Audyt Bezpieczeństwa Systemów IT
Testy penetracyjne aplikacji webowych

Szkolenie organizowane jest przez **Akademię Linux Magazine**, organizatora cyklu warsztatów i szkoleń poświęconych najnowszej wiedzy związanej z zagrożeniami i bezpieczeństwem systemów IT oraz tworzeniem i administrowaniem sieciami i serwerami komputerowymi.

Zasady uczestnictwa: Szkolenie to jest organizowane zarówno jako szkolenie otwarte jak i zamknięte. Koszt szkolenia podany w załączonym na ostatniej stronie formularzu dotyczy szkolenia otwartego. W przypadku szkoleń zamkniętych koszt ustalany jest indywidualnie z zamawiającym. Minimalna liczba uczestników szkolenia to 5 osób, maksymalna 12.

Szkolenie zamknięte może odbyć się we współpracującym z nami ośrodku szkoleniowym lub w siedzibie firmy klienta. Dodatkowo zależnie od potrzeb, program danego szkolenia może zostać dostosowany do wymagań zamawiającego.

Podstawowe informacje o szkoleniu:

W mediach coraz częściej pojawiają się informacje o problemach z **bezpieczeństwem serwisów WWW**. Problem ten dotyka nie tylko dużych portali internetowych, serwisów aukcyjnych czy społecznościowych, ale coraz częściej również serwisów internetowych firm i instytucji. Nic w tym dziwnego, gdyż coraz częściej serwis internetowy współczesnej instytucji, to bardzo złożona aplikacja, umożliwiająca klientom, partnerom czy pracownikom korzystanie ze specjalnie przygotowanych dla nich usług i informacji.

Istotniejsze zagrożenia związane z serwisem WWW to między innymi:

- wykorzystanie podmienionej strony do propagacji złośliwego oprogramowania i dokonywania oszustw,
- wykorzystanie przejętych kont uprawnionych użytkowników do podjęcia działań w ich imieniu, ale bez ich wiedzy i zgody,
- zablokowania dostępu do usług, z których korzystają uprawnieni użytkownicy.

Tego typu zdarzenia pociągają za sobą przede wszystkim **bezpośrednie straty finansowe,** związane z przerwami w dostępie do usług, koniecznością wypłaty kar umownych, ujawnieniem tajemnic handlowych czy konsekwencjami prawnymi (np. niedopełnienia wymagań związanych z ochrona danych osobowych klientów). Oprócz tego zdarzenia te powodują straty pośrednie. Ujawnienie zaistniałego incydentu zachwiania bezpieczeństwa ma znaczący wpływ na opinię publiczną i wizerunek firmy.

Aby uchronić się przed negatywnymi konsekwencjami nadużyć w serwisach WWW konieczne jest właściwe ich zaprojektowanie, zapewnianie jakości kodu i ich należyte przetestowanie. **Penetracyjny test bezpieczeństwa, czyli symulowany atak**, jest jednym z najskuteczniejszych sposobów testowania bezpieczeństwa systemów IT, a w tym aplikacji webowych i serwisów internetowych.

Szkolenie skierowane jest do testerów penetracyjnych, jak i do osób odpowiedzialnych za techniczny audyt systemów informatycznych i techniczną analizę ryzyka informacyjnego w instytucjach finansowych, firmach telekomunikacyjnych, przedsiębiorstwach branży energetycznej czy urzędach administracji publicznej. Zainteresują także architektów, projektantów i deweloperów aplikacji WWW, pozwalając w praktyce poznać sposób myślenia i działania włamywacza.

Zagadnienia poruszone podczas szkolenia:

1. Metodyka audytu i testów penetracyjnych
2. Identyfikacja i wykorzystanie podatności serwera WWW
3. Testowanie podatności aplikacji WWW na szereg ataków (XSS, XSRF, SQLI, i wiele innych)
4. Testowanie aplikacji AJAXowych
5. Metody ukrywania ataku i omijania filtrów
6. Przeprowadzanie testów penetracyjnych skomplikowanych aplikacji
7. Fuzzing aplikacji WWW

Najważniejsze korzyści dla uczestników, biorących udział w Szkoleniu:

1. Poznanie metodyki testów penetracyjnych
2. Bardzo szczegółowe zapoznanie się z bezpieczeństwem technologii webowych
3. Nabycie praktycznych umiejętności przeprowadzenia testu penetracyjnego aplikacji WWW
4. Poznanie i praktyczne wykorzystanie narzędzi wspomagających prowadzenie testu penetracyjnego aplikacji WWW
5. Umiejscowienie zdobytej wiedzy na temat aplikacji WWW w kontekście całościowego testu penetracyjnego

Wymagania względem uczestników: podstawowa znajomość protokołów TCP/IP, podstawowa wiedza o programowaniu, podstawowa znajomość SQLa, podstawowa wiedza z języka HTML/JS - np. tworzenie formularzy, znajomość środowiska Linux, znajomość trójwarstwowej architektury aplikacji WWW.

