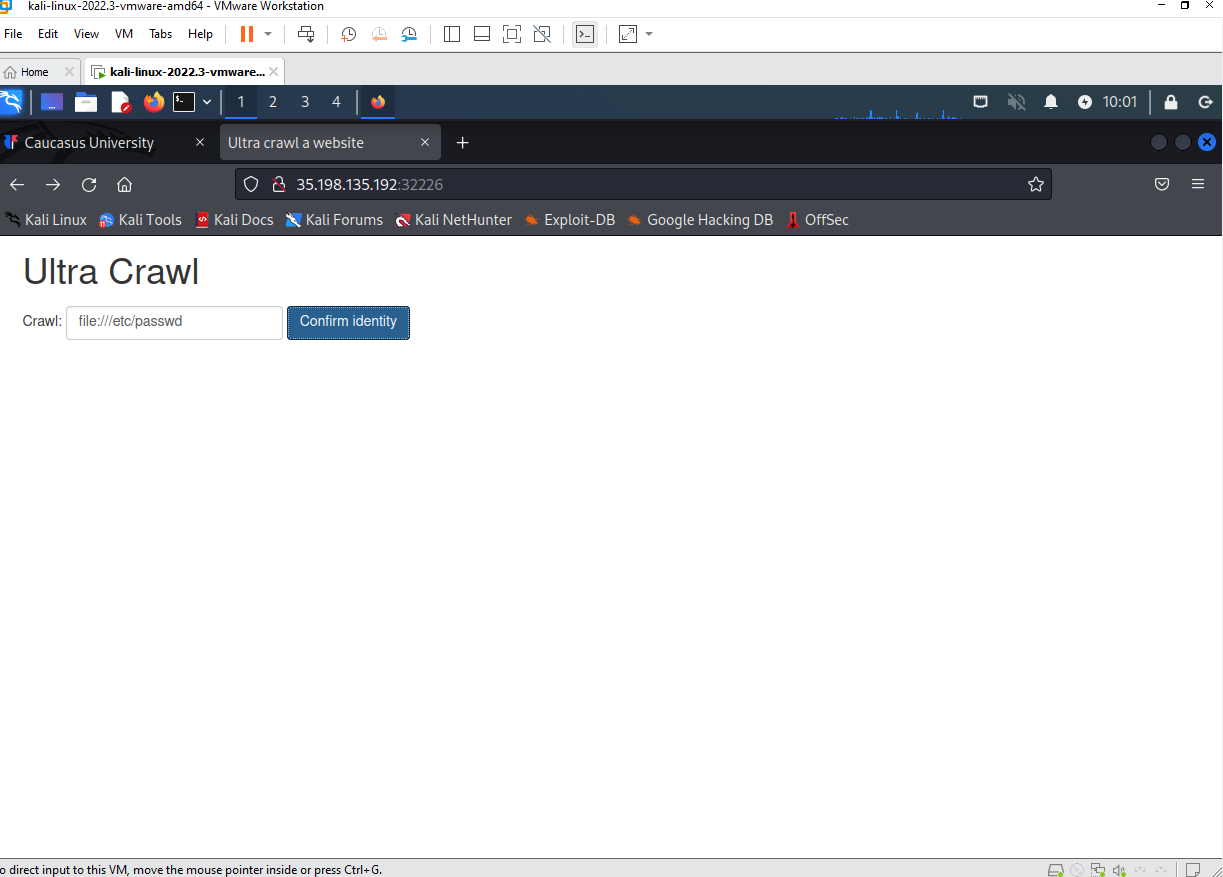
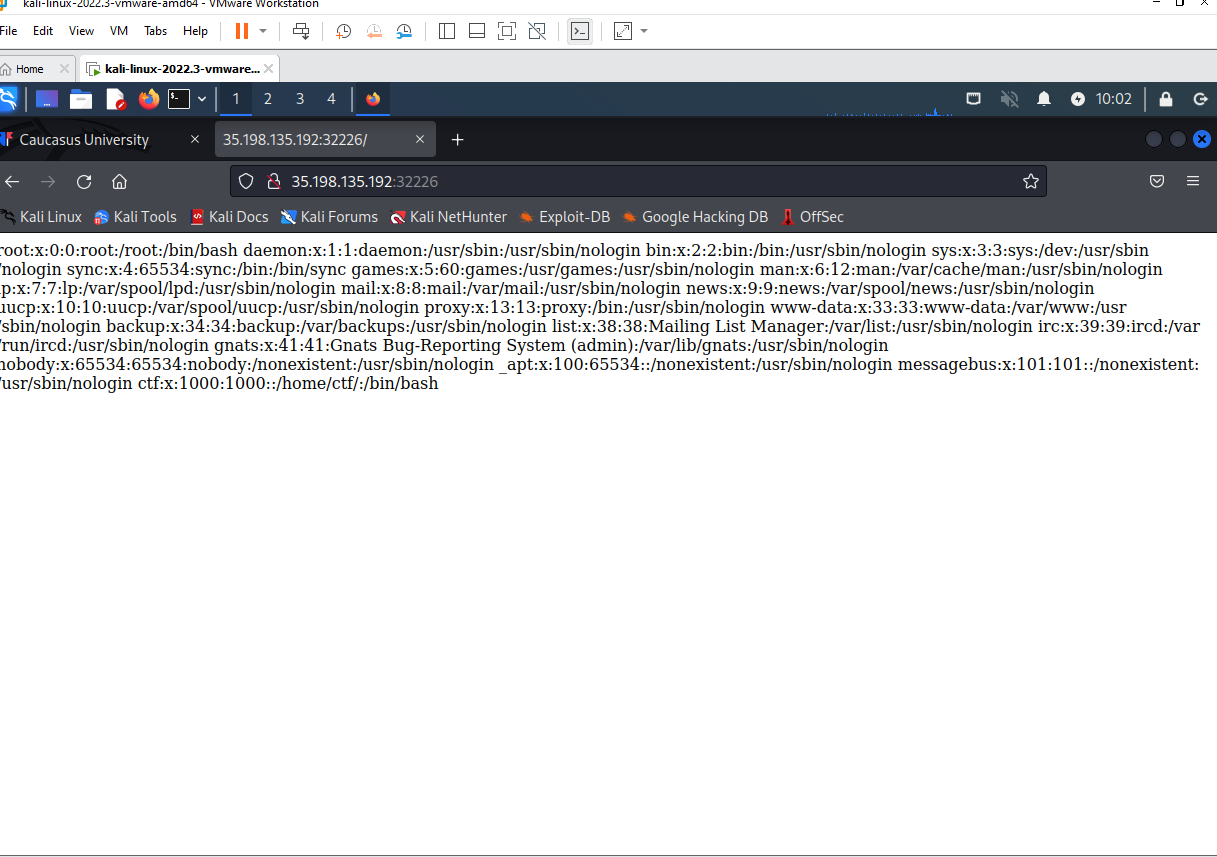
