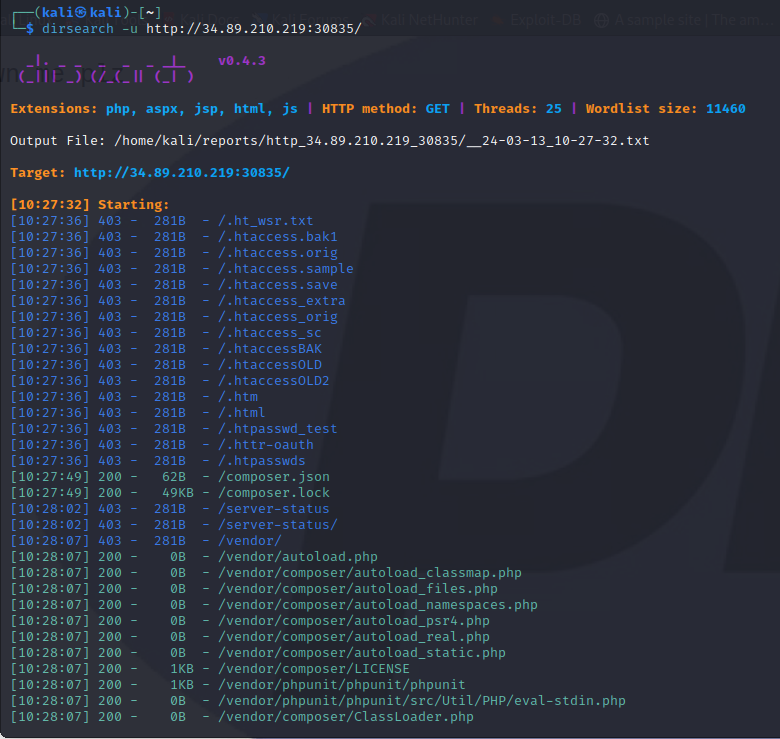
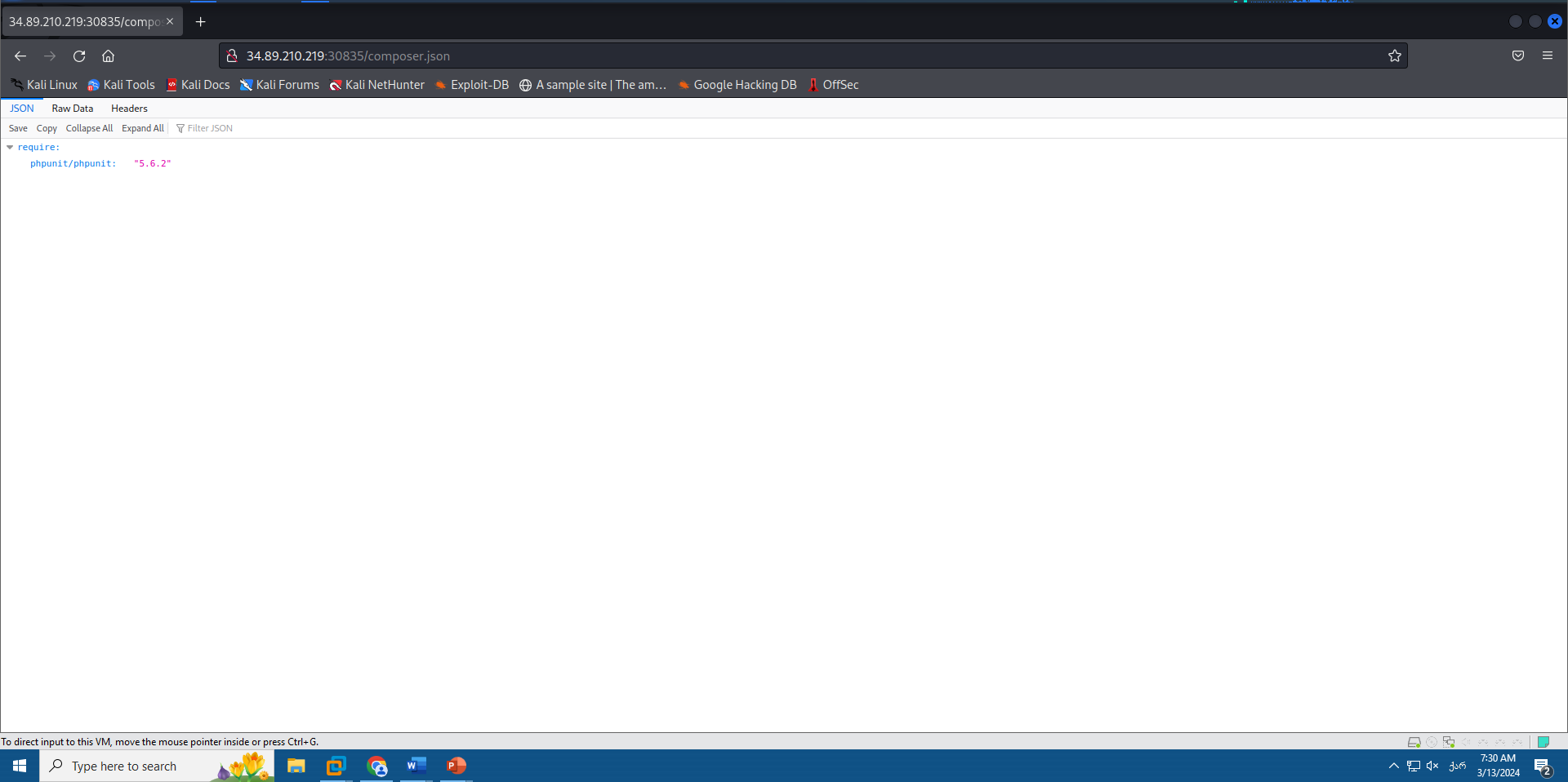
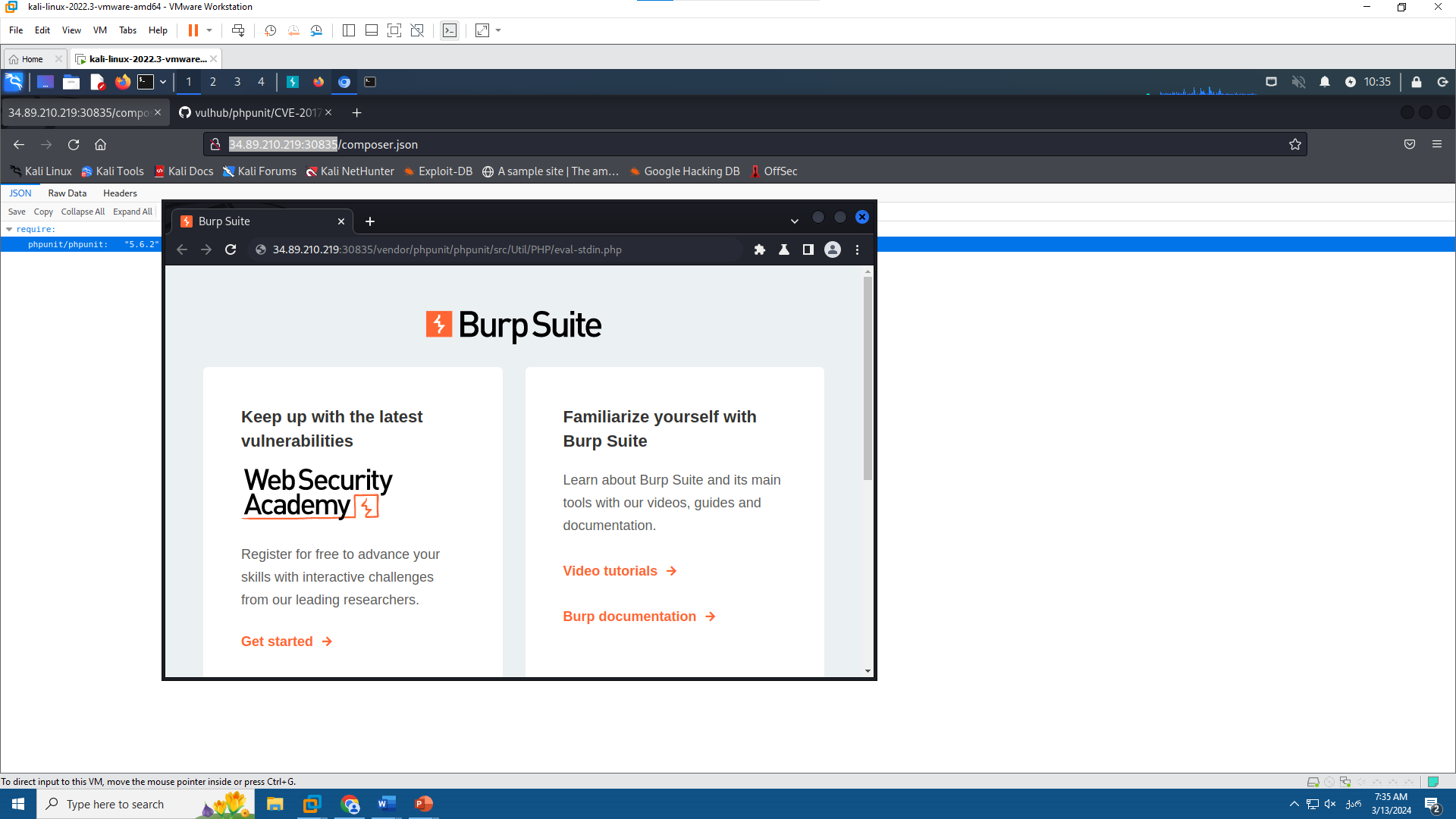
**სიმულაციური აქტივობა 1 (მაქსიმალური ქულა 12)**

ვებ შეღწევადობის ტესტირება II

