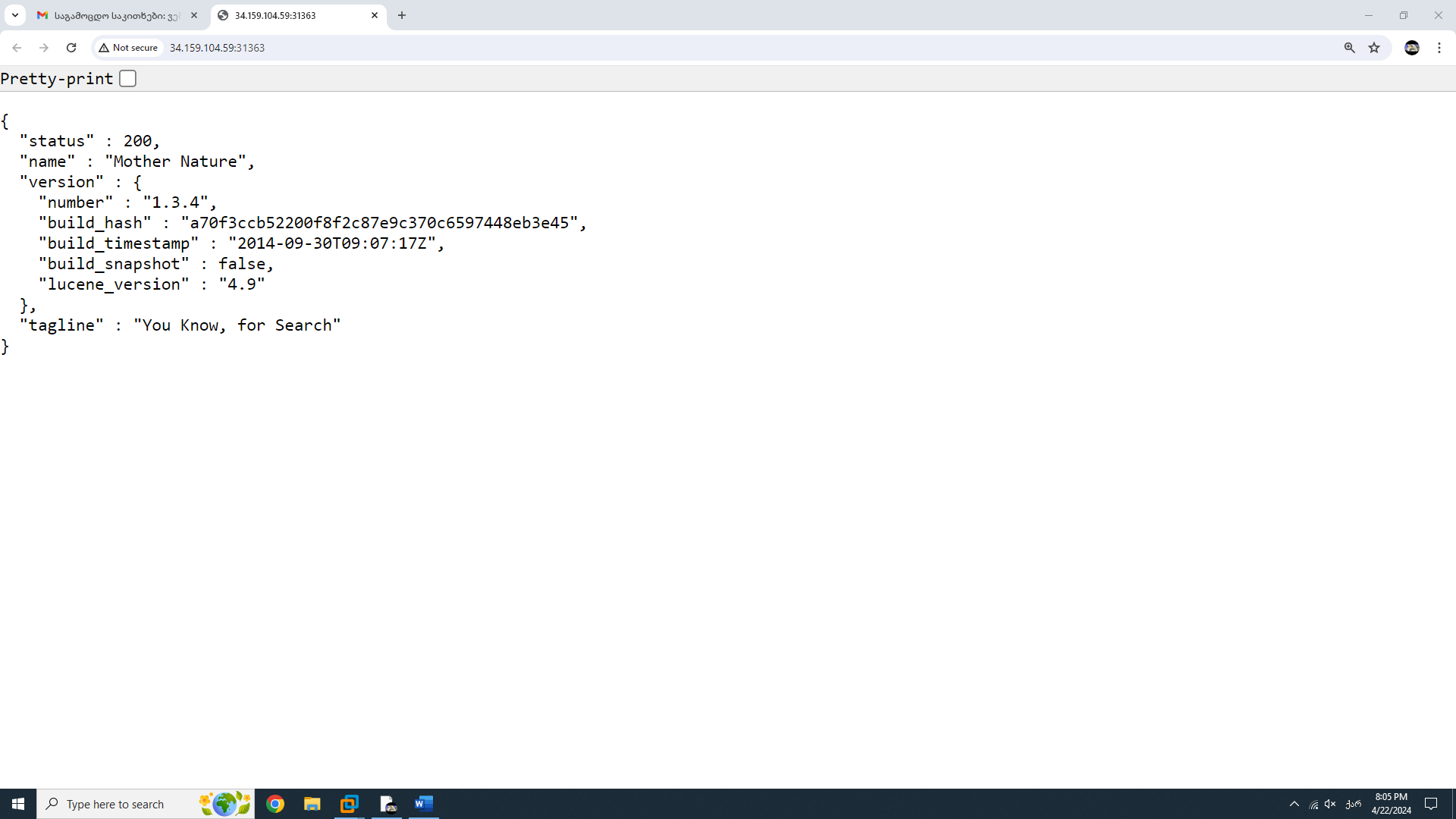
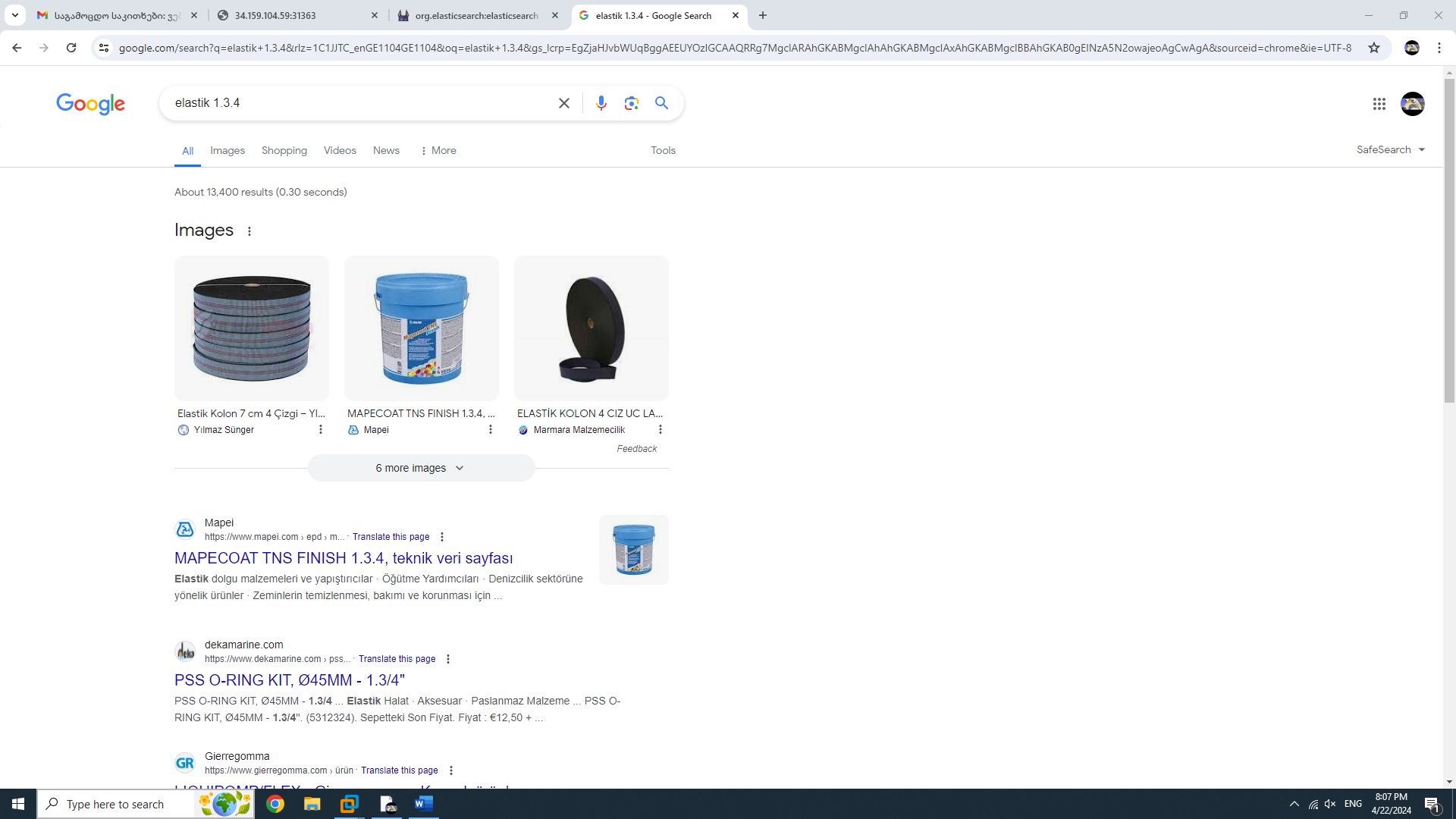
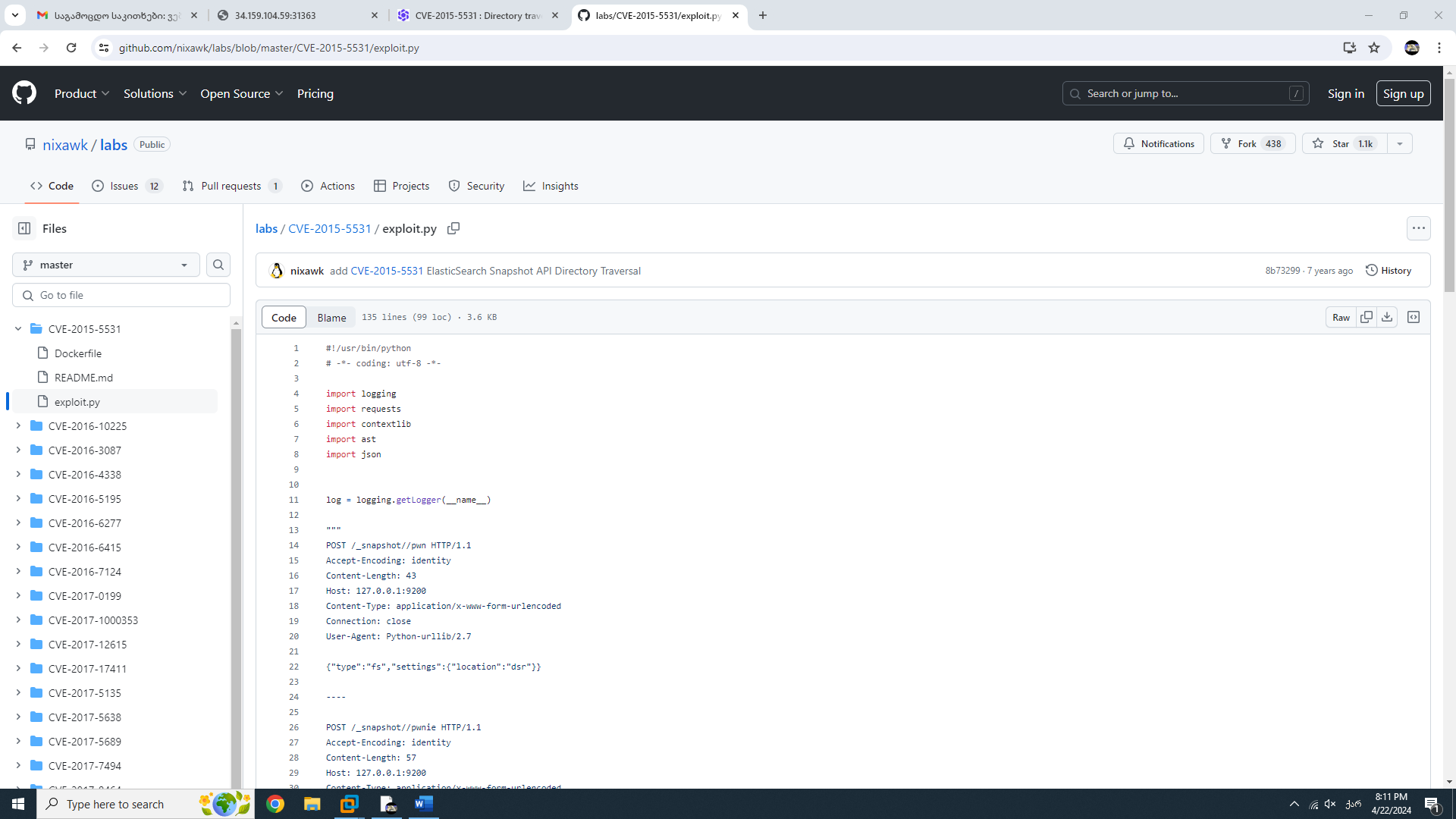
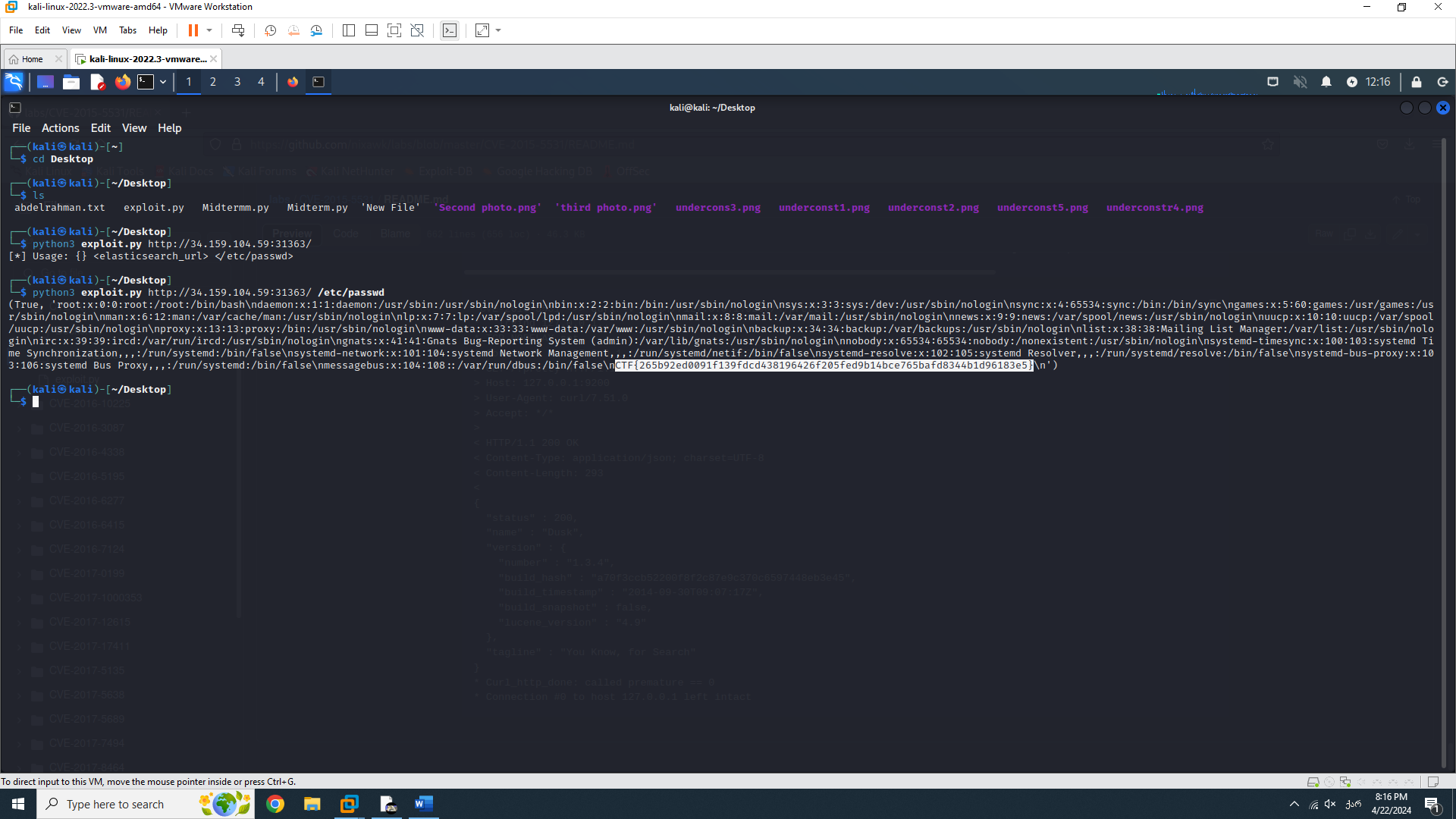
შუალედური: გიორგი მაკასარაშვილი

LAB: elastic

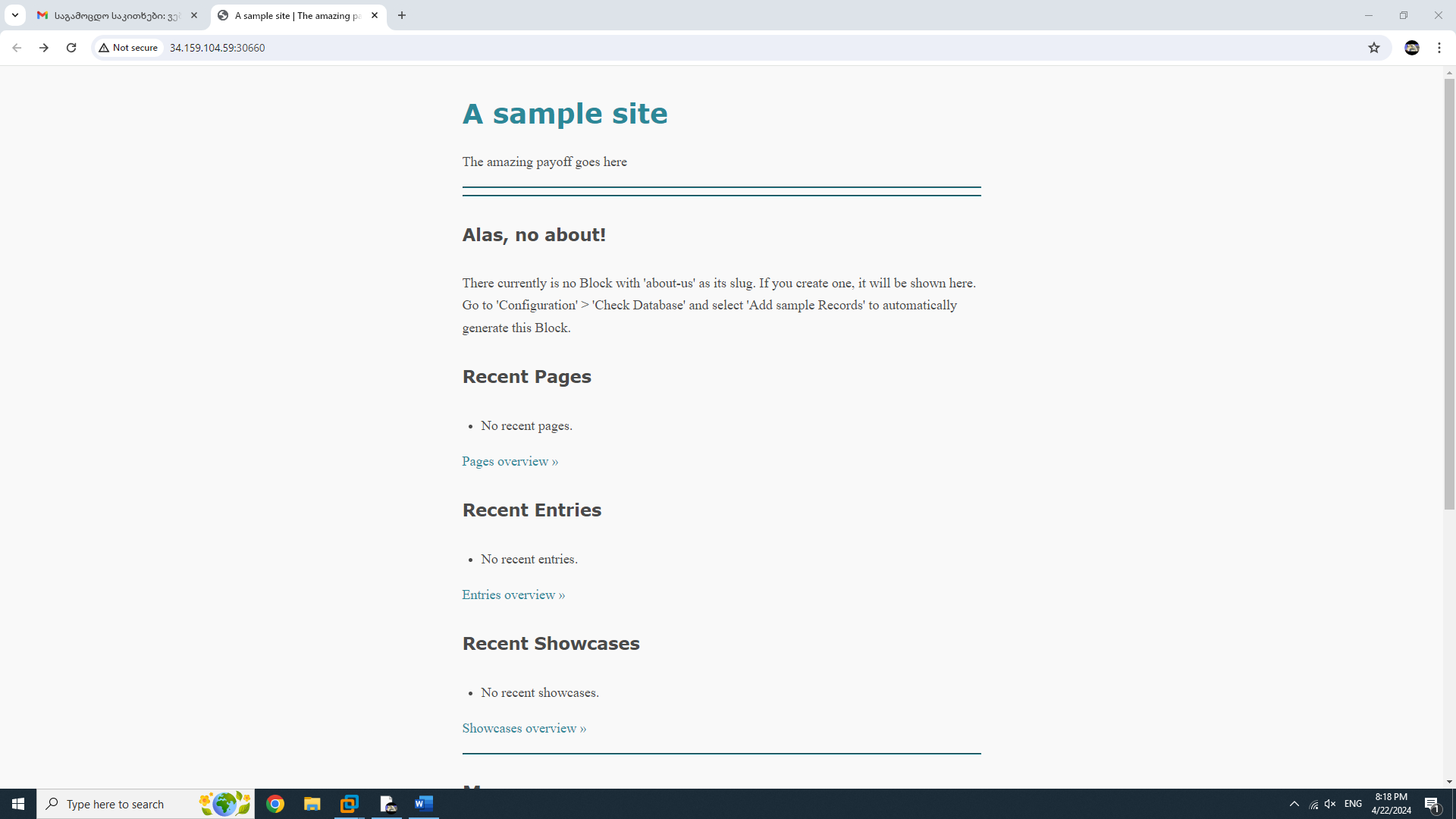
მოცემულ IP მისამართზე შესვლისას ვხედავ მოცემულ შედეგსუკვე ერთი შეხედვით საკმაოდ დიდ ინფორმაციას ვიღებთ. ერთ-ერთი ყველაზე მნიშვნელოვანია ვერსია. როგორც