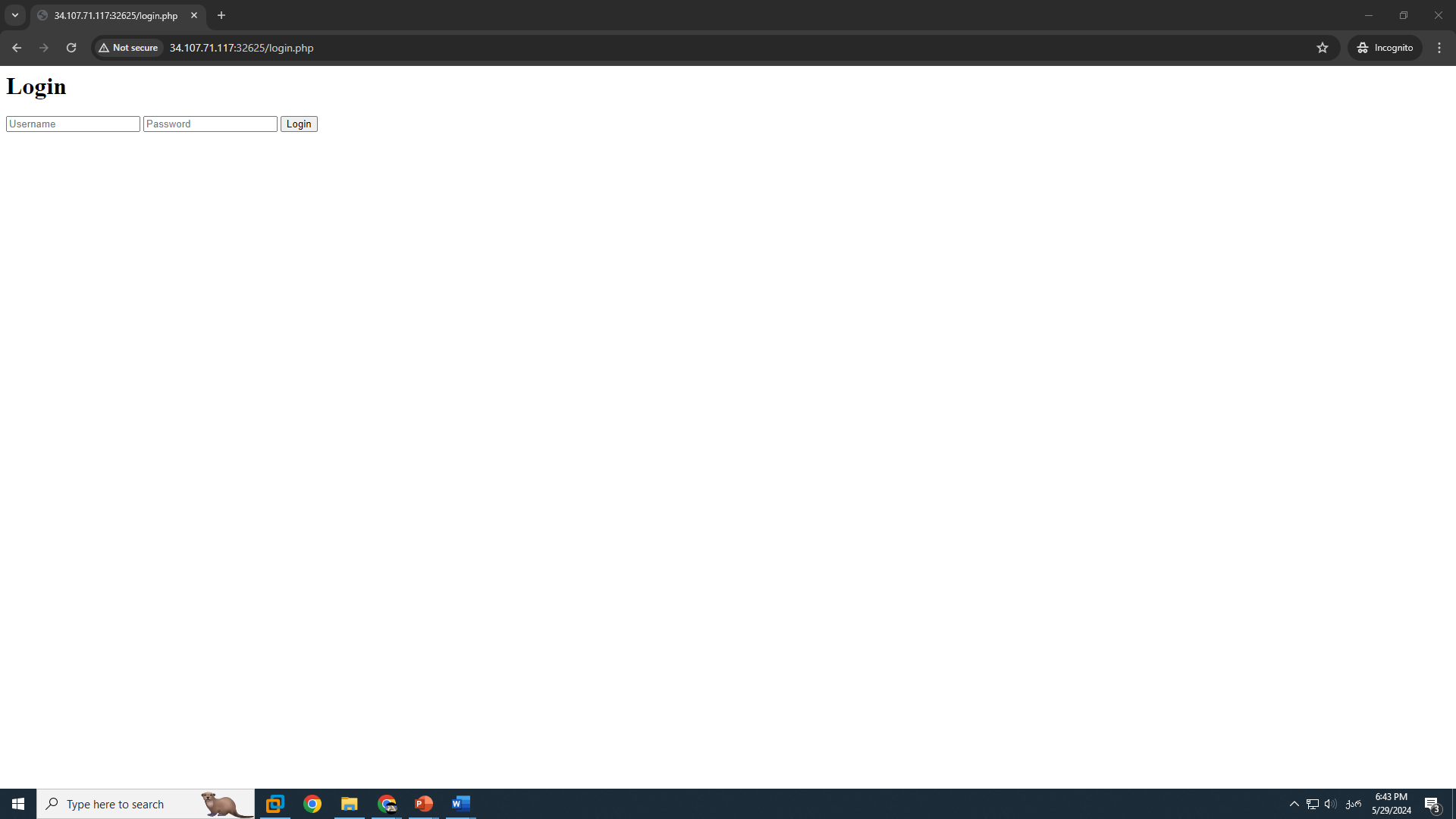
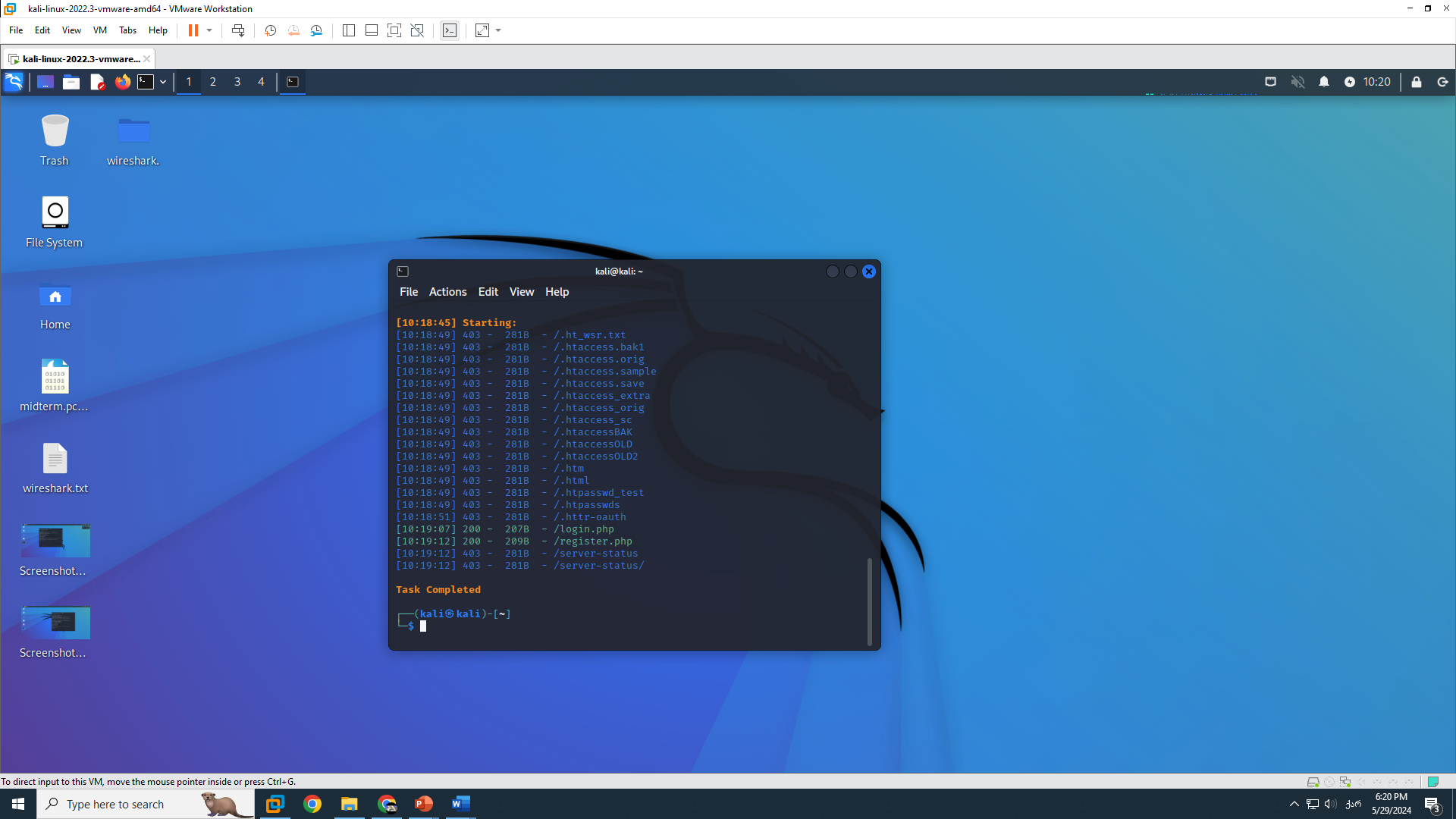
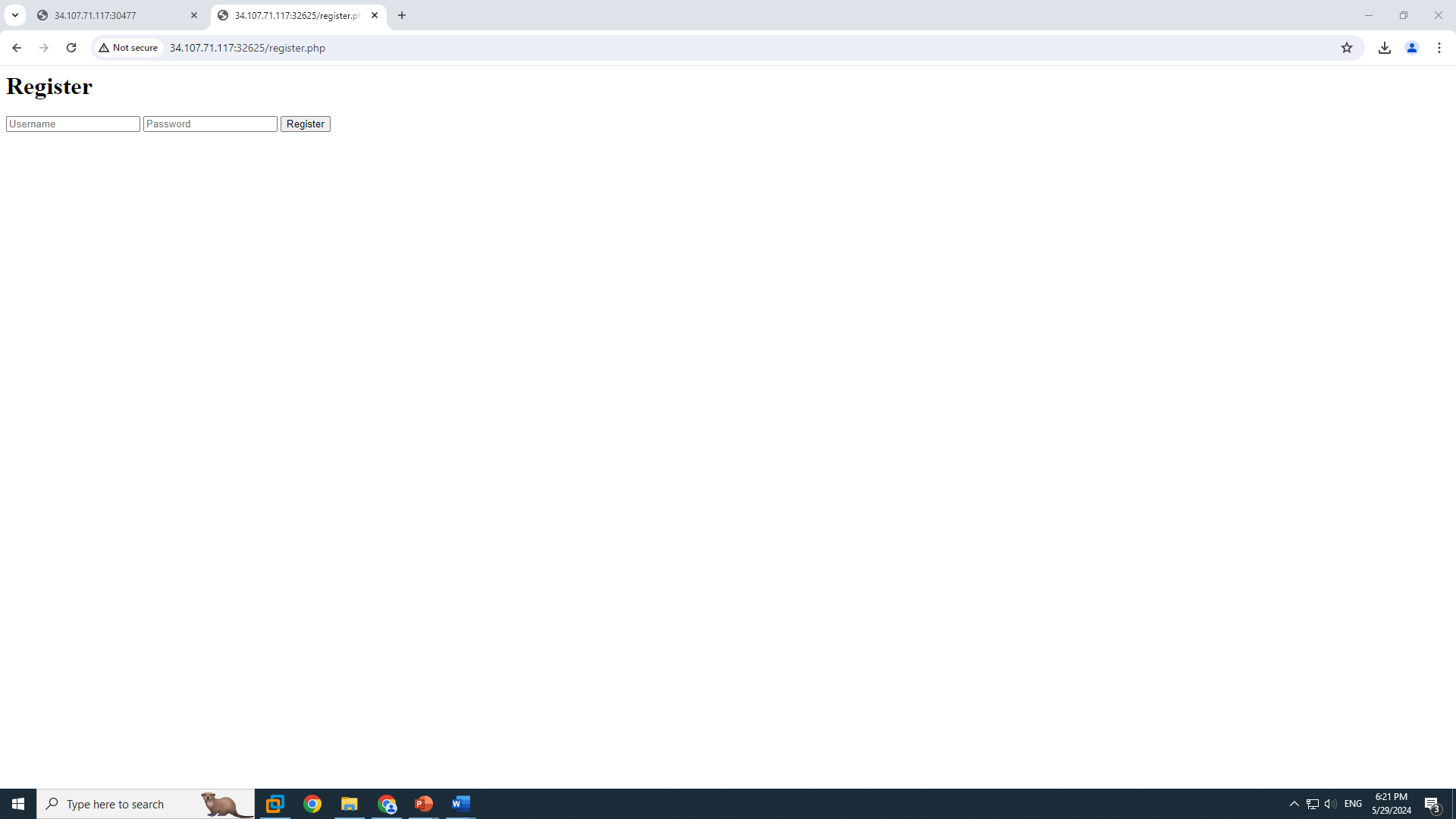
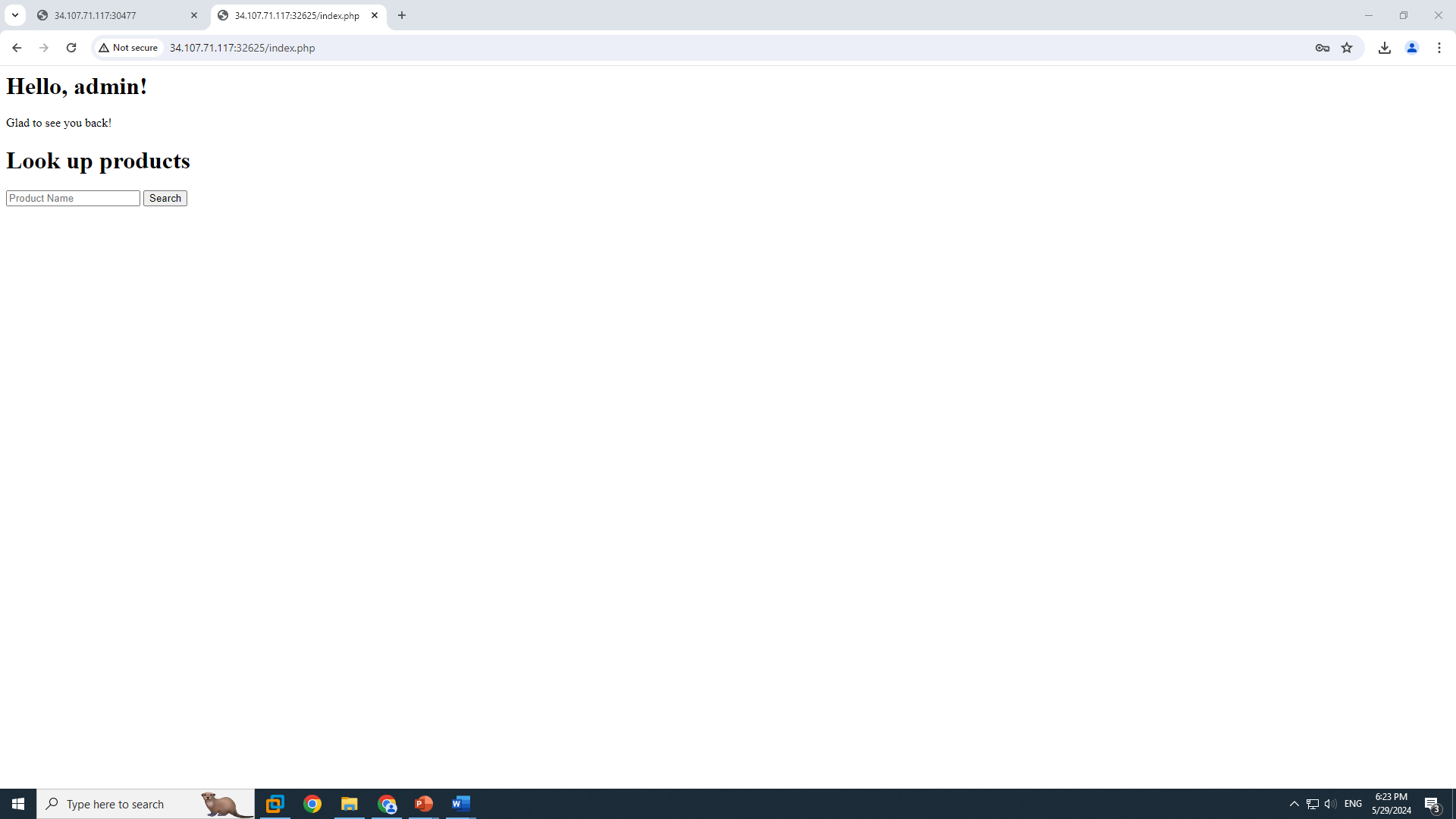
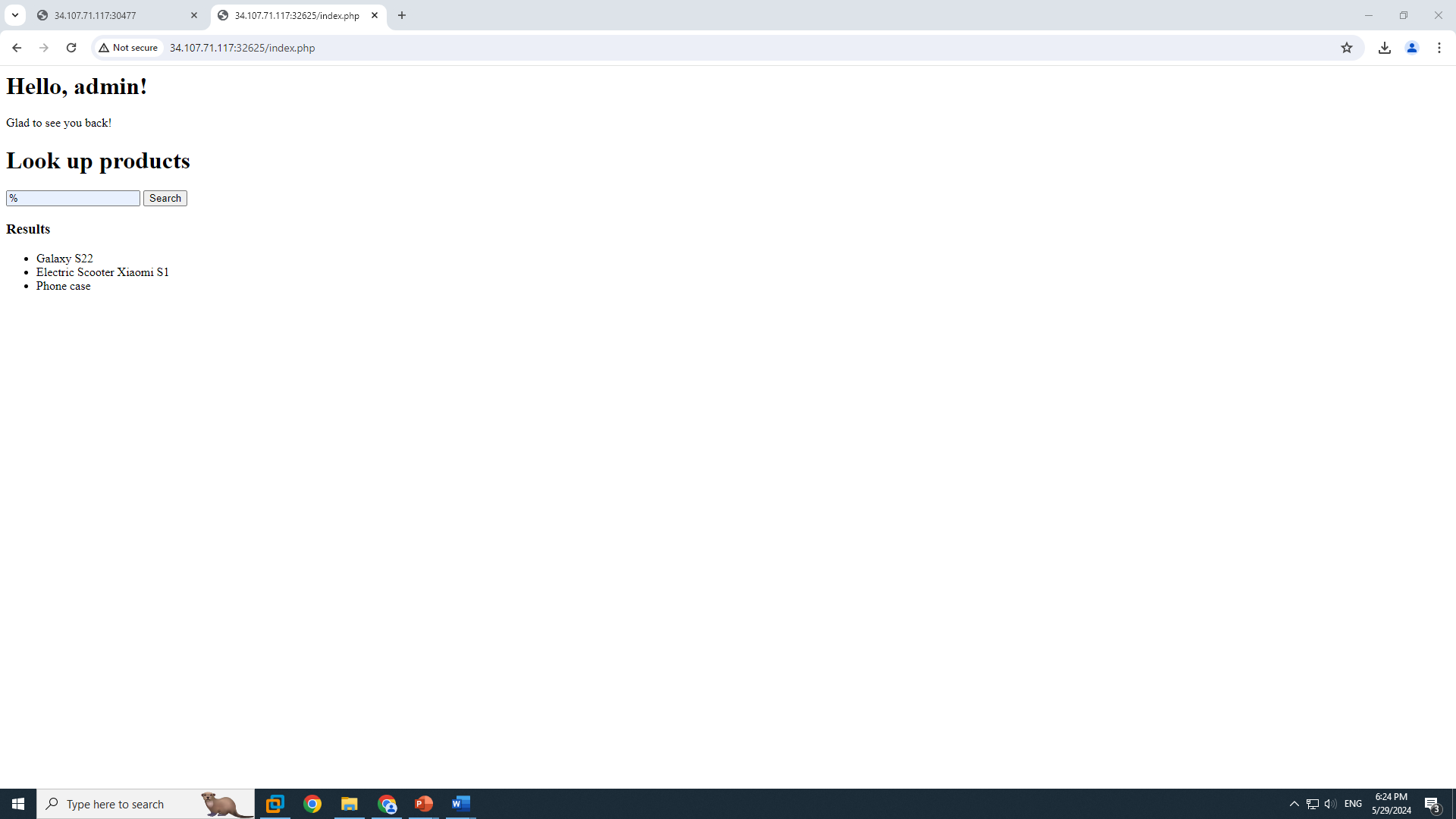
