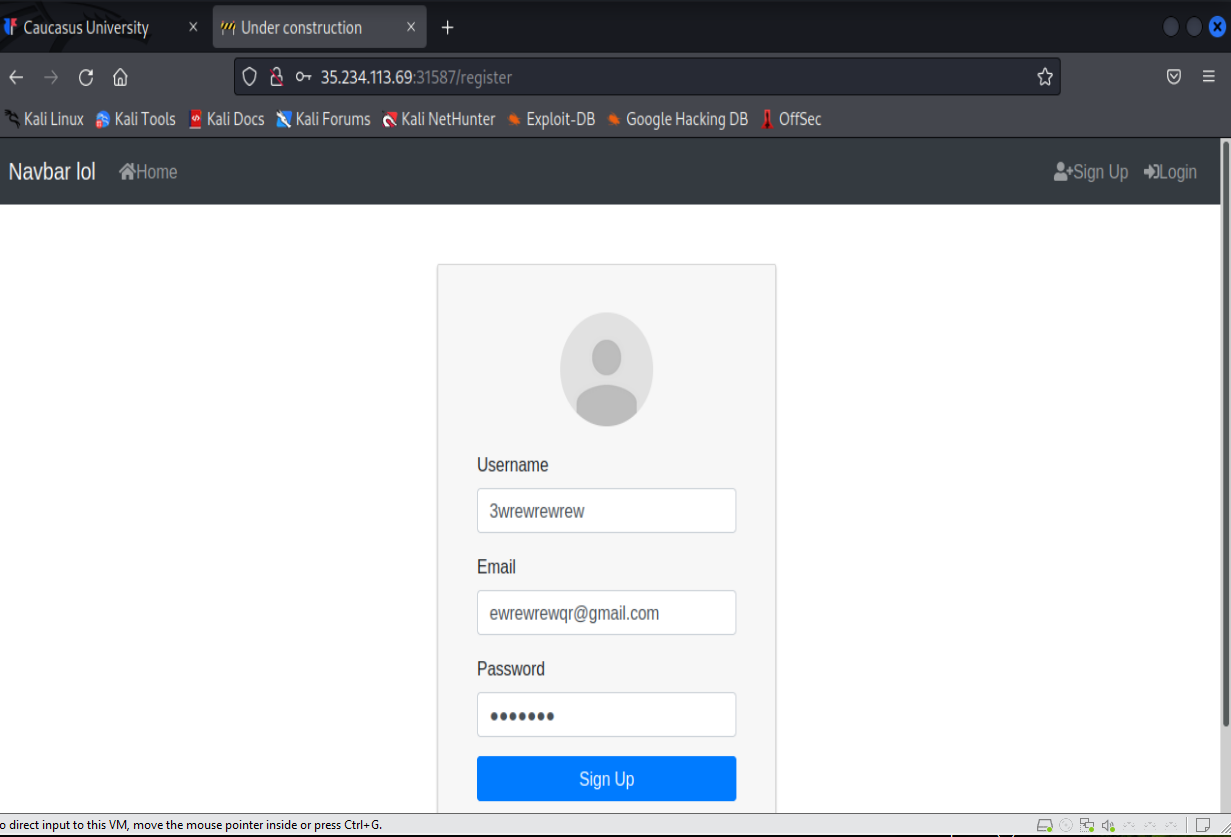
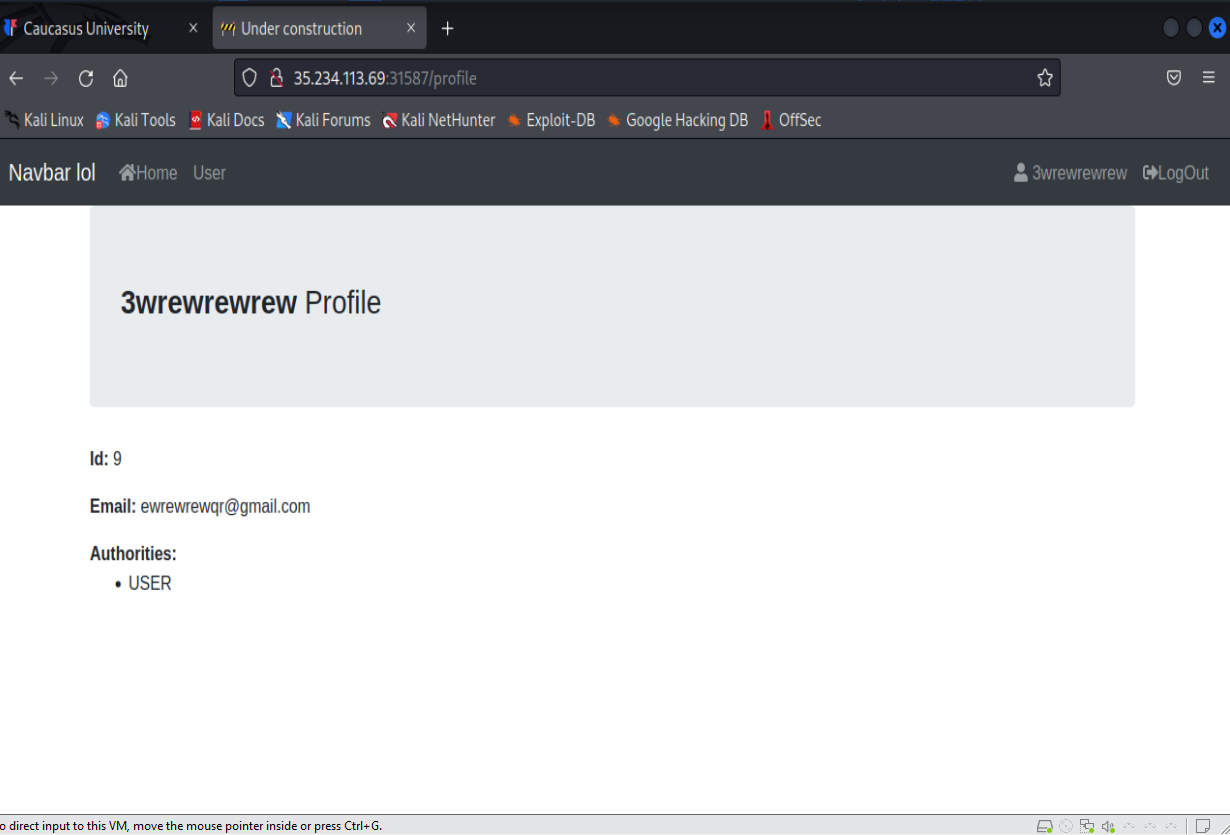
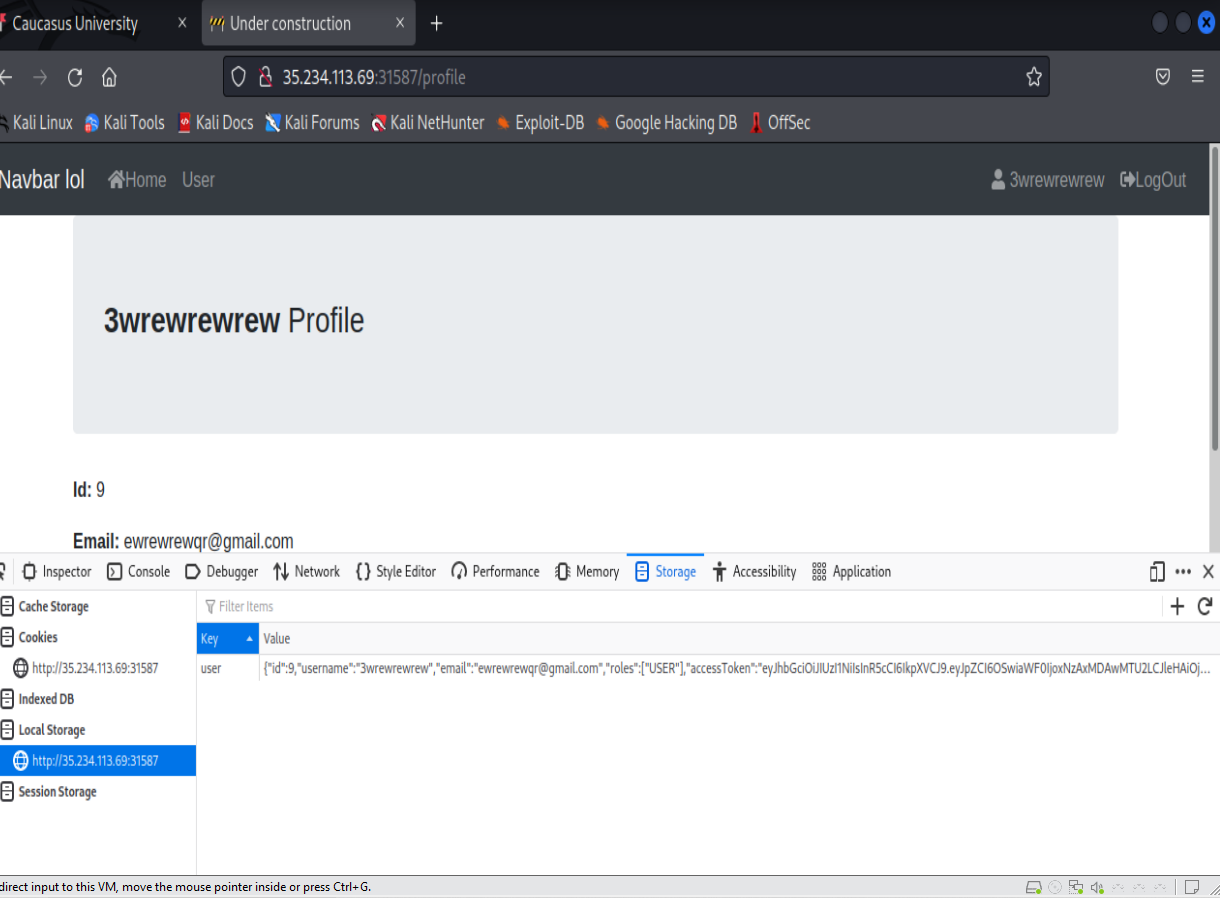
UNDER-CONSTRUCTION

