Bezpieczeństwo aplikacji webowych (kod: APPSEC-WEB)

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Opis i cel szkolenia

Praktyczny, dwudniowy warsztat, przede wszystkim dla osób, które budują lub utrzymują aplikacje webowe. I chcą zobaczyć, jak wygląda atak na nie z drugiej strony oraz obrona przed atakami.

Uczestnicy pracują na przygotowanych podatnych aplikacjach: sami wyszukują błędy, potwierdzają je i dopiero potem omawiamy, co należało zrobić inaczej w kodzie albo w konfiguracji.

Zakres obejmuje klasyczne klasy podatności aplikacji webowych — wstrzyknięcia, XSS, CSRF, błędy zarządzania sesją, path traversal, problemy z uploadem plików — oraz obszary, które w ostatnich latach stały się głównym źródłem incydentów: bezpieczeństwo API, kontrola dostępu i IDOR, SSRF, tokeny JWT. Do tego, omawiamy takie tematy, jak deserializacja danych wejściowych, konfiguracja nagłówków i polityki CSP.

Każdy blok ma tę samą strukturę: krótkie wprowadzenie, demonstracja ataku, samodzielne ćwiczenie uczestników, omówienie zabezpieczenia. Nie omawiamy ataku bez pokazania obrony. Szkolenie zamyka samodzielny test bezpieczeństwa aplikacji, w którym trzeba wykryć kilka niezależnych podatności, ocenić ich ryzyko i opisać je tak, żeby zespół rozwojowy wiedział, co poprawić.

Szkolenie różni się od kursów pentesterskich tym, że punktem odniesienia jest praca programisty i testera, a nie zawód pentestera. Celem nie jest wykonanie efektownego ataku, tylko umiejętność znalezienia błędu we własnej aplikacji, potwierdzenia go i naprawienia.

Po szkoleniu uczestnik potrafi:

- metodycznie zmapować powierzchnię ataku aplikacji i jej API,
- wykryć i potwierdzić najczęstsze klasy podatności, przygotowując czytelny proof of concept,
- wskazać konkretną poprawkę w kodzie lub konfiguracji dla każdej z nich,
- czytać ze zrozumieniem raport z testów penetracyjnych i ocenić pilność znalezisk.

Czas trwania

2 dni

Program

1. Powierzchnia ataku i metodyka testu
   - Budowa nowoczesnej aplikacji webowej i miejsca powstawania podatności
   - Zagrożenia po stronie serwera, przeglądarki, integracji i konfiguracji środowiska
   - OWASP Top 10, ASVS i Testing Guide — zastosowanie każdego z dokumentów
   - Raport z testów penetracyjnych: struktura, klasyfikacja znalezisk, sposób czytania
   - Klasy narzędzi w pracy testera: proxy przechwytujące, klienty HTTP, narzędzia deweloperskie przeglądarki
2. Rozpoznanie aplikacji i praca z ruchem HTTP
   - Mapowanie aplikacji i wyszukiwanie zasobów nieujętych w nawigacji

- Środowiska deweloperskie i testowe wystawione do internetu
- Rozpoznanie wersji komponentów, informacje wyciekające przez komunikaty błędów
- Wyszukiwarki i publiczne bazy zasobów jako źródło informacji o infrastrukturze
- Przechwytywanie i modyfikowanie żądań: parametry, nagłówki, pola ukryte
- Walidacja po stronie klienta i dlaczego nie jest zabezpieczeniem
- Techniki brute force i enumeracji zasobów