ვხედავთ ვერსიის ნომერია 1.3.4 ამიტომ ვცდილობთ მივიღოთ ინფორმაცია ელასტიკის 1.3.4 ვერსიის შესახებ.  
Elastic 1.3.4 -ის გუგლში მოძებნის შედეგად ვიღებთ ქვემოთ მოცემულ სურათს რაც ნამდვილად არ გვჭირდება

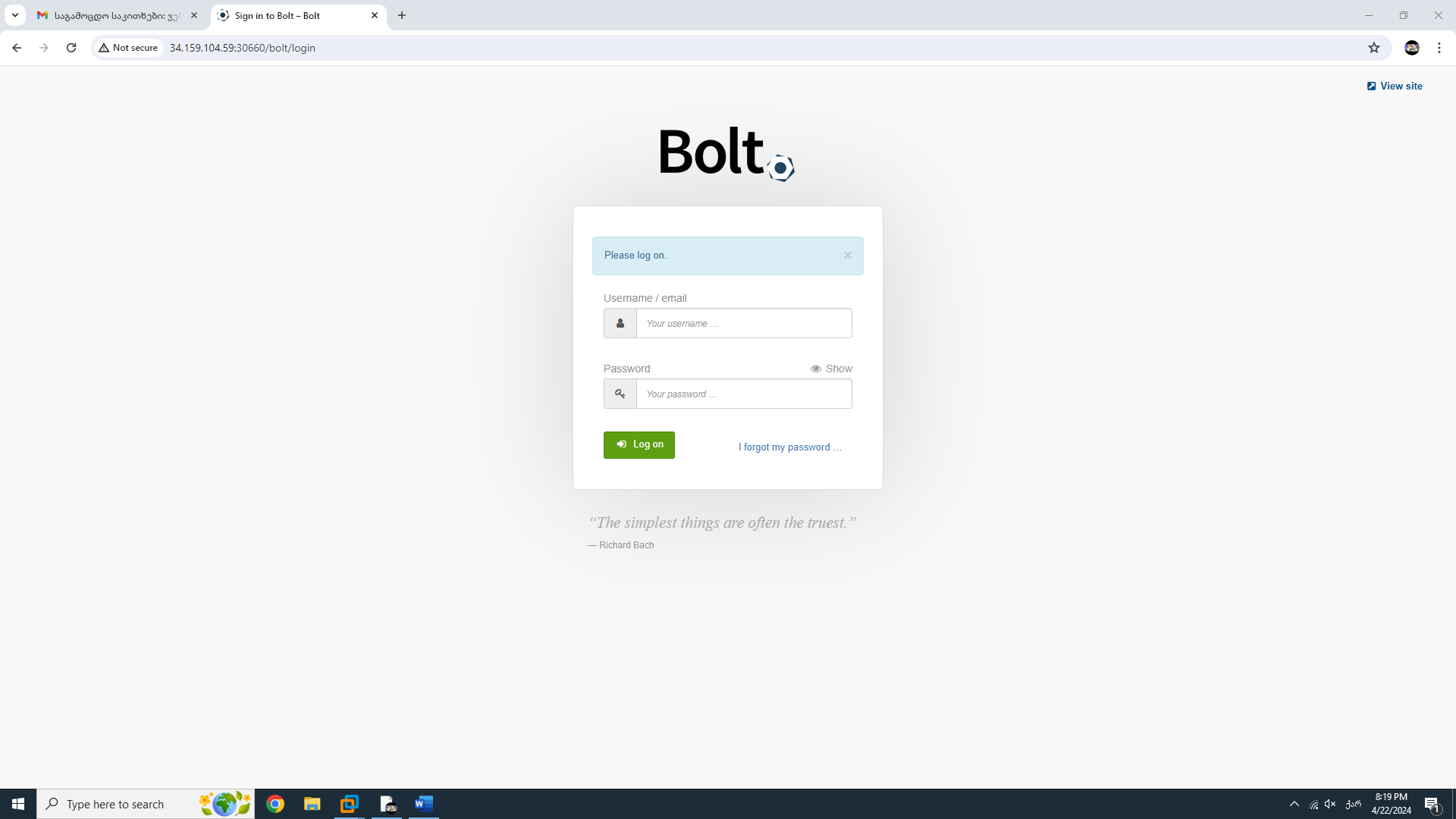
ამიტომ ვცდილობთ მოვძებნოთ აღნიშნული ვერსიის სისუსტეები. მცირე ძებნის შემდეგ გადავაწყდებით CVE-2015-5531 -ს რაზეც უკვე არსებობს exploit 

