OTWA

Ofensywne Testowanie Web Aplikacji

Najlepsze w Polsce szkolenie o bezpieczeństwie web aplikacji

DODAJ TESTOWANIE BEZPIECZEŃSTWA DO SWOJEGO ARSENAŁU

Ofensywne Testowanie Web Aplikacji (OTWA) to jedyne takie szkolenie **dla testerów, inżynierów QA, deweloperów, opsów i specjalistów bezpieczeństwa.** Nauczy ich przeprowadzać pentesty bezpieczeństwa web aplikacji, wykrywać i eliminować realne zagrożenia zgodnie ze standardami OWASP oraz efektywnie raportować rezultaty.

Korzyści dla firmy i zespołu:

- **Zidentyfikujesz i wyłapiesz podatności swoich aplikacji zanim trafią na produkcję.**
- **Zabezpieczysz obecne projekty poprzez ich atakowanie.**
- **Zadbasz o bezpieczeństwo swoich programów poprzez holistyczne przeszkolenie osób biorących udział w wytwarzaniu SD/LC.**

Dzięki formule online:

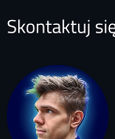
- **Nie odrywamy Twojego zespołu od bieżących projektów.**
- **Wszystkie nagrania i materiały są dostępne przez 365 dni.**
- **Bogata agenda: Fuzzing, DAST, XSS, IDOR, SSRF i wiele innych.**

Dołącz do Ofensywne Testowanie Web Aplikacji

Szczegółowy program: 👉 www.otwa.pl

Masz dodatkowe pytania?

Skontaktuj się z nami, odpowiemy szybko!



Rafał Goliszewski
Koordynator Kursu
rafal@bezpiecznykod.pl

Twórca Ofensywne Testowanie Web Aplikacji

Andrzej Dyjak

Prowadzi firmę doradczo-szkoleniową **Bezpieczny Kod**. W przeszłości pomógł poprawić bezpieczeństwo aplikacji firm takich jak **Apple**, **Google**, **Oracle**, **Mozilla** czy **Real Networks**.
W ostatnich latach przeszkolił **setki** specjalistów IT (QA, Dev, Ops) z tematów takich jak Testowanie Bezpieczeństwa, Modelowanie Zagrożeń, DevSecOps oraz Secure By Design.

Start: 31 marca
Zakończenie: 4 maja

Szkolenia Bezpiecznego Kodu ukończyło ponad 1500 inżynierek i inżynierów z firm takich jak Orange, BNP Paribas, XTB, Grupa Pracuj, Autopay i wielu innych.

Cena uczestnictwa

1490 zł + 23%VAT **/ od osoby**
1832,70 zł brutto

3-5 osób	-10%
6-30 osób	-15%
30+ osób	-20%

Możliwe finansowanie:
– 2 raty 0%.

OTWA

Moduł 0	Tematy	Rezultaty	Projekty i Bonusy
Fundamenty OTWA aka „Bootloader”	**Orientacja na temat kursu OTWA i jego przebiegu** **Ważne projekty OWASP z punktu widzenia testera bezpieczeństwa** **Podstawy działania sieci Web (HTTP, DOM, SOP, CORS)** **Sposoby oceny bezpieczeństwa aplikacji i systemów IT** **Testowanie Black-box, Gray-box i White-box**	• Przypomnisz sobie w jaki sposób działa sieć Web oraz przeglądarka • Poznasz fundamenty bezpieczeństwa aplikacji • Zrozumiesz czym i w jaki sposób można oceniać bezpieczeństwo aplikacji i systemów IT	• Budowa planu przerabiania kursu

Moduł 1	Tematy	Rezultaty	Projekty i Bonusy
Rekonesans i enumeracja	**Mapowanie powierzchni ataku** **Pliki specjalne obecne na web serwerze** **Problemy z HTTPS i jego brakiem** **Sniffing lokalnego ruchu sieciowego** **Wykrywanie mechanizmów obronnych web aplikacji**	• Odkryjesz stos technologiczny web aplikacji • Wykonasz skan web aplikacji pod kątem dostępnych zasobów i funkcjonalności • Przeprowadzisz automatyczny skan podatności web serwera • Zweryfikujesz bezpieczeństwo certyfikatu SSL/TLS web aplikacji • Wykonasz aktywny podsłuch ruchu sieciowego • Przeskanujesz aplikacje pod kątem używanego WAF-a	• Budowa własnego laboratorium do testowania bezpieczeństwa web aplikacji • ⚡ BONUS: Archiwalne nagrania podcastu “Bezpieczna Produkcja”