მოცემულ გვერდზე დავრეგისტრირდებით,შვევალთ ჩვენ პროფილზე და შემდეგ inspect->application->localstorage-> სადაც ვნახავთ ჩვენი user-ს დეტალებს

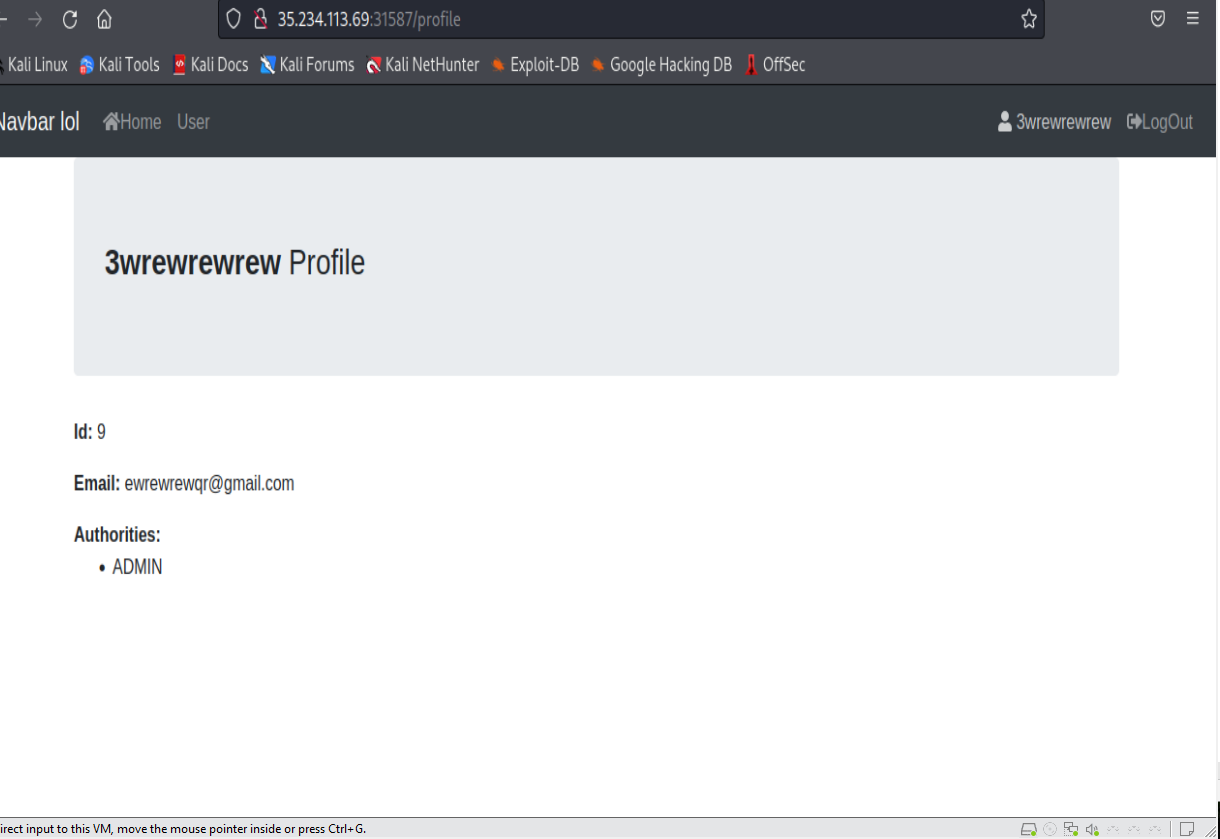




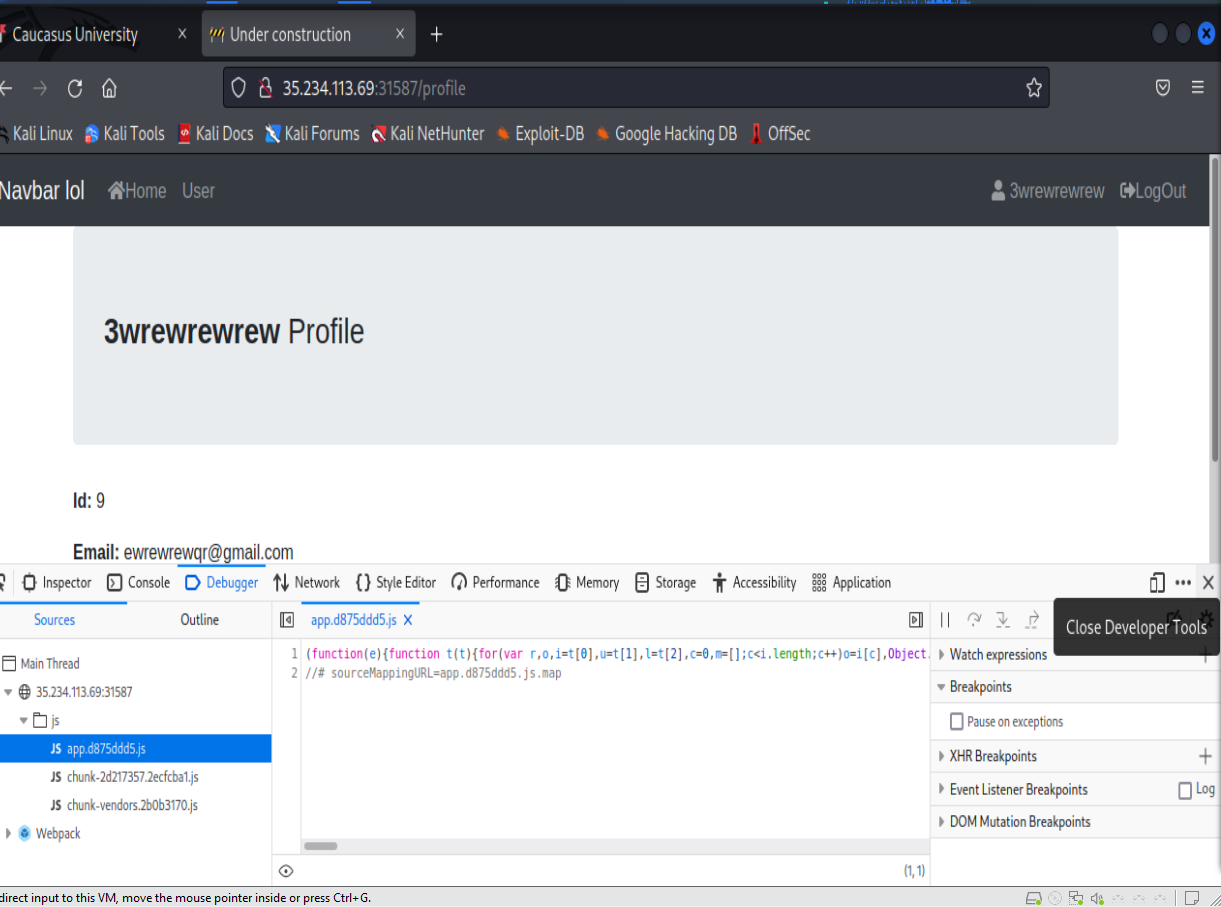


