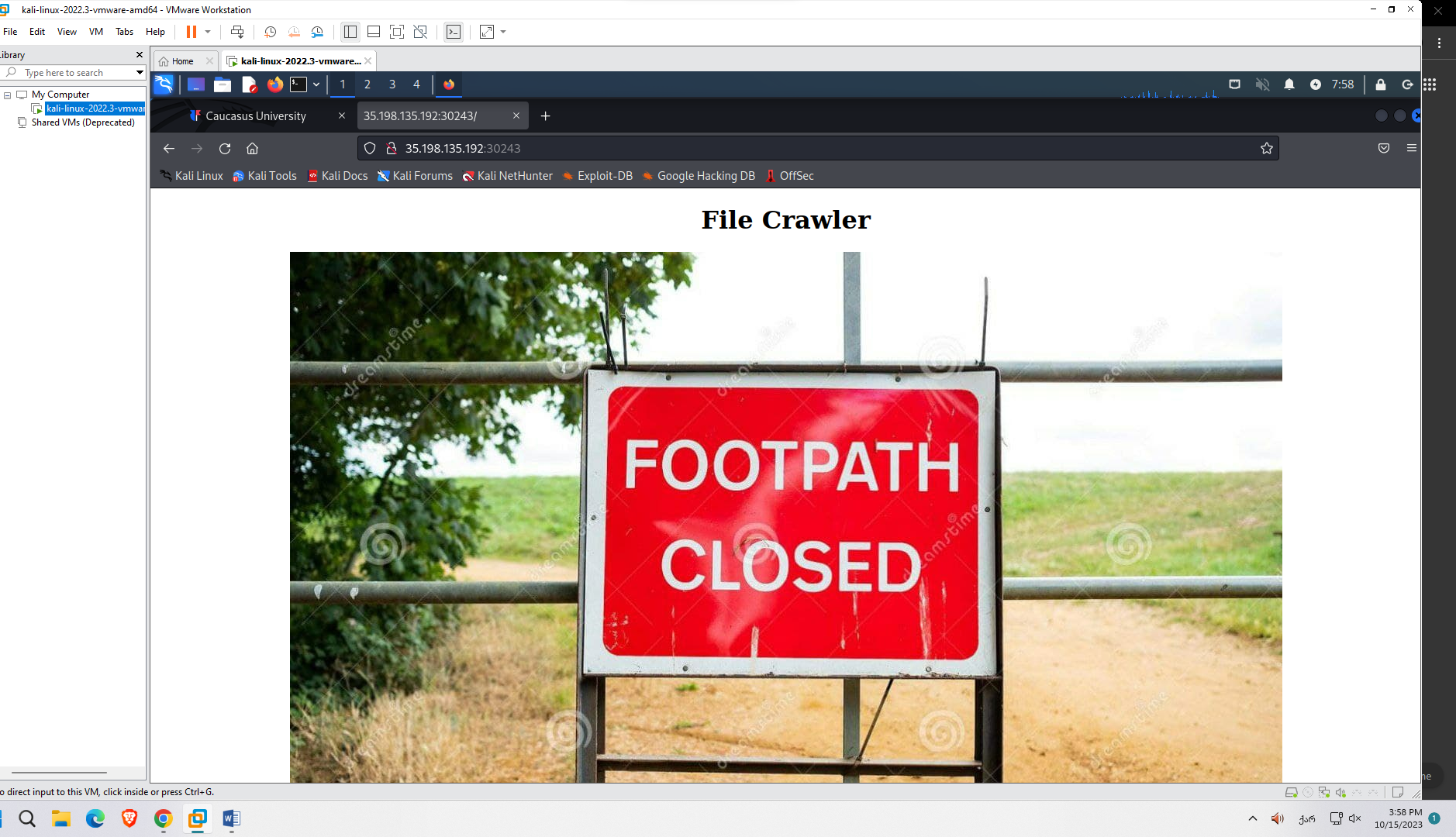
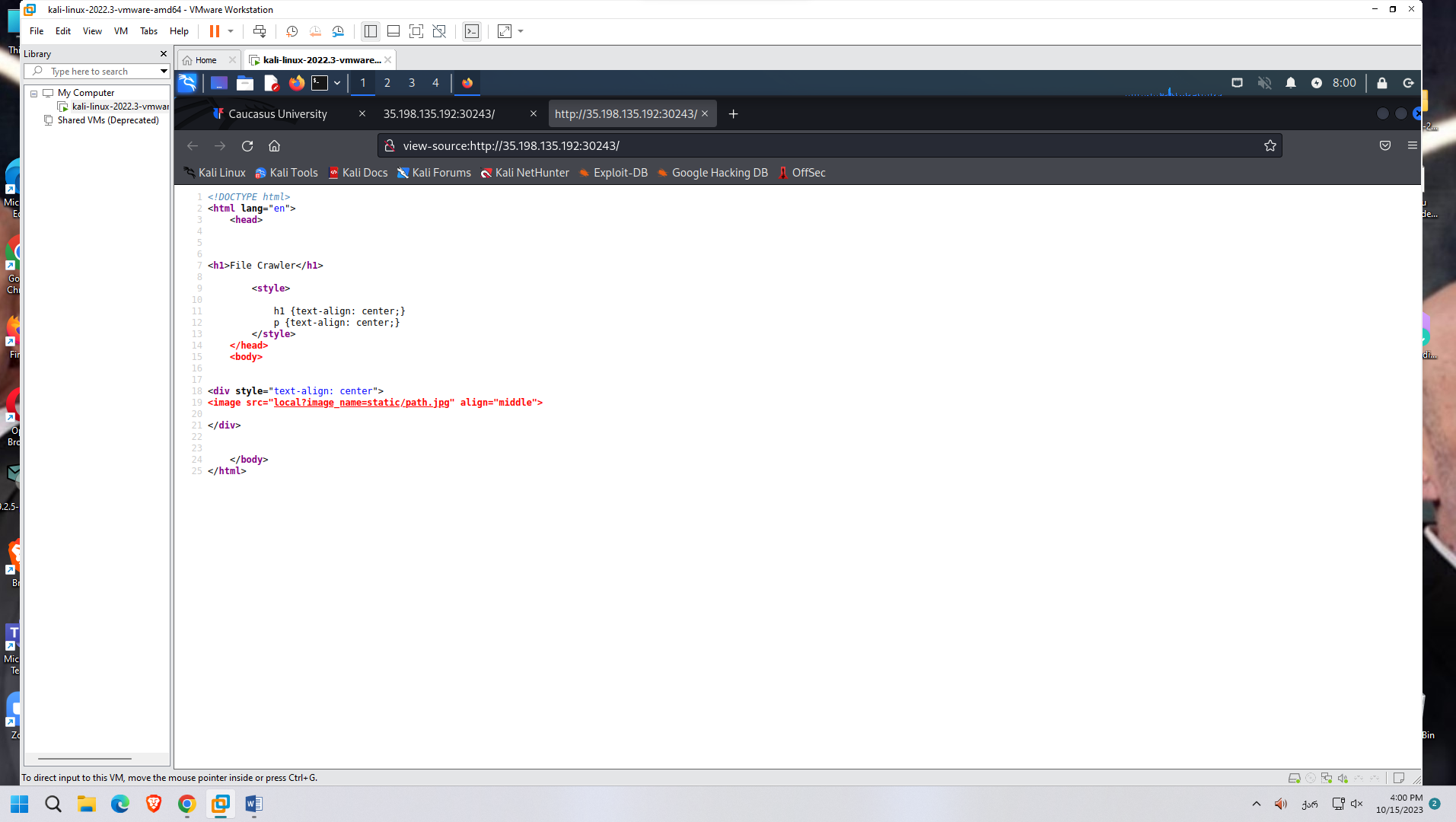
კონსტანტინე სალუქვაძე

