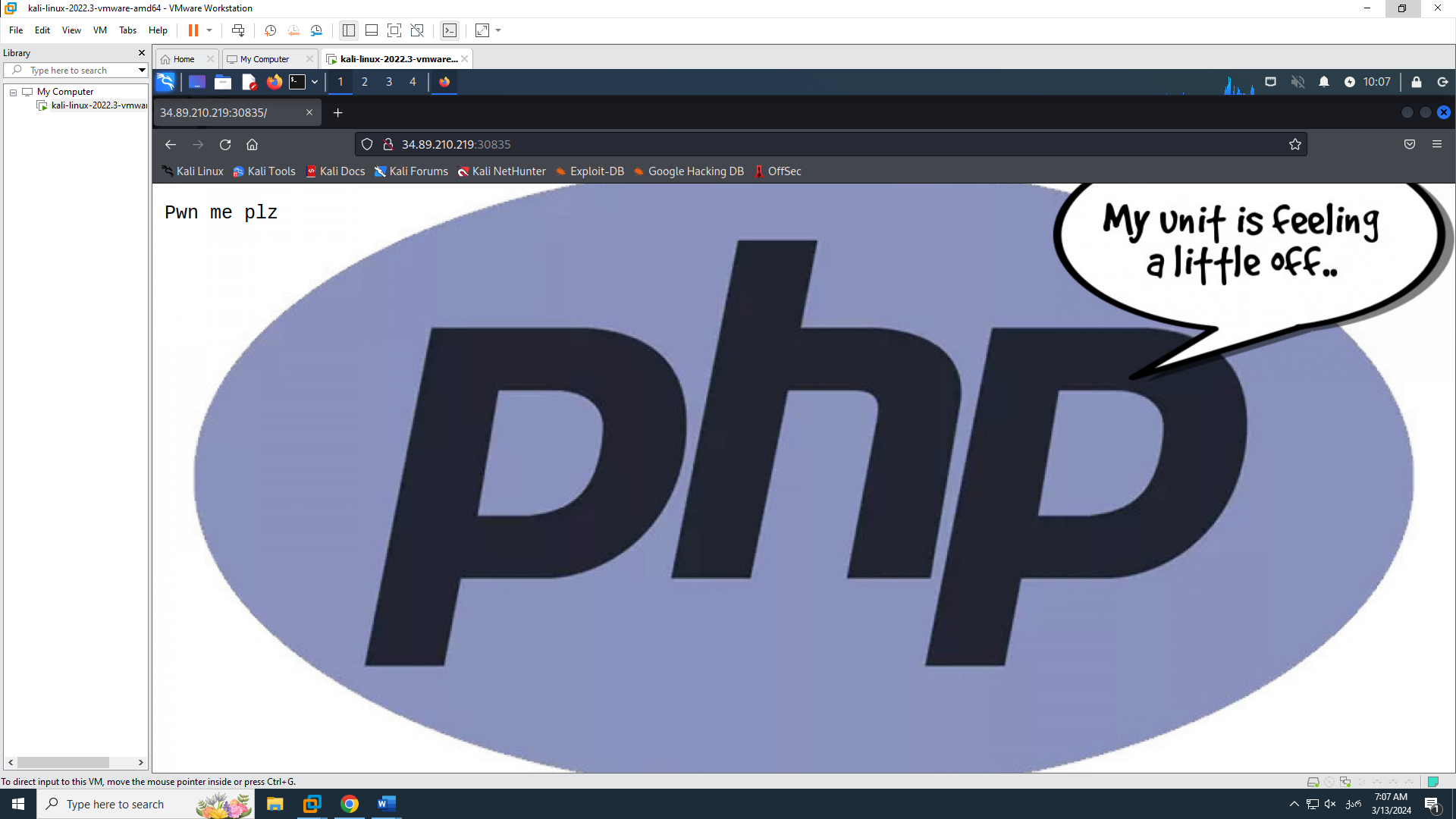
