Kodowanie i bezpieczeństwo

Laboratorium - lista nr 6, 11 XII

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) Jeżeli na liście 4 Twym zadaniem był "Helios", to poproś kogoś o udostępnienie zadania "bankowego". 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.