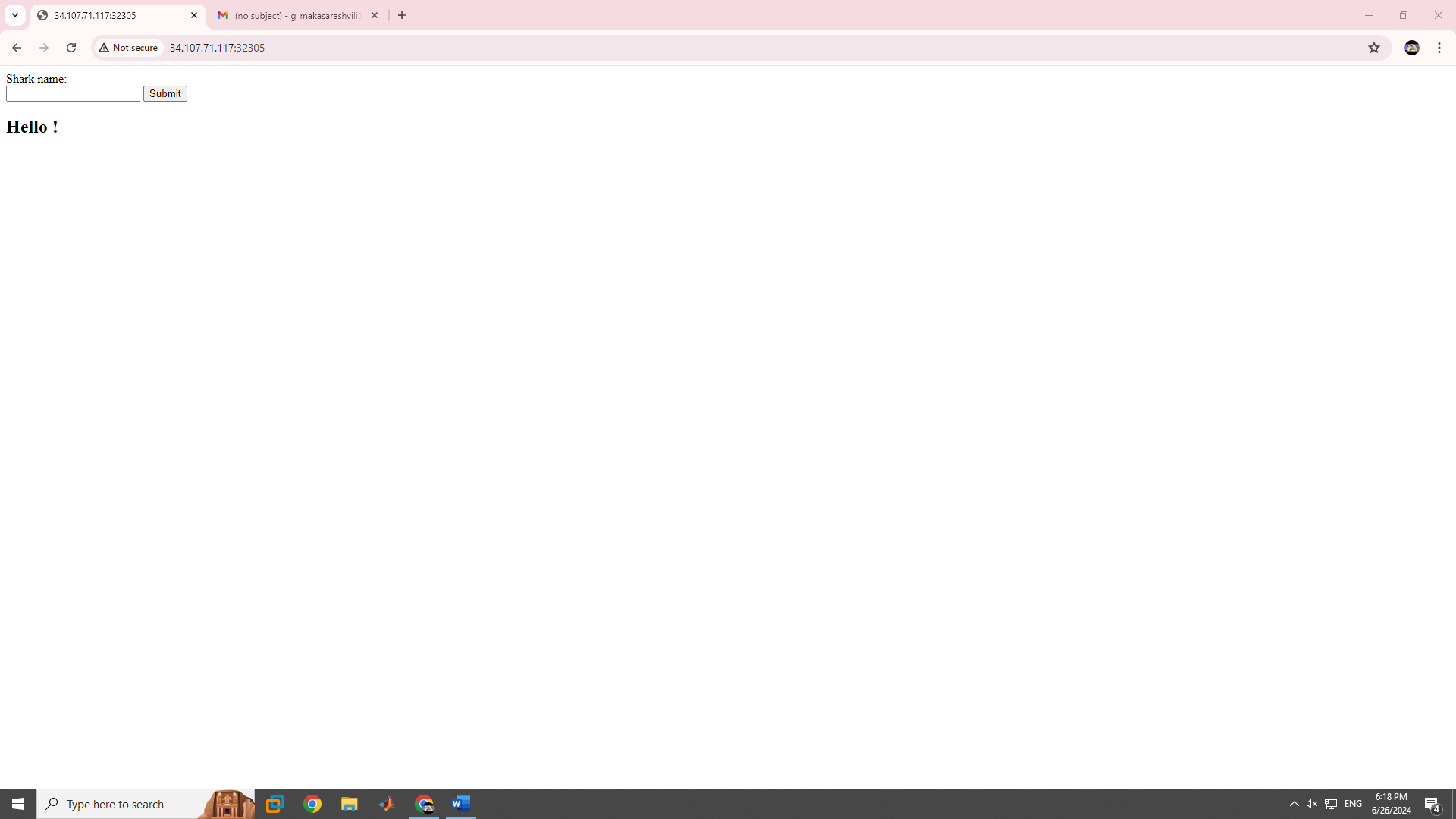
სიმულაციური აქტივობა

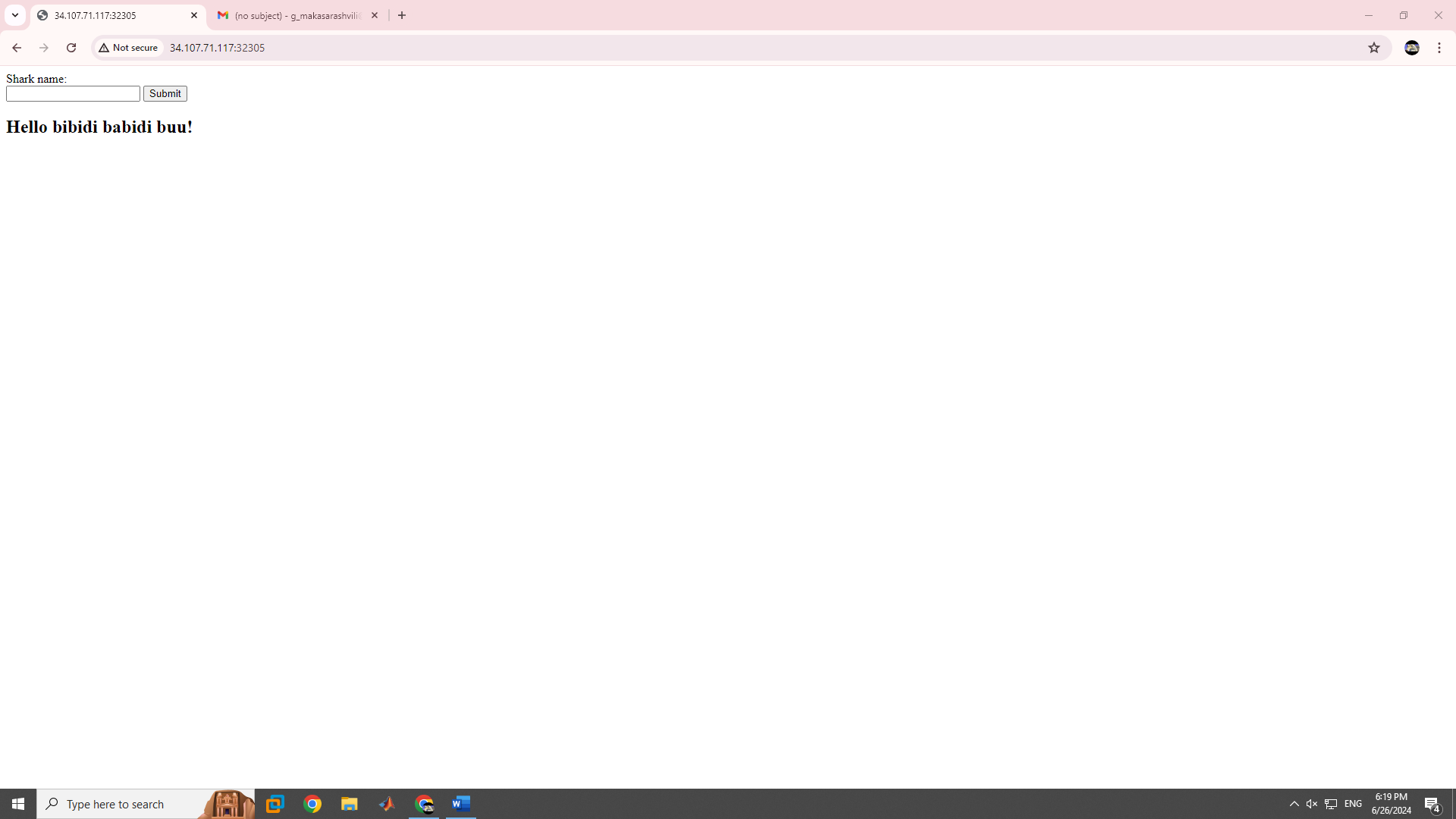
გიორგი მაკასარაშვილი

LAB: shark

