Sprawozdanie 5

Ciszewski Jakub 311192

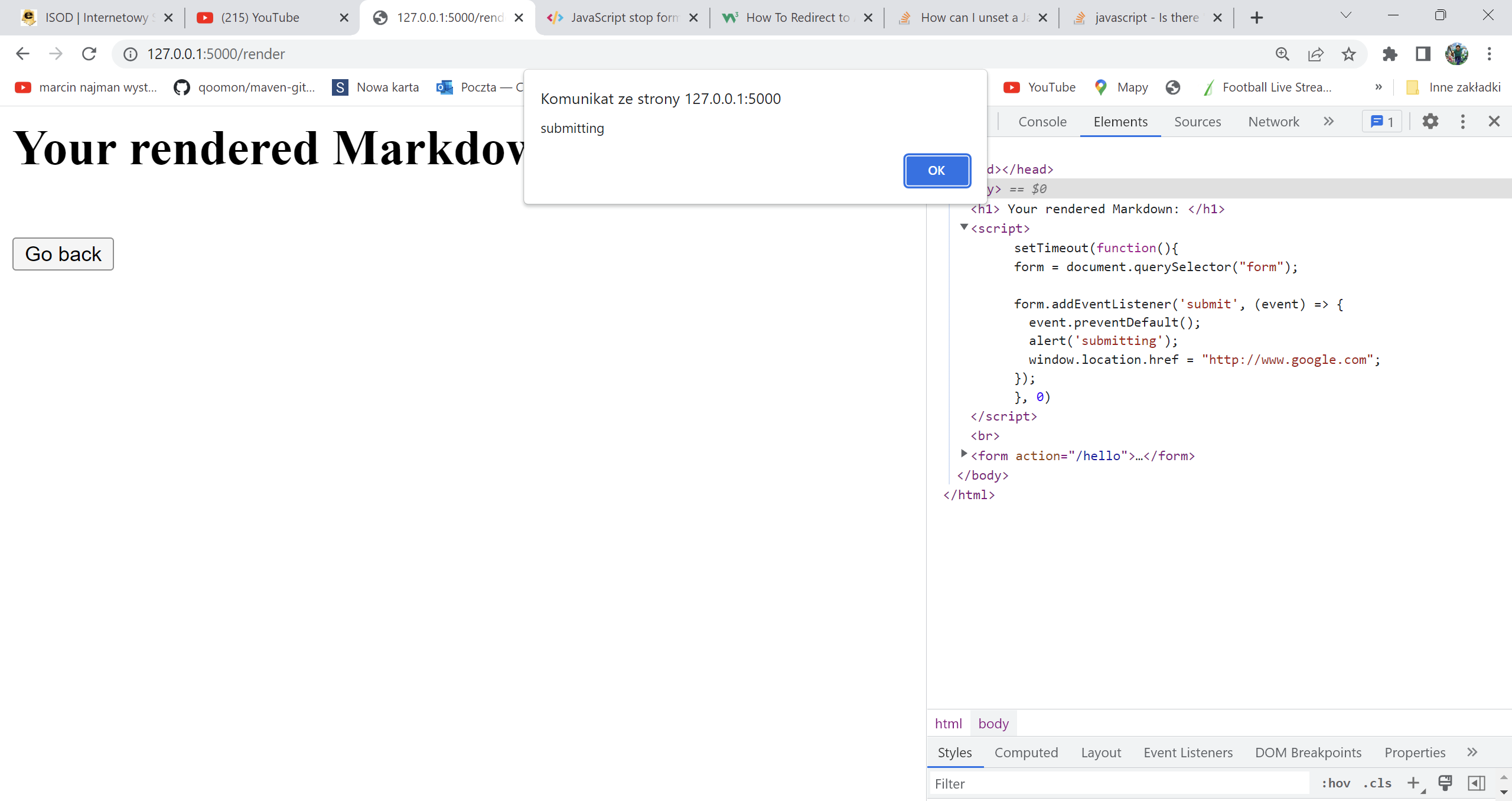
Wykonać atak XSS polegający na wstrzyknięciu do wiadomości Markdown kodu JavaScript zmieniającego adres pod który prowadzi przycisk "Go back".

