie firma — konkretni ludzie)?
- Ile testów tego typu zespół wykonał w ostatnich dwunastu miesiącach?
- Czy dostanę przykładowy raport (choćby zanonimizowany) przed podpisaniem umowy?
- Jaki procent pracy jest manualny, a jaki to skanowanie automatyczne?
- Czy retest jest w cenie, czy płatny osobno?
- Kto jest właścicielem danych z testu i jak długo są przechowywane?
- Czy wykonawca ma ubezpieczenie odpowiedzialności cywilnej zawodowej?

Uwaga dla podmiotów finansowych. Jeśli test wynika z rozporządzenia DORA i ma być testem TLPT, wymogi wobec wykonawcy określa art. 27 DORA — obejmują certyfikację, niezależne poświadczenie zarządzania ryzykiem testu oraz obowiązkowe ubezpieczenie OC zawodowej. Dostawca wywiadu o zagrożeniach musi być podmiotem zewnętrznym.

8. Kryteria wyboru oferty

Zanim zbierzesz oferty, ustal wagi. Najniższa cena przy najszerszym zakresie zwykle oznacza, że któryś z wykonawców rozumie zakres inaczej niż pozostali.

Kryterium	Waga (%)
Cena	
Doświadczenie zespołu w tej technologii	
Udział pracy manualnej	
Jakość przykładowego raportu	
Termin realizacji	

PENTESTICA · testy penetracyjne, audyty IT, red teaming, wdrożenia NIS2, DORA i MiCA
hello@pentestica.pl · 324 412 813 · pentestica.pl

Ten wzór możesz wykorzystać bez ograniczeń, także w zapytaniach do innych wykonawców. Jeśli chcesz, żebyśmy pomogli go wypełnić — napisz. Odpowiadamy w ciągu jednego dnia roboczego.