მოცემულ მისამართზე შესვლისას ვხედავთ მხოლოდ ერთ input ველს

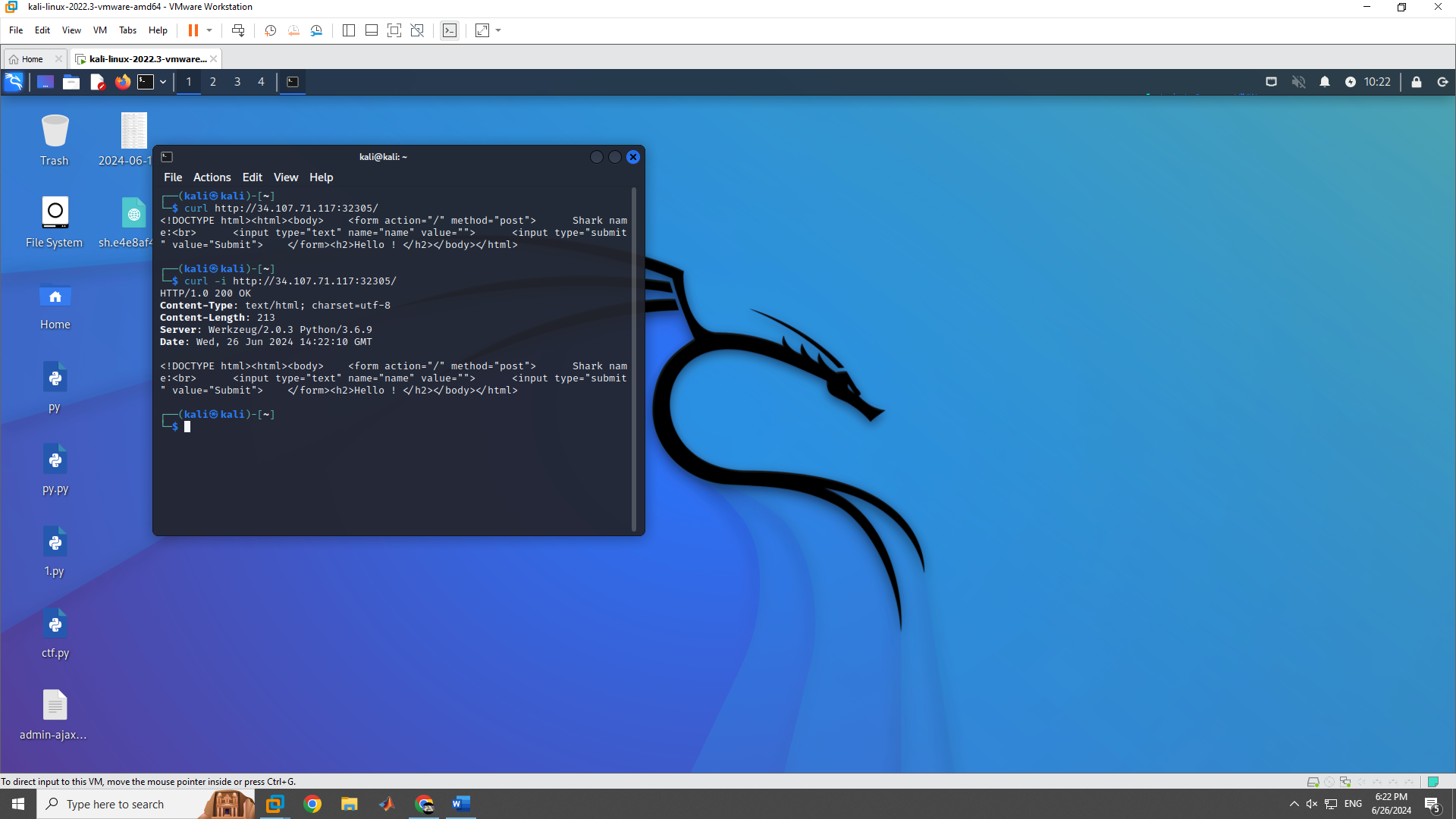


ამ ველში ნებისმიერი რამის ჩაწერის დროს, იგივე რამ გვიბრუნდება უკან