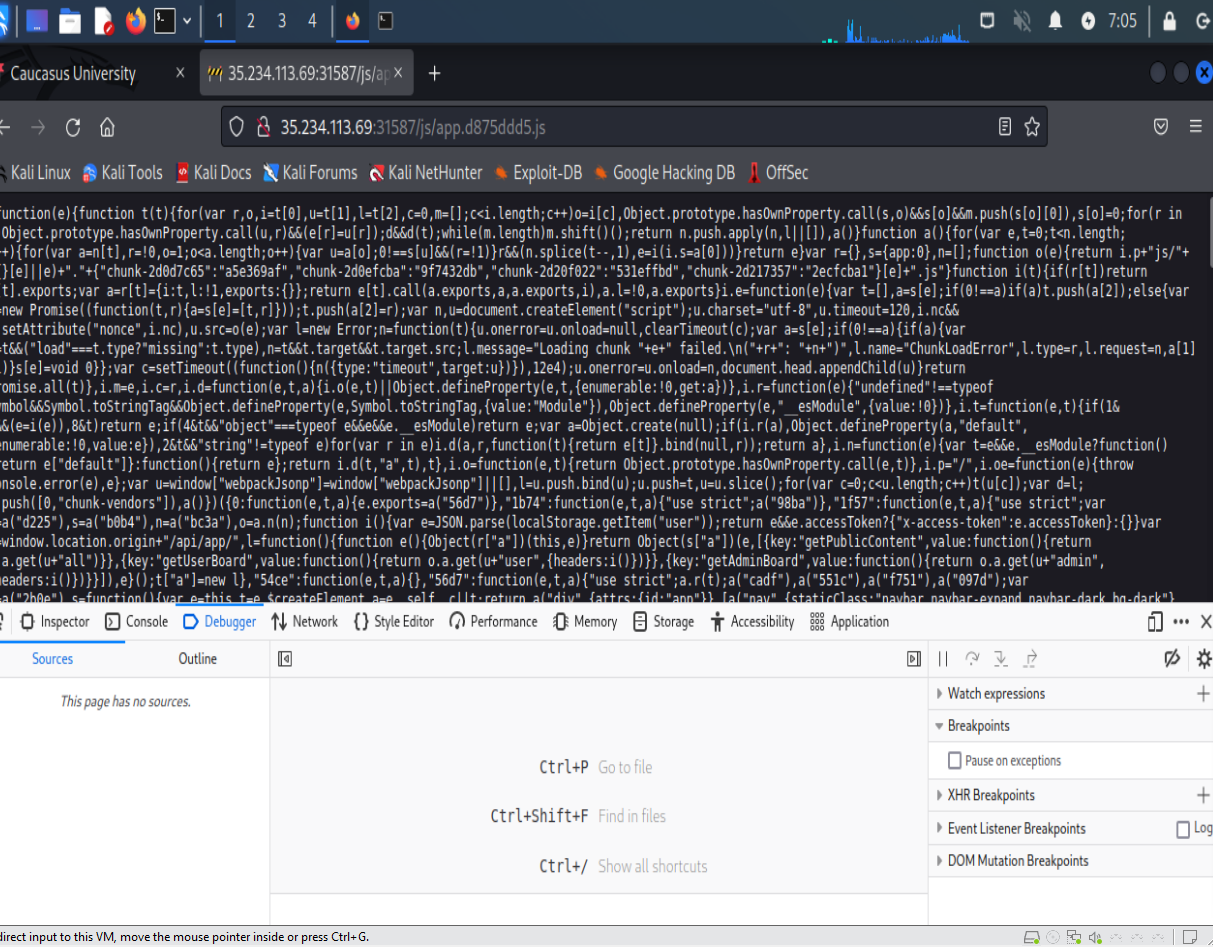
აქ ჩვენთვის არის ორი საინტერესო ველი role და accessToken.

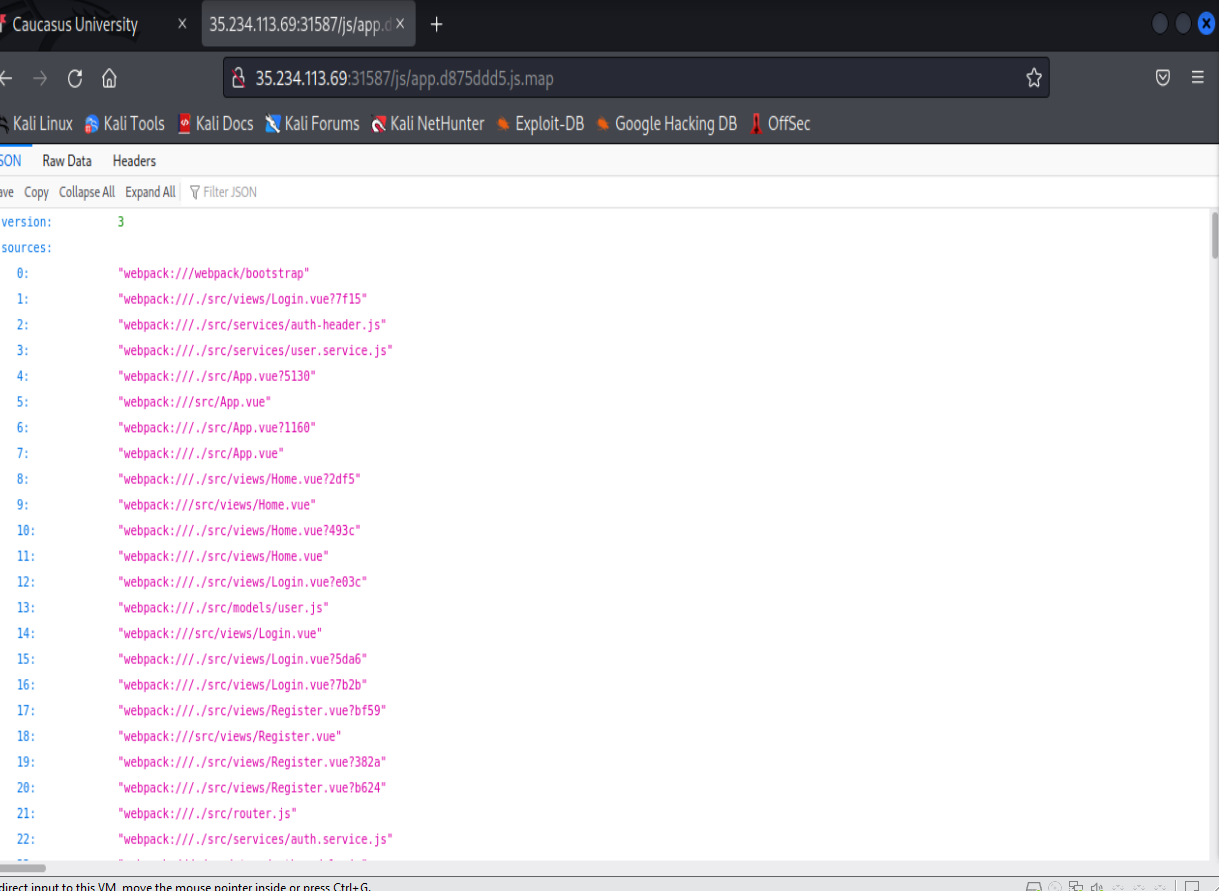
რადგან ვიცით რომ სიატზე მხოლოდ ADMIN პანელია გაკეტებელი შეგვილია ჩვენი role მასზე შევჩალოთ