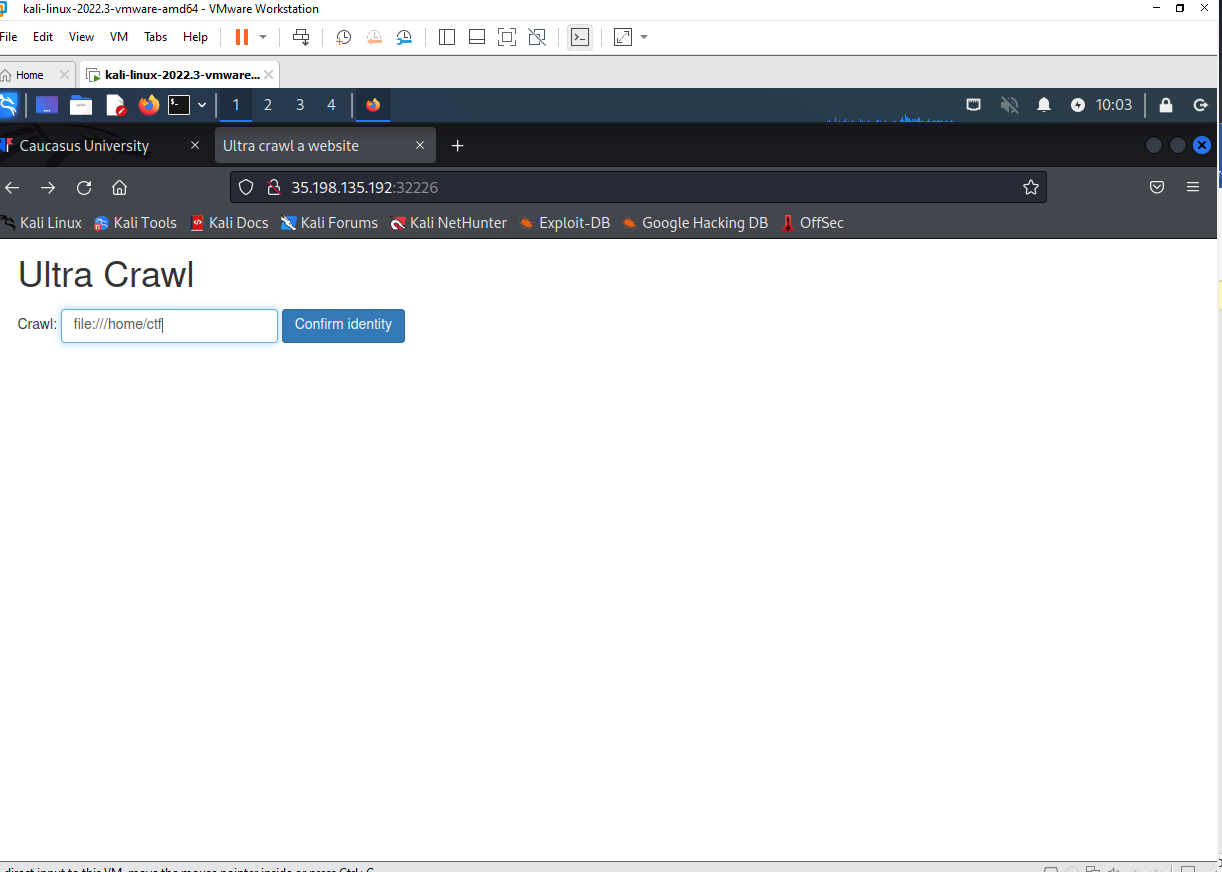