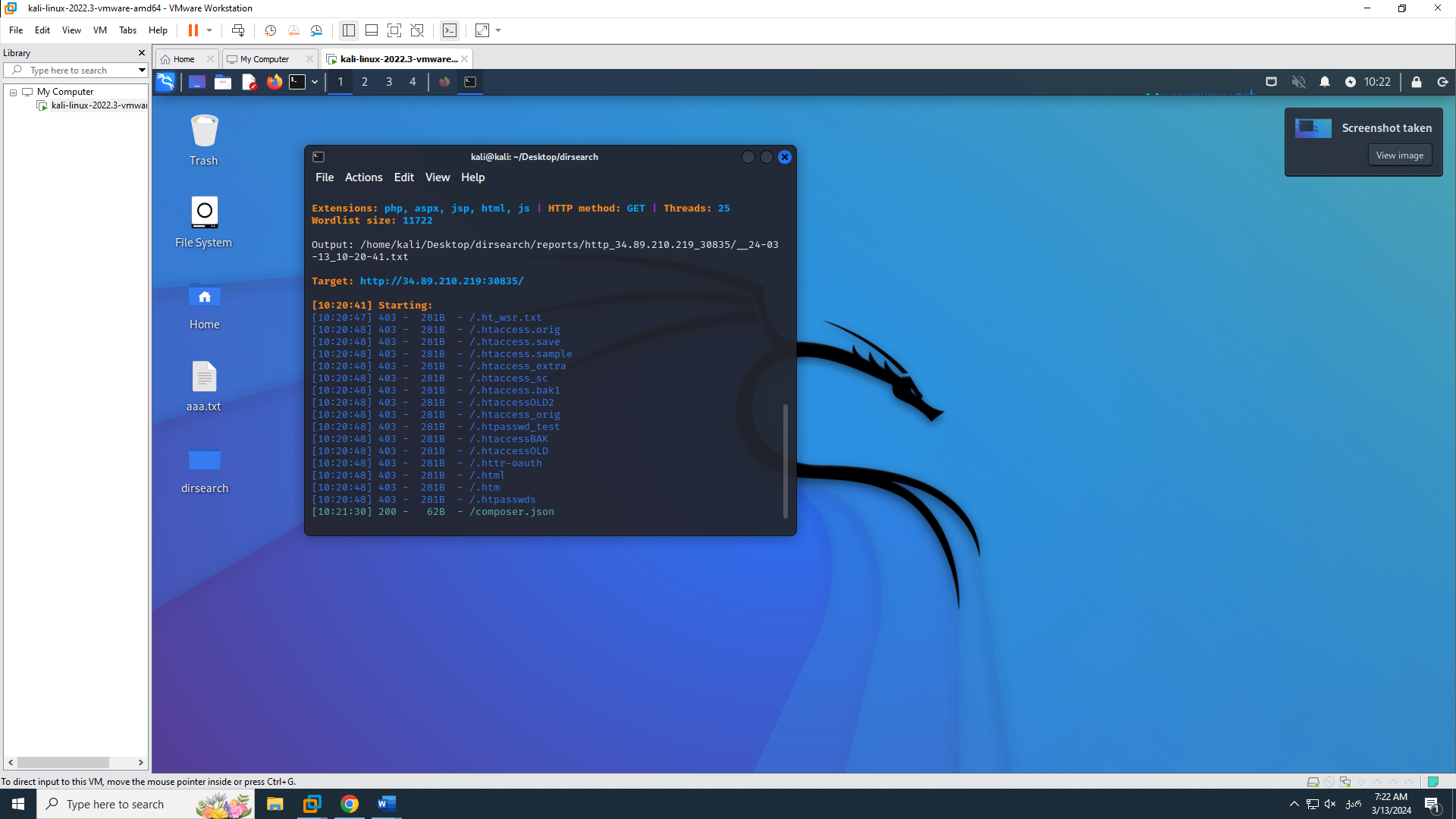
