PROGRAM SZKOLENIA

Szkolenie z zakresu atakowania i ochrony aplikacji webowych (webaplikacji)

Tematyka zajęć: Usługa przeprowadzenie szkolenia z zakresu atakowania i ochrony aplikacji webowych (webaplikacji) w ramach projektu„Cyberbezpieczeństwo dla gospodarki przyszłości”
Uczestnicy szkolenia: kadra naukowo dydaktyczna Politechniki Wrocławskiej

Organizator: MrCertified
Trener: Rafał Wójcicki

Termin szkolenia:
22-23.09.2022 r. w godz. 9:00-16:00

Łączna liczba zajęć: 16 godzin dydaktycznych, (2 dni)

Wymagania techniczne:

- Maszyna wirtualna Kali Linux 2021.3: https://www.osboxes.org/kali-linux/#kali-linux-2021-3-vmware
- Maszyna wirtualna metasploitable2: https://sourceforge.net/projects/metasploitable/
- Narzędzie do wirtualizacji VMWare Player: https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html
- 20 GB wolnego miejsca na dysku
- 4 GB RAM

Program warsztatów:

Dzień	Liczba godzin	Zakres
Dzień 1	1	• Wstęp, ustalenie zasad szkolenia, Test kompetencji - Pre test • Wprowadzenie do podstaw www. Współczesne problemy bezpieczeństwa aplikacji webowych
	1	• Ataki na aplikacji webowe - Omówienie OWASP TOP 10 • Omówienie podatności SQL Injection

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Politechnika Wrocławska
Unia Europejska Europejski Fundusz Społeczny

Projekt współfinansowany ze Środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego, Program Operacyjny Wiedza Edukacja Rozwój, Priorytet III Szkolnictwo Wyższe dla gospodarki i rozwoju, Działanie 3.5 Kompleksowe programy szkół wyższych w ramach konkursu nr POWR.03.05.00-IP.08-00-PZ3/18 na Zintegrowane Programy uczelni – Ścieżka III, nr umowy POWR.03.05.00-00-Z308/18-00
Tytuł projektu: „Cyberbezpieczeństwo dla gospodarki przyszłości”

		○ Opis ○ Przykłady ○ Narzędzia ○ Przeciwdziałanie
	1	• SOP & CORS • Omówienie podatności XSS ○ Opis ○ Przykłady ○ Przeciwdziałanie
	2	• Omówienie podatności CSRF ○ Opis ○ Przykłady ○ Przeciwdziałanie • Omówienie zagadnień związanych z bezpieczeństwem haseł
	1	• Problemy wynikające z przeglądarek • Omówienie zagadnień związanych z przejmowaniem sesji • Omówienie podatności File inclusion ○ Opis ○ Przykłady ○ Przeciwdziałanie
	1	• Omówienie zagadnień związanych z niezabezpieczonym przesyłaniem plików • Omówienie zagadnień związanych z wstrzykiwaniem poleceń systemowych
	1	• Pentesty www e2e: od analizy ryzyka po tworzenie raportu

Dzień	Liczba godzin	Zakres
Dzień 2	2	• Konfiguracja środowiska • Testy wskazanej aplikacji pod kątem występowania: SQLI i Blind SQLI

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Politechnika Wrocławska
Unia Europejska Europejski Fundusz Społeczny

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego, Program Operacyjny Wiedza Edukacja Rozwój, Priorytet III Szkolnictwo Wyższe dla gospodarki i rozwoju, Działanie 3.5 Kompleksowe programy szkół wyższych w ramach konkursu nr POWR.03.05.00-IP.08-00-PZ3/18 na Zintegrowane Programy uczelni – Ścieżka III, nr umowy POWR.03.05.00-00-Z308/18-00
Tytuł projektu: „Cyberbezpieczeństwo dla gospodarki przyszłości”

	2	• Testy wskazanej aplikacji pod kątem występowania: CSRF, File inclusion, wstrzykiwania poleceń systemowych
	1,5	• Testy wskazanej aplikacji pod kątem występowania: Reflected i Stored XSS
	1,5	• Testy wskazanej aplikacji pod kątem występowania: podatności na hasła i niezabezpieczone przesyłanie plików • Przegląd narzędzi automatyzujących wykrywanie podatności
	1	• Podsumowanie szkolenia, Test kompetencji - Post test

Opis metod i technik wykorzystywanych podczas szkolenia

- Interaktywny wykład, demonstracja
- Praktyczne ćwiczenia indywidualne, warsztat komputerowy
- Dyskusja moderowana, Q&A

Proces certyfikacji

Uzyskanie certyfikatu ukończenia szkolenia – warunkiem jest ukończenie kursu oraz zaliczenie Post Testu (uzyskanie wyniku co najmniej na poziomie 60%)

Efekty uczenia się w ramach szkolenia

Uczestnicy:

- Będą znali podstawowe podatności na aplikacje www, w tym metody przeprowadzania ataków i ich przeciwdziałania
- Będa znali podstawy analizy ryzyka
- Uczestnicy dzięki ćwiczeniom będą w stanie m.in:
  - Znajdować podstawowe podatności www
  - Przeprowadzać atak z wykorzystaniem podatności
- Będą gotowi:
  - Przeprowadzić test bezpieczeństwa aplikacji www, którego wyniki zostaną przedstawione w raporcie

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Politechnika Wrocławska
Unia Europejska Europejski Fundusz Społeczny

Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego, Program Operacyjny Wiedza Edukacja Rozwój, Priorytet III Szkolnictwo Wyższe dla gospodarki i rozwoju, Działanie 3.5 Kompleksowe programy szkół wyższych w ramach konkursu nr POWR.03.05.00-IP.08-00-PZ3/18 na Zintegrowane Programy uczelni – Ścieżka III, nr umowy POWR.03.05.00-00-Z308/18-00
Tytuł projektu: „Cyberbezpieczeństwo dla gospodarki przyszłości”