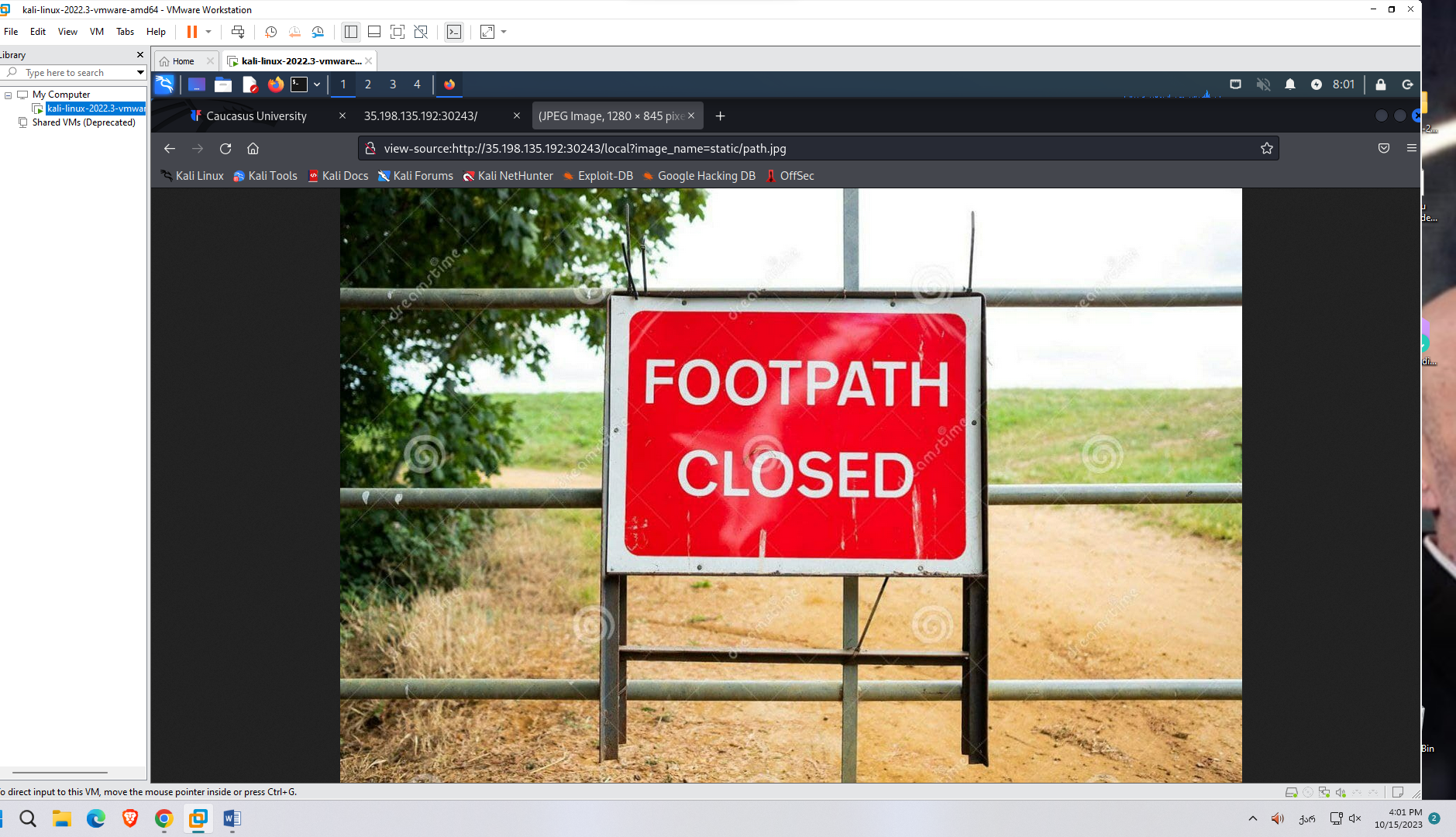
Lab:file-crawler

1. 

