|  |
| --- |
| Politechnika Wrocławska, Informatyka Stosowana |
| Web security cz.1 |
| Cyberbezpieczeństwo, Laboratorium nr.13 - raport |

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

**4. Pytania**

**Pytanie 1;**

Nagłówek (http) X-Content-Type-Options – kiedy jest ustawiony na wartość nosniff, uniemożliwia przeglądarce interpretowanie plików o innym typie MIME niż zadeklarowany w odpowiedzi serwera. Chroni przed atakami, w których złośliwy plik (np. skrypt JavaScript) zostaje uruchomiony jako inny typ pliku.

Nagłówek X-Frame-Options kontroluje czy strona może być osadzona w ramkach (tzw. iframe). Ustawienia, takie jak DENY (blokowanie wszystkich ramek) lub SAMEORIGIN (dozwolone tylko z tej samej domeny) chronią przed atakami typu „clickjacking”.

Ataki SQL Injection: Pozwalają na wstrzyknięcie złośliwego nieporządanego kodu SQL poprzez niezabezpieczone pola wejściowe. Osoba atakująca może wykonać takie akcje jak:

* Kradzież danych (np. wyciąganie haseł czy adresów e-mail).
* Modyfikowanie danych (np. zmiana wartości konta).
* Usuwanie baz danych lub całych tabel.
* Uzyskanie dostępu administracyjnego do systemu.

**Pytanie 2;**

Jest to istotne, bo zapewnia ochronę przed znaczną częścią ataków wykorzystujących luki w walidacji po stronie klienta czy serwera:

Po stronie klienta:

* Zapewnia lepszą wydajność i szybsze reagowanie dla użytkownika (np. walidacja e-maila przed wysłaniem formularza).

Po stronie serwera:

* Chroni przed manipulacjami, ponieważ walidacja po stronie klienta może być pominięta przez złośliwego użytkownika. Niezabezpieczony serwer jest narażony na ataki, takie jak SQL Injection, XSS lub wysyłanie nieprawidłowych danych.

**Pytanie 3;**

* Uwierzytelnianie: upewnić się, że użytkownik jest zalogowany (np. JWT, sesje).
* Autoryzacja: weryfikacja ról i uprawnień użytkownika przed udzieleniem dostępu do zasobu (np. RBAC, czyli „Role-Based Access Control”).
* Mechanizmy na poziomie serwera: Korzystanie z reguł zapory sieciowej, kontroli dostępu (ACL) i odpowiednio skonfigurowanych serwerów aplikacji.
* Zasada najmniejszych uprawnień: Użytkownicy powinni mieć dostęp tylko do zasobów niezbędnych dla ich roli.

**5. Zadania**

**Zadanie 0;**

Adresy IP maszyn:

**Kali linux**: 172.16.96.8/24

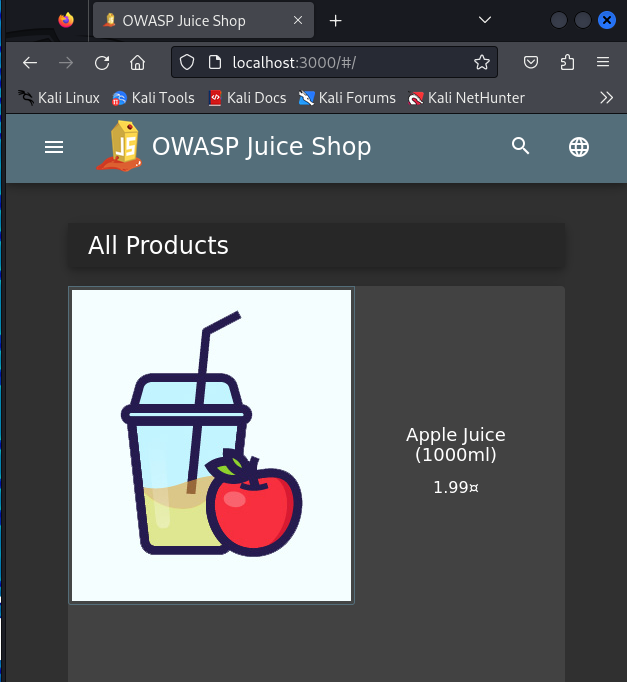
**Adres sieci:** 172.16.96.0/24

**Zadania 1-3;**

Uruchamiam juice-shop

Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Oprogramowanie multimedialne

Opis wygenerowany automatycznie



**Zadanie 4;**

Skanowanie pokazało flagi: (łącznie 13):