Obraz zawierający tekst

Opis wygenerowany automatycznie

Obraz zawierający tekst

Opis wygenerowany automatycznie



Obraz zawierający tekst

Opis wygenerowany automatycznie  
Wykonać atak XSS polegający na wstrzyknięciu do nazwy użytkownika kodu JavaScript, który nie wpłynie na działanie aplikacji, ale w tle prześle na zewnętrzny serwer treść notatki wprowadzonej przez użytkownika na podstronie /hello (najlepiej wykorzystać webhook.site)

Obraz zawierający tekst

Opis wygenerowany automatycznie

Obraz zawierający tekst

Opis wygenerowany automatycznie

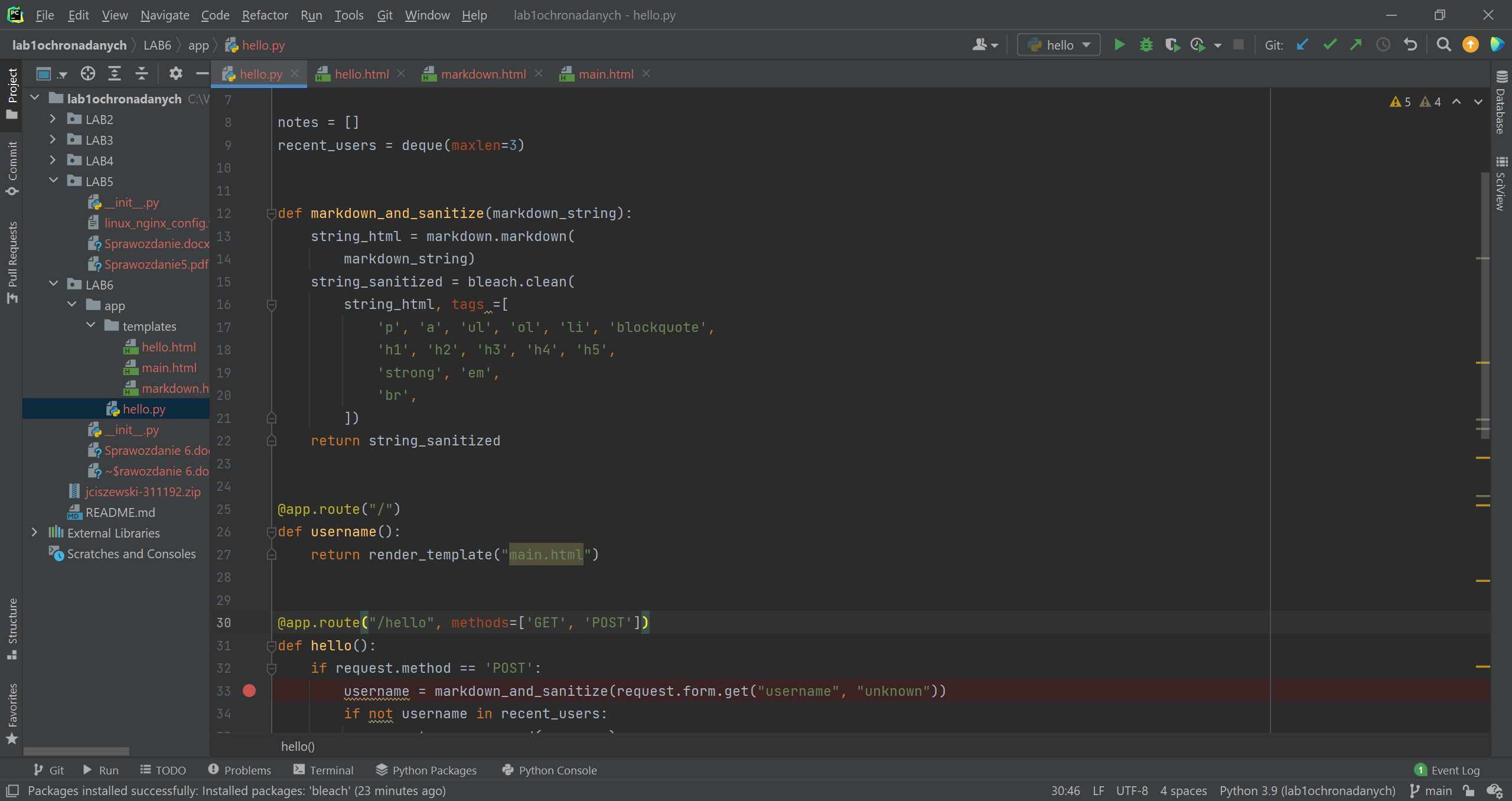
Obraz zawierający tekst

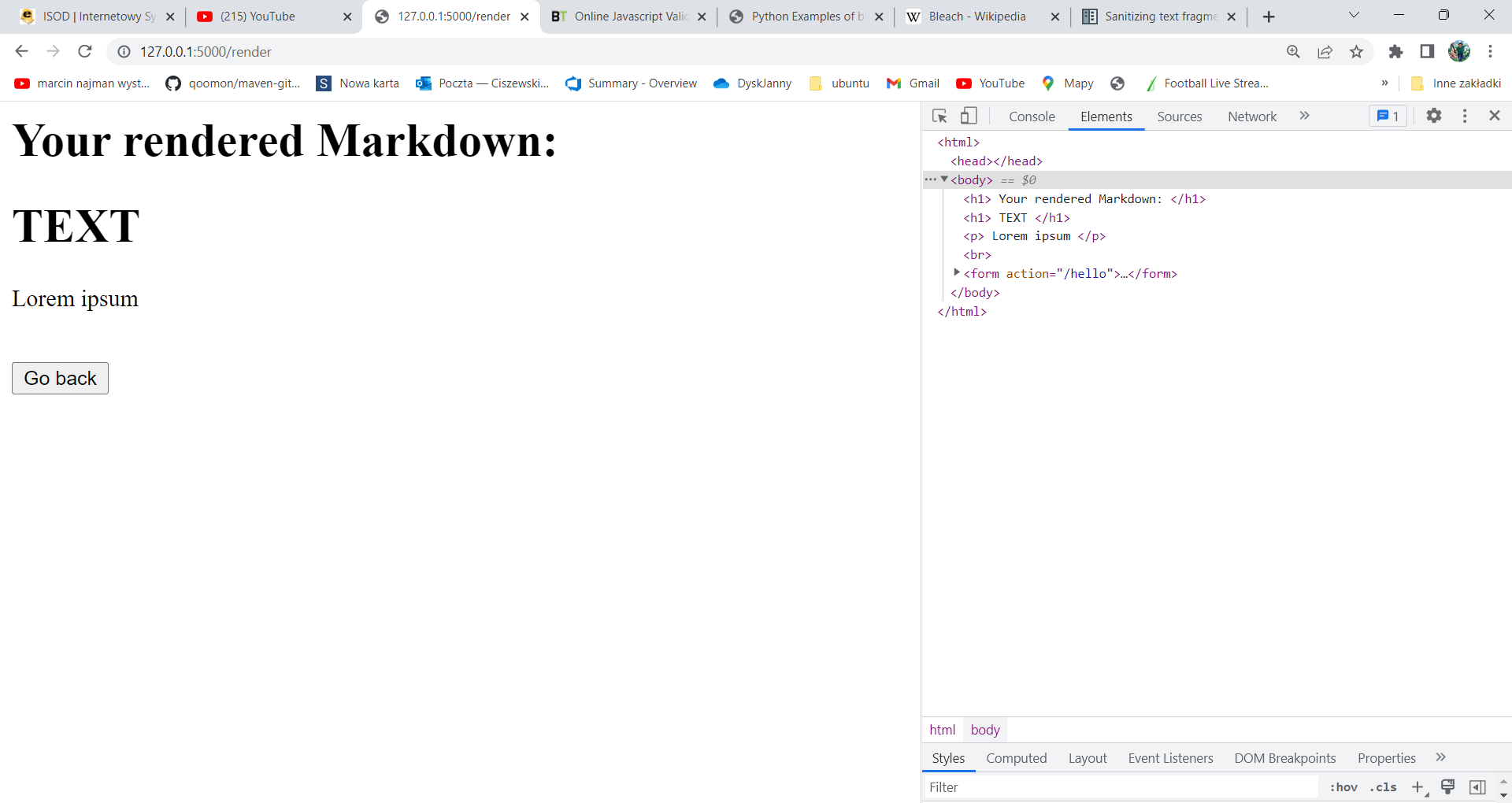
Opis wygenerowany automatycznie

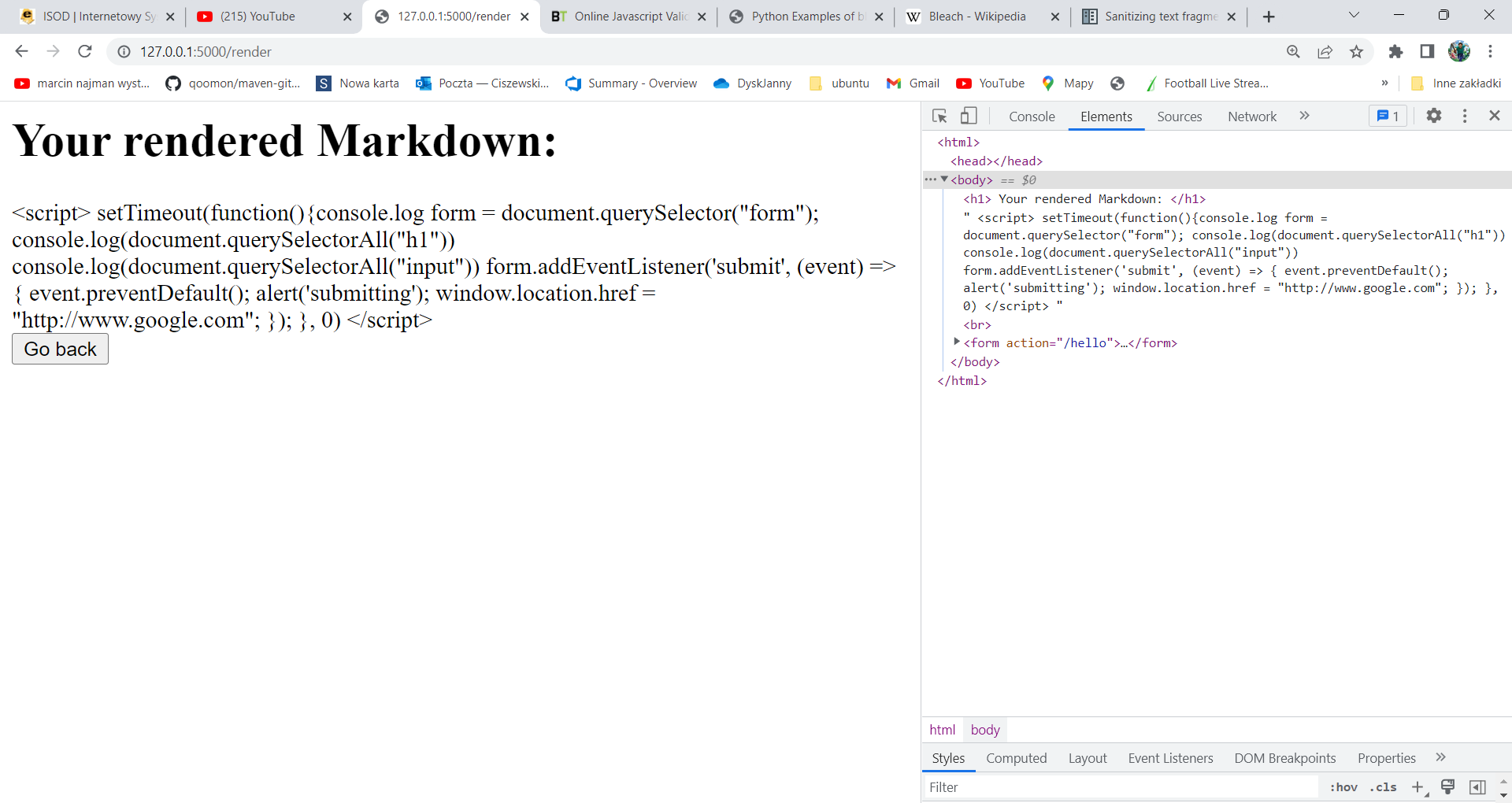
Obraz zawierający tekst, zrzut ekranu, wewnątrz

Opis wygenerowany automatycznie  
Dodać dodatkową sanityzację dla wiadomości Markdown i przy username (NIE wyłączać flagi "safe"), która zlikwiduje podatność XSS w tych punktach aplikacji. Można wykorzystać takie biblioteki jak Bleach.

Dodałem funkcję sanityzującą przy użyciu biblioteki bleach(wybrane znaczniki renderują się poprawnie inne zostają w formie tekstowej):







Tekst po spreparowaniu nie jest wysyłany do webhook.site(brak wiadomości):