ცოტა უფრო მეტი ინფორმაცია რომ მოვიძიოთ მის შესახებ მაგალითად სერვერის,

უნდა გამოვიყენოთ curl



ვხედავთ რომ ეს არის Werkzeug. ინტერნეტ სივცეში მრავალი ძებნის შემდეგ

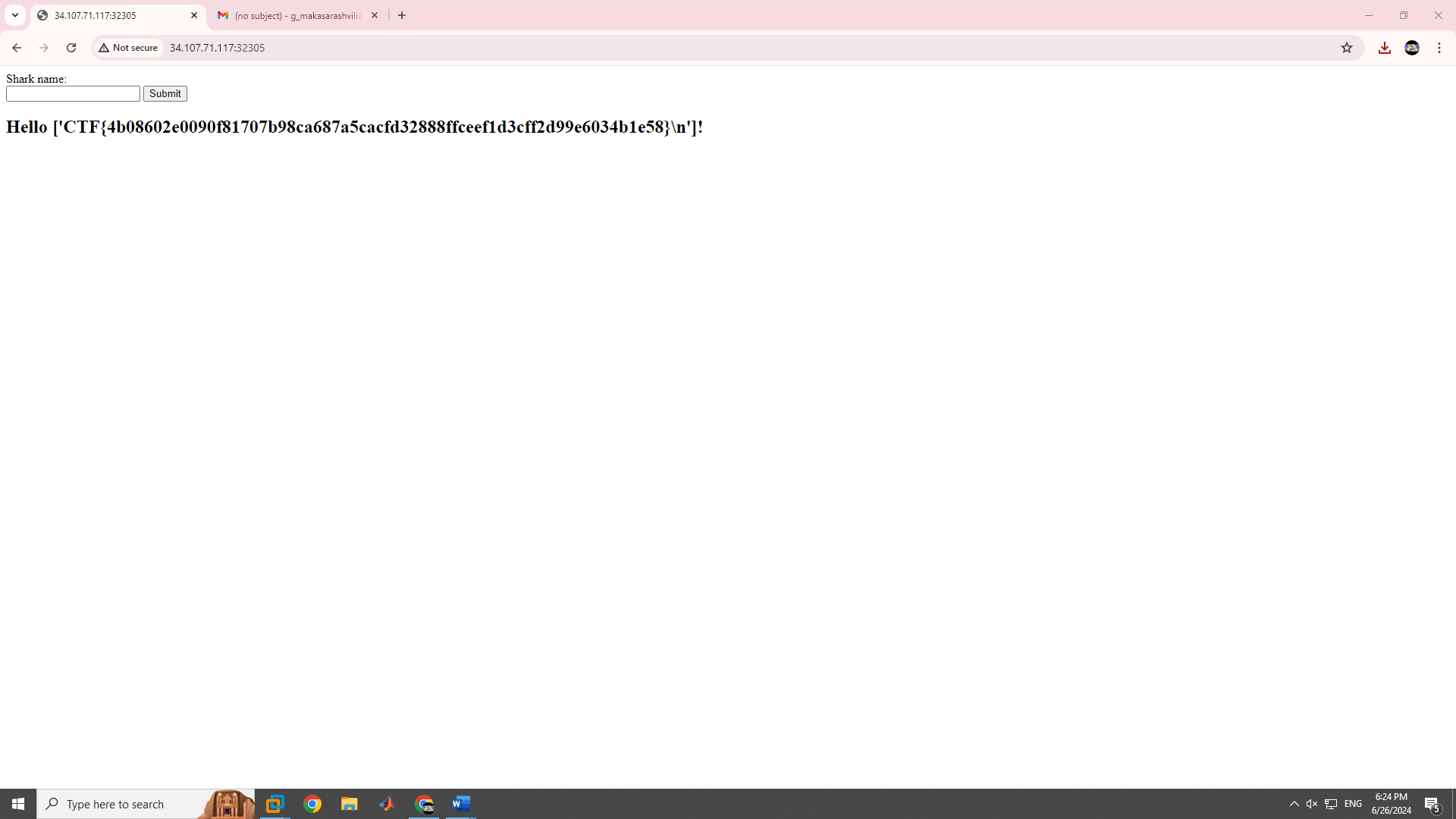
მივაკვლევთ შესაბამის ბრძანებას, რისი გაშვების შემდეგაც ვიპოვით ctf-ს