ამ კოდის გაანალიზების შემდეგ ვხვდებით რომ მის გამოსაყენებლად საჭიროა შემდეგი ბრძანების გამოყენება: python3 exploit.py http://34.159.104.59:31363/ /etc/passwd

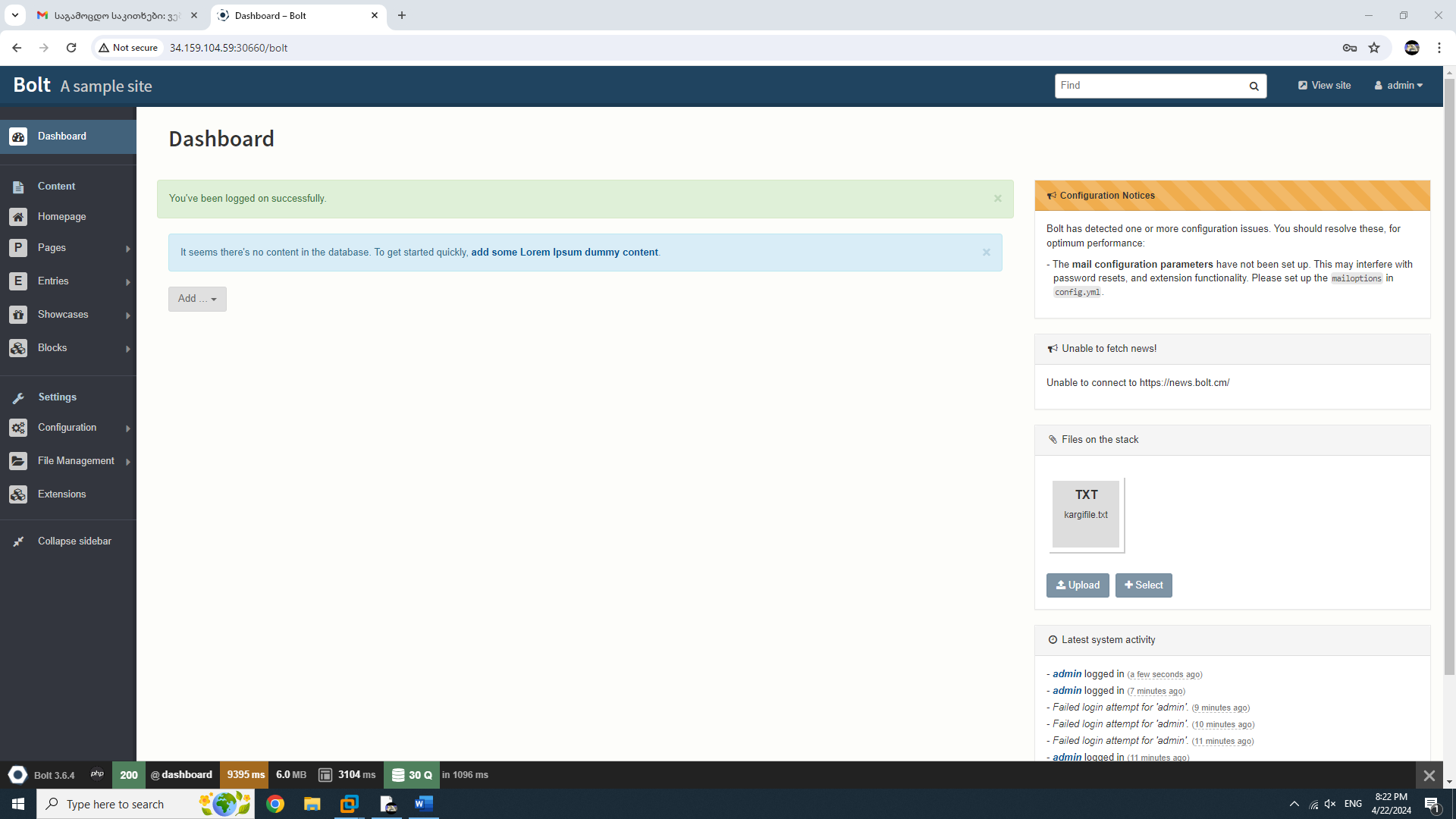
და აი ჩვენი CTF-იც

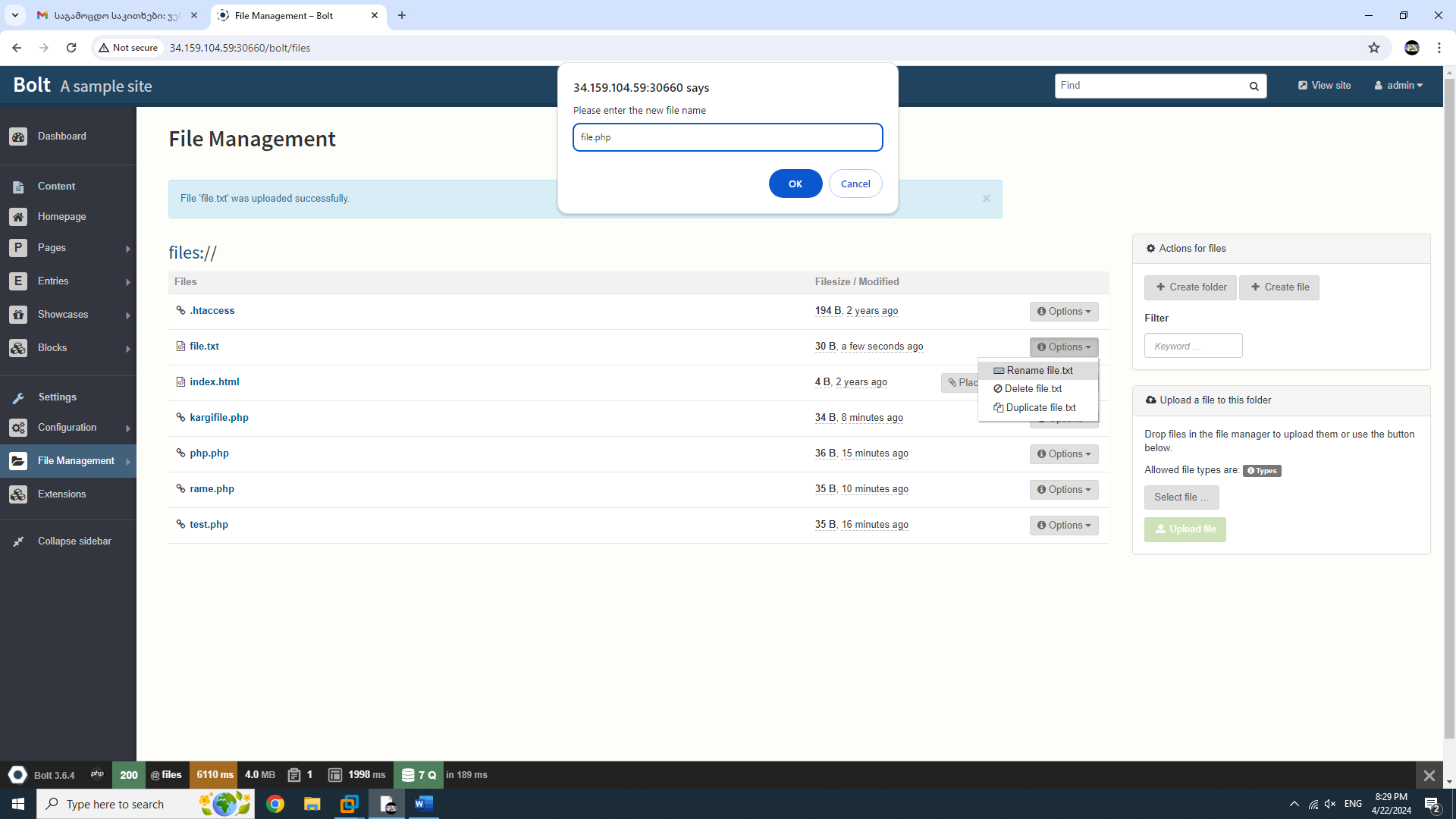
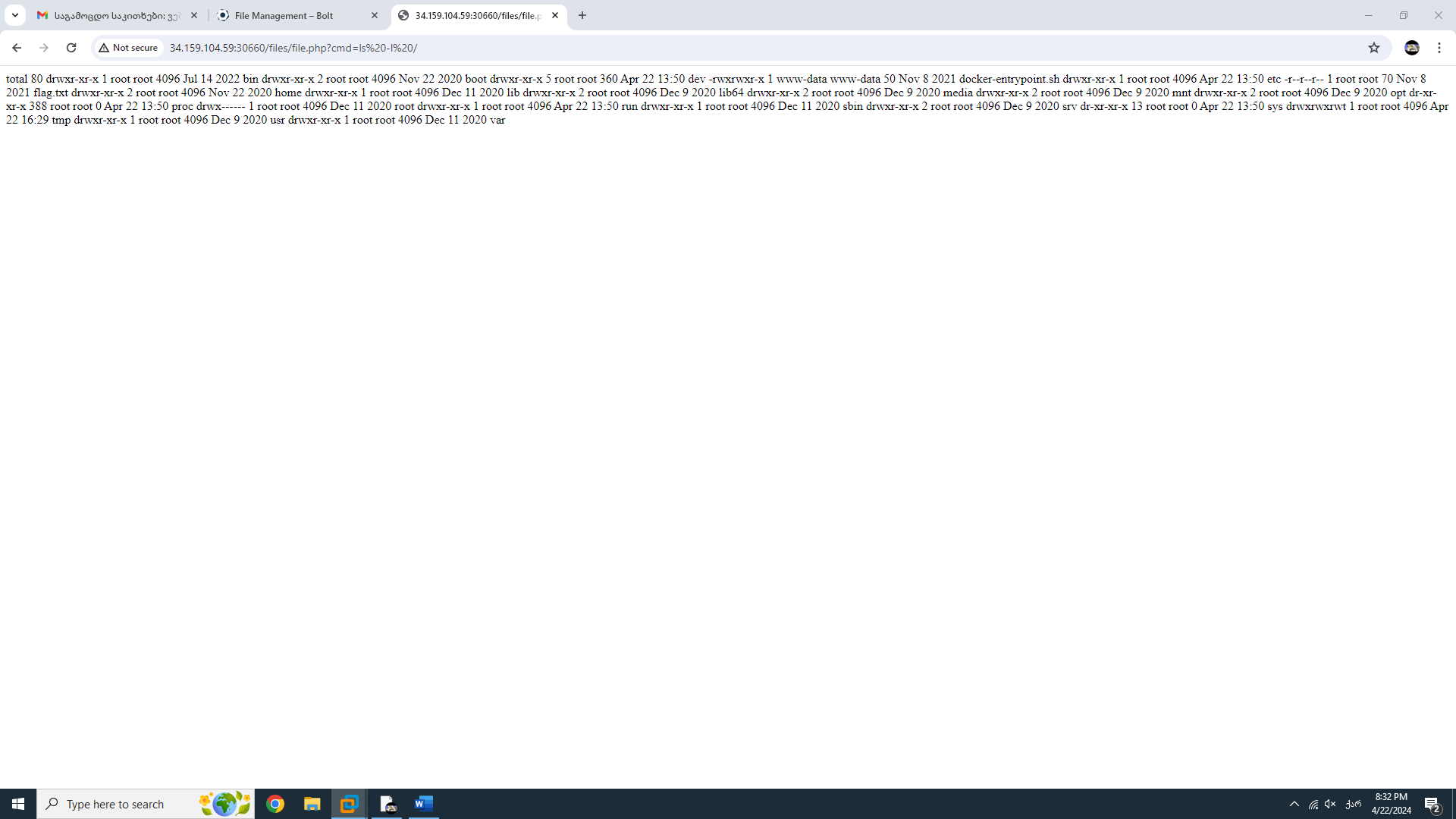
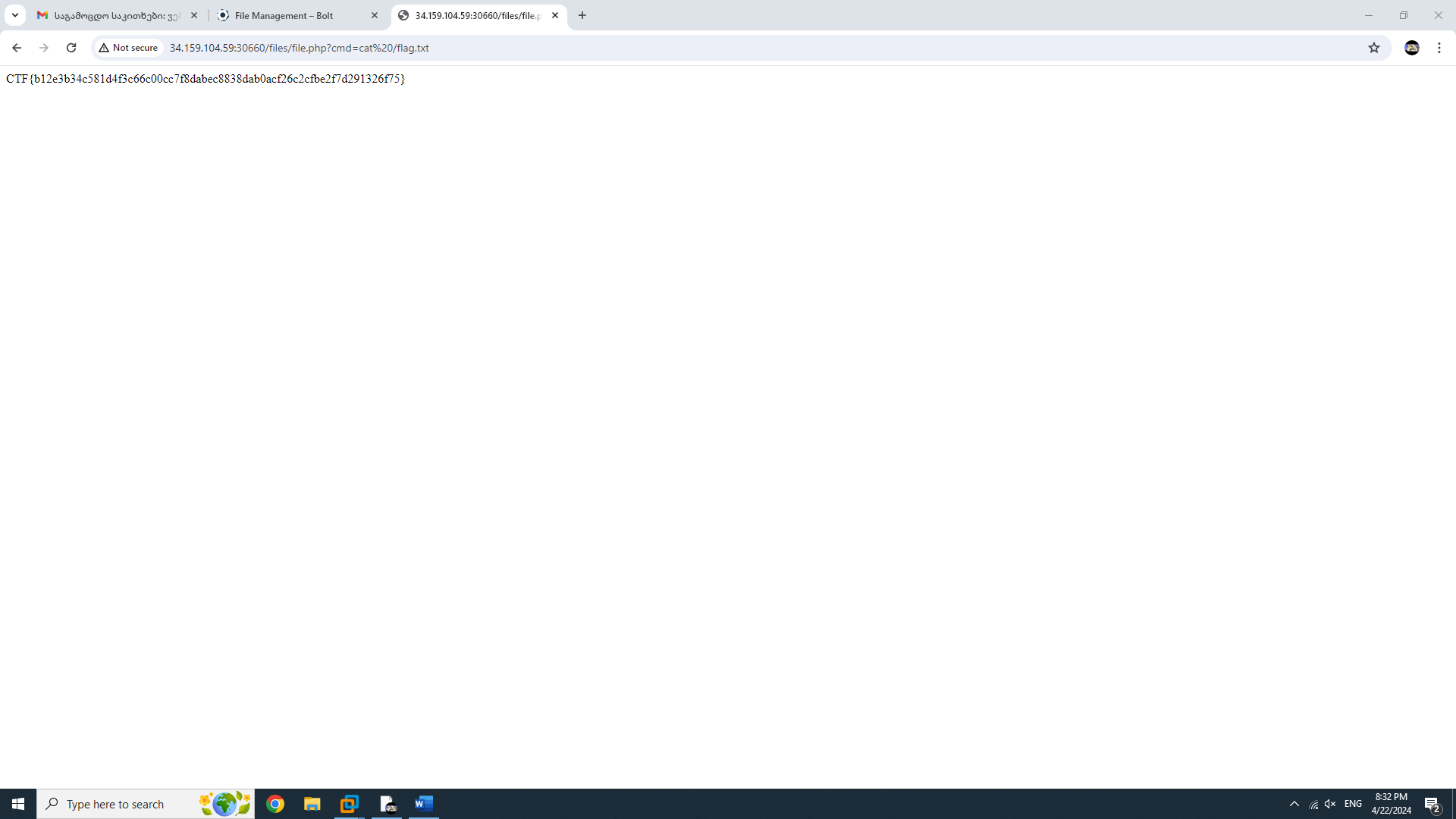
LAB: BOLT

მოცემულ მისამართზე შესვლისას გვხვდება ქვემოთ მოცემული შედეგი