2.view-pagesource – access რომ მოგცვეს ფოტოზე

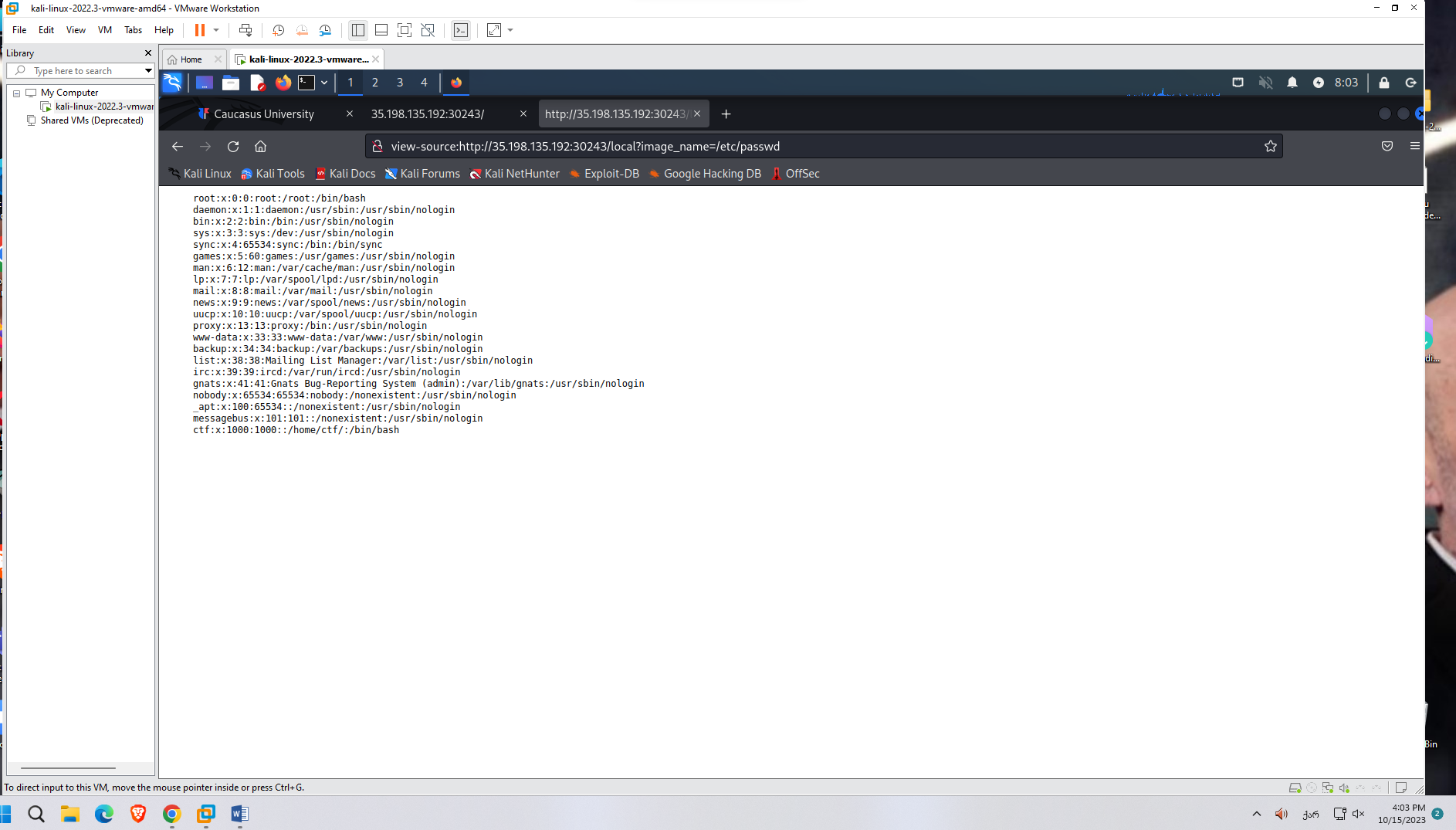
3. 

