Kodowanie i bezpieczeństwo

Laboratorium - lista nr 5, 28 XI

Zadanie 1 (2 pkt) Zainstaluj skaner *skpifish* i wykonaj pełen skan (ze słownikiem complete.wl) swojej strony bankowej (z listy 4). Zachowaj wyniki skanu i zapoznaj się z nimi. (Pamiętaj, aby umożliwić skipfish'owi zalogowanie się do serwisu). Jakie ataki na Twój serwis były możliwe, jakie mogłyby być ich skutki, co było ich przyczyną, co należałoby zmienić, aby ich uniknąć.

Zadanie 2 (8 pkt) Zmodyfikuj (jeżeli to konieczne) działanie serwisu z listy 4: zarówno dane dotyczące przelewów jak i loginy/hasła mają być przechowywane w bazie. Dodaj logowanie dla administratora, który ma możliwość zatwierdzania przelewów – taki przelew klientowi będzie się pokazywał jako zrealizowany.

Przeprowadź ataki SQL Injection, XSS i XSRF na swój serwis. W szczególności dla SQL injection: przygotuj następujące zapytania:

1. umożliwiające obejrzenie danych, do których nie powinniśmy mieć dostępu (np. dane dotyczące przelewów zleconych przez innego klienta);
2. zatwierdzające zlecony przelew (pomimo tego, że nie jesteśmy administratorami serwisu);
3. pokazujące pliki w systemie operacyjnym (jeżeli wykorzystana baza danych ma takie funkcje/uprawnienia).

Dla XSS, XSRF przygotuj kod, który spowoduje wykonanie operacji zatwierdzenia przelewów przez administratora.

Celem zadania jest uświadomienia sobie zagrożeń związanych z tymi typami ataków. Jeżeli Twoja strona została przygotowana we frameworku, który automatycznie zabezpiecza przed atakami typu XSS, XSRF, ... to na potrzeby zadania wyłącz te zabezpieczenia (w większości przypadków można to bezproblemowo zrobić w plikach konfiguracyjnych).