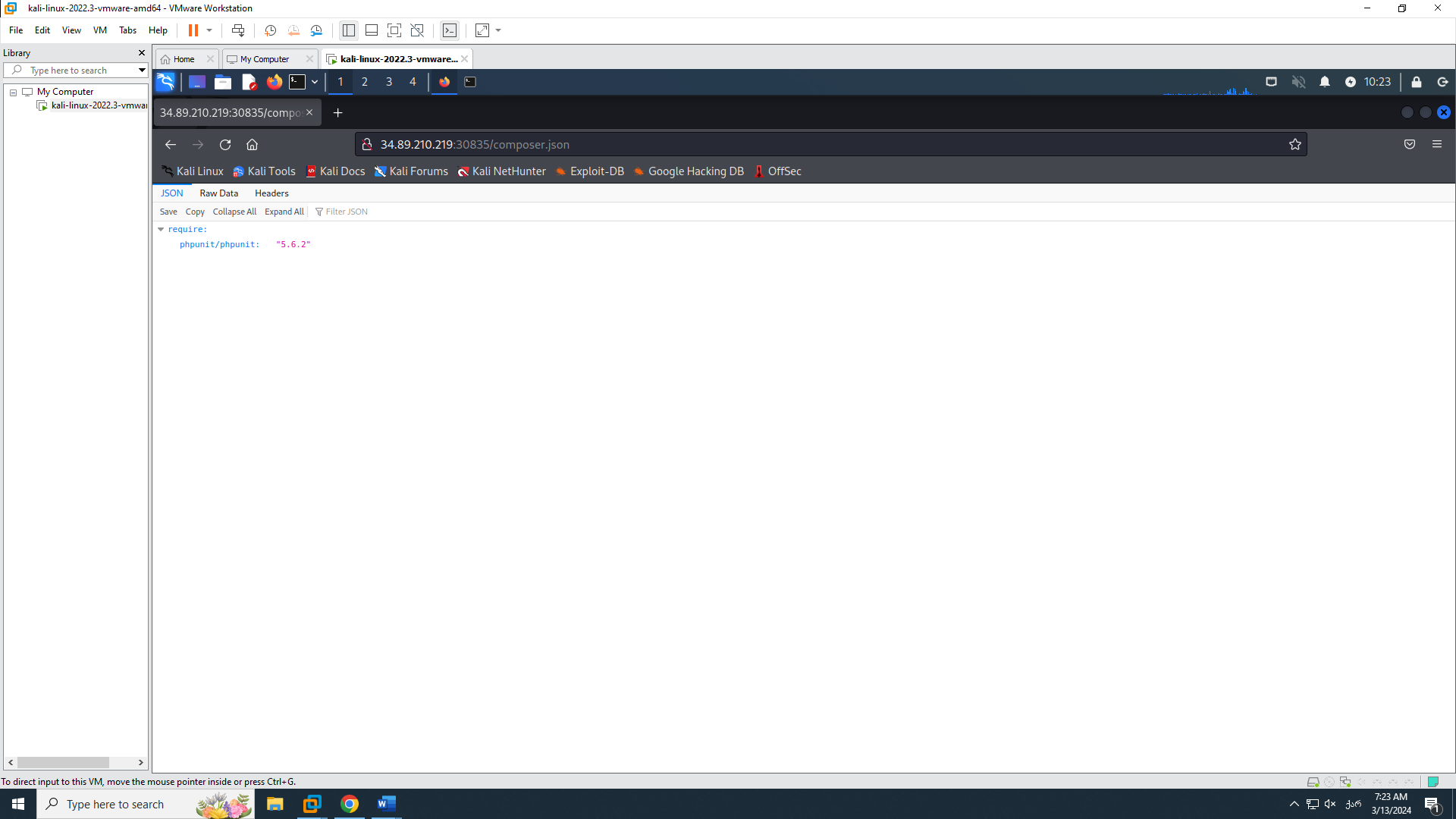
სიმულაციური აქტივობა 1

