Ministerstwo Cyfryzacji

PWCyber

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Departament Cyberbezpieczeństwa

SZKOLENIE ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

3 lutego 2026 r.
Typ 300
Analiza podatności i testy bezpieczeństwa oprogramowania
EFIGO

9.45 – 10.00	**Logowanie**
10.00 – 10.05	**Zasady organizacyjne przebiegu szkolenia** *Przedstawiciel Departamentu Cyberbezpieczeństwa MC*
10.05 – 12.00	**Wprowadzenie do testów** • Rodzaje testów oprogramowania (Bloackbox, Whitebox, Graybox) • Główne rodzaje testowanego oprogramowania i różnice w podejściu (web, mobile, client) • Framework'i testowania oprogramowania **Specyfika pracy pentestera** • Skąd biorą się podatności • Jak budować wiedzę i rozwijać kompetencje • Najważniejsze narzędzia **Anatomia Testu Penetracyjnego: Od Rekonesansu po Przejęcie Kontroli** • Faza I: Polowanie na Informacje – Sztuka Rekonesansu • Faza II: Poszukiwanie Pęknięć w Murze – Analiza Podatności • Faza III: Przełamanie Linii Obrony – Sztuka Eksploatacji **Raportowanie** • Ocena podatności w skali CVSS • Struktura i treść poprawnego raportu *Ekspert „Efigo”: Maksym Brzęczek*
12.00 – 12.10	**Sesja pytań i odpowiedzi do ekspertów**