securitum

Websecurity **Master**

Najbardziej praktyczny i kompleksowy kurs dotyczący bezpieczeństwa aplikacji webowych na rynku!

12 4-godzinnych sesji szkoleniowych w przystępnej formule

MODUŁ 1

Podstawy bezpieczeństwa aplikacji webowych

1950 ZŁ NETTO

MODUŁ 2

Zaawansowane bezpieczeństwo aplikacji webowych

1950 ZŁ NETTO

POŁĄCZ I ZYSKAJ

Moduł PODSTAWOWY I ZAAWANSOWANY

3500 ZŁ NETTO

DLACZEGO TEN KURS JEST TAK DOBRY

- Łącznie ponad 50 godzin szkoleniowych warsztatowej wiedzy od trenerów-praktyków
- Optymalna formuła: online, 4-godzinne sesje na żywo raz w tygodniu, czas trwania kursu: 12 tygodni
- Elastyczna możliwość uczestnictwa w jednym bądź dwóch modułach
- Dostęp do dedykowanego LAB-u szkoleniowego do samodzielnych ćwiczeń
- Dostęp do nagrań z sesji na żywo przez sześć miesięcy
- Dostęp do platformy wymiany wiedzy (Discord), konsultacje z trenerami i uczestnikami
- Certyfikat uczestnictwa w szkoleniu (w językach polskim i angielskim)

GRATIS!

E-book
bestsellerowej książki *Bezpieczeństwo aplikacji webowych*

CO ZYSKA UCZESTNIK KURSU

- Umiejętność identyfikacji potencjalnych ataków na aplikacje webowe
- Możliwość zastosowania poznanych metod ochrony przed atakami
- Zdolność do samodzielnego przeprowadzania testów penetracyjnych
- Informacje na temat kluczowych narzędzi i dokumentacji
- Unikalną wiedzę od praktyków, pomocną w rozwoju kariery

CO ZYSKA FIRMA

- Zwiększenie odporności organizacji na cyberataki
- Podniesienie jakości tworzonego kodu aplikacji
- Przyśpieszenie procesu wdrożenia i odbioru aplikacji
- Cenną wiedzę ekspercką dla organizacji
- Wyróżniającą się formę wsparcia dla pracowników

START KURSU: 8 KWIETNIA 2025 R.

https://websec.sekurak.pl/

DLA KOGO

PODZIAŁ KURSU
na dwa moduły
odpowiada na potrzeby
początkujących
i zaawansowanych
uczestników

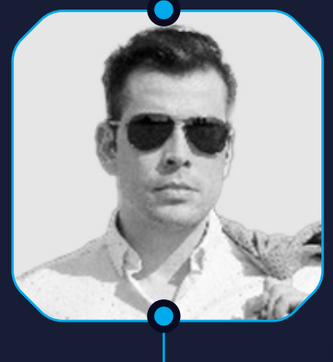
- Testerzy
- Programiści
- DevOpsi
- Pentesterzy
- Administratorzy systemów

TRENERZY

Marek Rzepecki. Zawodowy, etyczny hacker z zespołu Securitum i pasjonat tematyki ofensywnego cyberbezpieczeństwa. Przeprowadził setki niezależnych audytów bezpieczeństwa aplikacji webowych i mobilnych, infrastruktur sieciowych oraz testów odporności na ataki typu DDoS dla największych firm – zarówno polskich, jak i zagranicznych. Trener, który przeszkolił tysiące osób w Polsce i za granicą w zakresie bezpieczeństwa aplikacji i infrastruktury IT. Prelegent na konferencjach branżowych i autor materiałów edukacyjnych.

Kamil Jarosiński. Konsultant do spraw bezpieczeństwa IT w Securitum. Na co dzień testuje bezpieczeństwo aplikacji WWW, API, środowisk chmurowych, hardware w największych bankach, u operatorów telefonii komórkowej czy w branży e-commerce. Aktywny trener, prelegent na konferencjach branżowych. W wolnych chwilach uczestnik programów *bug bounty* ze zgłoszonymi podatnościami w Sony, HCL Software czy Telekom Deutschland.

Mateusz Lewczak. Doświadczony programista, zainteresowany niskopoziomowymi aspektami Security, w wolnym czasie wykorzystuje swoją kreatywność do tworzenia narzędzi hackerskich. Wielokrotnie nagradzany za wybitne osiągnięcia w nauce (w tym Stypendium Prezesa Rady Ministrów). Konsultant do spraw bezpieczeństwa IT w Securitum oraz członek międzynarodowego instytutu IEEE zrzeszającego ambitnych specjalistów ze świata IT.



Robert Kruczek. Pentester, socjotechnik, etyczny hacker z zespołu Securitum, w wolnych chwilach programista, gracz. Uczestnik programów *bug bounty* – miejsce w Hall of Fame OLX. Ma na swoim koncie zgłoszone błędy bezpieczeństwa między innymi dla: BlaBlaCar, OVH, ERCOM... Doświadczony pentester aplikacji desktopowych i webowych. Człowiek, który skutecznie przełamuje zabezpieczenia fizyczne (i nie tylko), weryfikując podczas testów socjotechnicznych bezpieczeństwo organizacji. Prelegent na konferencjach branżowych, autor tekstów na sekurak.pl.