4. გადავდივართ ფოტოს ლინკზე

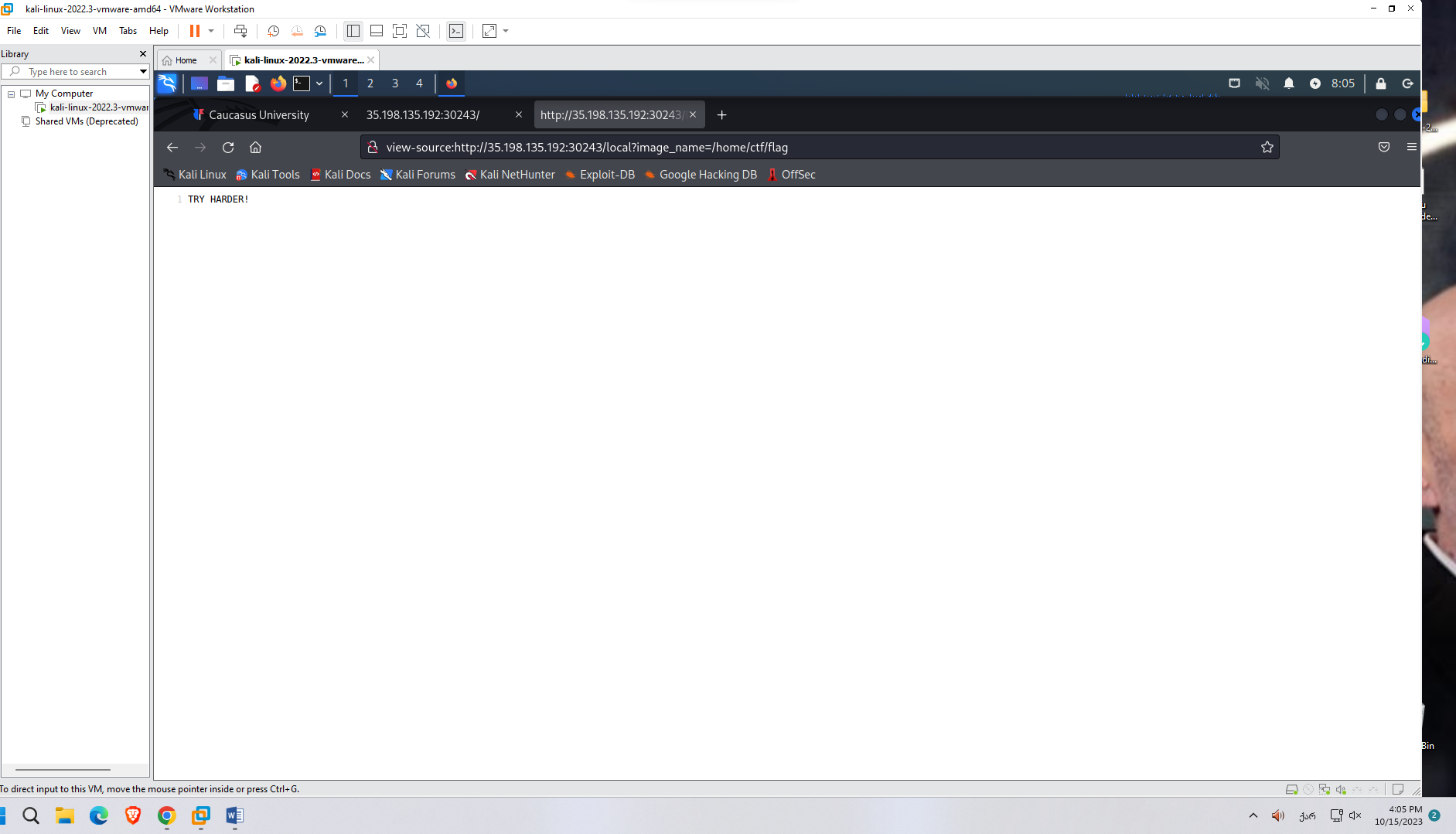


5.ვაკვირდებით url-s და ვნახულობთ რამე restriction თყ ადევს სხვადასხვა char-ებს

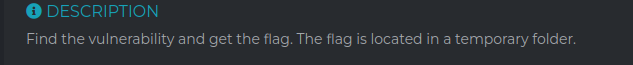
6.მაგალითად შეგვიზლია ვცადოთ /etc/passwd სადაც ინფო ინახება ხოლმე



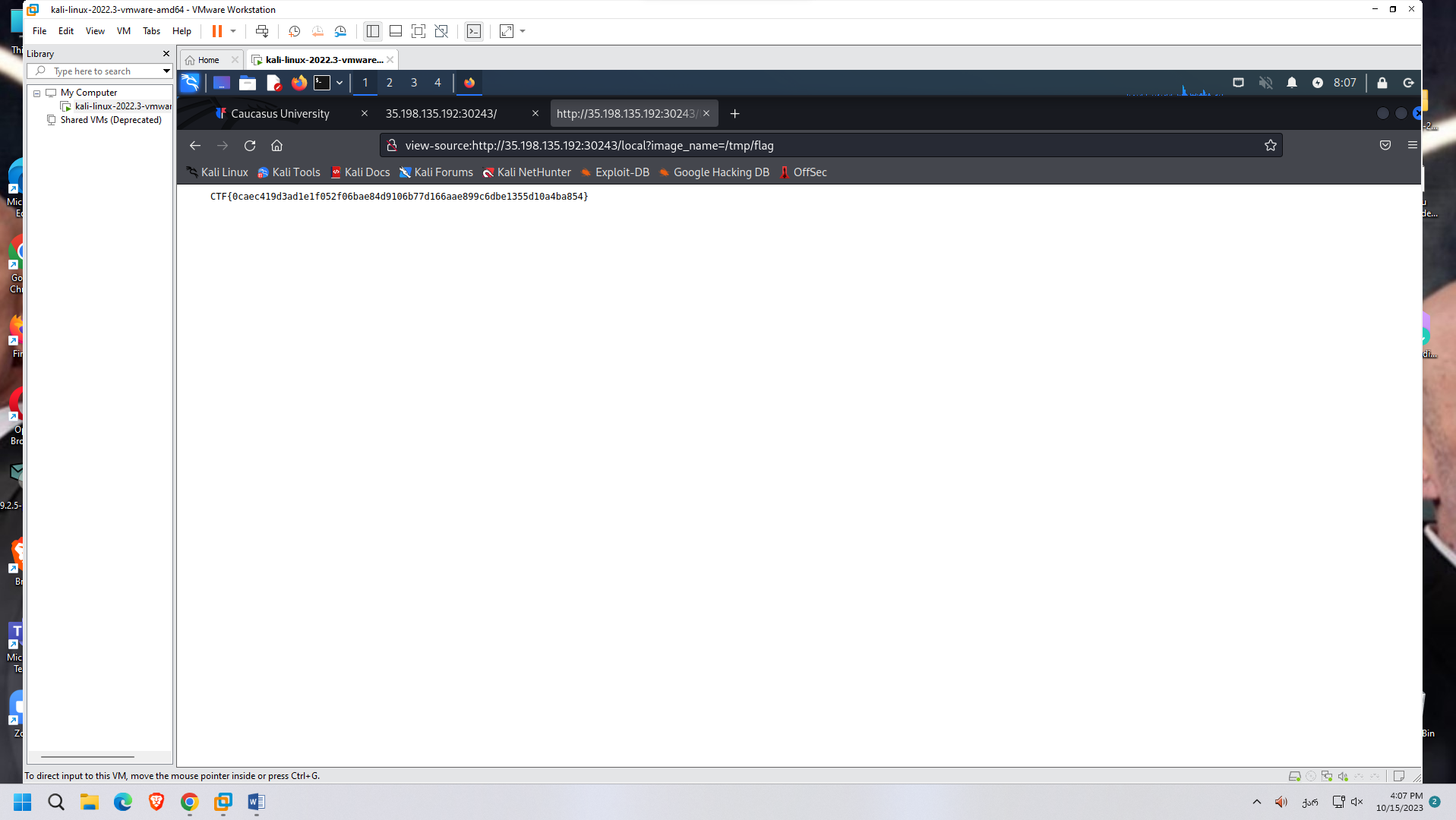
7.  ვტესტათ ამას url-ში და ვიღებთ შემდეგ pageს