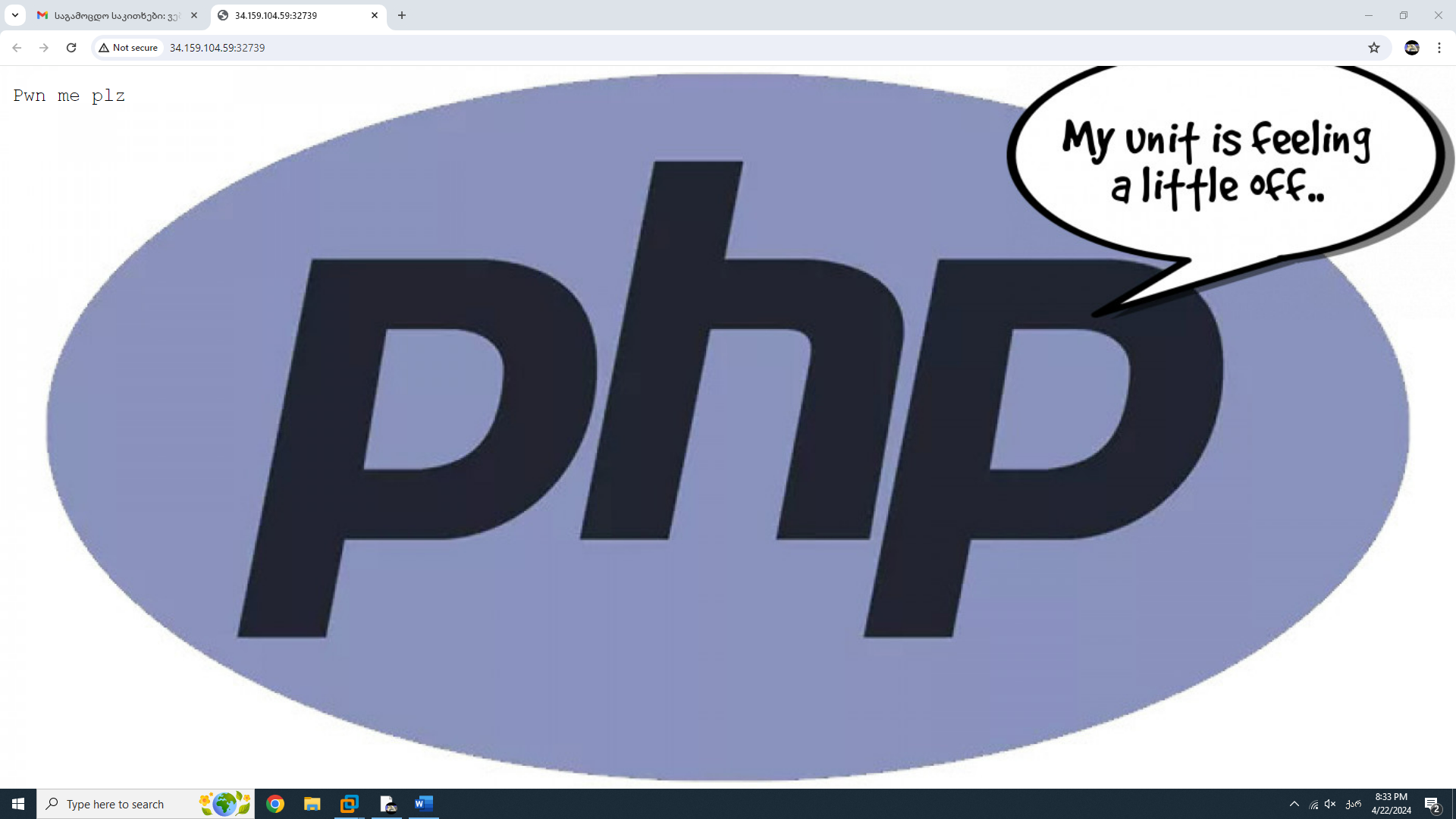
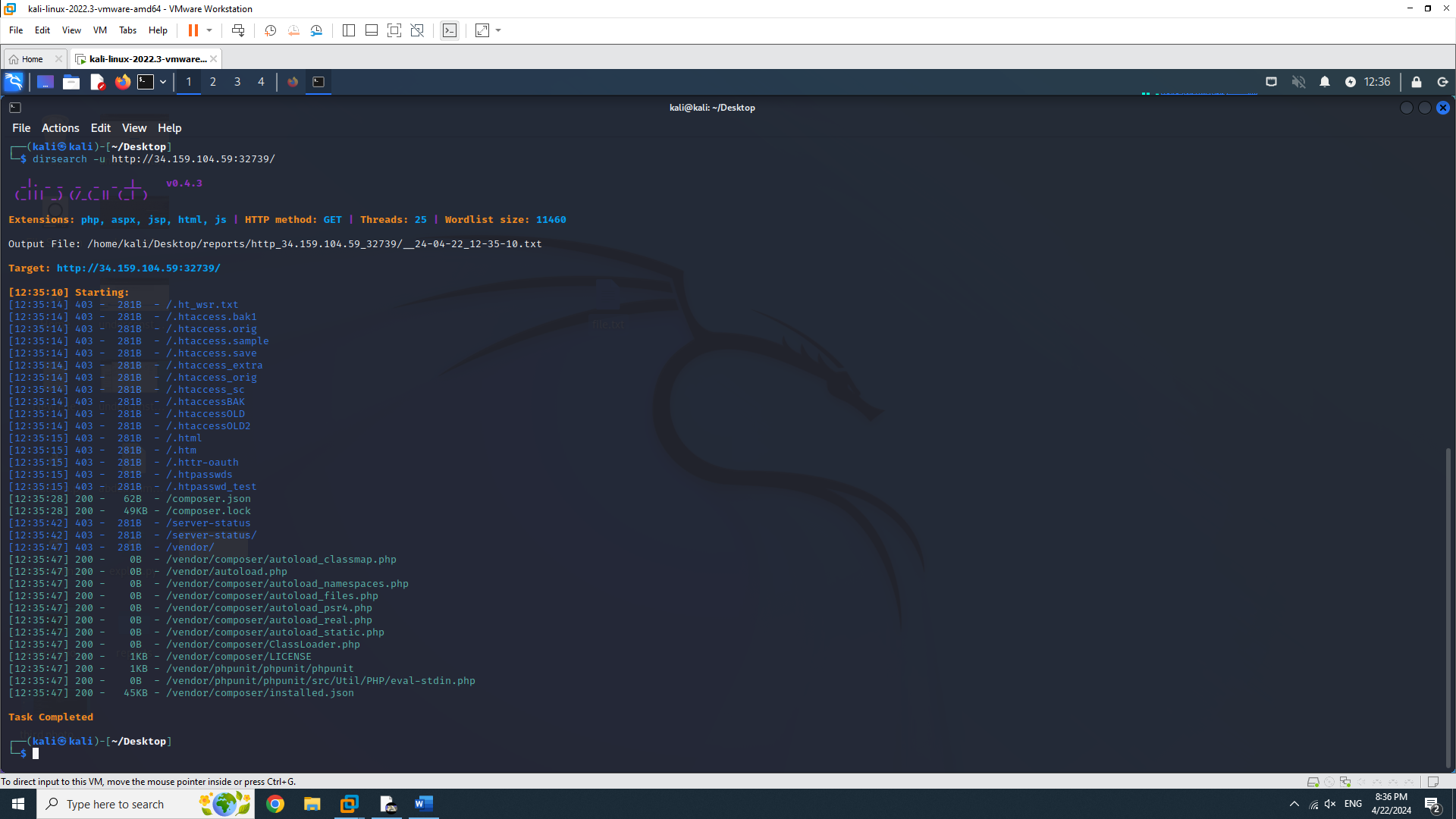
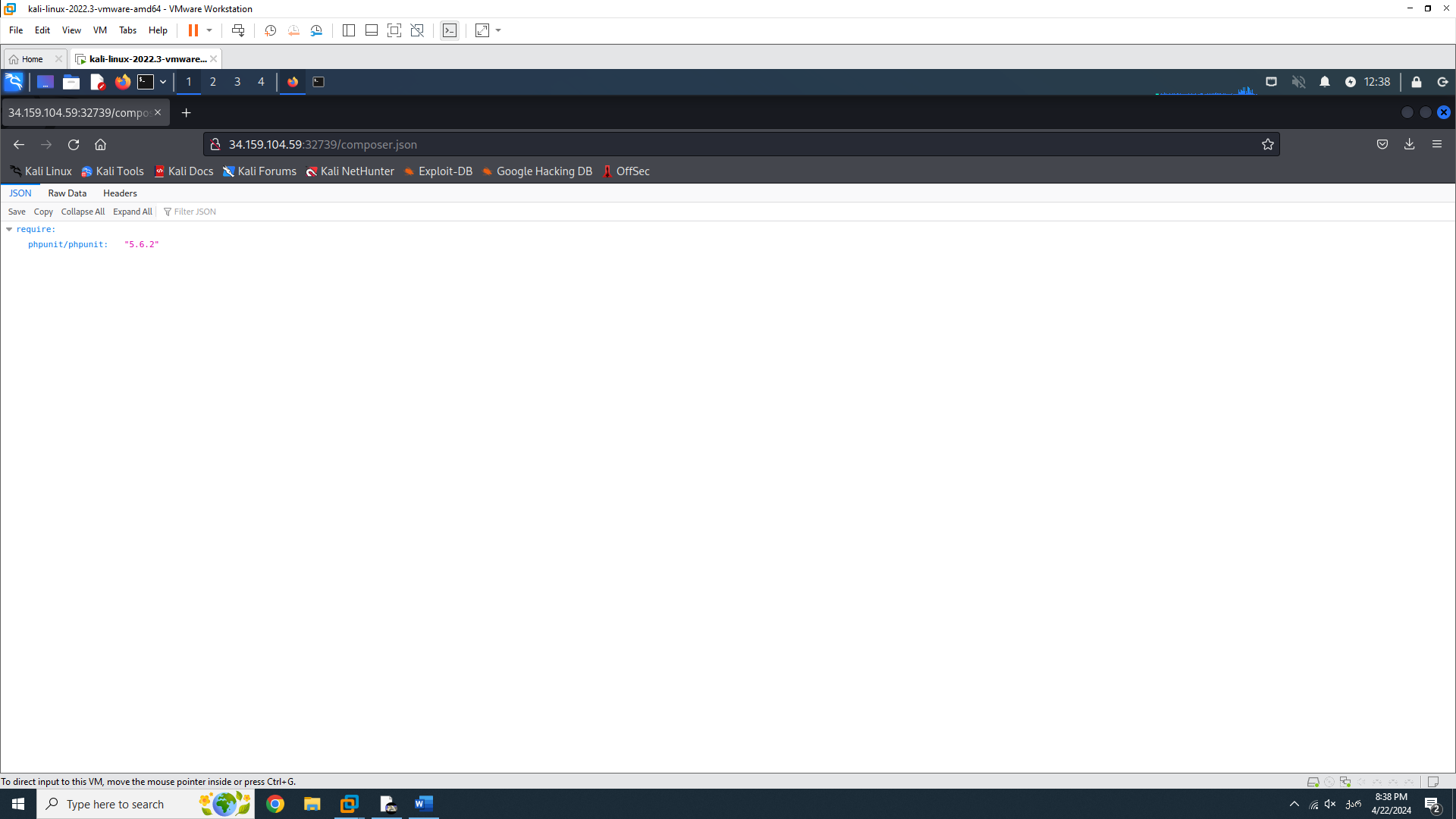
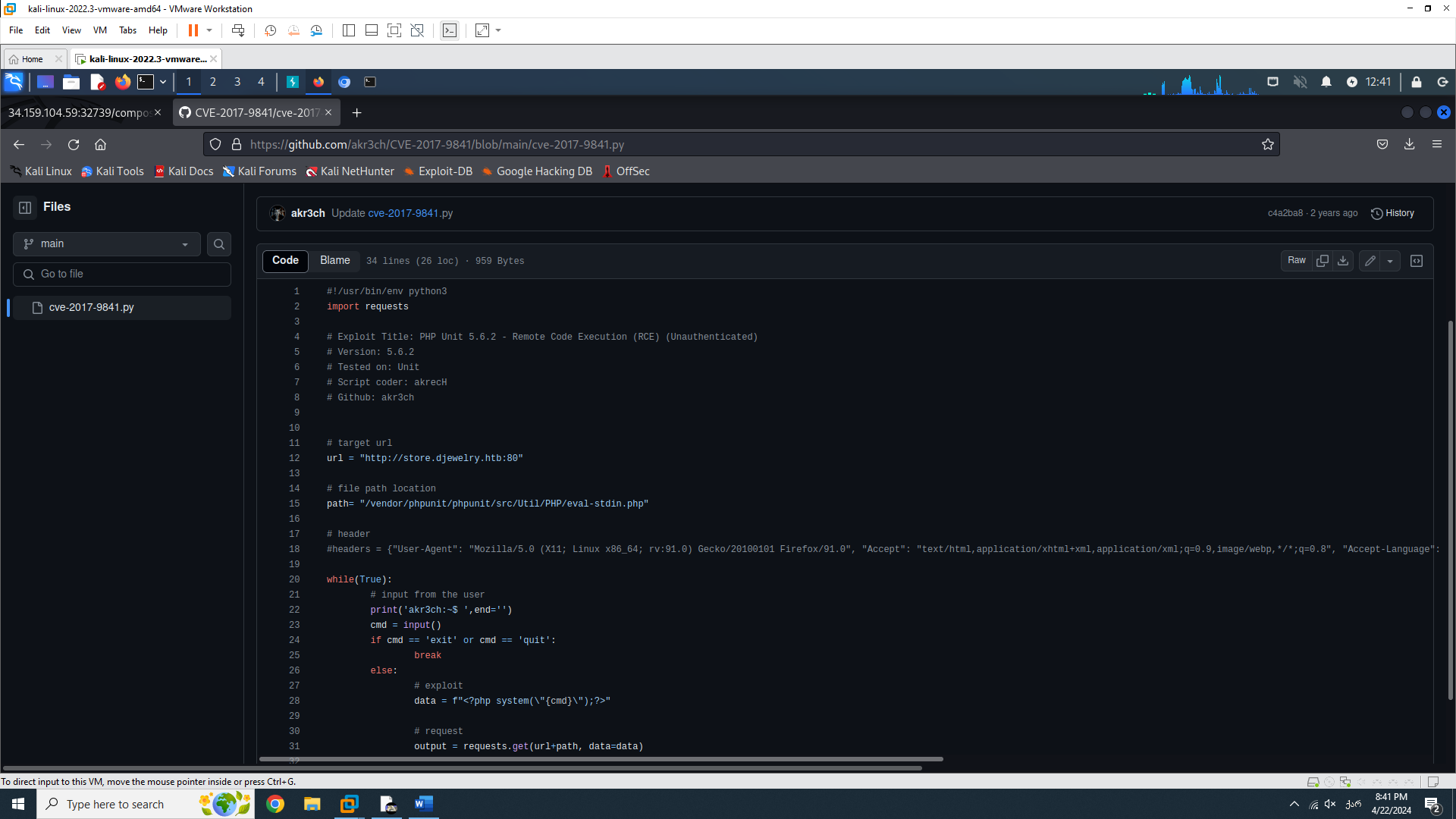
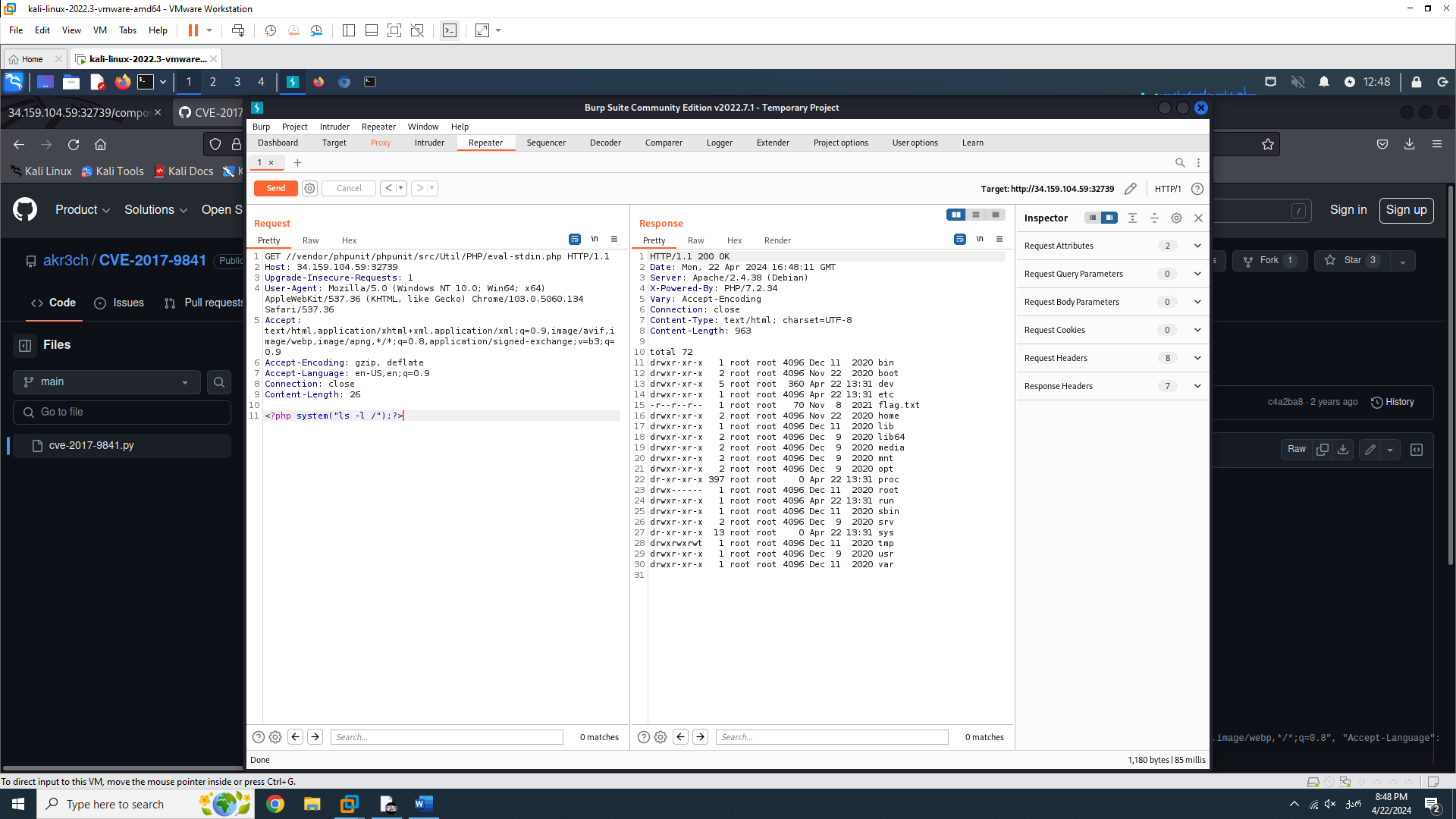
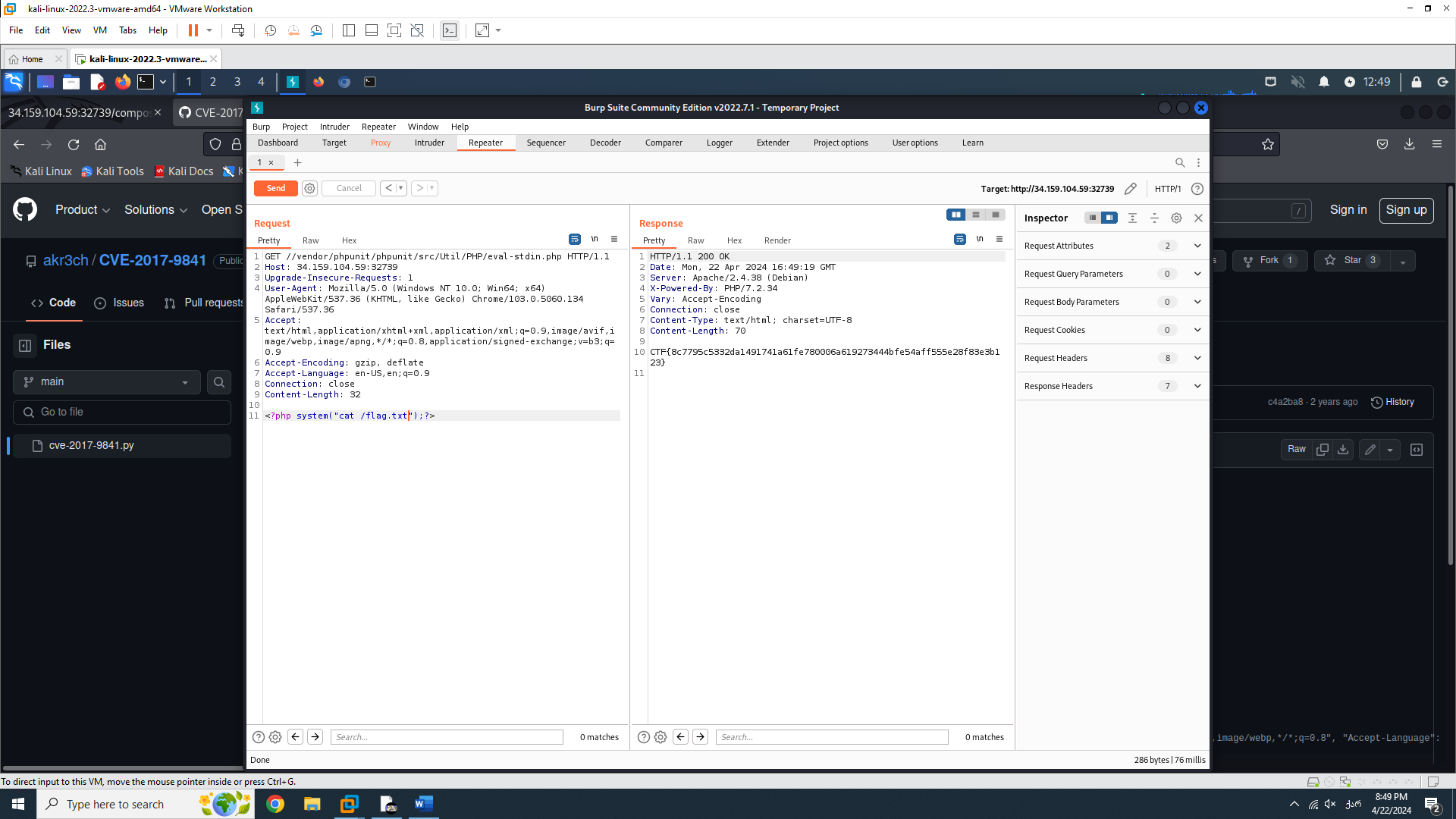
არსებული საიტის სორს კოდის ანალიზის შედეგად ვხვდებით რომ URL-ში უნდა მივმართოთ http://34.159.104.59:30660/bolt-ს რის შედეგადაც ვხვდებით ავტორიზაციის გვერდზე