Moduł 2	Tematy	Rezultaty	Projekty i Bonusy
Podatności w AuthZ i wstrzyknięcia kodu	**Wykrywanie i weryfikacja podatności w kontroli dostępu na przykładzie Insecure Direct Object Reference (IDOR)** **Wykrywanie i weryfikacja podatności typu wstrzyknięcia na przykładzie Cross-Site Scripting (XSS)** **Wykorzystanie automatyzacji do weryfikacji znalezionych podatności oraz do szukania nowych podatności**	• Otrzymasz dostęp do danych innych użytkowników dzięki podatności IDOR • Wykradniesz ciasteczka użytkownika wykorzystując podatność XSS (symulacja realnego ataku) • Wykonasz automatyczny skan podatności web aplikacji wykorzystując niestandardowe payloady (Fuzzing)	• Rozpoczęcie raportowania podatności w szkoleniowej aplikacji • ⚡ BONUS: Szablon raportu z testów bezpieczeństwa web aplikacji • ⚡ BONUS: Poradnik “Jak napisać dobry raport z testów bezpieczeństwa”

Moduł 3	Tematy	Rezultaty	Projekty i Bonusy
Błędna logika, konfiguracja & podatne biblioteki	**Wykrywanie i weryfikacja podatności wynikających z logiki biznesowej na przykładzie mechanizmu uwierzytelniania** **Wykrywanie i weryfikacja podatności wynikających z konfiguracji na przykładzie nagłówków bezpieczeństwa** **Polityki Strict Transport Security (HSTS) oraz Content Security Policy (CSP)** **Problemy związane z użyciem zewnętrznych komponentów na przykładzie web aplikacji oraz jej kontenera**	• Poznasz proces Modelowania Zagrożeń i pryncypia bezpiecznej architektury • Zbadasz bezpieczeństwo serwowanych przez aplikację nagłówków • Ocenisz serwowaną politykę CSP pod kątem poprawności • Przeskanujesz obraz Dockerowy pod kątem bezpieczeństwa	• Dalsze uzupełnianie raportu z testów • ⚡ BONUS: Webinar na temat Modelowania Zagrożeń

Moduł 4	Tematy	Rezultaty	Projekty i Bonusy
Podatności w AuthN, integralność & automatyzacja ataków	**Ataki siłowe na mechanizm uwierzytelniania web aplikacji oraz na dostępne usługi (OpenSSH)** **Automatyzacja procesu szukania podatności (Analiza Dynamiczna - DAST)** **Atakowanie łańcucha dostawczego a mechanizm Subresource Integrity (SRI)**	• Przeprowadzisz atak siłowy na hasło użytkownika web aplikacji • Przeprowadzisz atak “Credential Stuffing” na użytkowników web aplikacji • Odkryjesz nowe podatności w aplikacji testowej dzięki automatyzacji (DAST) • Przeprowadzisz zautomatyzowany atak na użytkowników usługi OpenSSH • Wykonasz symulację ataku na łańcuch dostawczy po stronie front-end (CDN)	• Dalsze uzupełnianie raportu z testów • ⚡ BONUS: Dostęp do GPT wytrenowanego na materiale Programu OTWA

Moduł 5	Tematy	Rezultaty	Projekty i Bonusy
Podatność SSRF i Raportowanie	**Wykrywanie i weryfikacja podatności Server-Side Request Forgery (SSRF)** **Ocena krytyczności znajdywanych problemów bezpieczeństwa** **Identyfikacja znanych podatności oraz klasyfikacja nowych podatności** **Charakterystyka dobrego raportu z testów bezpieczeństwa** **Szyfrowanie z wykorzystaniem PGP** **Dalsze ścieżki rozwoju**	• Wykorzystasz podatność, która spowodowała wielomilionowe ($$$) wycieki danych • Poznasz rynkowe narzędzia do oceny krytyczności oraz klasyfikacji znajdywanych podatności • Wygenerujesz swój klucz PGP i użyjesz go do zaszyfrowania finalnego raportu (tak jak ma to miejsce w realnych testach) • Skończysz pisać raport i oddasz go do mojej oceny	• Uzupełnienie raportu o finalną podatność • Oddanie raportu do oceny • ⚡ BONUS: Webinar na temat bezpieczeństwa i zagrożeń związanych z AI oraz użyciem LLM w web aplikacjach? • ⚡ BONUS: Poradnik “Jak ulepszyć swój profil LinkedIn”

Masz dodatkowe pytania?

Skontaktuj się z nami, odpowiemy szybko!

Rafał Goliszewski
Koordynator Kursu
rafal@bezpiecznykod.pl