<%

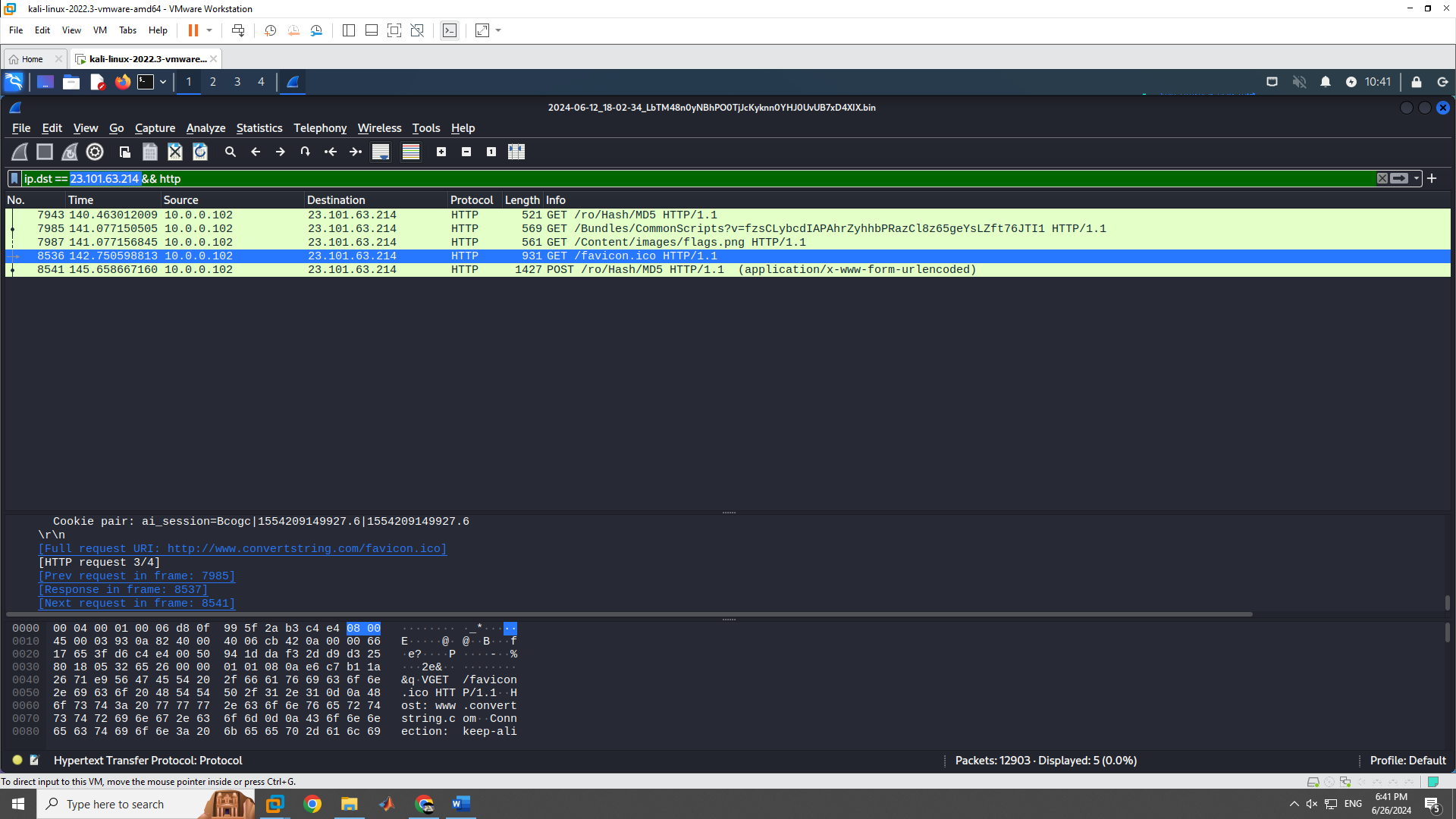
x=open("flag","r")