- 2 czerwone

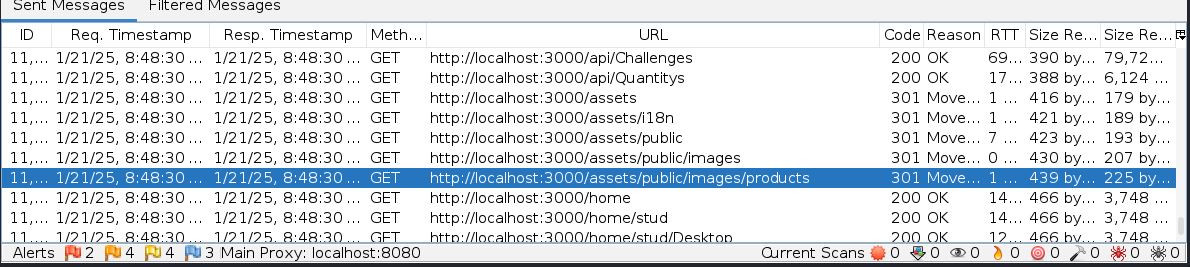
- 4 bursztynowe

- 4 żółte

- 3 niebieskie

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

Opis wygenerowany automatycznie**

Skanowanie ujawniło między innymi katalog /assets/public/image/products/ który można wyświetlić w przeglądarce:  


Obraz zawierający tekst, Ludzka twarz, zrzut ekranu, uśmiech

Opis wygenerowany automatycznie

Skanowanie nie wykryło żadnego ryzyka związanego bezpośrednio z ciasteczkami (cookies), ale w przypadku alertu „Session ID in URL Rewrite” można użyć między innymi ciasteczek aby taki alert naprawić. (Solution)

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

Opis wygenerowany automatycznie**

**Zadania 5-7;**

W historii zapa pojawia się request z naszej sesji firefoxa.

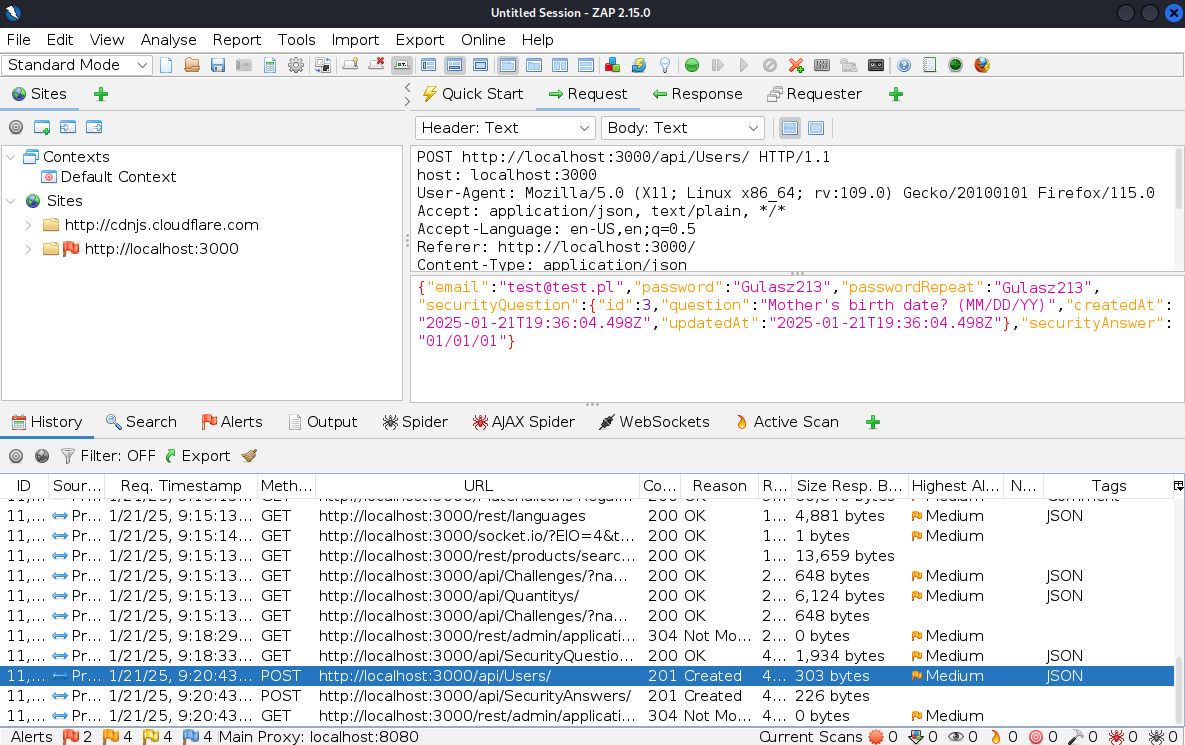
**Obraz zawierający tekst, Czcionka, zrzut ekranu, numer

