Lista kontrolna bezpieczeństwa

OWASP Top 10:2025 dla aplikacji webowych

Kontrola dostępu (A01)

- [ ] Każdy endpoint sprawdza uprawnienia po stronie serwera
- [ ] UUID zamiast sekwencyjnych identyfikatorów zasobów

Kryptografia (A04)

- [ ] Hasła hashowane bcrypt / scrypt / Argon2 (nigdy MD5 ani SHA1)
- [ ] HTTPS na całym ruchu aplikacji
- [ ] Sekrety i klucze w zmiennych środowiskowych lub menedżerze sekretów

Zapytania do bazy (A05)

- [ ] Wyłącznie zapytania parametryzowane (prepared statements) lub ORM
- [ ] Zero konkatenacji stringów w zapytaniach SQL

Łańcuch dostaw i zależności (A03)

- [ ] Automatyczne skanowanie zależności przy każdym pull requeście
- [ ] Aktualizacje bibliotek minimum raz w miesiącu

Konfiguracja (A02)

- [ ] Tryb debugowania wyłączony na produkcji
- [ ] Nagłówki bezpieczeństwa (HSTS, X-Frame-Options, nosniff)
- [ ] CORS ograniczony do zaufanych domen
- [ ] Brak domyślnych loginów i haseł w panelach

Uwierzytelnianie (A07)

- [ ] Dwuskładnikowe logowanie (2FA) dla kont administracyjnych
- [ ] Ciastka sesji z flagami HttpOnly, Secure oraz SameSite
- [ ] Regeneracja identyfikatora sesji po zalogowaniu
- [ ] Limit prób logowania (rate limiting)

Dane wejściowe (A05)

- [ ] Walidacja i escapowanie wszystkich danych od użytkownika
- [ ] Nagłówek Content Security Policy (CSP)
- [ ] Sanityzacja HTML tam, gdzie dozwolone jest formatowanie

SSRF (część Broken Access Control, A01)

- [ ] Lista dozwolonych domen przy pobieraniu adresów URL
- [ ] Blokada adresów prywatnych (RFC 1918) i link-local
- [ ] IMDSv2 na instancjach AWS

Logowanie i alerty (A09)

- [ ] Rejestrowanie nieudanych logowań, zmian uprawnień i dostępu do danych wrażliwych
- [ ] Alerty przy anomaliach (np. seria nieudanych logowań z jednego adresu)
- [ ] Retencja logów minimum przez rok

Lista kontrolna bezpieczeństwa

OWASP Top 10:2025 dla aplikacji webowych

Obsługa błędów i CI/CD (A10)

- [ ] Domyślna odmowa dostępu przy każdym wyjątku (fail-closed)
- [ ] Skan bezpieczeństwa (ZAP baseline) przy każdym wdrożeniu
- [ ] Analiza składu oprogramowania (SCA) i statyczna analiza kodu (SAST)