Bezpieczeństwo aplikacji internetowych

Laboratorium 2

CSRF

Mateusz Pawełkiewicz

1. **Projektowanie i Tworzenie Aplikacji:**
    a. **Tworzenie Aplikacji:** Student ma za zadanie zaprojektować i zaimplementować prostą aplikację webową umożliwiającą operacje CRUD na danych użytkownika, takie jak dodawanie, wyświetlanie, modyfikowanie i usuwanie informacji. Przykładem może być aplikacja do zarządzania listą zadań.
    b. **Technologie:** Można użyć dowolnych technologii webowych, takich jak HTML, CSS, JavaScript dla frontendu oraz Python z Flaskiem lub Node.js z Express.js dla backendu.
2. **Symulacja Ataku CSRF:**
    a. **Analiza Podatności:** Zrozumienie, w jaki sposób aplikacja może być podatna na ataki CSRF.
    b. **Projektowanie Ataku:** Tworzenie złośliwej strony lub skryptu, który będzie wykonywać nieautoryzowane operacje (np. zmiana danych użytkownika) poprzez wykorzystanie uwierzytelnienia ofiary.
    c. **Przeprowadzenie Ataku:** Demonstracja działania ataku, pokazująca, jak łatwo może zostać wykonane żądanie bez wiedzy użytkownika.
3. **Implementacja Zabezpieczeń:**
    a. **Tokeny CSRF:** Wprowadzenie mechanizmu tokenów CSRF, gdzie każda forma lub żądanie AJAX musi zawierać token wygenerowany po stronie serwera, który zostanie zweryfikowany przy każdym żądaniu.
    b. **Weryfikacja Refererów:** Implementacja sprawdzenia nagłówków **Referer** lub **Origin**, aby zapewnić, że żądania pochodzą z zaufanego źródła.
    c. **Testy Obrony:** Testowanie zabezpieczeń aplikacji, sprawdzając, czy zaimplementowane mechanizmy skutecznie blokują złośliwe działania.