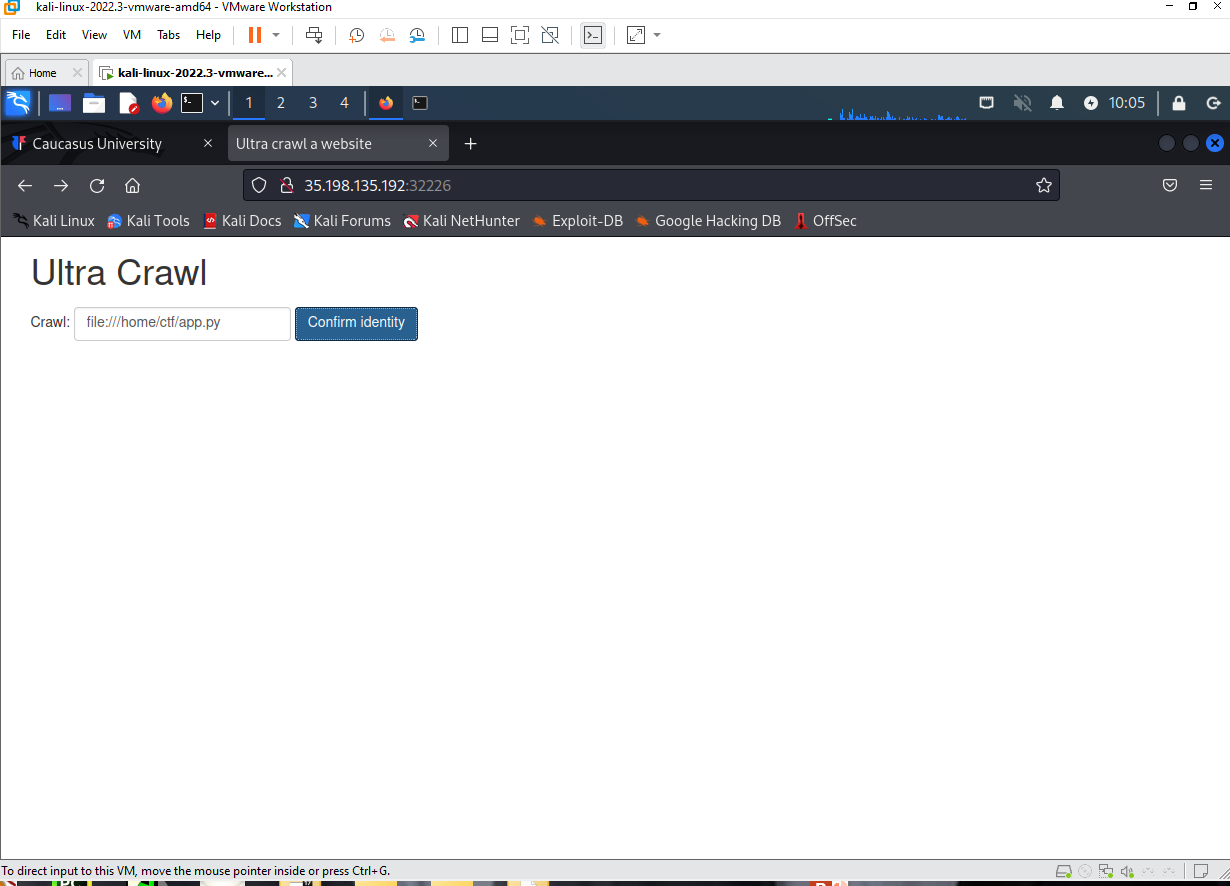
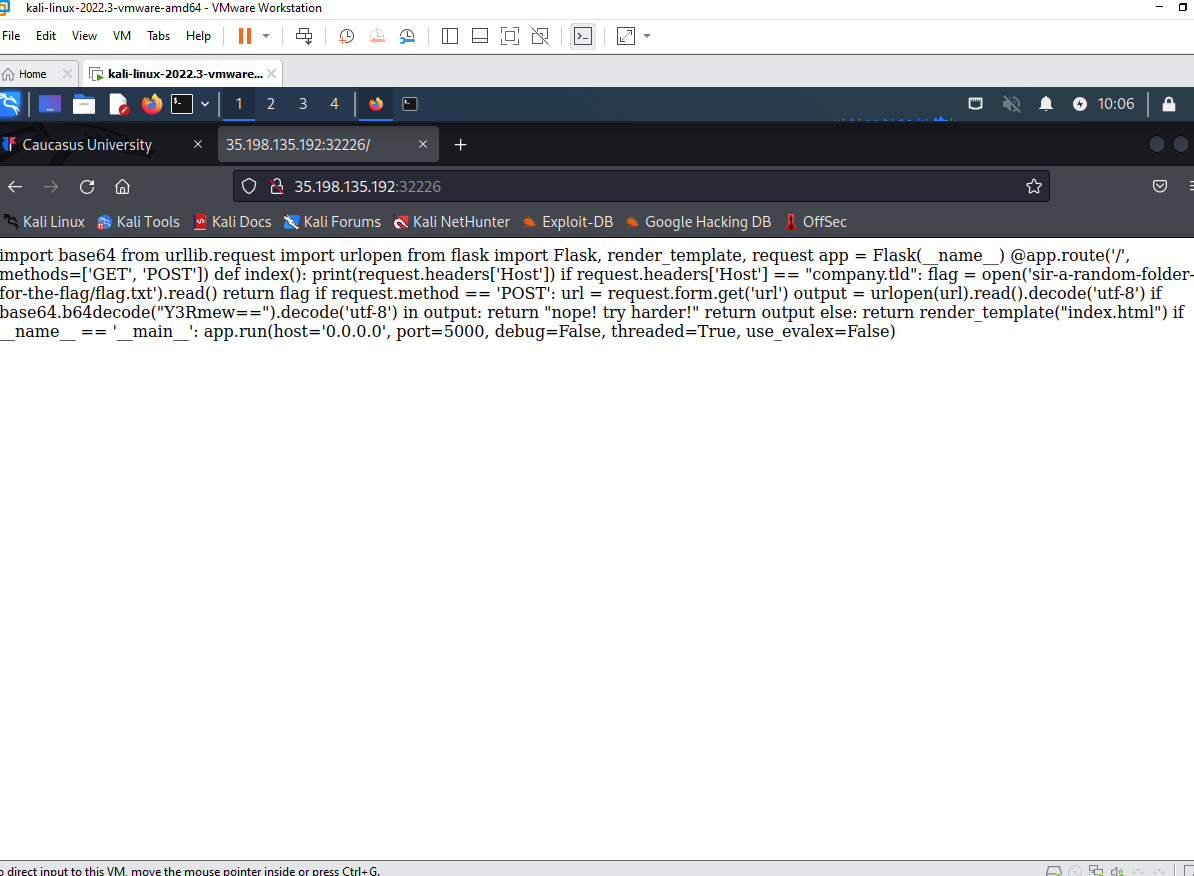