ZAPISY I SZCZEGÓŁY

https://websec.sekurak.pl/

Dodatkowe pytania: Aneta Jandziś
aneta.jandzis@securitum.pl
tel. +48 (12) 352 33 82
+48 516 824 029

AGENDA

MODUŁ 1

Podstawy bezpieczeństwa aplikacji webowych

Sesja nr 1: Praktyczne wprowadzenie do bezpieczeństwa aplikacji webowych:

- Przegląd prawdziwych, aktualnych podatności w aplikacjach webowych (z ostatniego roku). Pokazy na żywo.
- Podstawy rekonesansu aplikacji webowych.
- Podstawy korzystania z narzędzia Burp Suite oraz podstawy protokołu HTTP.
- Pokaz wieloetapowego ataku na aplikację webową.
- Wprowadzenie do testowania bezpieczeństwa aplikacji webowych:
  1. jak zaplanować testy bezpieczeństwa aplikacji,
  2. testy automatyczne *vs* testy ręczne,
  3. raportowanie.

Sesja nr 2: Skondensowane wprowadzenie do *OWASP Top Ten*:

- Przegląd wszystkich 10 klas podatności.
- Omówienie ogólnych strategii obrony aplikacji przed atakami.
- Pokazy na żywo.
- LAB do realizacji przez uczestników.

Sesja nr 3: Podatności/problemy w mechanizmach uwierzytelnienia/autoryzacji:

- Bezpieczne przechowywanie haseł w aplikacji.
- W jaki sposób hackerzy potrafią ominąć uwierzytelnianie dwuskładnikowe? Jak temu zapobiec?
- Problemy z mechanizmami resetu hasła.
- Podatności klasy IDOR.
- Bezpieczeństwo JWT.
- Przegląd nietypowych podatności umożliwiających ominięcie uwierzytelnienia/autoryzacji.
- LAB do realizacji przez uczestników.

Sesja nr 4: Przegląd częstych podatności w aplikacjach webowych (część I):

- Podatności klasy RCE/*Command Injection*:
  1. mechanizmy uploadu,
  2. przegląd podatności *Command Injection*,
  3. problemy w bibliotekach,
  4. inne podatności prowadzące do wykonania kodu w systemie operacyjnym (przegląd).
- LAB do realizacji przez uczestników.

Sesja nr 5: Przegląd częstych podatności w aplikacjach webowych (część II):

- Przegląd częstych podatności występujących w aplikacjach webowych:
  1. *SQL Injection*,
  2. *NoSQL Injection*,
  3. manipulacje plikami XML w celu zdobycia nieautoryzowanego dostępu do danych na serwerze (XXE),
  4. podatność SSRF,
  5. podatność *Path Traversal*,
- LAB do realizacji przez uczestników.

Sesja nr 6: Wieloetapowe ćwiczenie podsumowujące podstawowy moduł szkolenia:

- Rekonesans.
- Wykorzystanie kilku podatności.
- Podniesienie uprawnień w atakowanym systemie.

MODUŁ 2

Zaawansowane bezpieczeństwo aplikacji webowych

Sesja nr 1: Zaawansowane bezpieczeństwo aplikacji webowych (przegląd podatności, część I):

- Podatności związane z deserializacją.
- Podatność SSTI.
- Podatność *Mass Assignment*.
- Jak włączone mechanizmy debug mogą prowadzić do przejęcia kontroli nad aplikacją webową?
- LAB do realizacji przez uczestników.

Sesja nr 2: Zaawansowane bezpieczeństwo aplikacji webowych (przegląd podatności, część II):

- Czym jest WAF?
- Techniki omijania WAF.
- *HTTP request smuggling*.
- Wybrane problemy bezpieczeństwa mechanizmów *cache* w aplikacjach webowych.
- Mechanizmy przeglądarkowe służące do zabezpieczania aplikacji webowych i ich użytkowników.
- LAB do realizacji przez uczestników.

Sesja nr 3: Bezpieczeństwo API REST:

- Omijanie zabezpieczeń dostępu do metod HTTP.
- Podatności *Server-Side Request Forgery* (SSRF) oraz XXE w kontekście API REST.
- Wycieki kluczy API.
- Bezpieczeństwo OAuth2.
- Wybrane klasyczne podatności webowe w kontekście API REST.
- LAB do realizacji przez uczestników.

Sesja nr 4: Podstawy bezpieczeństwa frontendu aplikacji webowych (część I – Podatność XSS):

- *Cross-Site Scripting* – najistotniejsza podatność świata *client-side*.
- Omówienie *Same Origin Policy* i trening praktycznych skutków XSS.
- Typy XSS.
- Omówienie punktów wejścia XSS (parametry GET/POST, pliki Flash, pliki SVG, upload plików).
- Charakterystyka punktów wyjścia XSS (niebezpieczne funkcje JS, konteksty w HTML).
- Omówienie metod ochrony przed XSS, techniki omijania filtrów XSS.
- XSS a dopuszczanie fragmentów kodu HTML.
- LAB do realizacji przez uczestników.

Sesja nr 5: Podstawy bezpieczeństwa frontendu aplikacji webowych (część II – Inne podatności frontendowe):

- Biblioteki JS (jQuery, Angular, React, Knockout).
- **Wybrane problemy dotyczące bezpieczeństwa elementów API HTML5.**
- Podatność CSRF.
- LAB do realizacji przez uczestników.

Sesja nr 6: Wieloetapowe ćwiczenie podsumowujące zaawansowany moduł kursu:

- Wykorzystanie kilku podatności.
- Ominięcie filtrów/WAF.
- Wykorzystanie problemów bezpieczeństwa w klasycznych aplikacjach oraz w API REST.