უნდა ვეცადოთ შევიდეთ ადმინის უფლებებუით, რამდენიმე მარტივი ცდის შემდეგ ჩვენ შეგვიცლია გამოვიცნოთ მომხმარებლის სახელი და პაროლი რადგან არც თუ ისე ძლიერი პაროლი და default მომხმარებლის სახელი არის გამოყენებული.



შესვლისას და აღნიშნული dashboard-ის დათვალიერებისას ვხედავთ რომ შეგვიძლია ფაილების ატვირთვა, თუმცა არა ყველა ფორმატის, ასევე შეგვიძლია ფაილის ფორნმატის შეცვლა. უნდა ვცადოთ სასურველი ფაილის ფორმატის ატვირთვა და შემდეგ ამ ფაილის ტიპის შეცვლა. ავტვირთოთ TXT ტიპის ფაილი, რომკელშიც იქნება PHP-ის კოდი ჩაწერილი, მაგალითისთვის: <?php system($\_GET['cmd']) ?> რომელიც ქომანდ ლაინზე მოგვცემს წვდომასა და ბრძანებების გაშვების შესაძლებლობას.ატვირთვის შემდეგ უნდა შევუცვალოთ ფაილს გაფართოება და გავხადოთ PHP. ფაილის გახსნის შემდეგ გადავდივართ ახალ გვერდზე. მოდი ვცადოთ რაიმე ქომანდის გაშვება URL-ის საშუალებით.