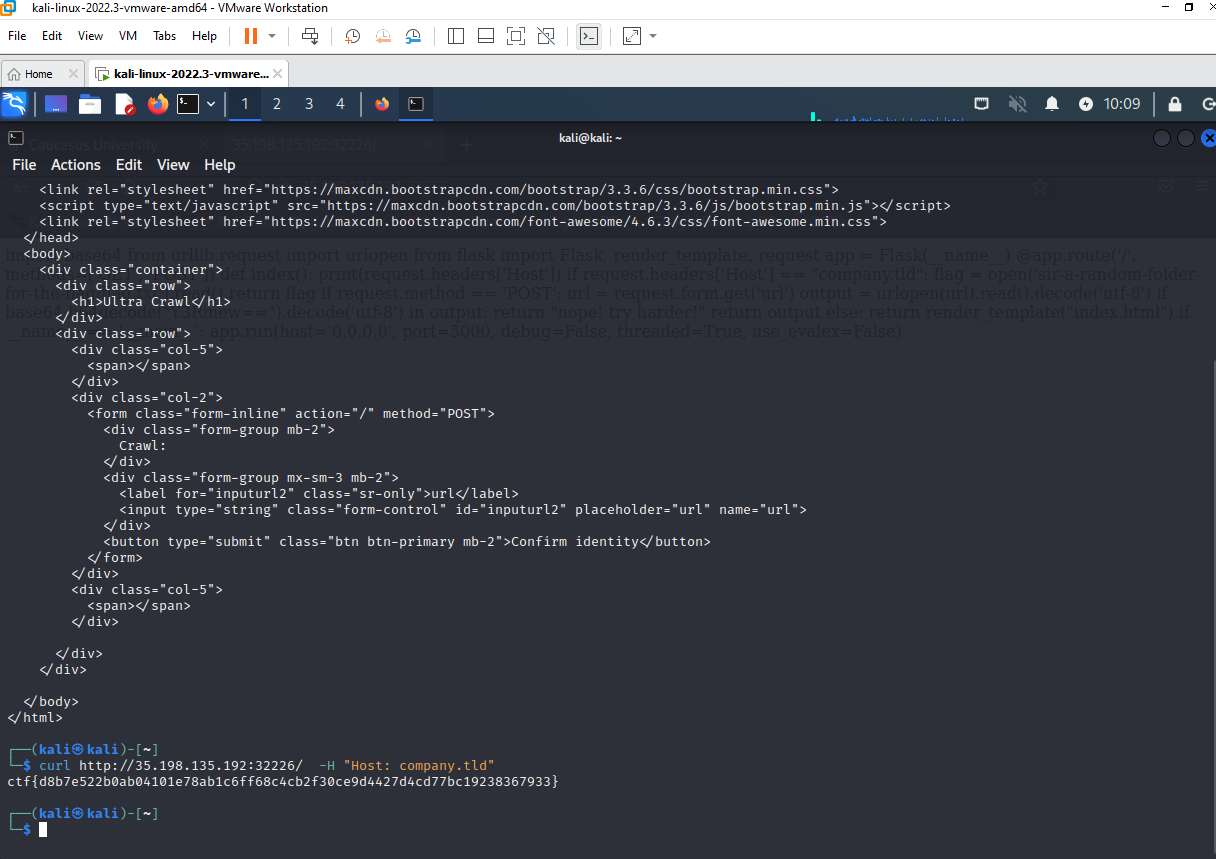
Ultra-crawler:

1. 
2. ვწერთ ამ კომანდს და enter-ს, შემდეგ ვნახულობთ შემდეგ page-ს.
3. 
4. ჩვენთვის კონკრეტულად საინტერესოა home/ctf/ - რომელსაც ახლა გავტესტავთ და ვნახავთ თუ რას მოგვცემს
5. 
6. რადგან ვნახეთ რომ ეს საიტი Pyhtonzea შეგვიძლია ვივარადუოთ რომ app.py-ში იქნება ჩვენთვის ხელ-საყრელი რამ ამიტომ ვწერთ შემდეგ კომანდას ‘home/ctf/app.py
7. 



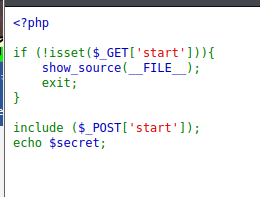
ვიღებთ ამ SCREENS-ს და ვხედავთ რომ თუ გაგზავნილ REQUEST-ში ჰედერი HOST იენქბეა compant.tld მივიგებთ flag-ს.



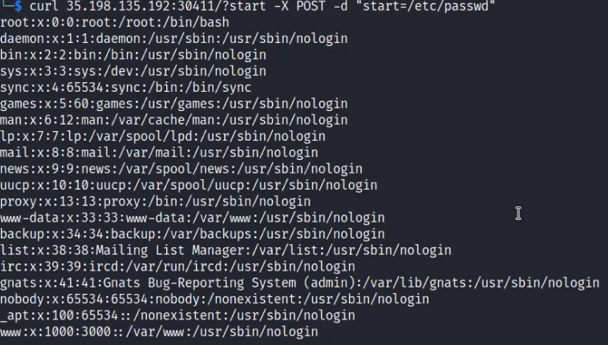
Cmd-ში curl კომანდის საშუაკებით ვცვლით hosts-ს company.tld-ზე და ვიგებთ ctf-ს