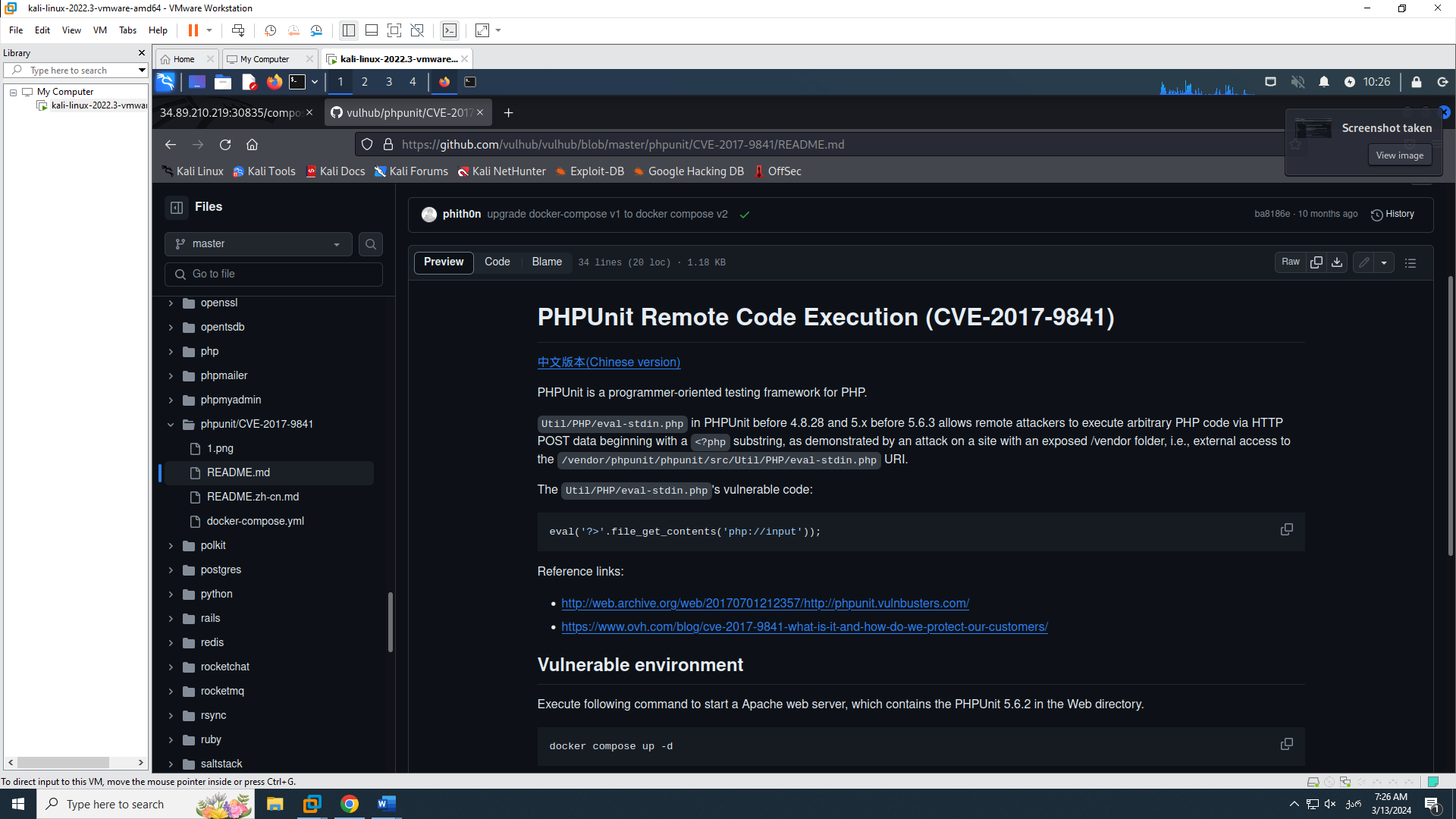
გიორგი მაკასარაშვილი

Lab: PHP-Unit