შედეგი გვაქვს და აქვრ ვხედავთ ფაილს სახელად flag.txt. უნდა წავიკითხოთ ეს ფაილი შესაბამისი ბრძანებით: cat /flag.txt ჩვენი ფლეგიც.

LAB: PHP unit

მისამართზე შესვლისას ვხედავთ შემდეგ სურათს პირველ რიგში ვცდილობთ მაქსიმალურრად მეტი ინფორმაცია მივიღოთ ამ საითის შესახებ. ერთ-ერთი გზა არის dirsearch მისი გამოყენების შემდეგ თვალში საინტერესოდ ხვდწება რამდენიმე ქვედირექტორია ერთ-რთი არის composer.json. შესაბამის მისამართზე შესვლისას ვხედავთ ვერსიის ნომერს. ახლა საჭიროა ამ ვერსიის PHP-ზე ვნახოთ შესაბამისი სისუსტეები. როგორც ჩანს მოცემულ მისამართზე შესვლისას ჩვენ გვაქ შესაძლებლობა გავუშვათ ბრძანებები. მოდი ვცადოთ burpsuite-ს გამოყენებით. პირველ რიგში გავუშვათ ls -l / რათა ვნახოთ თუ რა არის განთავსებული იქ აქვე ვხედავთ ფაილს სახელად flag.txt მოდი ვნახოთ რა არის მანდ. ჩვენი ფლეგი.