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:
3 dni, 19 – 21 wrzesień 2023

Łączna liczba zajęć: 24 godzin dydaktycznych, (3 dni)

Wymagania techniczne:

- Maszyna wirtualna Kali Linux 2021.3: https://www.osboxes.org/kali-linux/#kali-linux-2021-3-vmware
- Narzędzie do wirtualizacji VMWare Player: https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html
- 40 GB wolnego miejsca na dysku
- 4 GB RAM (rekomendowane 8 GB)
- 4 wątki logiczne vCPU (rekomendowane 6)

Program warsztatów:

Dzień	Liczba godzin	Zakres
Dzień 1	2	• Wstęp, ustalenie zasad szkolenia, Test kompetencji - Pre test • Omówienie współczesnych problemów bezpieczeństwa aplikacji webowych • Ataki na aplikacji webowe - Omówienie OWASP TOP 10 2023

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”

		• Wstęp - OWASP ASVS, HSTS, HTML5 security, SAST (ochrona pasywna) • Fazy ataku, rozpoznanie, enumeracja, detekcja, obsługa, ataki na warstwy sieciowe,
	3	• Ataki bazującę na wstrzyknięciach do baz danych: ○ Przypomnienie podstaw związanych z bazami danych typu SQL oraz NoSQL ○ sposoby testowania aplikacji pod kątem podatności wstrzyknięć, ○ wyszukiwanie podatności, eksploitacja, kradzież danych, RCE ○ Blind SQLI ○ zabezpieczenia przed wstrzyknięciami
	3	• Ataki bazujące na wstrzyknięciach/Client-side - "stored", "reflected", "aggregated", "replied", atakach "jamming", "fuzzing" • Ataki na Client-side: • XSS ○ Rodzaje XSS, ○ Przypomnienie javascript ○ Wyszukiwanie podatności ○ Tworzenie exploitów ○ metody obrony przed XSS • Ataki CSRF oraz XSRF ○ Teoria związana z CSRF-token oraz ciasteczkami ○ wyszukiwanie podatności ○ kradzież tokena oraz ciasteczek ○ tworzenie exploita ○ metody obrony
	2	• Ataki na aplikację webowe: SSTI + RCE ○ Teoria ataków Server-Side Template Injection ○ Wyszukanie podatności ○ Wstrzykiwanie komend ○ Eksploitacja ○ Remote Code Execution ○ Przejęcie kontroli nad serwerem www, działania post-eksploitacyjne

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”

Dzień	Liczba godzin	Zakres
Dzień 2	2	• Omówienie zagadnień związanych z niezabezpieczonym przesyłaniem plików ○ Omówienie zagadnień związanych z wstrzykiwaniem poleceń systemowych ○ Atak zip-symlink oraz zip slip
	3	• Ataki związane z XML, SSRF ○ Teoria dotycząca XML, encji, XXE, ○ Rodzaje XML, rodzaje podatności XXE, ○ XML bombs, Billion Laughs, Quadratic Blowup, ○ Atak Server-Side Request Forgery, ○ Zaawansowany atak wykorzystujący dwie mniejsze podatności w celu uzyskania RCE (XXE + SSRF) ○ Zabezpieczenia przed atakami XXE i SSRF
	3	• Obchodzenie advanced Web Application Firewall ○ Open-source WAF vs. F5 BIG-IP WAF ○ Mechanizmy obrony WAF ○ Sposoby obchodzenia WAF ○ Testy skuteczności WAF z wykorzystaniem narzędzi automatyzujących ○ IDPS, AGP, Proxy

Dzień	Liczba godzin	Zakres
Dzień 3	6	• Wyzwania pentesterskie podsumowujące zdobytą wiedzę. ○ Autorski CTF “Injections” ○ Autorski CTF “Entities”
	1	• Pentesty www e2e: od analizy ryzyka po tworzenie raportu

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”

	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”