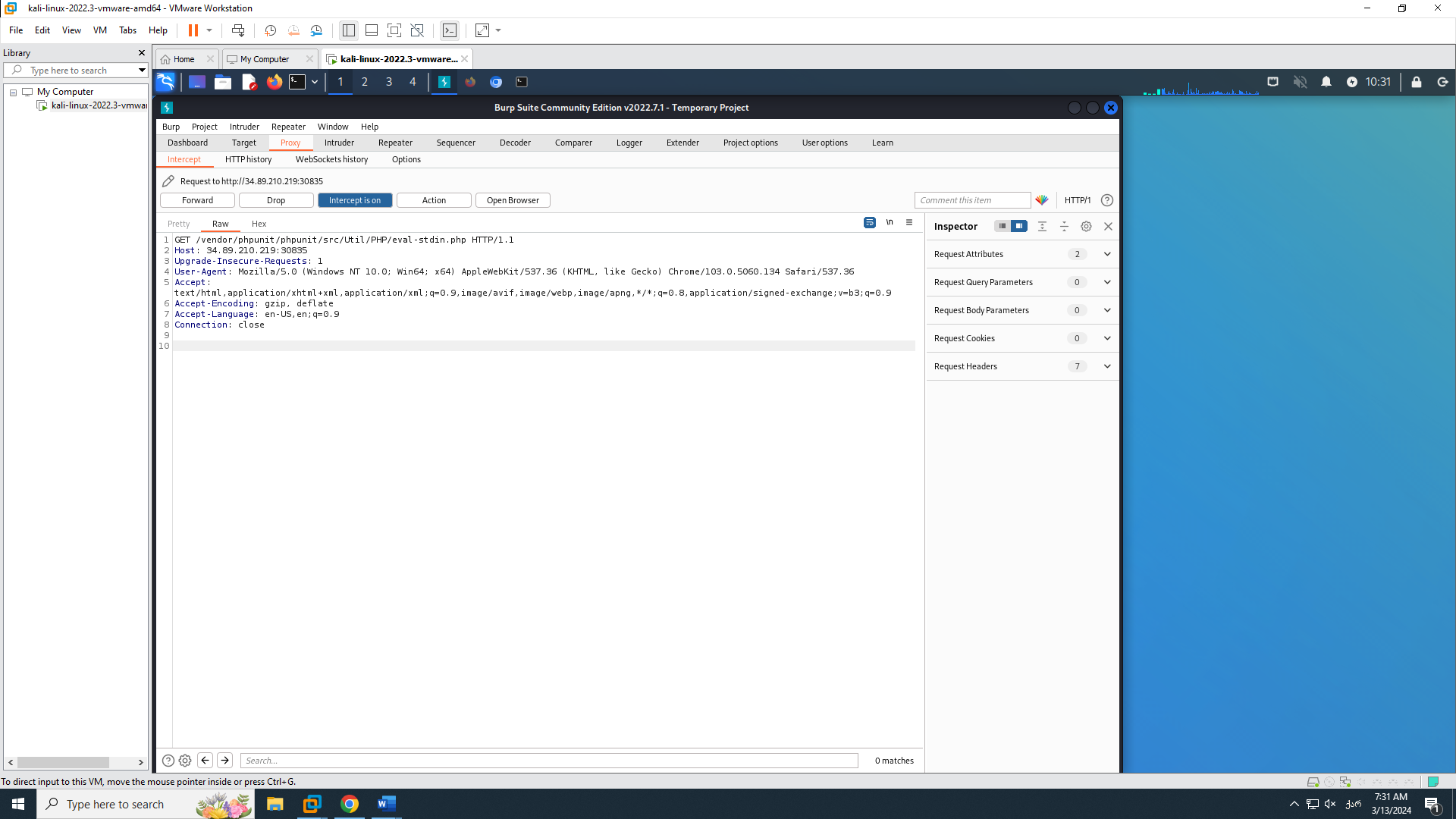
მოცემულ IP მისამართზე შესვლისას ვხედავთ შემდეგ სურათს. 

