

Atakowanie i ochrona aplikacji webowych

Nasze szkolenie posiada unikatową formułę: **minimum teorii, maksimum praktyki**. Każde z omawianych zagadnień poprzedzamy teoretycznym wstępem oraz demonstracją ataku w wykonaniu trenera, ale główny nacisk kładziemy na ćwiczenia praktyczne wykonywane przez uczestników.

Ćwiczeniom praktycznym poświęcamy najwięcej czasu, ponieważ pozwalają każdemu uczestnikowi szkolenia **własnoręcznie przeprowadzić omawiany atak**. Podczas szkolenia do dyspozycji uczestników oddajemy sieć laboratoryjną, w której znajdują się specjalnie przygotowane webaplikacje, wykorzystujące spotykane w rzeczywistym świecie oprogramowanie (wraz z występującymi w nim dziurami).

Dlaczego stawiamy na praktykę? Bo sama teoria w bezpieczeństwie nie wystarcza.

powiedz mi, a zapomnę, pokaż — a zapamiętam, pozwól mi działać, a zrozumiem!

Po naszym szkoleniu będziesz naprawdę zmęczony, ale uwierz nam, że zamiast o odejściu od komputera będziesz myślał wyłącznie o tym, jak dalej pogłębiać swoją wiedzę.

Dzięki naszemu szkoleniu...

- * poznasz **techniki ataków i programy** wykorzystywane przez współczesnych włamywaczy
- * nauczysz się korzystać z **kilkudziesięciu narzędzi** do testowania bezpieczeństwa webaplikacji
- * dowiesz się w jaki sposób można **zabezpieczyć aplikacje webowe** przed atakami
- * własnoręcznie **przeprowadzisz skuteczne ataki** na webaplikacje
- * sam wykonasz **test aplikacji webowej** (od analizy ryzyka poprzez identyfikację podatności aż do raportu)

Do kogo jest kierowane szkolenie?

Szkolenie kierujemy przede wszystkim do osób, których praca ociera się o aplikacje webowe, a więc:

- **programistów i testerów,**
- **audytorów i pentesterów,**
- **architektów i projektantów systemów komputerowych**
- **oficerów zespołów bezpieczeństwa**

...ale tak naprawdę, każdą osobę która chce podnosić swoje kwalifikacje i wiedzę w temacie bezpieczeństwa aplikacji internetowych powitamy z otwartymi ramionami — dla nas wszyscy jesteście żądnymi wiedzy ludźmi, a nie stanowiskami ;-)

Każdy uczestnik naszych szkoleń musi podpisać deklarację, że z poznane ataki i narzędzia będzie wykorzystywał wyłącznie w celu testowania bezpieczeństwa swoich własnych sieci i webaplikacji.

Termin szkolenia

Szkolenie jest **2-dniowe**. Startujemy o **9:00**, a kończymy w momencie w którym z sił opadnie ostatnia osoba. Dokładne terminy szkoleń dostępne są pod adresem: <http://niebezpiecznik.pl/szkolenia>
Ponieważ szkolenia informatyczne to nie tylko wiedza, ale i okazja żeby nawiązać wartościowe znajomości, po pierwszym dniu zajęć zapraszamy na popołudniowe afterparty w jednym z krakowskich pubów. W luźnej atmosferze wymienimy się ciekawymi historiami z wykonanych testów penetracyjnych (oczywiście bez podawania nazw firm ;). Jedyna taka okazja, żeby usłyszeć jak w firmie X rozwiązano problem Y...