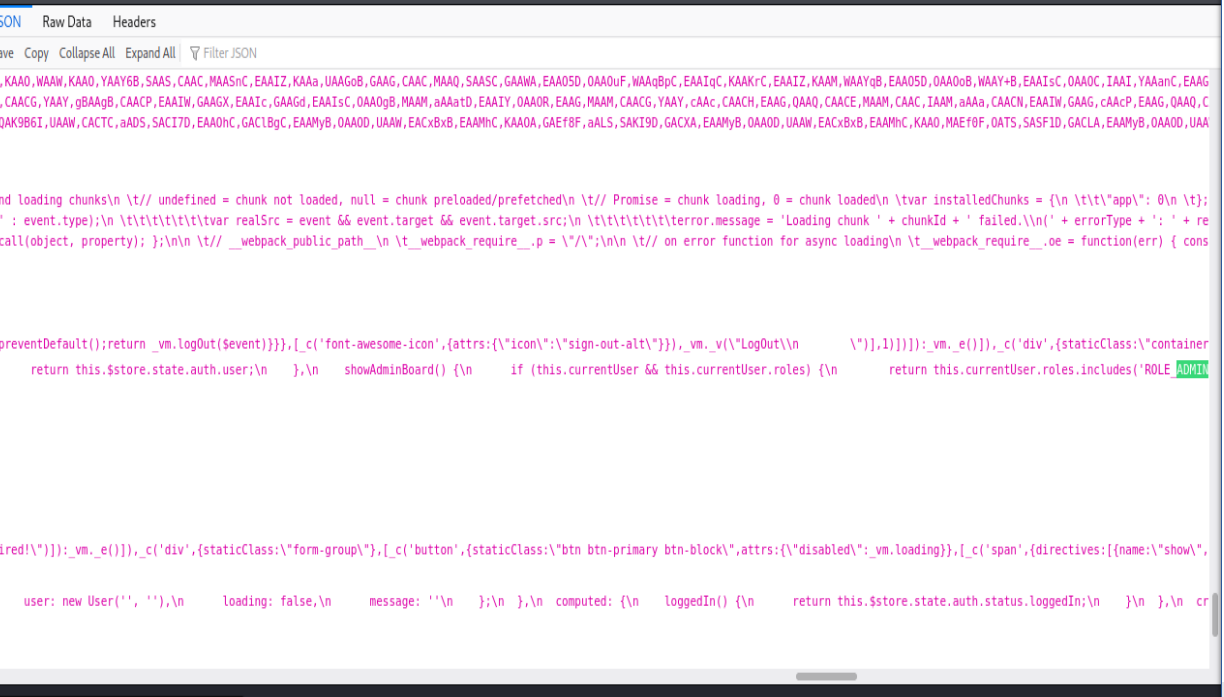


შემდეგ ვნახავთ ჯავასკირპტის კოდს app.d875ddd5.js და მას დავუმატბეთ .map-ს რათა უფრო თვალსაჩინო იყოს