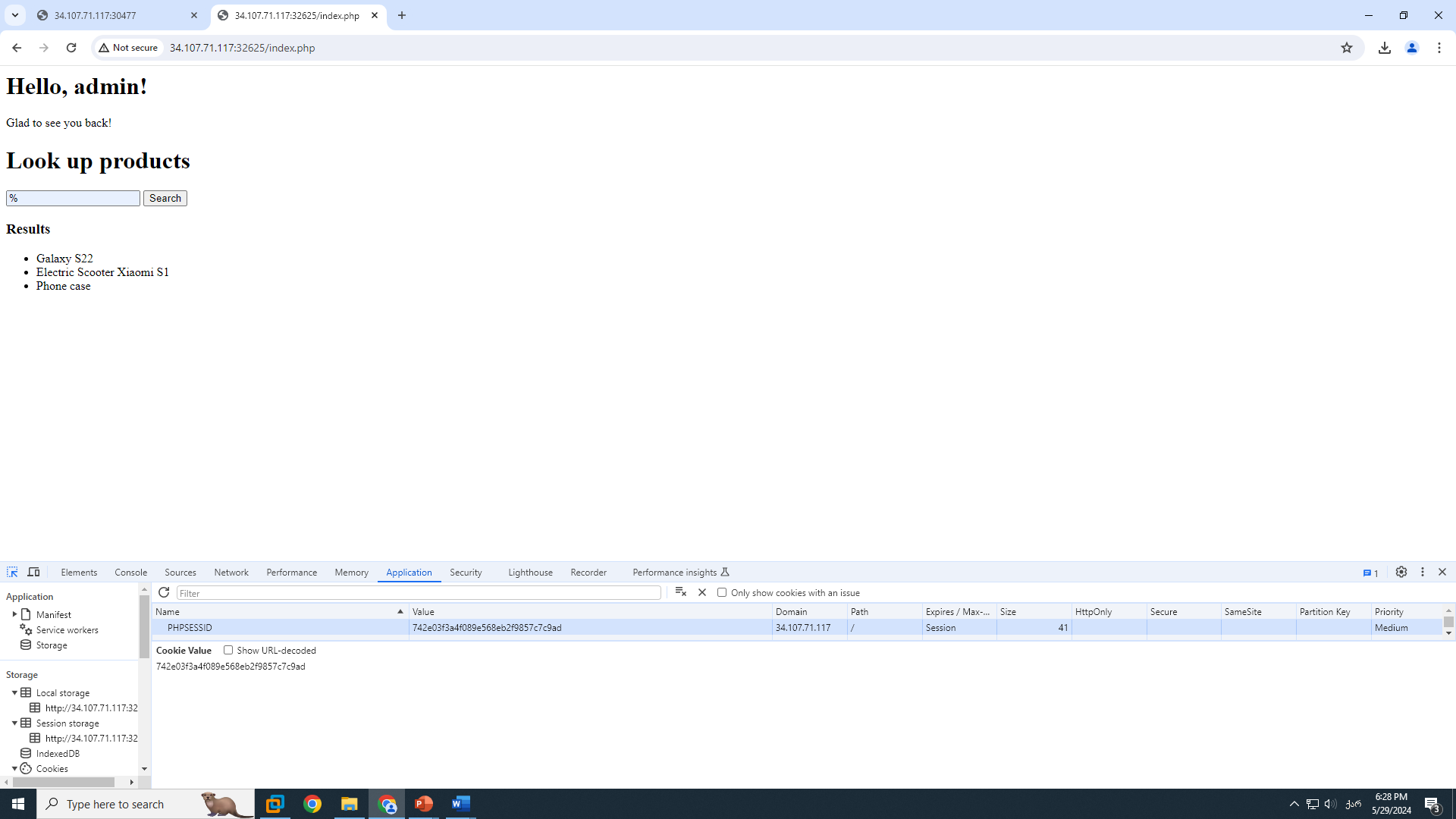
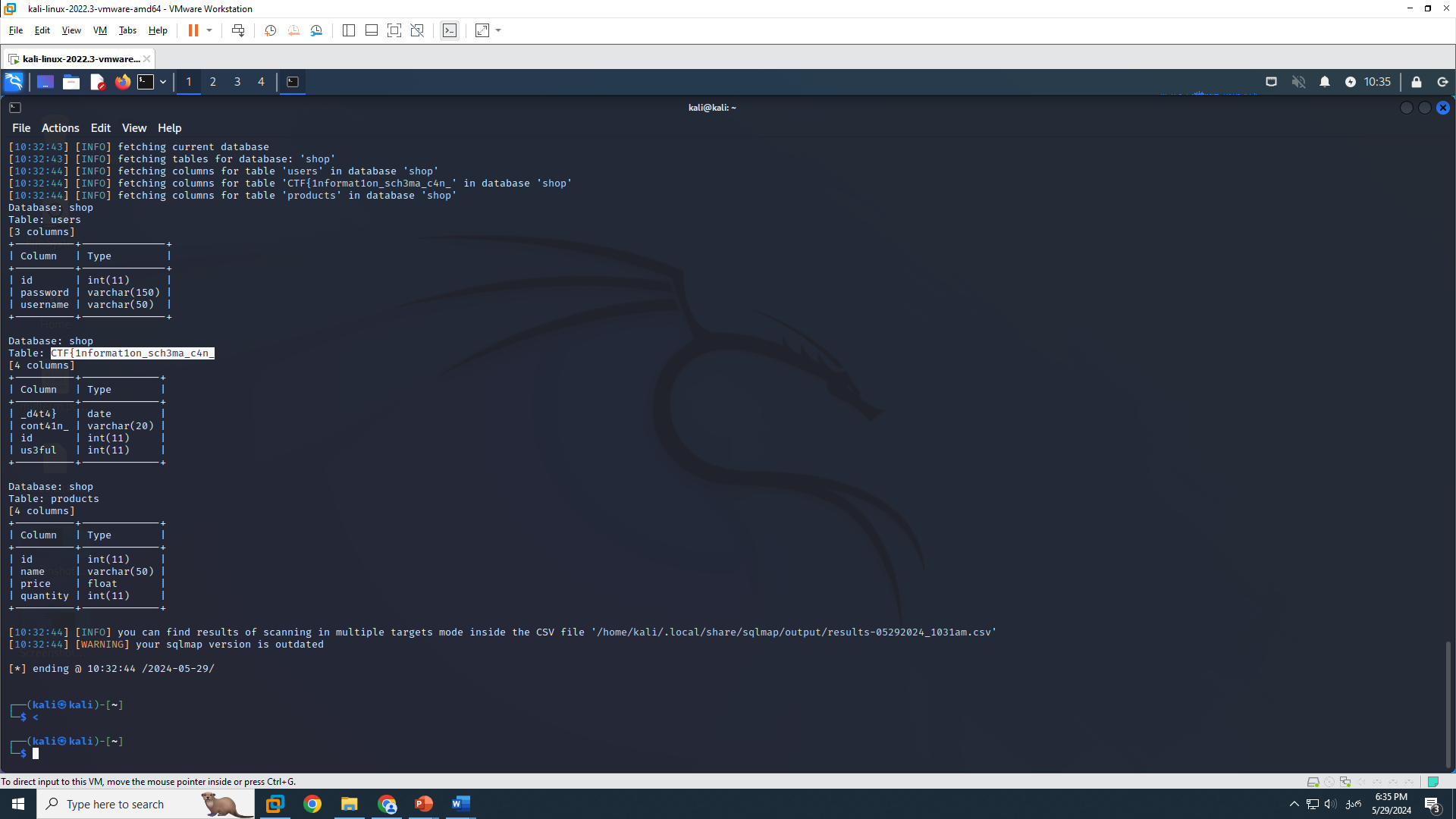
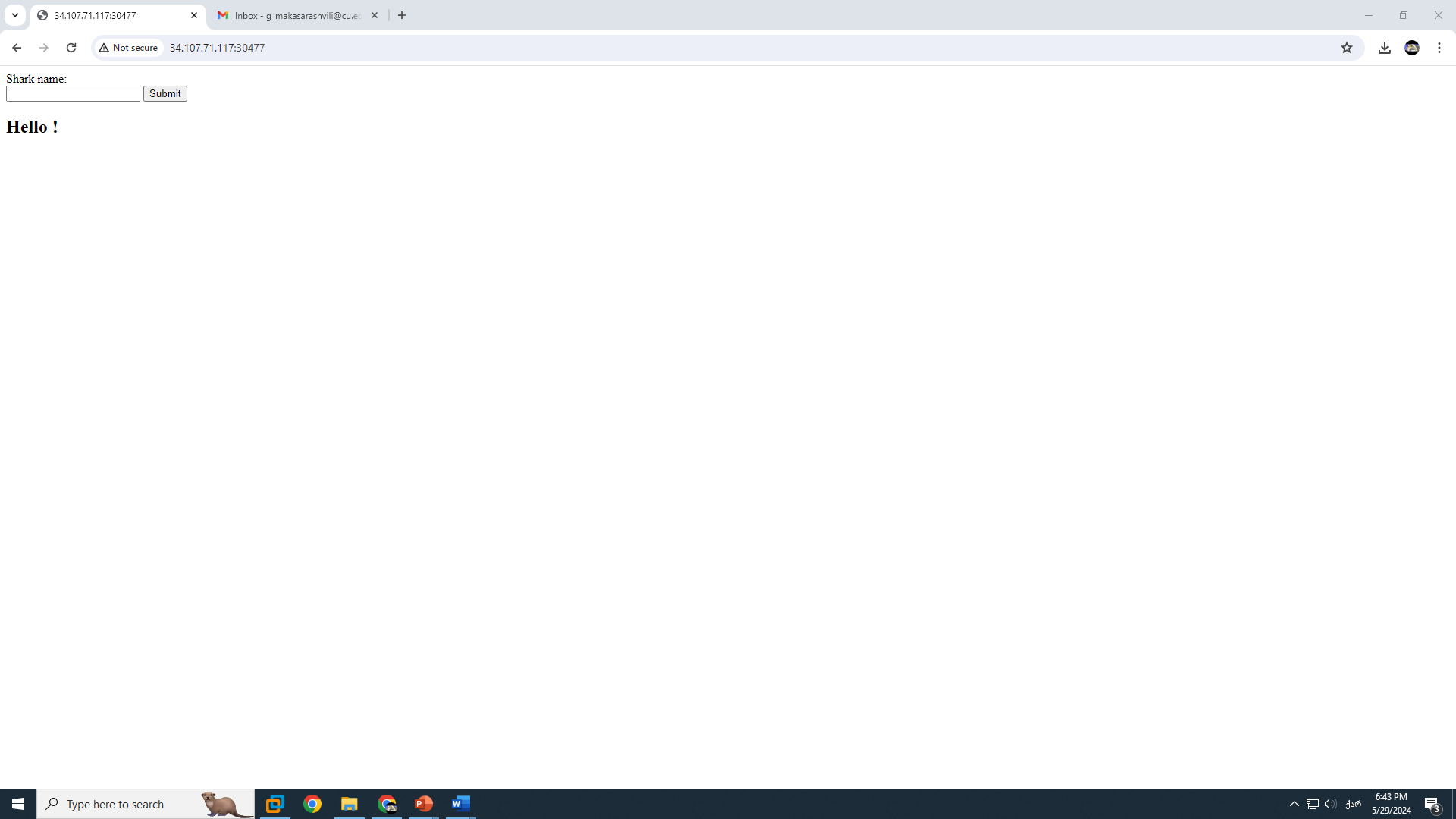
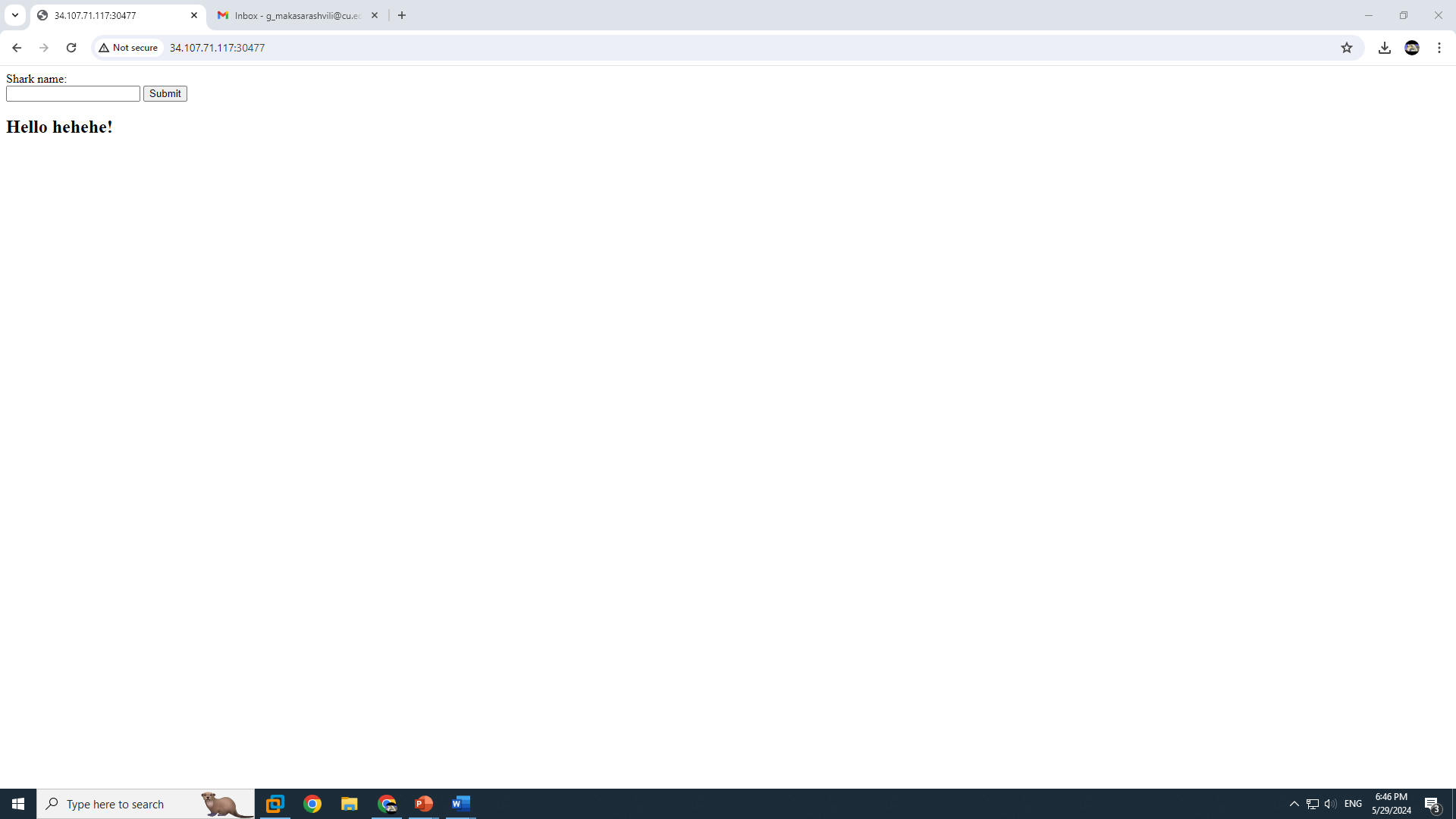
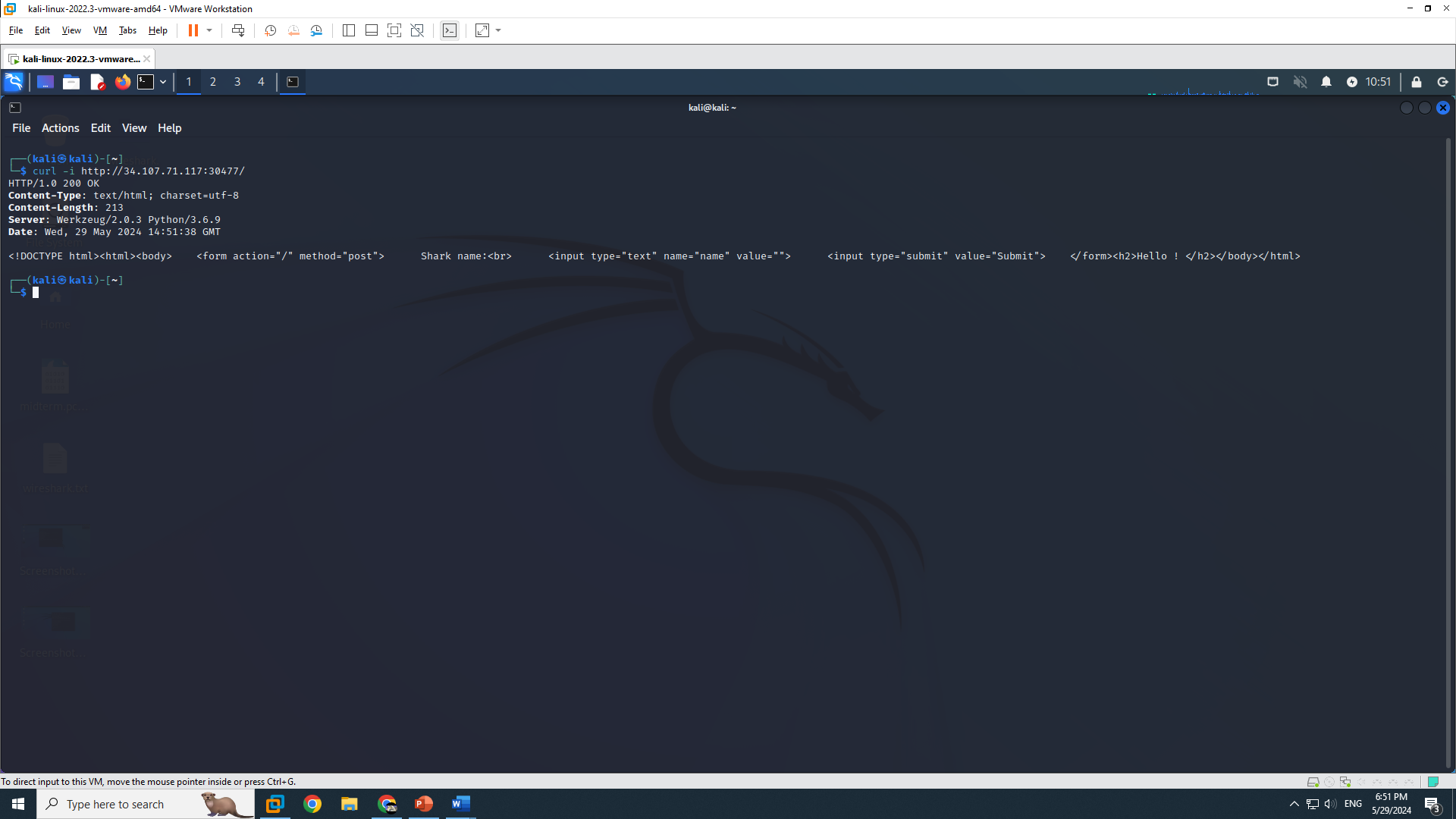
სიმულაციური 2: გიორგი მაკასარაშვილი  
  
  
