Bezpieczeństwo komputerowe

semestr letni 2023/24

Lista nr 6

(laboratorium)

Terminy oddania: przed 15.06.2024

Zadanie 1. OpenSSL, weryfikacja certyfikatu (5 pkt). Jeżeli jeszcze nie jest zainstalowany, to pobierz i zainstaluj OpenSSL dla swojego systemu operacyjnego (`https://www.openssl.org`). Następnie:

- w przeglądarce internetowej odwiedź dowolną stronę wspierającą HTTPS (na przykład `https://pwr.edu.pl`). Pobierz certyfikat SSL/TLS tej strony. W jakiej formie jest ten certyfikat? Upewnij się, że zapisałeś/aś certyfikaty pośrednie i główny (root CA), które są wymagane do pełnej weryfikacji certyfikatu
- używając polecenia `openssl x509` z różnymi opcjami, dowiedz się, kto podpisał certyfikat strony, jaki jest algorytm podpisu, jaka jest data ważności certyfikatu, dla kogo jest certyfikat, jakie domeny obejmuje (zobacz rozszerzenie X509v3 Subject Alternative Name) jakie rozszerzenia X509 są obecne, jakie jest URI do list CRL i URI do serwisu OCSP?
- używając polecenia `openssl verify` sprawdź, czy certyfikat jest prawidłowy i czy istnieje zaufana ścieżka do jednego z głównych certyfikatów zaufania na Twoim komputerze (podpowiedź: może być konieczne podanie certyfikatów pośrednich)
- używając polecenia `openssl ocsp` i znalezionego wcześniej adresu dla OCSP sprawdź status OCSP certyfikatu strony

Zadanie 2. Generowanie certyfikatów (5 pkt). Wykorzystaj OpenSSL do wygenerowania:

- pary klucz prywatny - klucz publiczny,
- żądania certyfikatu (CSR, ang. *Certificate Signing Request*) dla swojej domeny.

Następnie na podstawie posiadanego CSR wygeneruj certyfikat, wykorzystując darmowe CA Let's Encrypt (`https://letsencrypt.org/`). W tym celu wykorzystaj Certbot (`https://certbot.eff.org/`). Jest to rekomendowany podstawowy klient, który automatyzuje proces uzyskiwania i odnawiania certyfikatów Let's Encrypt. Sprawdź,

w jaki sposób należy skonfigurować serwer webowy, aby używał nowego certyfikatu i klucza prywatnego.

Zadanie 3. WebGoat (10 pkt). Zapoznaj się z celowo niezabezpieczoną aplikacją internetową WebGoat (https://github.com/WebGoat/WebGoat/). Uruchom ją i wykonaj lekcje dotyczące XSS (Cross-Site Scripting). Odpowiedz na pytania prowadzącego odnośnie wykonanych zadań.