------------------------------ALIEN-INCLUSION :-----------------------------------------------

საიტზე რომ შევდივარტ ვხედავთ შემდეგ კოდს



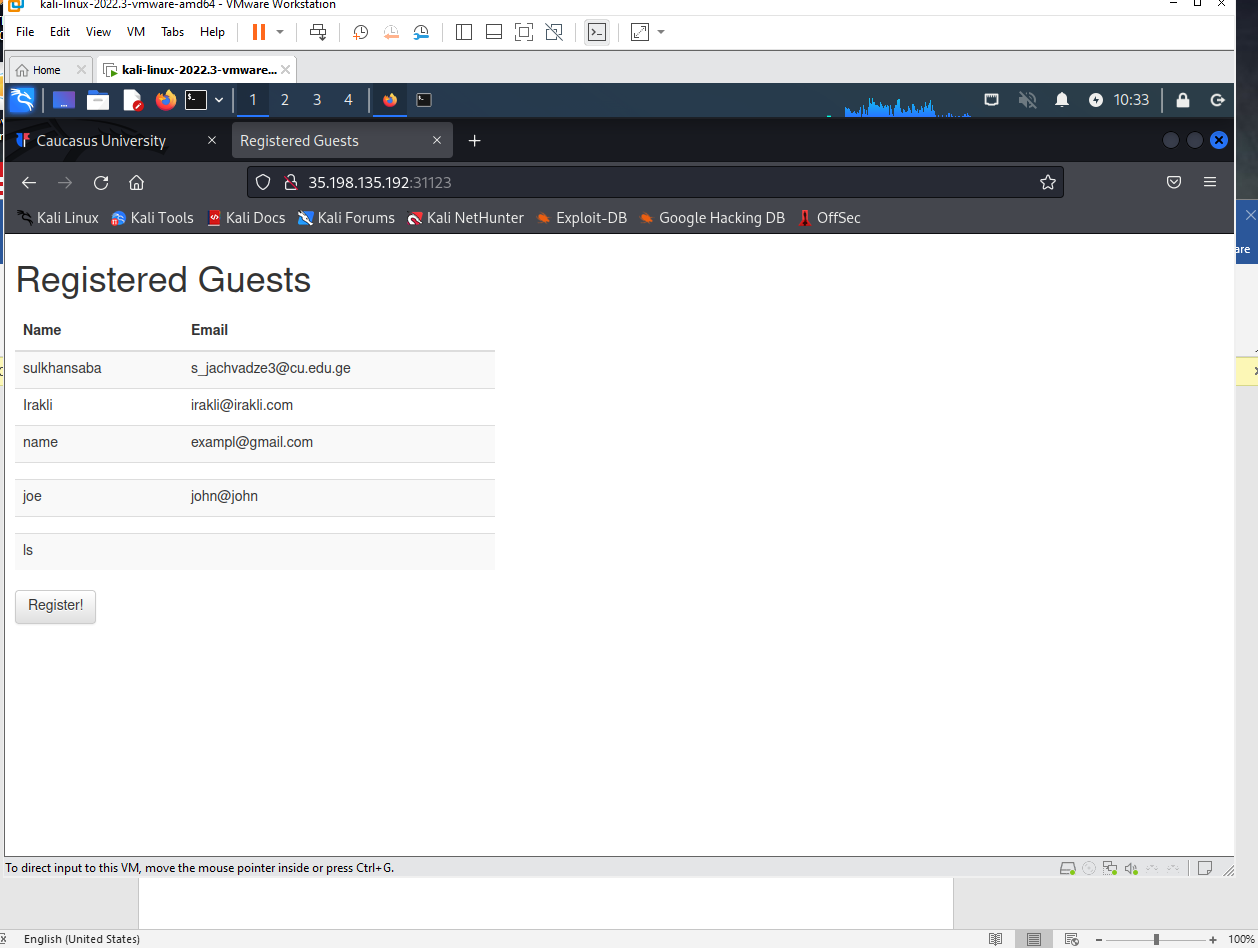
შეგვიძლია მანიპლურირება მოვახდინოთ if function-ძე კერძოდ start--ზე რომლის საშუალებითაც მივიგებთ რაც გვჩირდება, ამიტომ cmd-ში გამოვიყენებთ curl-ს კომანდს