Informacja o prowadzącym szkolenie: ***Przemysław Skowron***, od 8 lat związany jest z branżą IT, a od 5 zajmuje się bezpieczeństwem systemów teleinformatycznych. Swoje doświadczenie zdobywał m.in. w dużym portalu internetowym oraz fundacji zajmującej się szkoleniami. Aktualnie pracuje przy projektach bezpieczeństwa IT dla nowo powstałego banku. Wykonuje testy penetracyjne, udziela konsultacji, tworzy standardy i prowadzi badania różnych technologii bezpieczeństwa. Od roku 2007 związany z organizacją OWASP. Prelegent, autor wielu prezentacji, artykułów oraz szkoleń traktujących o bezpieczeństwie.

Audyt Bezpieczeństwa Systemów IT
Testy penetracyjne aplikacji webowych

Agenda - dzień pierwszy

09:20-09:50	*Rejestracja*
09:50-10:00	*Powitanie*
10:00-10:40	**Wprowadzenie: Teoria audytu i testów penetracyjnych; Metodyki audytu**
10:40-11:00	*Przerwa*
11:00-12:20	**Rozpoznawanie ataków oraz architektura aplikacji WWW** Pasywne oraz aktywne rozpoznawanie (identyfikacja serwerów WWW, identyfikacja wersji serwera i OS, identyfikacja punktów wejścia do aplikacji), architektura aplikacji WWW i potencjalne miejsca ataku
12:20-12:40	*Przerwa*
12:40-13:40	**Rozpoznawanie ataków oraz architektura aplikacji WWW c.d.; Bezpieczeństwo serwera WWW**
13:40-14:20	*Obiad*
14:20-17:00	**Podstawowe narzędzia testera aplikacji WWW; Łamanie haseł chroniących aplikacje WWW**
17:00-17:10	*Podsumowanie I dnia*

Agenda - dzień drugi

09:25-09:30	*Rozpoczęcie drugiego dnia*
09:30-10:30	**Najpopularniejsze błędy i podatności w aplikacjach WWW - część 1** Modyfikacja parametrów i formularzy, Cross Site Scripting (XSS), Injection Flaws
10:30-10:50	*Przerwa*
10:50-12:20	**Najpopularniejsze błędy i podatności w aplikacjach WWW - część 2** Directory Traversal/Forceful Browsing, SQL Injection, Malicious File Execution, PHP Remote File Include
12:20-12:40	*Przerwa*
12:40-13:40	**Najpopularniejsze błędy i podatności w aplikacjach WWW - część 3** Insecure Direct Object Reference, Cross Site Request Forgery (CSRF)
13:40-14:20	*Obiad*
14:20-16:30	**Najpopularniejsze błędy i podatności w aplikacjach WWW - część 4** Information Leakage and Improper Error Handling, Broken Authentication and Session Management, Insecure Cryptographic Storage
16:30-16:40	*Podsumowanie II dnia*

Agenda - dzień trzeci

09:25-09:30	*Rozpoczęcie drugiego dnia*
09:30-10:30	**Najpopularniejsze błędy i podatności w aplikacjach WWW - część 5** Insecure Communications, Failure to Restrict URL Access, Buffer overflow, Format string
10:30-10:50	*Przerwa*
10:50-13:00	**Najpopularniejsze błędy i podatności w aplikacjach WWW - część 6** Modyfikowanie logów, Ukrywanie ataku, fuzzing, AJAX
13:00-13:20	*Przerwa*
13:20-14:50	**Utrzymanie dostępu i zacieranie śladów**
14:50-15:00	*Podsumowanie i zakończenie*
15:00-15:40	*Obiad*

Dodatkowe informacje i zapisy:

W celu uzyskania dodatkowych informacji zapraszamy do odwiedzenia naszej strony internetowej. Z chęcią odpowiemy również na wszelkie pytania pod podanymi numerami kontaktowymi. Zapisów na szkolenie można dokonywać na stronie Akademii (**akademia.linuxmagazine.pl**) lub wysyłając zgłoszenie faksem lub emailem.

Kontakt: Akademia Linux Magazine, alm@alm.org.pl, tel.: 022 742 14 57.