|  |
| --- |
| Politechnika Wrocławska, Informatyka Stosowana |
| Web security cz.2 |
| Cyberbezpieczeństwo, Laboratorium nr.14 - raport |

|  |
| --- |
| Autor: Aleksander Stepaniuk  Nr. Indeksu: 272644 |

**4. Pytania**

**Pytanie 1;**

Różnice pomiędzy atakami XSS (DOM, Persistent, Reflected):

* DOM-based XSS działa w przeglądarce poprzez manipulację istniejącym skryptem JS w strukturze DOM
* Persistent XSS zapisuje złośliwy kod na serwerze, np. w bazie danych i atakuje wszystkich użytkowników odczytujących dane
* Reflected XSS wymaga interakcji użytkownika, gdzie złośliwy kod jest odbijany od serwera i wykonuje się w przeglądarce

Kiedy użytkownik jest narażony:

* DOM: podczas korzystania z dynamicznych stron z nieprawidłowym przetwarzaniem JSa
* Persistent: gdy wchodzi na strony z danymi zapisanymi przez atakującego
* Reflected: klikając w spreparowane linki

**Pytanie 2;**

Atakujący może wykradać dane, modyfikować je, usuwać, tworzyć nowe konta, omijać logowanie, a także uzyskać kontrolę nad serwerem bazy danych.

**Pytanie 3;**

Złośliwy kod może być ukryty w plikach HTML, JS, XML, ale także w obrazach (SVG, PDF), a nawet dokumentach (np. DOCX). Deserializacja plików binarnych niesie za sobą ryzyko, gdy dane wejściowe nie są weryfikowane, co umożliwia wykonanie złośliwego kodu.

**5. Zadania**

**Zadanie 0;**

Adresy IP maszyn:

**Kali linux**: 172.16.96.8/24

**Adres sieci:** 172.16.96.0/24

**Zadanie 1;**

Uruchamiam juice-shop

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

**Zadania 2-6;**

Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie**

Uruchamiam w prostszy sposób: (OR TRUE, a dalszą część komentujemy za pomocą „--”) – hasło może być więc dowolne

**Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie**

**Obraz zawierający zrzut ekranu, tekst, Oprogramowanie multimedialne, oprogramowanie

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**

**Zadanie 4;**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

Po errorze widać że juice shop korzysta z SQLite.

Próbowałem z tą wiedzą zdobyć więdzej danych o tabelach, ale niestety bezskutecznie (syntax error więc jakiś mały błąd musiałem robić)

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Strona internetowa

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Opis wygenerowany automatycznie**

**Zadania 7-10;**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, elektronika, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Strona internetowa

Opis wygenerowany automatycznie**

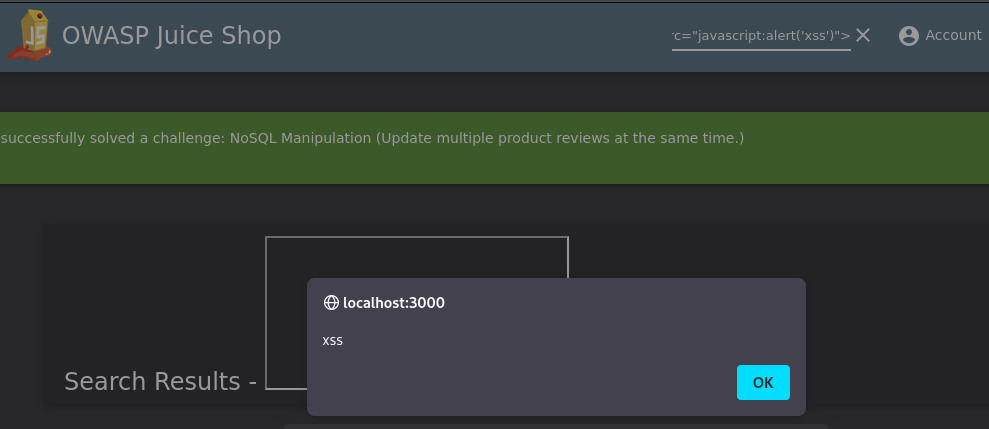
**Obraz zawierający tekst, zrzut ekranu, Czcionka, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, System operacyjny, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

**Zadania 11-14;**

****

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, Oprogramowanie multimedialne, oprogramowanie

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

**Zadania 15-22;**

**Obraz zawierający tekst, zrzut ekranu, Czcionka, oprogramowanie

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, oprogramowanie, Oprogramowanie multimedialne, zrzut ekranu

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, Czcionka, zrzut ekranu

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Czcionka

Opis wygenerowany automatycznie**

**Obraz zawierający Oprogramowanie multimedialne, Oprogramowanie graficzne, oprogramowanie, zrzut ekranu

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**

**Zadania CSRF;**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie**

Niestety, nie zmieniło nazwy (prawdopodobnie posiadam zbyt nową przeglądarkę):**Obraz zawierający kapelusz, zrzut ekranu, tekst, kreskówka

Opis wygenerowany automatycznie**