და ვნახავთ რომ მუსშაობს start-ზე მანიპულირება და რადგან cyberedu-ს საიტძე hint გვაქ რომ ფლაგი არის flag.php-ში უბრალოდ შევცვლით start=flag.php-ზე მივიგებთ ctf-ს

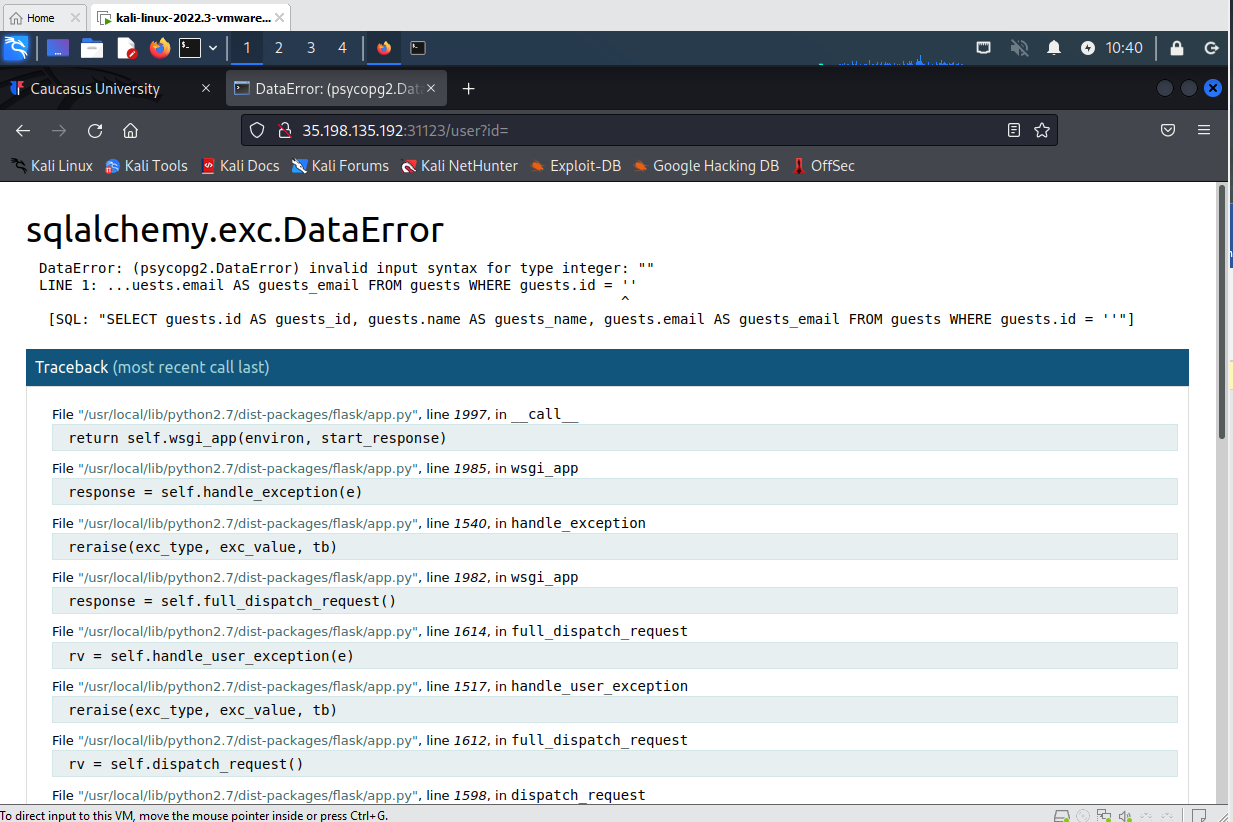


---------------------small data leak ----------------------------------

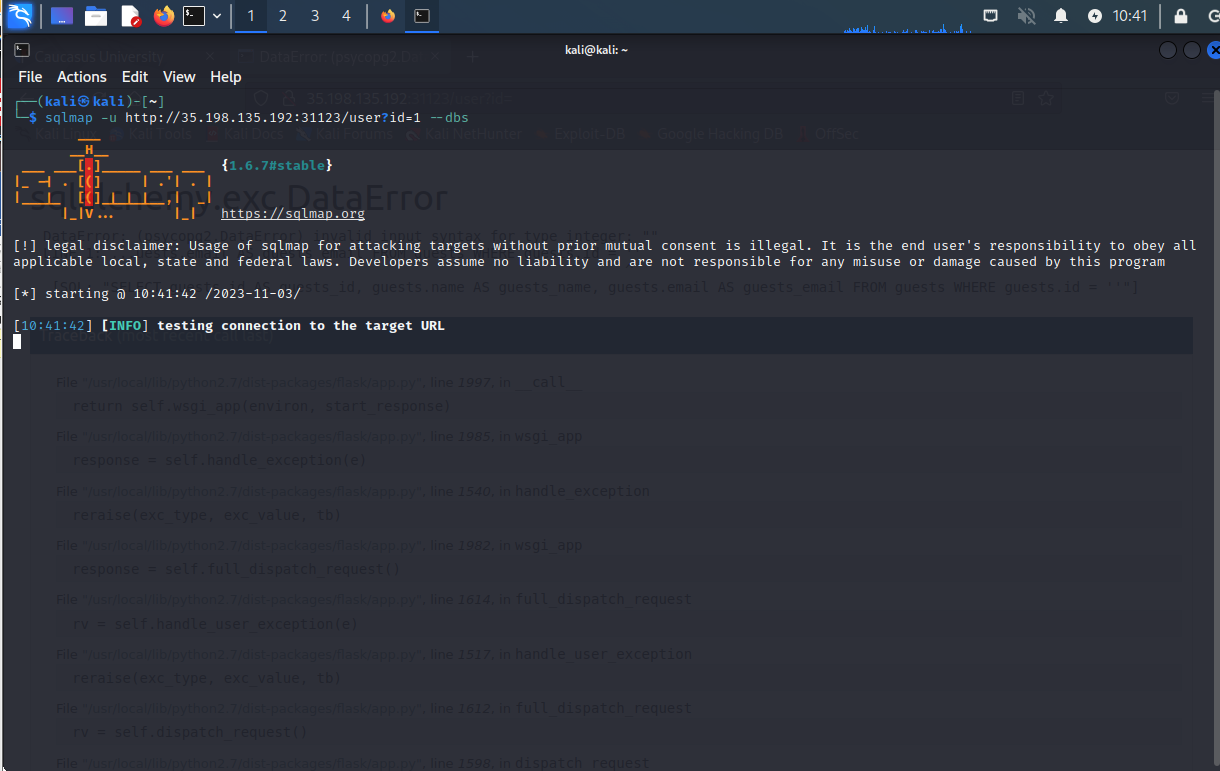


მოცემული გვაქ სქლ database რომლეზეც შეგვიძლია გამოვიყენოთ tool – “sqlmap”

Cyberedu-ზე გვაქვს hint: /user?id= რომელსაც გამოვიყნებთ url-ში და ასევე გამოვიყენებთ sqlmap-ის ერთ-ერთ ფუნქციას ორმელიც ეძებს database-ებს



ვხედავთ რომ id-ს შედმეგ აგაც აკლია ანუ error-ს აგდებს და ამიტომ ვწერთ 1ს sqlmap-ს command-ში



ვიყენებთ ფუნქლიას რომელიც --dbs ძებნის database-ბს

ამ კომანდის გაშვების შემდეგ sqlmap უნდა იპოვოს database-ები როგორც მახსოვს არის სულ 3 ცალი და datebase public-ში არის flag

Sqlmap -u საიტი -D public - - tables მოგვცემს ნახევარ ctf პასუხს

ამის შემდეგ ვიყენებთ შემდგე commands:

Sqlmap -u საიტი -D public -t ‘ctf ის ნაწილი რაც ზემოდან მივიგეთ’ - - columns და ამ კომანდის შემდეგ მივიგებთ საბოლოო პასუხს.