Testy penetracyjne aplikacji www – Warszawa, 17-18.09.2009r.

Program szkolenia

Dzień 1 (11:00 - 18:00)

10:15-10:45 -- Rejestracja
10:45-11:00 -- Powitanie. Przestawienie prelegenta oraz tematyki szkolenia
11:00-11:45 -- Testy penetracyjne - wprowadzenie
- Rodzaje audytów bezpieczeństwa IT
- Audyt aplikacji
- Testy penetracyjne

11:45 - 12:00 -- Przerwa
12:00 - 13:00 -- Aplikacje www
- Architektura aplikacji webowych vs architektura sieciowa systemu
- Ciekawe przykłady komunikacji http – śledzenie ruchu z wykorzystaniem http proxy
- Przykłady http serwerów i ich reakcji na niestandardowe requesty http
- Funkcjonalności oprogramowania Burp Suite Pro (część 1)

13:00 - 14:00 -- Obiad
14:15 - 15:45 -- SQL injection
- Charakterystyka
- Skutki wykorzystania błędu
- Metody detekcji
- Praktyczny pokaz ataku na system – wykonywany w czasie rzeczywistym. Zdalne przejęcie uprawnień administracyjnych w portalu
- Metody zapobiegania atakom

15:45 - 16:00 -- Przerwa
16:00 - 17:15 -- SQL Injection – mini case studies
- Uzyskanie dostępu do konsoli administracyjnej portalu oraz automatyczne przeniesienie ataku na inne serwisy
- Wyciek danych + ominięcie firewalla aplikacyjnego. Pokaz odbywający się w czasie rzeczywistym - atak na system zabezpieczony firewallem aplikacyjnym
- Google hacking + whitebox audit = mass SQL injection
- Metody zapobiegania atakom

17:15-18:00 -- Konsultacje z prelegentem
18:30 -- Kolacja

Dzień 2 (9:00 - 16:15)

8:15 - 8:45 -- Śniadanie
8:45 - 9:00 -- Poranna kawa
9:00 - 10:30 -- XSS (Cross Site Scripting)
- Charakterystyka
- Skutki wykorzystania błędu
- Metody detekcji
- Funkcjonalności oprogramowania Burp Suite Pro (część 2)

10:30 - 10:45 -- Przerwa
10:45 - 11:45 -- XSS – zaawansowane ataki oraz mini case studies
- Praktyczny pokaz przygotowania exploitu oraz ataku na system - w czasie rzeczywistym Zdalne przejęcie uprawnień administracyjnych w portalu

- Serwis społecznościowy - czy przeglądanie profilu innych użytkowników jest bezpieczne?
- Persistent XSS - czyli jak zostać administratorem bloga
- Metody zapobiegania atakom

12:00 - 13:00 -- obiad
13:15 - 14:15-- XSRF (Cross Site Request Forgery)

- Charakterystyka
- Skutki wykorzystania błędu
- Metody detekcji
- Praktyczny pokaz exploitu oraz ataku na system - wykonywany w czasie rzeczywistym. Zdalne przejęcie kontroli nad urządzeniem sieciowym
- Często powtarzane mity dotyczące błędów SQL injection, XSS, XSRF
- Metody zapobiegania atakom

14:15- 14:30-- Przerwa
14:30- 15:15 -- Narzędzia wspomagające testy penetracyjne - przegląd

- Narzędzia komercyjne
- Narzędzia darmowe
- Porównanie: testy manualnych vs testy zautomatyzowane

15:15 - 15:30 -- Zakończenie szkolenia
15:30 - 16:15 -- Konsultacje z prelegentem

Grupa docelowa

Szkolenie przeznaczone jest dla:

- Pracowników departamentów bezpieczeństwa firm
- Osób odpowiedzialnych za audyt zewnętrzny/wewnętrzny organizacji
- Osób związanych z branżą informatyki śledczej (computer forensic)
- Pracowników działów IT - w tym programistów aplikacji webowych

Od uczestników wymagana jest wiedza ogólna z zakresu:

- bezpieczeństwa aplikacji
- znajomości protokołu http, języka HTML - w tym JavaScript
- składni języka SQL
- Uwaga: szkolenie przeznaczone jest dla osób zaawansowanych

Prowadzący szkolenie

Michał Sajdak jest dyrektorem d/s rozwoju oraz konsultantem w firmie Securitum.

- Absolwent Uniwersytetu Jagiellońskiego (informatyka)
- Posiada wieloletnie doświadczenie w dziedzinach: bezpieczeństwa IT, tworzenia oprogramowania (głównie aplikacje dla instytucji finansowych) oraz administracji systemami
- Posiadacz certyfikatu CISSP (#338973)
- Wykonywał audyty bezpieczeństwa – w tym testy penetracyjne – dla największych organizacji w Polsce

Cena szkolenia

Cena szkolenia wynosi 2850 PLN netto / osobę i zawiera:

- Udział w szkoleniu
- Jednomiesięczną licencję oprogramowania Burp Suite Professional, zawierającą m.in.:
  - Burp intruder (zaawansowany fuzzer http)
  - Burp scanner (moduł automatycznych testów penetracyjnych www).
  - Książkę: "The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws".
- Nocleg w hotelu trzygwiazdkowym (pokoje jednoosobowe)
- Dostępne w trakcie szkolenia: kawa, herbata, woda, soki, ciasteczka - bez limitu
- Wyżywienie (śniadanie, 2 x obiad, kolacja)
- Konspekt szkolenia
- Certyfikat ukończenia szkolenia

W przypadku uczestnictwa w szkoleniu dwóch lub większej ilości osób z jednej firmy - dla każdego kolejnego uczestnika udzielamy 20% rabatu.