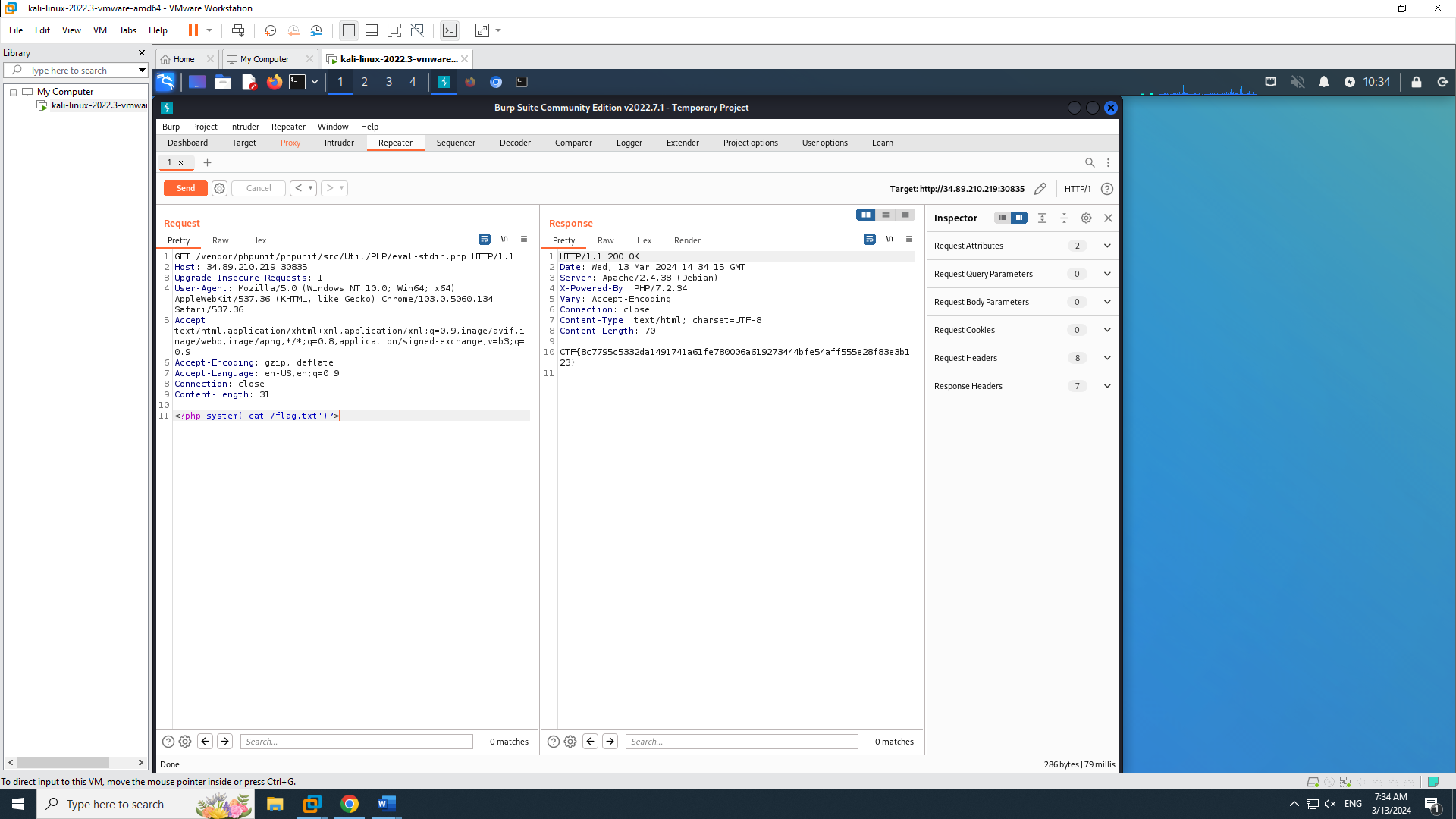
ახლა ვცდილობთ რაც შიძლება მეტი ინფორმაცია მივიღოთ ამ გვერდის შესახებ. საკმაოდ დიდ ინფორმაციას მივიღებთ თუ გამოვიყენებთ dirsearch-ს, რომელიც დაგვეხმარება ფოლდერებისა და ფაილდების bruteforce-ში. იმისთვის რომ ეს გამოვიყენოთ უნდა დავაყენოთ dirsearch და გავუშვათ შემდეგი ბრძანება ./dirsearch.py -u http://34.89.210.219:30835/ -w ./db/dicc.txt 

თვალში გვხვდება composer.json, მოდი ვნახოთ რა არის მანდ.

ჰოი საოცრებავ, ვიგებთ PHP-ს ვერსიას. ახლა შეგვიძლია ინტერნეტში მოვძებნოთ თუ არის ამ ვერსიაზე უკვე რაიმე ცნობილი სისუსტე.