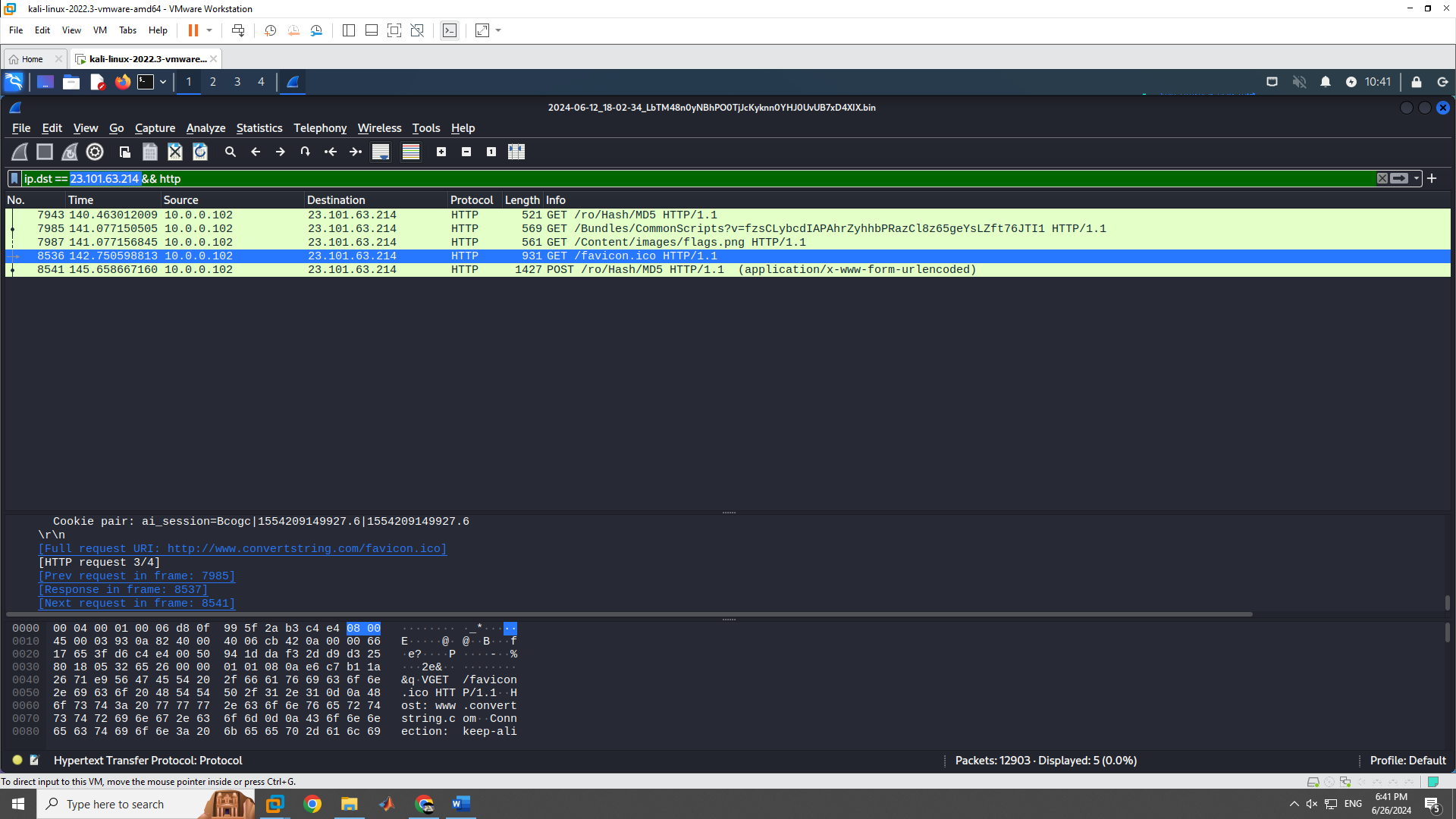
%>

${x.readlines()}



LAB: online encryption

მოცემულია wireshark ფაილი, ამ ფაილში უნდა მოვძებნოთ ინფორმაცია შესაბამისი ფილტრების გამოყენებით, პირველ რიგში უნდა გავფილტროთ http. ამის შემდეგ დავაკვირდებით რომ საინტერესო ინფორმაცია არის გაგზავნილი მისამართზე 23.101.63.214, ამიტომ ვადებთ 2 ფილტრს. მიმღები რომ იყოს აღნიშნული მისამართი და გამოყენებული იყოს http. 

შედეგად ვხედავთ რამდენიმე გაგზავნილ პაკეთს, ყურადღებას იქცევს post მეთოდი რადგან ის დაშიფრულია MD5-ით. მცირე ძებნისას ვაწყდებით დაშიფრულ სტრიქონს.

ინტერნეტში ძებნისას შეგვიძლია მივაკვლიოთ მისი გაშიფრის ხერხს.