Tematyka szkolenia

- **Współczesne problemy bezpieczeństwa aplikacji webowych**
 - zagrożenia wynikające z architektury webaplikacji (CGI, SSI, etc.)
 - zagrożenia wynikające z języków programowania (PHP, ASP, JSP, JS, etc.)
 - problem styku webaplikacji z bazą danych
 - interfejsy zewnętrzne webaplikacji
 - zagrożenia po stronie serwera a zagrożenia po stronie klienta
- **Ataki na aplikacje webowe**
 - Brak obsługi błędów
 - Manipulacje parametrami (metody GET, POST)
 - Techniki podsłuchu i manipulowania transmisją
 - Atak Forcefull browsing
 - Atak Path Traversal
 - Technika Google Hacking
 - **Wstrzyknięcie kodu** (PHP shell) i komend systemowych
 - Ataki XSS (persistent, reflected, etc)
 - Problem filtrowania danych wejściowych
 - Omijanie filtrowania danych wejściowych i wyjściowych
 - **Ataki na sesję aplikacji webowej**
 - Podsłuchiwanie sesji i kradzież ciasteczek HTTP
 - Ataki session fixation i session adoption
 - Ataki CSRF
 - Jak poprawnie zarządzać sesją w webapikacji?
 - Szyfrowanie danych w webaplikacji
 - **Ataki na bazy danych**
 - Ataki SQL injection i Blind SQL injection
 - cechy charakterystyczne środowisk Oracle, Microsoft SQL, MySQL i PostgreSQL
 - ochrona przed atakami SQL injection
 - Szyfrowanie połączenia i ataki na SSL
 - Podsumowanie zagrożeń i przegląd OWASP TOP10
- **Problemy przeglądarek**
 - Same Origin Policy
 - Rich Internet Applications
 - Dziury w przeglądarkach
 - Ataki DNS-Rebinding
 - Wtyczki i pluginy podnoszące bezpieczeństwo i pomagające w testowaniu aplikacji webowych
- **Ochrona**
 - pozaprogramistyczne środki ochrony (systemy IDS/IPS, WAF)
 - ochrona przed spamem
 - bezpieczeństwo webserwera
 - szyfrowanie połączeń do webserwera (SSL)
- **Przeгляд narzędzi automatyzujących wykrywanie podatności**

Każdy z podpunktów związany jest z praktycznym ćwiczeniem. Podczas omawiania konkretnego ataku, zawsze pokazujemy jak się przed nim obronić. Dla przejrzystości konspektu, nie zostało to wyszczególnione powyżej.

Trener

Szkolenie poprowadzi Piotrek Konieczny, założyciel Niebezpiecznika. Piotrek od 5 lat prowadzi szkolenia autorskie i warsztaty z bezpieczeństwa dla polskich i zagranicznych firmam oraz instytucjami, prowadzącymi swój biznes w sektorach takich jak: bankowość, telekomunikacja, wojsko i administracja rządowa. Z tematu atakowania i ochrony webaplikacji Piotrek przeszkolił już ponad 200 osób, które swoje zadowolenie ze zdobytej wiedzy wyrażały na piśmie w poszkoleniowych ankietach oraz w rekomendacjach na LinkedIn http://www.linkedin.com/profile?viewProfile=&key=4733826&locale=en_US&trk=tab_pro#recommendations.

Miejsce szkolenia

Kraków, rzut pakietem od Rynku Głównego ;-) Szczegółowa lokalizacja zostanie podana przed szkoleniem.

Nasza sala szkoleniowa jest klimatyzowana i w pełni wyposażona w sprzęt komputerowy. Każdy z Was będzie miał do dyspozycji swojego laptopa z systemami Windows oraz Linux, (pokażemy ataki specyficzne dla jednego i drugiego systemu). Programy, z których będziemy korzystać podczas szkolenia otrzymacie od nas na własność na płytach CD.

Cena:

W przedsprzedaży: 1999 PLN + 23% VAT

Cena katalogowa: 2199 PLN + 23% VAT

(od 2011 roku tylko instytucje w co najmniej 70% finansowane z budżetu państwa są zwolnione z VAT)

Cena obejmuje:

- 2 dni szkoleniowe,
- 2 dwudaniowe obiady w pobliskiej restauracji,
- catering w przerwach (kawa, herbata, soki, ciasteczka),
- materiały szkoleniowe (podręcznik, zapis prezentacji, plus płyta CD z oprogramowaniem do przeprowadzania testów penetracyjnych aplikacji webowych),
- certyfikat ukończenia szkolenia
- gadżety-niespodzianki rozdawane pod koniec szkolenia, a związane z bezpieczeństwem :-)
- wieczysty, Nielimitowany dostęp do serwera FTP na którym znajdują się dodatkowe materiały

Aktualne ceny znajdą Państwo na stronie <http://niebezpiecznik.pl/szkolenia/>

UWAGA!!! Dla waszej wygody i komfortu ograniczamy liczbę osób, która może brać udział w szkoleniu do 10 osób. Kto pierwszy, ten lepszy!

Pytania? Złozzenia? Pisz na szkolenia@niebezpiecznik.pl