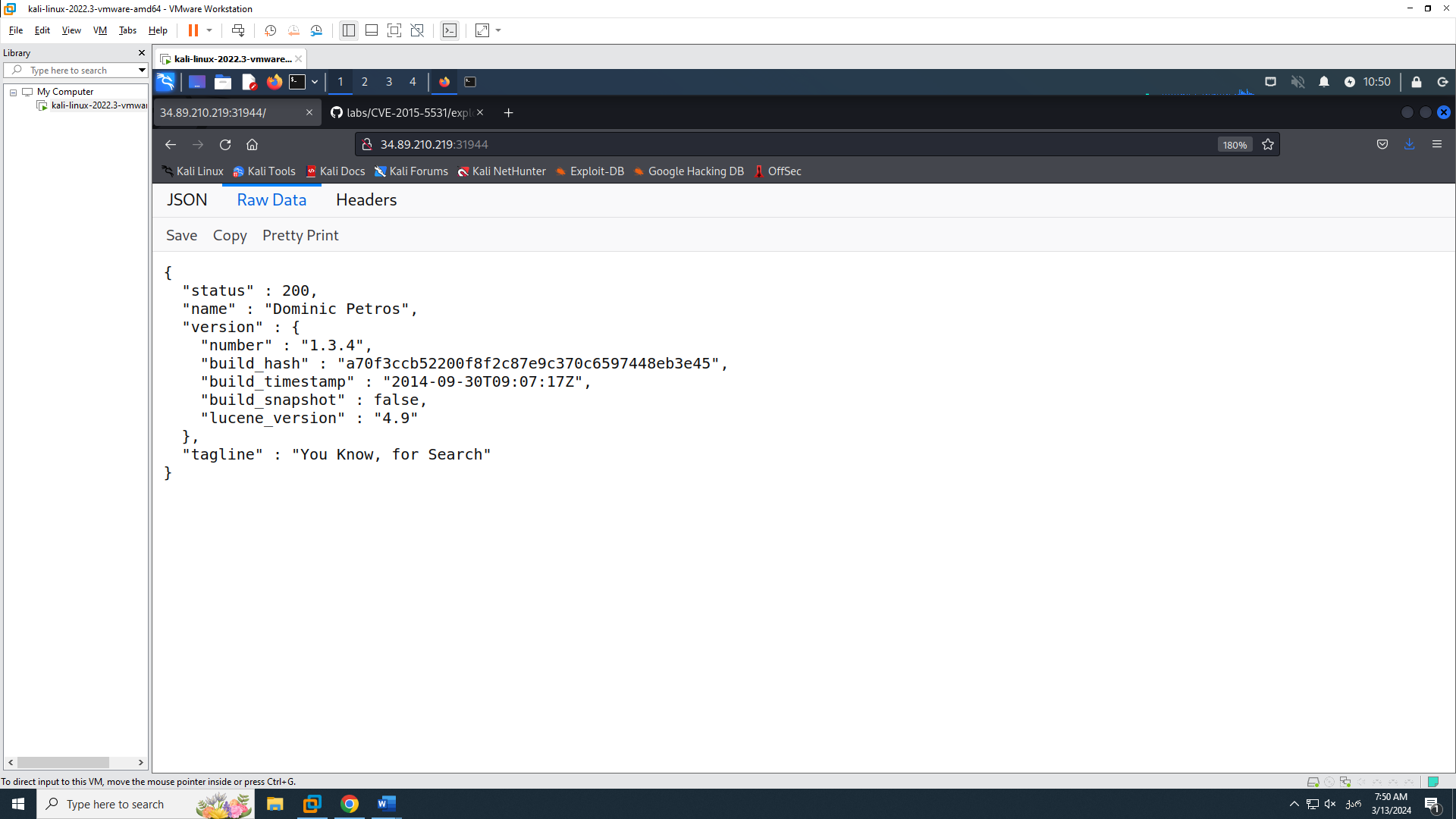
ყოფილა, PHPUnit Remote Code Execution (CVE-2017-9841), გადაკითხვის შედეგად ვიგებთ რომ თურმე შეგვიძლია ჩვენთვის სასურველი php კოდის გაშვება, აბა ვცადოთ....

ამისთვის /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php უნდა დავამატოთ url-ს და გავუშვათ post request. ამაში burpsuite დაგვეხმარება.