8. 

8. ახლოს ვართ და ვნახულობთ რომ არანაირი restriciotn არ არდესვ url-ს fields-ს და შეგვიძ₾ია მისი დახმარებით ნავიგაცია.

9. ასევე lab-ის page-ზე გვაქ tip: 

10. ეს გვეუბნება რომ flag aris temporray file-ში

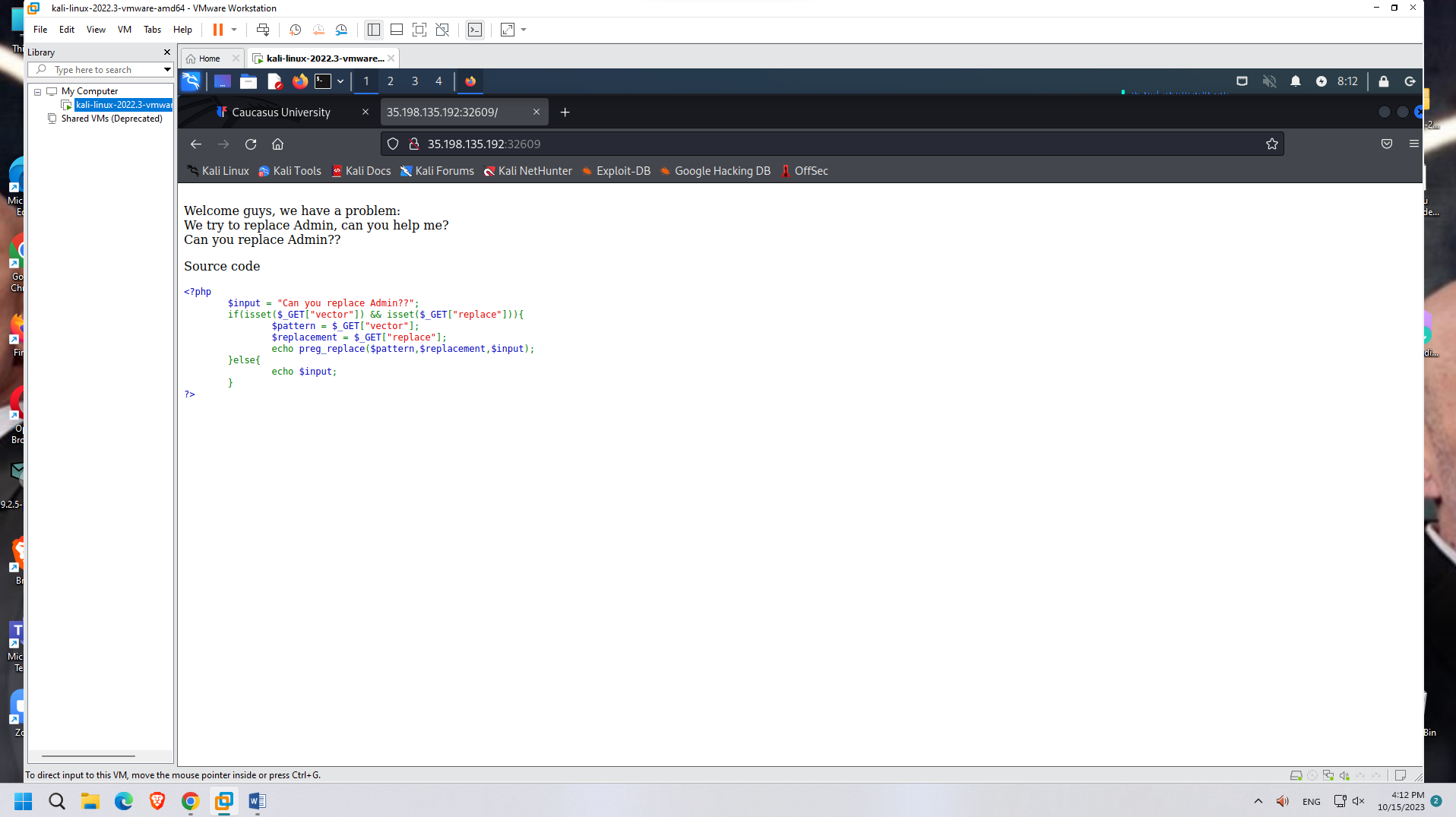
11. 