Opis wygenerowany automatycznie**

**Zadania 8-11;**

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

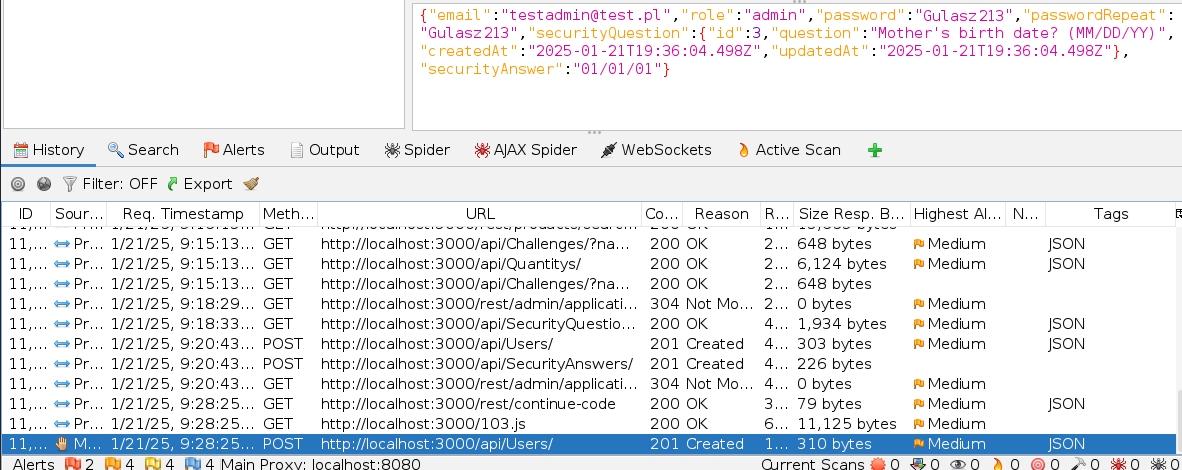
Opis wygenerowany automatycznie**

****

Rejestracja użytkownika odbywa się poprzez 2 żądania, w pierwszym są dane z formularza (gdzie hasło jest niezaszyfrowane) w drugim odpowiedz na pytanie bezpieczenstwa (co jest duplikatem).

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

Opis wygenerowany automatycznie**

****

**Zadania 12-17;**

Składamy complainta (file size = 25kb)

**Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie**

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

Opis wygenerowany automatycznie**

Teraz próbujemy złożyć complainta co waży ponad 100kb (file size = 125kb) i nie pozwala

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

Opis wygenerowany automatycznie**

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

Opis wygenerowany automatycznie**

Udało się wrzucić przez ZAPa plik powyżej 100kb.

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

Opis wygenerowany automatycznie**

Teraz próba wrzucenia pliku powyżej 200kb: (błąd)

**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, Ikona komputerowa

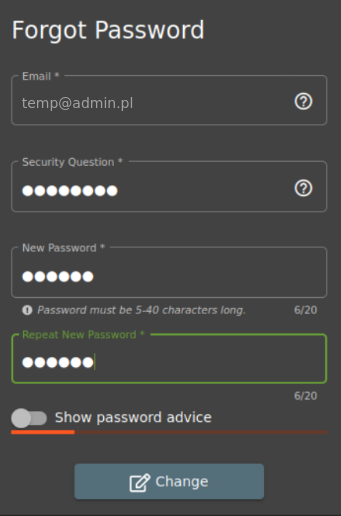
Opis wygenerowany automatycznie**

Teraz wniosek jest taki, że największy możliwy do wrzucenia plik przez interfejs webowy to 100kb, natomiast błędna walidacja danych wejściowych po stronie serwera sprawia, że limit ten wynosi tak naprawdę 200kb.

**Zadania 18-20;**

**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**

****

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

Opis wygenerowany automatycznie**

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

Opis wygenerowany automatycznie**

Przypadkowo przekroczyłem limit zapytań (bo w fuzzerze podałem liczby naturalne od 1 do 31, natomiast poprawna wartość to 01, więc nie wpisał jej i wyczerpał się limit powiadomień. Tak czy siak finalnie zgadł poprawną odpowiedź.

**Zadania 21-25;**

Id koszyka głównego: (basket id = 6);

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

Opis wygenerowany automatycznie**

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

Opis wygenerowany automatycznie**

Id nowego koszyka: (basket id = 7);

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

Opis wygenerowany automatycznie**

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

Opis wygenerowany automatycznie**

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

Opis wygenerowany automatycznie**