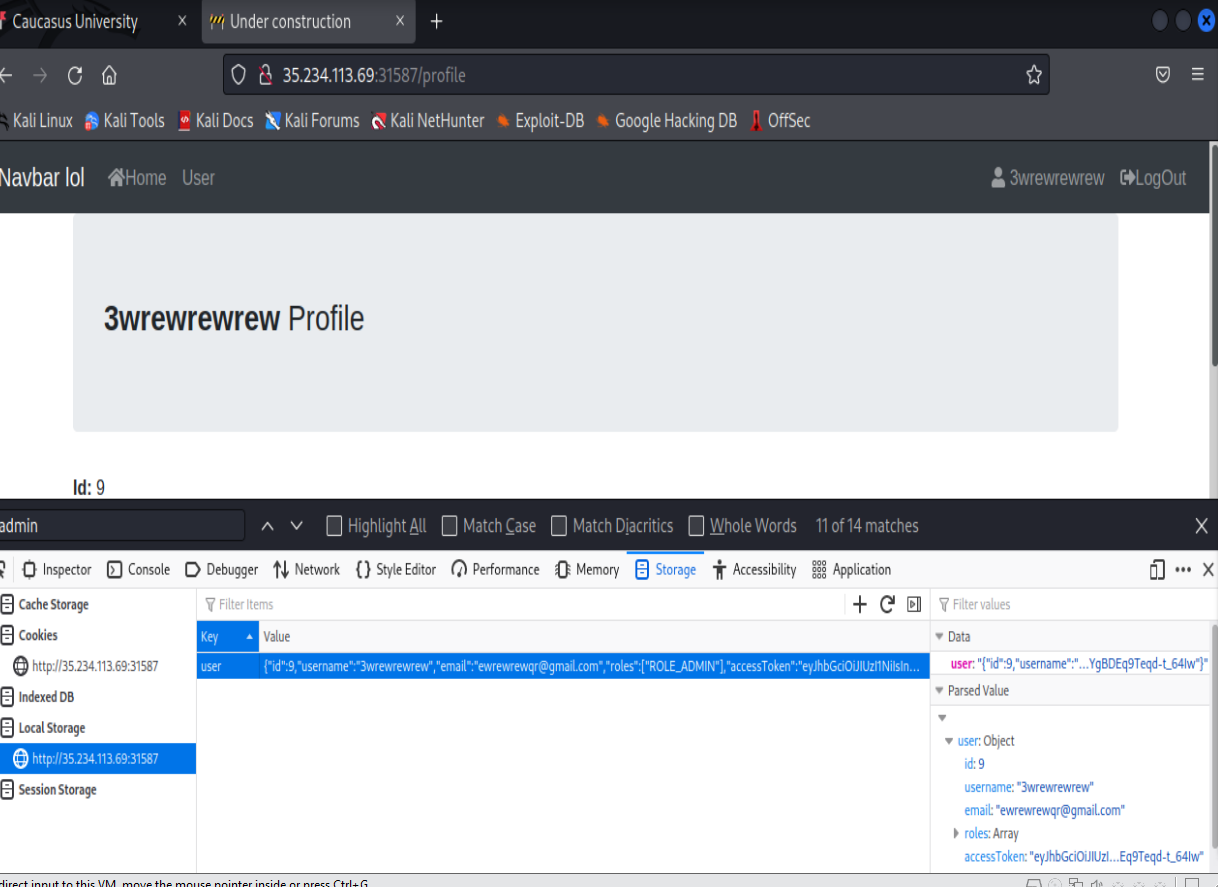


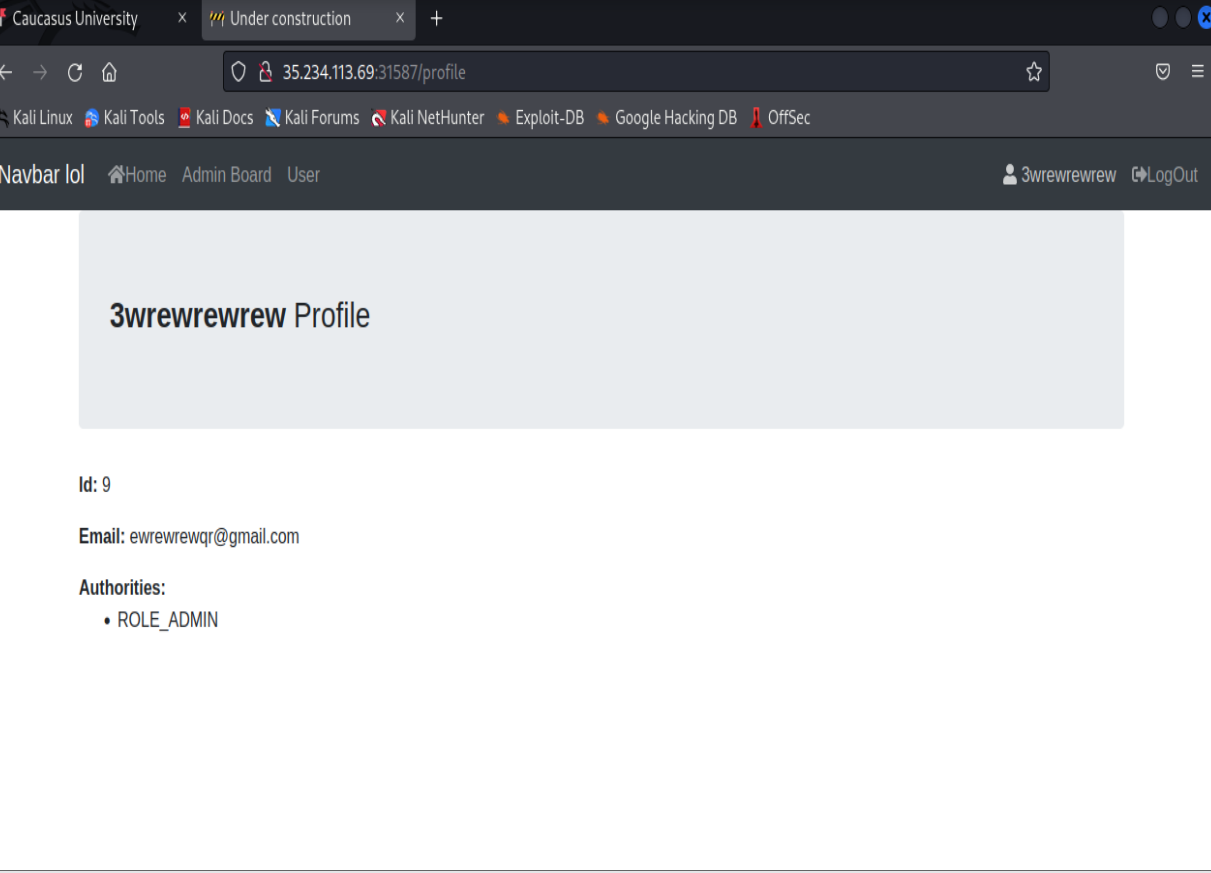




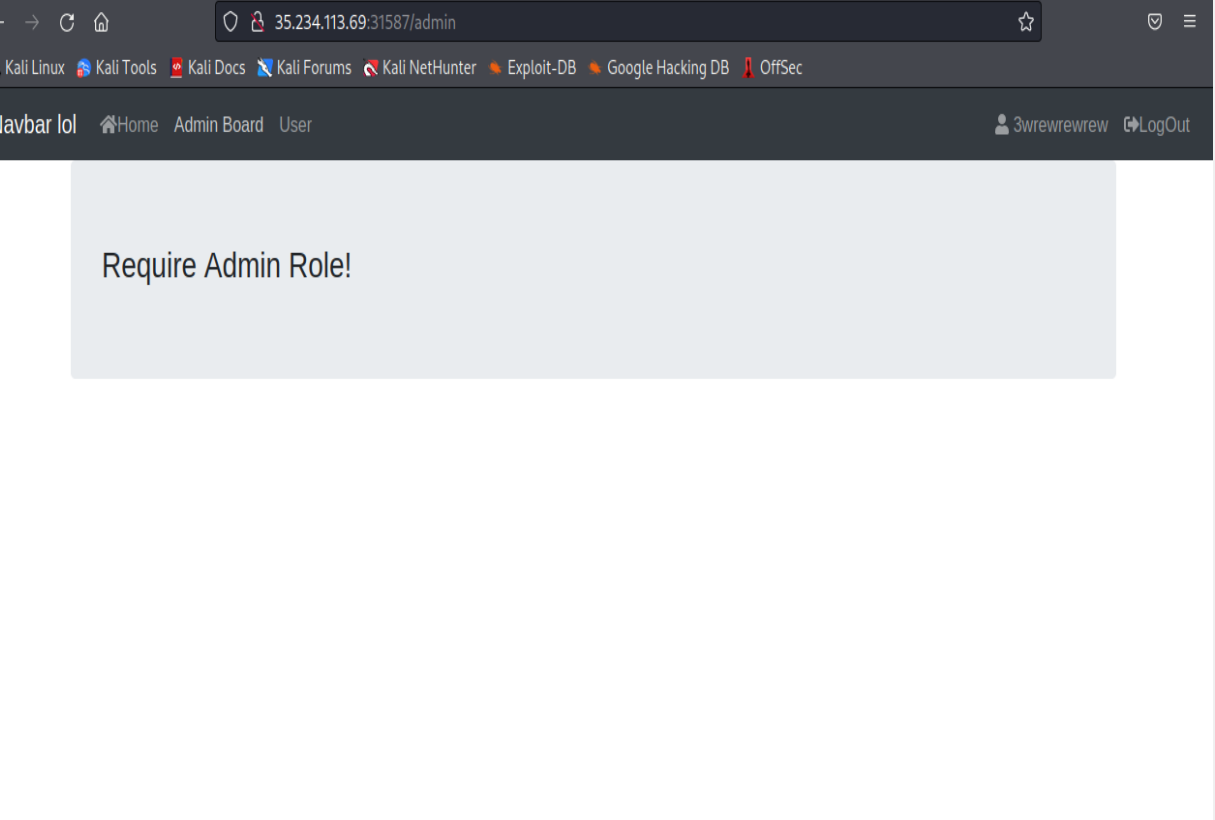


შემდეგ კოდის ლოგიკაში ვხედავთ რომ ადმინის პანელს გვანახებს იმ შემთხვევაში თუ ჩვენი როლია ROLE\_ADMIN