შემდეგი კომანდა გვაძლევს პასუხს /tmp/flag

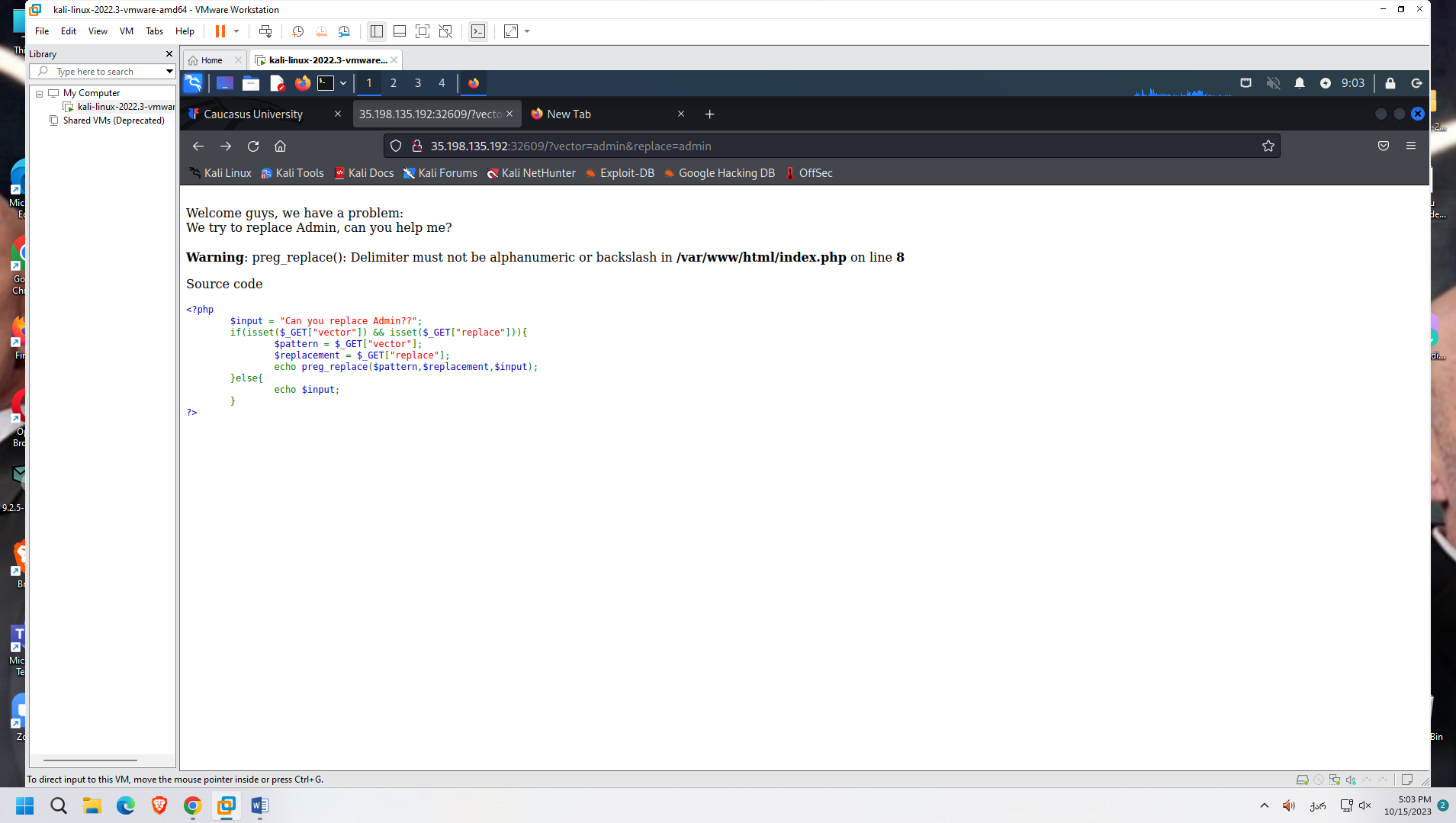
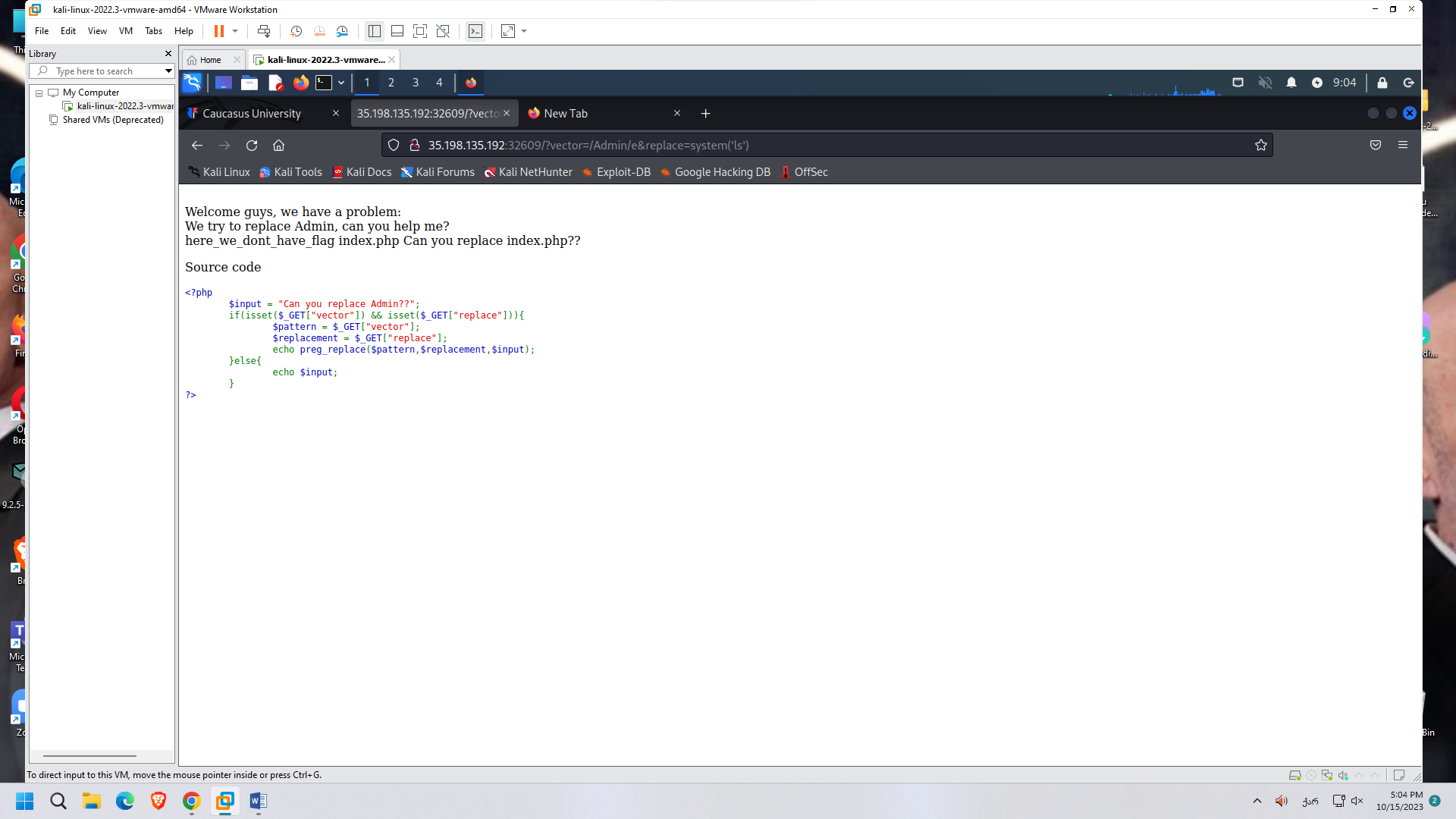
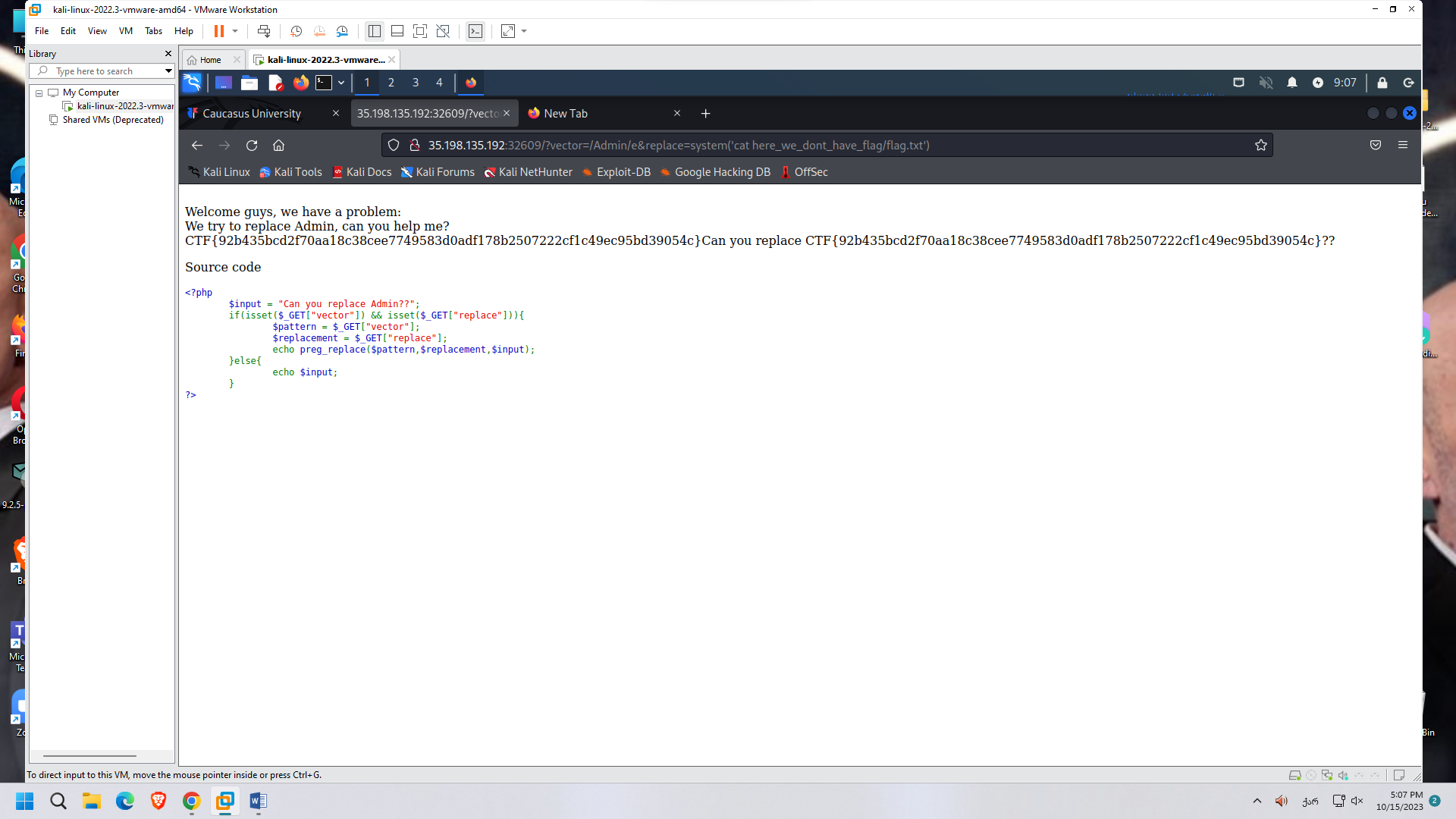
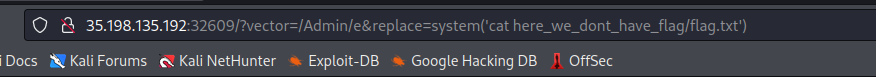
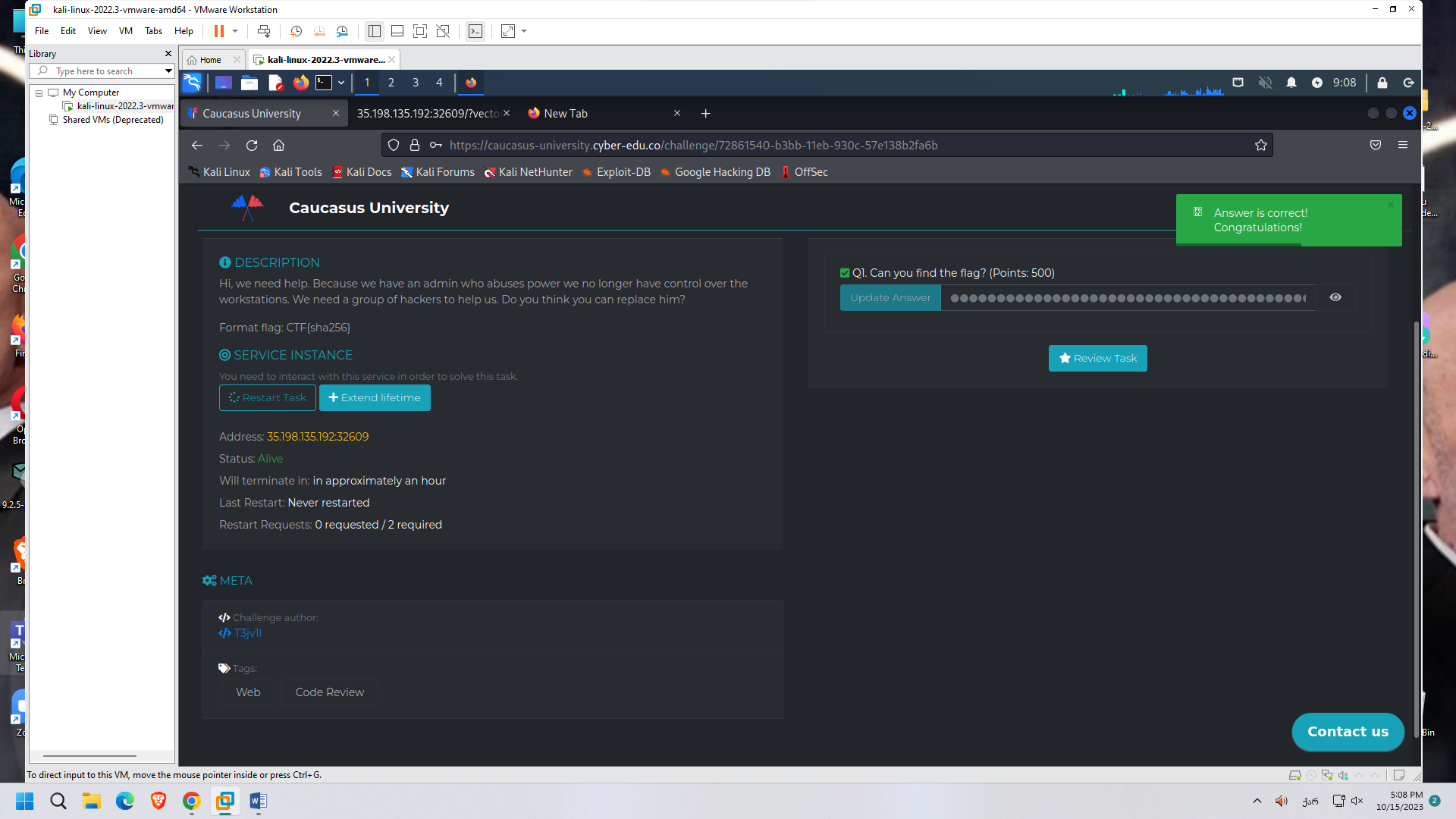
12. ამის თავიდან ასაცილებლად ყველაზ ემარტივი გზა არის რო char-ს ან თუნდაც სიტყვებს restiricion დაედოს , საიტის ქონდეს ssl certificate რო http გარდაიქმნას https-ze

Lab:sabtitute

1.



2PREG\_ REPLACCE ზე შეგვიძლია მანიპულირება

1. 
2. ვხედავთ რომ URL-ის საშუალებით შეგვიძ₾ია მანიპულირება
3. 
4. გამოვიყენეთ LS-ი და ვანხეთ რომ გავქვს here\_we\_dont\_have\_flag
5. ვიყენებთ cat ფუნქციას რათა flag.txt-ში ვნახოთ ჩვენი ctf-ი
6. 
7. 
8. 

.