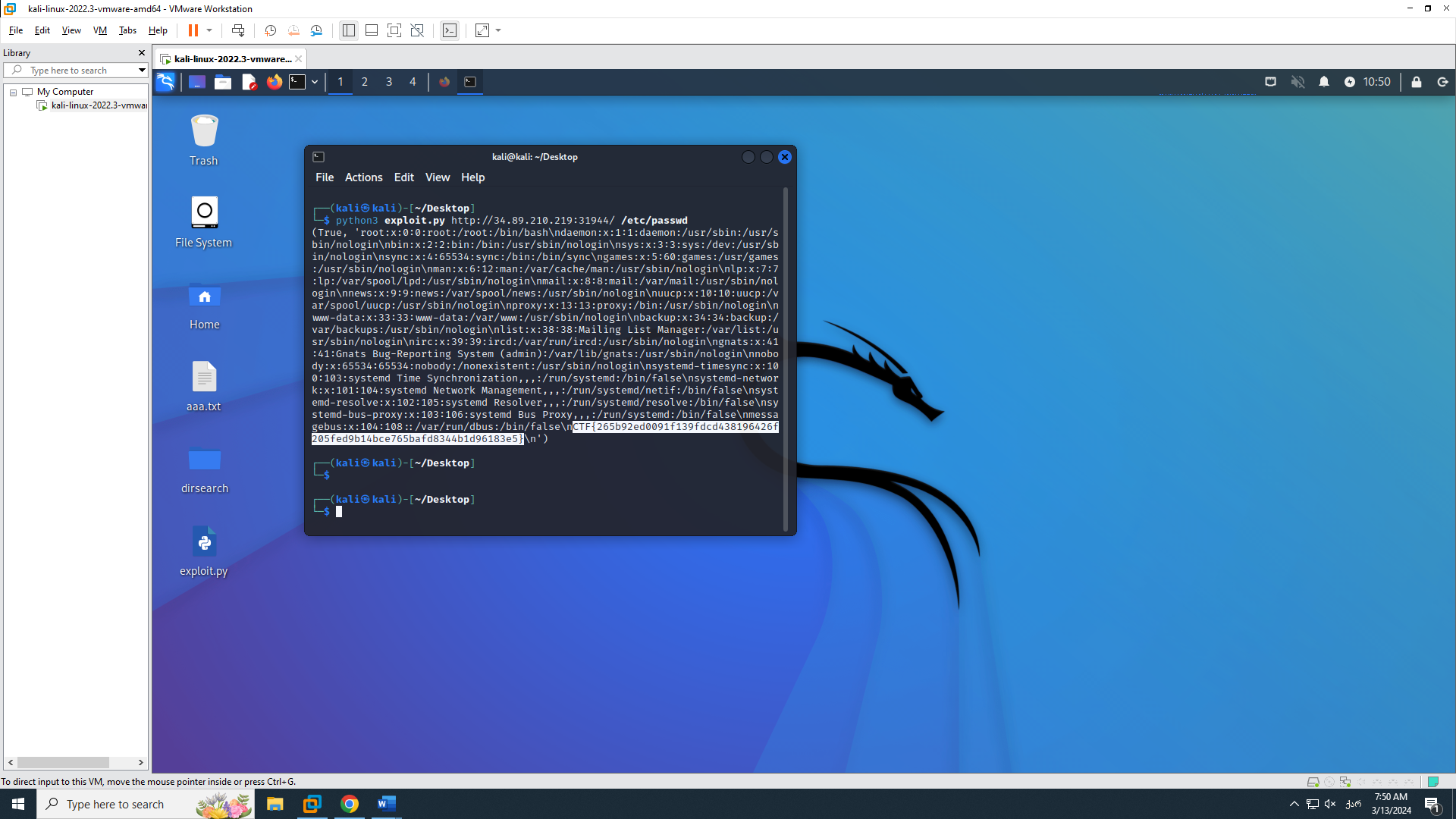
Burpsuite-ში ჩავრთავთ proxy-ს და მივუთითებს შესაბამის მისამართს, ამის შემდეგ გადაგვაქ repeater-ში და დავატებთ ჩვენთვის სასურველ php კოდს

ვუალაა!!! ფლეგი ნაპოვნია.

Lab: elastic

მოცემულ IP მისამართზე შესვლისას ვხედავთ შემდეგ სურათს. 

უკვე საკმაოდ დიდ ინფორმაციას ვიღებთ. ყველაზე მნიშვნელოვანი არის ვერსია 1.3.4  
ინტერნეტში მოვძებნოთ თუ არის რაიმე ცნობილი სისუსტე elastic 1.3.4-ზე. მრავალი ძებნის შემდეგ წავაწყდით exploit-ს: <https://github.com/nixawk/labs/tree/master/CVE-2015-5531>

ამ exploit-ის გამოყენებისთვის უნდა გავუშვათ შემდეგი ბრძანება:   
python3 exploit.py http://34.89.210.219:31944/ /etc/passwd 

დაბრუნებულ შედეგში ჩანს ჩვენი CTF.