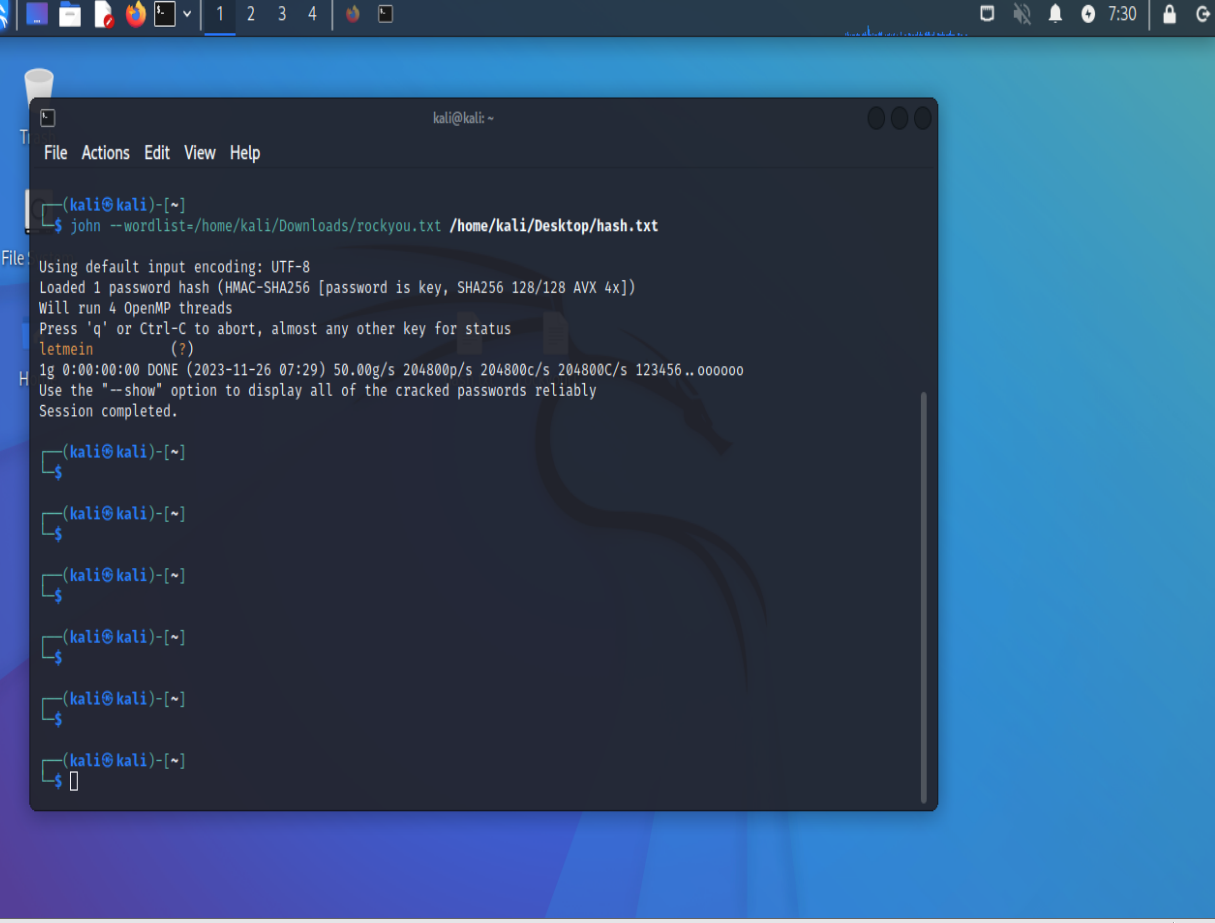




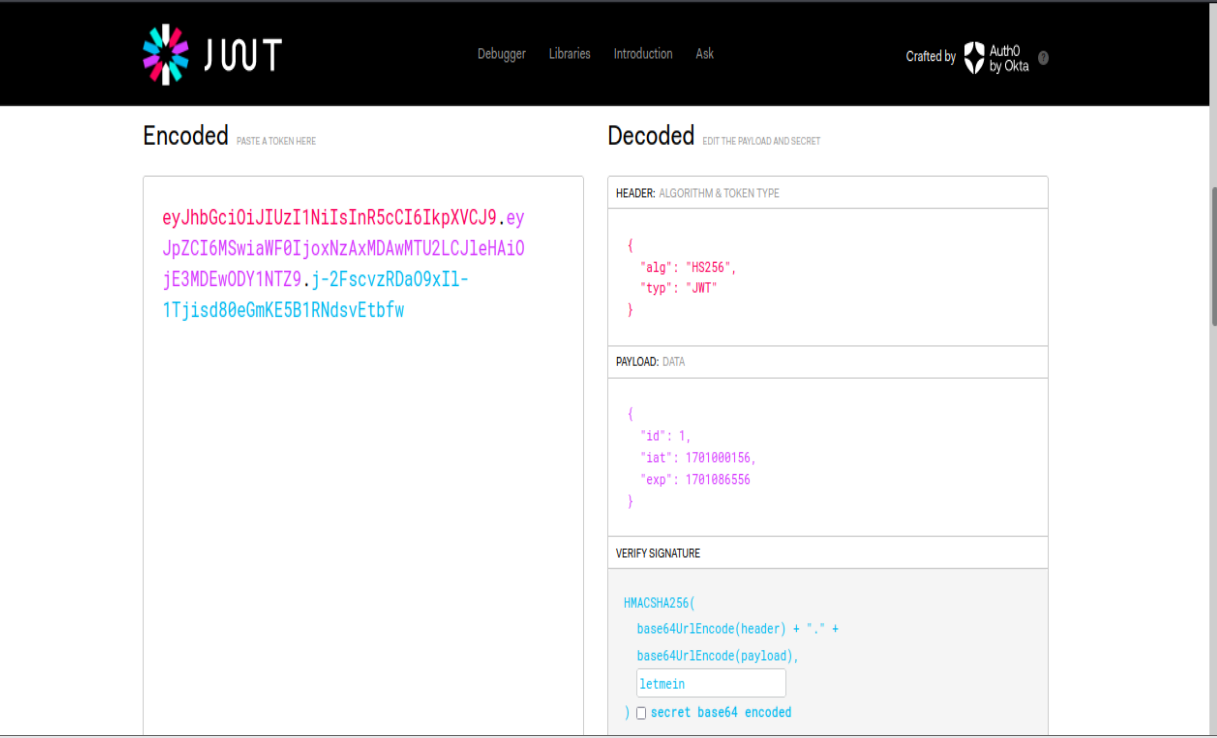
იგივე ნაირად რომ შევცვლით ჩვენ როლს: ROLE\_ADMIN-ზე, როგორც ზემოთ გავაკეთეთ გამოგვიჩნდება ახალი ღილაკლი “Admin Board” რომელზეც წვდომა არ გვაქვს, access token-ის გამო



ჩვენ ამ ტოკენს დავაბრუტე ფორცებთ მაგალითად john-ით მივიგებთ passcode:letmein

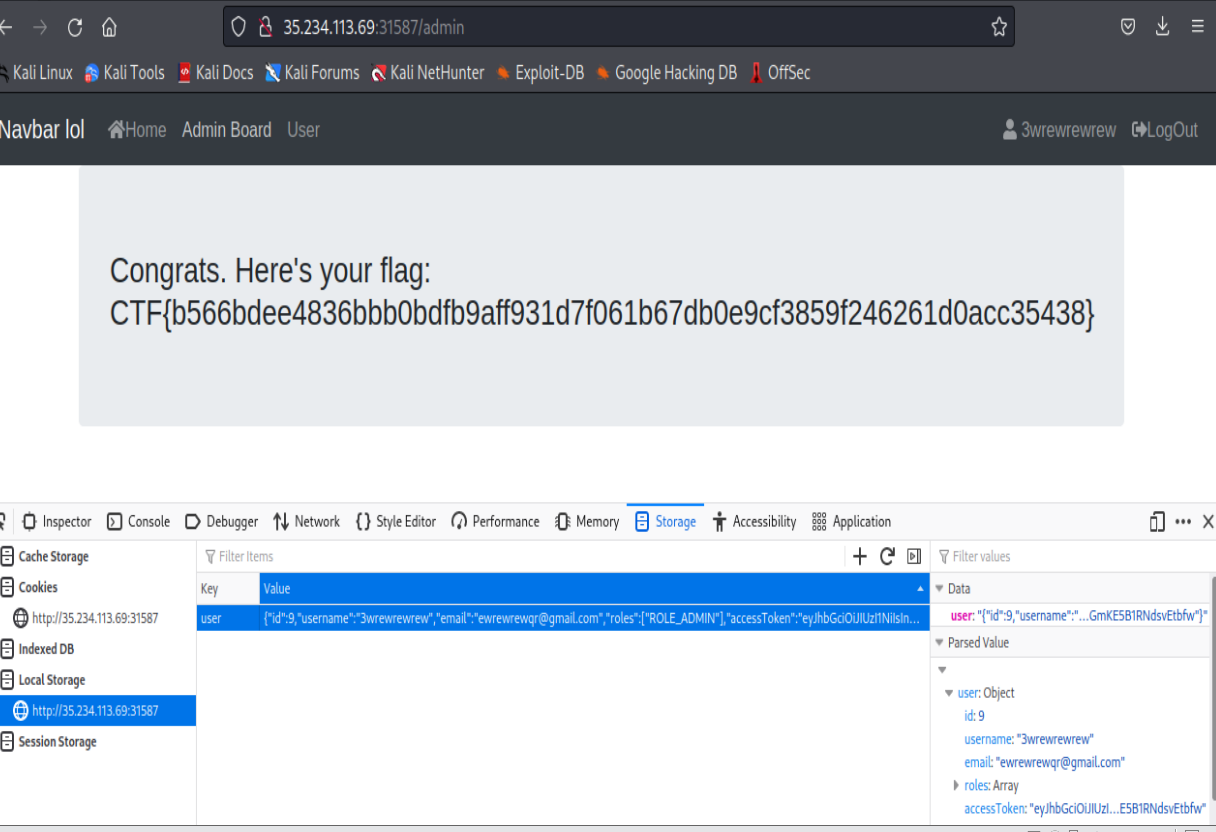


შემდეგ მოვძებნით JWT დეკოდერს მაგალითად jwt.io და შევიყვანთ ჩვენს ტოკენს. აქ ვხედავთ რომ მონიჩებული გვაქ რაღაც id შეგვიძლია ვივარაუდოთ,რომ admin id იქნება 1 და ამას შევცვლით, რათა ამ ეს ვერიფაიდ იყოს letmein-ს ჩავწერეთ აგერეთვე რადგან და მივიგებთ ახალ ტოკენს.