ლაბი:   
მოცემულ აიპი მისამართზე შესვლისას ვხედავთ შემდეგ სურათს  
პირველ რიგში უნდა მოვიძიოთ რაც შეიძლება მეტი ინფორმაცია. ამის ერთ-ერთი საშუალებაა dirseach. მისი გამოყენების შედეგად თვალში გვხვდება რამდენიმე დეტალი. ერთ-ერთია რეგისტრაციის გვერდი.ამ გვერდზე გადასვლისას ვხედავთ შემდეგ სურათსვცადოთ რეგისტრაცია სახელი:admin პაროლი:Giorgi  
ამის შემდეგ ვცადოთ login  
input ველში ვცადოთ სხვადასხვა მნიშვნელობების ჩაწერა. მაგალითისთვის როგორც ჩანს %ის ჩაწერის დროს ყველანაირ პროდუქტს გვაჩვენებს, რაც იმას ნიშნავს რომ საიტი მოწყვლადია SQLi injection-ის მიმართ.  
ახლა შევამოწმოთ cookie, რადგან ვნახოთ დალოგინებისას რაიმე თუ შეინახა იქ. რაღაც გვაქახლა ის უნდა გამოვიყენოთ sql injection-ში, რომლესაც sqlmap-ის საშუალებით ვიზავთ.  
sqlmap --cookie="PHPSESSID=742e03f3a4f089e568eb2f9857c7c9ad" -u http://34.107.71.117:32625/index.php --forms --columns --random-agent ბრძანების გაშვების შემდეგ ვიღებთ შედეგს სადაც ცხრილის სახელად ვხედავთ ctf-ის ნაწილს CTF{1nformat1on\_sch3ma\_c4n\_ , ხოლო მეორე ნაწილი იმავე ცხრილში სვეტში ერთ-ერთი მნიშვნელობაა: \_d4t4}  
 CTF{1nformat1on\_sch3ma\_c4n\_d4t4}  
  
  
  
  
ლაბი: shark  
მოცემულ მისამართზე შესვლისას ვხედავთ მხოლოდ ერთ input ველსამ ველში ნებისმიერი რამის ჩაწერის დროს, იგივე რამ გვიბრუნდება უკანცოტა 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()}