3. Wstrzyknięcia po stronie serwera
   - SQL injection klasyczne i ślepe: wykrywanie, potwierdzenie, pobranie danych
   - Techniki omijania filtrów danych wejściowych
   - Ochrona: zapytania parametryzowane, warstwa ORM, uprawnienia konta bazodanowego
   - Wstrzykiwanie komend systemowych i kodu do aplikacji
   - Path traversal i dostęp do plików spoza katalogu aplikacji
   - Bezpieczny upload plików i błędy walidacji opartej o rozszerzenie
4. Przetwarzanie danych strukturalnych i wyczerpywanie zasobów
   - XXE — nieautoryzowany dostęp do plików przez przetwarzanie XML
   - Niebezpieczna deserializacja danych wejściowych
   - ReDoS oraz spreparowane archiwa i dokumenty jako wektor odmowy usługi
   - Ochrona przed atakami wolumetrycznymi i aplikacyjnymi na poziomie aplikacji i infrastruktury
5. Ataki po stronie przeglądarki
   - XSS odbity, trwały i oparty o DOM
   - Omijanie filtrów oraz kodowania danych wyjściowych
   - Kradzież sesji i danych użytkownika przez XSS
   - CSRF: mechanizm ataku, warunki powodzenia i skuteczne zabezpieczenia
   - Clickjacking i ochrona przed osadzaniem aplikacji w ramkach
   - Same Origin Policy i CORS — konsekwencje poluzowania polityki
   - Content Security Policy: zakres ochrony i ograniczenia
   - Ochrona: kodowanie kontekstowe, tokeny, atrybuty ciasteczek, nagłówki bezpieczeństwa
6. Sesje, uwierzytelnianie i kontrola dostępu
   - Zarządzanie sesją: generowanie, rotacja, unieważnianie, czas życia
   - Ciasteczka i ich atrybuty bezpieczeństwa
   - Tokeny JWT — typowe błędy implementacji i weryfikacji
   - Ścieżka logowania: enumeracja kont, brute force, ograniczanie liczby prób
   - Reset hasła jako najsłabsze ogniwo procesu uwierzytelniania
   - Uwierzytelnianie wieloskładnikowe i sposoby jego obchodzenia
   - Błędy kontroli dostępu: IDOR, eskalacja pozioma i pionowa uprawnień
7. Bezpieczeństwo API
   - Specyfikacja API jako mapa powierzchni ataku
   - Autoryzacja na poziomie zasobu i pojedynczej operacji
   - Nadmiarowe przypisanie parametrów i nadmiarowe dane w odpowiedziach
   - Ograniczanie liczby żądań i ochrona przed nadużyciem interfejsu
   - SSRF: wykorzystanie aplikacji do sięgania po zasoby wewnętrzne
   - Testowanie usług REST i SOAP, generowanie żądań na podstawie specyfikacji
8. Konfiguracja, komponenty i ochrona brzegowa
   - Nagłówki bezpieczeństwa i konfiguracja serwera aplikacyjnego
   - Konfiguracja TLS i błędy w zabezpieczeniu transmisji
   - Przechowywanie haseł i danych wrażliwych w aplikacji

- — Sekrety w repozytorium, plikach konfiguracyjnych i zmiennych środowiskowych
- — Podatności w zależnościach i komponentach zewnętrznych oraz narzędzia do ich wykrywania
- — WAF, IDS i IPS: realny zakres ochrony, ograniczenia i techniki omijania
- — Skanery podatności: co wykrywają, czego nie wykryją, jak weryfikować wyniki

9. Test całościowy i raportowanie
   - — Samodzielny test bezpieczeństwa aplikacji podsumowujący zakres szkolenia
   - — Wykrycie i potwierdzenie kilku niezależnych klas podatności
   - — Ocena ryzyka i priorytetyzacja znalezisk
   - — Opis podatności i rekomendacji w formie użytecznej dla zespołu rozwojowego

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl

Przeznaczenie i wymagania

Szkolenie przeznaczone przede wszystkim dla:

- — Programistów, webowych, backendowych i full-stack, którzy tworzą lub utrzymują aplikacje webowe i/lub API,
- — Testerów i inżynierów QA rozszerzających plany testów o testy bezpieczeństwa,
- — Administratorów i inżynierów DevOps odpowiedzialnych za aplikacje wystawione do internetu,
- — Architektów i liderów technicznych, którzy muszą oceniać ryzyko i priorytetyzować poprawki,
- — Osób rozpoczynających pracę w obszarze testów bezpieczeństwa aplikacji.

Oczekiwania wobec uczestników:

- — Znajomość protokołu HTTP, umiejętność czytania kodu HTML i JavaScript, podstawy SQL.
- — Umiejętność programowania w dowolnym języku.

Nie wymagamy doświadczenia w bezpieczeństwie ani w testach penetracyjnych — szkolenie jest wejściem w ten obszar.

Szkolenie będzie za proste dla osób zawodowo wykonujących testy penetracyjne aplikacji webowych. Może być trudne dla osób bez żadnego praktycznego kontaktu z aplikacjami webowymi i kojarzeniem protokołu HTTP.

Certyfikaty

Uczestnicy szkolenia otrzymują imienne certyfikaty sygnowane przez ALX.

Lokalizacje

- — Warszawa – ul. Jasna 14/16A
- — Zdalnie – zajęcia realizowane poprzez platformę Zoom
- — Kraków – ul. św. Filipa 23
- — Warsaw (English) – Jasna 14/16A
- — Online (English) – your home, office or wherever you want
- — na życzenie dowolne miejsce w Polsce, lub UE (zajęcia prowadzone w języku angielskim)

Cena szkolenia

2090 PLN netto (VAT 23%)

W cenę szkoleń organizowanych w naszej siedzibie wliczone są:

— autorskie materiały szkoleniowe,
— indywidualne stanowisko komputerowe do pracy podczas zajęć,
— certyfikaty ukończenia szkolenia,
— drobny poczęstunek oraz ciepłe i zimne napoje,
— możliwość jednorazowego kontaktu z instruktorem (instruktorami) po szkoleniu i zadawania pytań dotyczących materiału szkolenia.

Cena szkolenia nie zawiera obiadów. Można je dokupić w cenie 35 zł netto za obiad.

Zapytaj o szczegóły
tel. 22 63 64 164
akademia@alx.pl