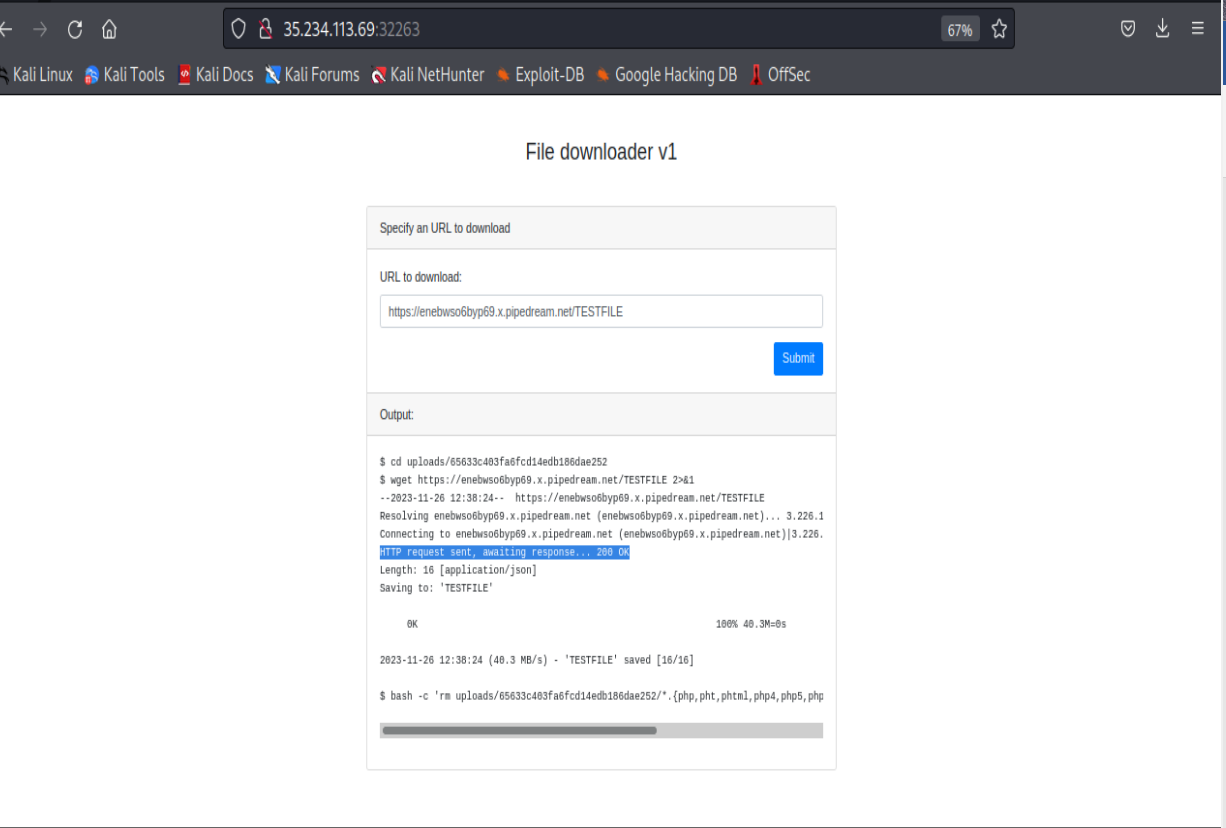
შემდეგ კი ძველ ოტკენს ამ ახალი ტოკენით ჩავანაცვლებთ

და მივიღებთ flag-ს

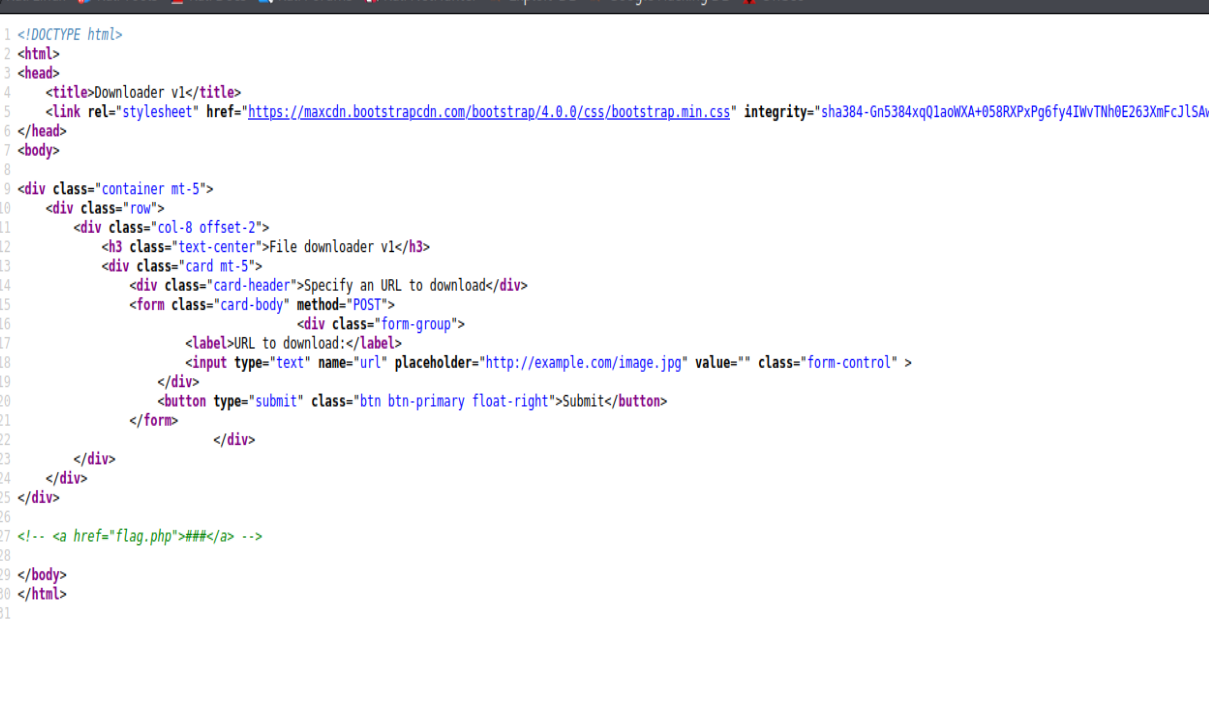


Downloader v1

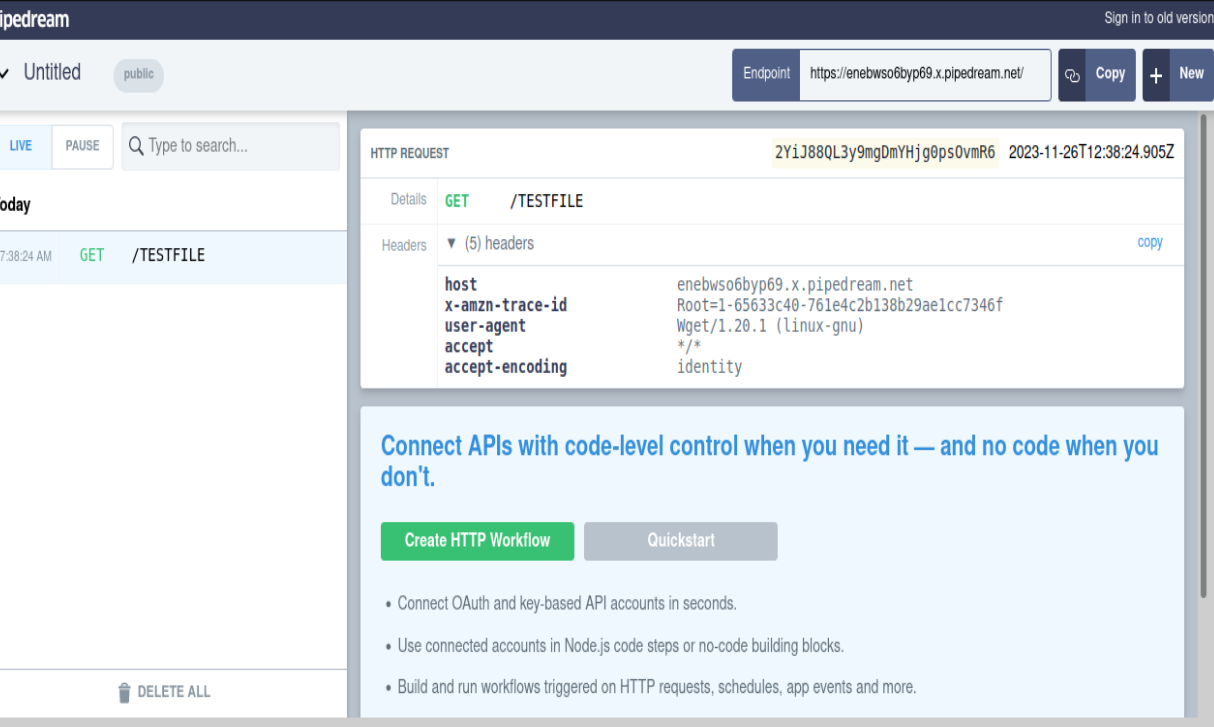
საიტზე ვხვდებით არის ველი რომლიდანაც შეგვიძლია ფაილის ჩამოტვირთვა. Requestbin-ის დახმარებით, ჩვენ შეგვიძლია მივიღოთ სერვერის მიერ ჩვენ მითითებულ URL-ზე გაგზავნილ მოთხოვნები. მაგალითად მოვითხოვოთ არარსებული TESTFILE ფაილი.



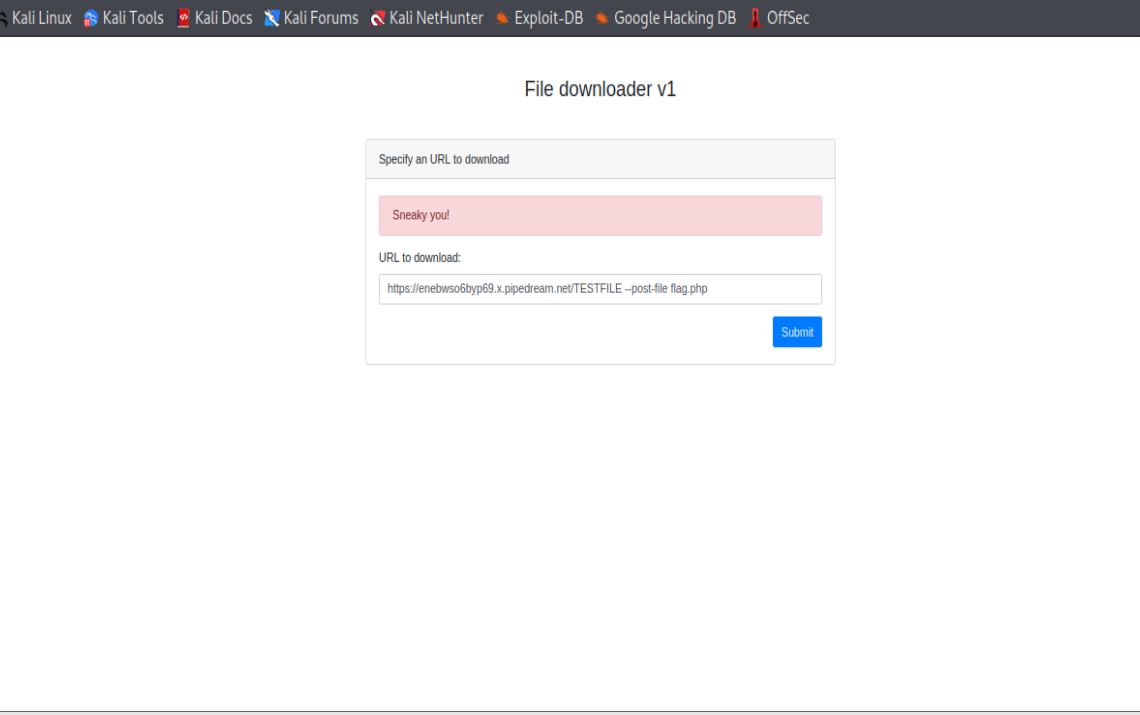
ასევე საიტის სორს თუ ვნახავთ იქ ასეთი რაღაც წერია flag.php შეგვიძლია ვივარაუდოთ,რომ ზუსტად აქ ინახება ფლაგი.



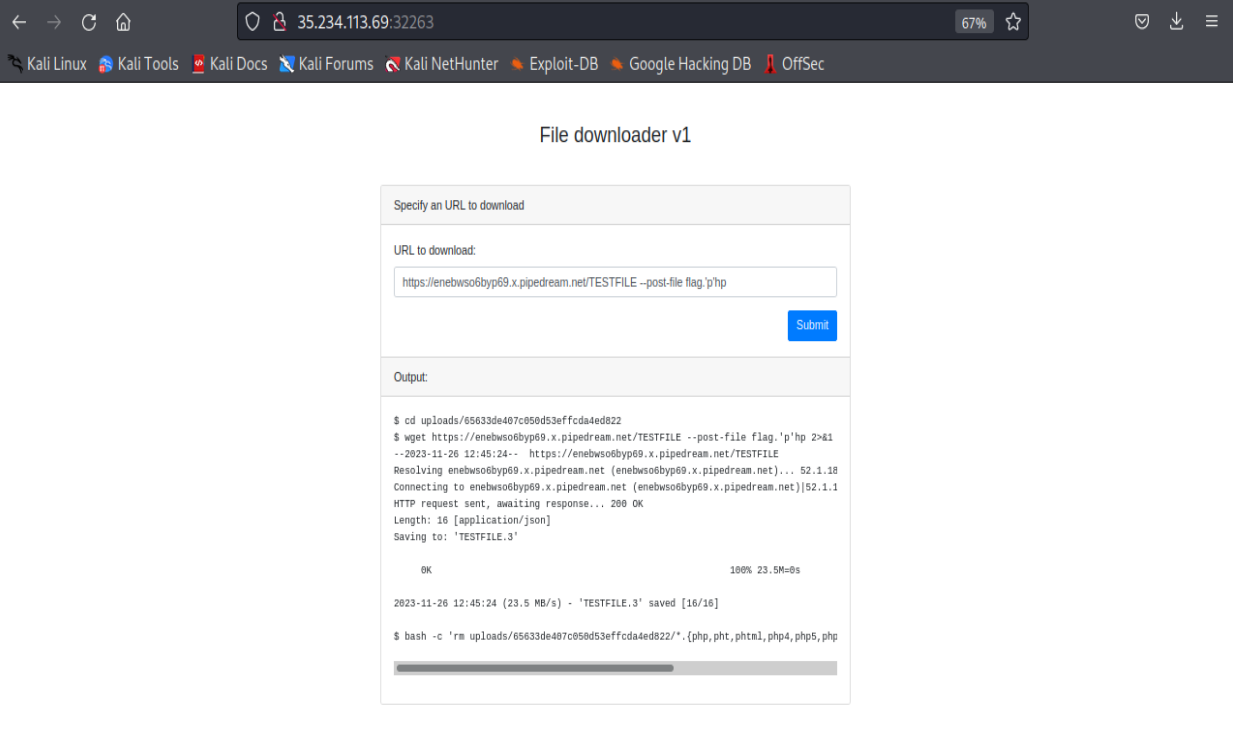
Requestbun საიტზე მივიღეთ ეს შედეგი



და ვხედავთ რომ საიტი ხმარობს wget-ს ფაილების ჩამოსატვირთად, ამიტომ შეგვიძლია გმოვიყენოთ --post -file flag.php



ვხედავთ რომ საიტი აკეთებს ვალიდაცია ამიტომ ‘ ‘ ვუმატებთ php-ს და თავიდან ვცდით



მივიგეთ ფლაგი