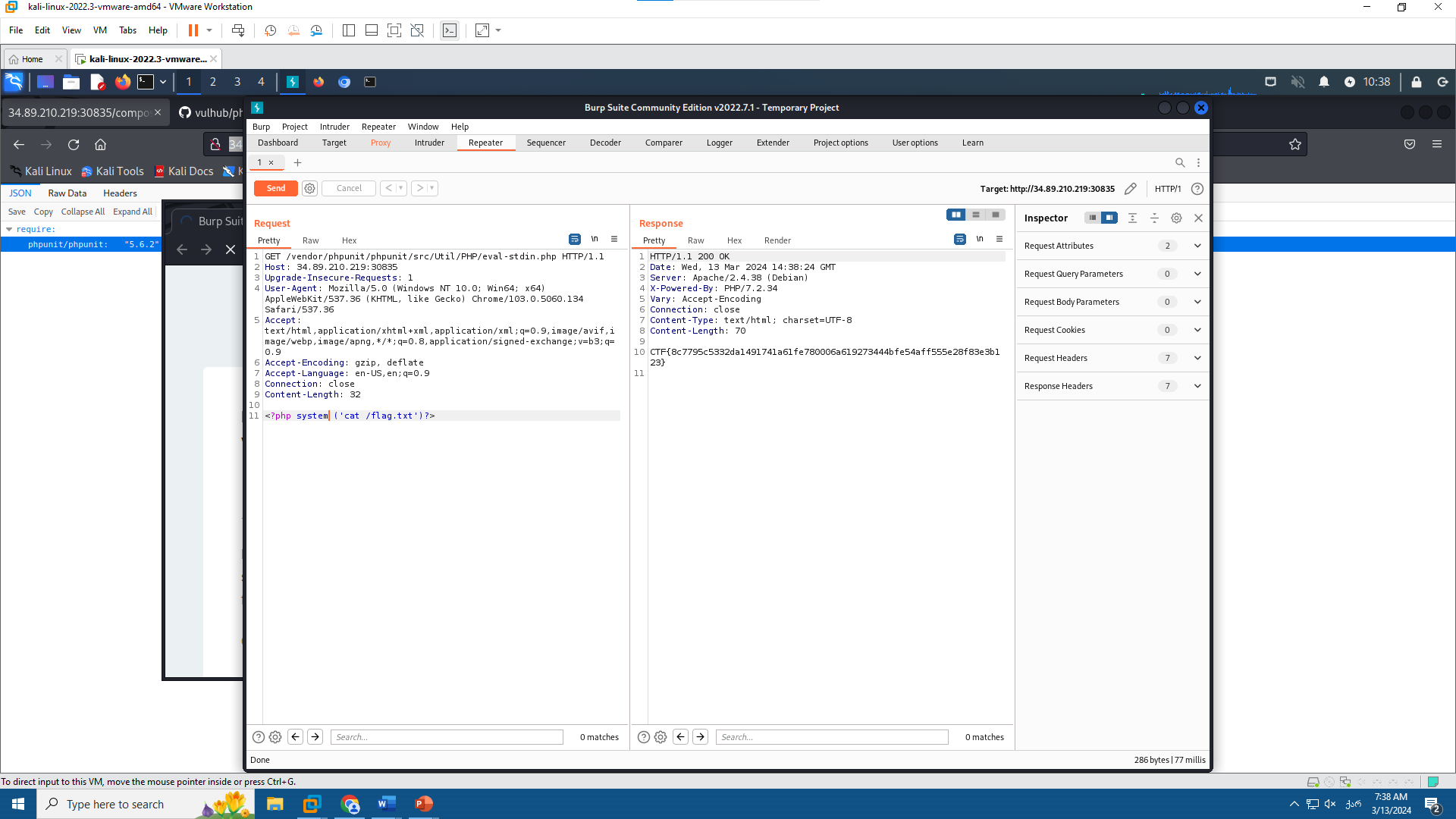
**Lab:** [**http://34.89.210.219:30835/**](http://34.89.210.219:30835/) **(php unit) *(მაქსიმუმ 6 ქულა)***

მოცემულია ვებსაიტი რომელზეც მინიშნებად გვაქვს my unit is feeling a little off. ამიტომ პირველ რიგში შეგვიძლია ვეცადოთ php unit-ის გაგება. მაგალითად შეგვიძლია გამოვიყენოთ ავტომატური ხელსაწყო Dirsearch რომელიც ბრუტფორსით ეძებს დირექტორიებში სისუსტეებს. 

ამ მისამართებიდან შეგვიძლია ჩვენთვის საინტერესოები ამოვარჩიოთ.

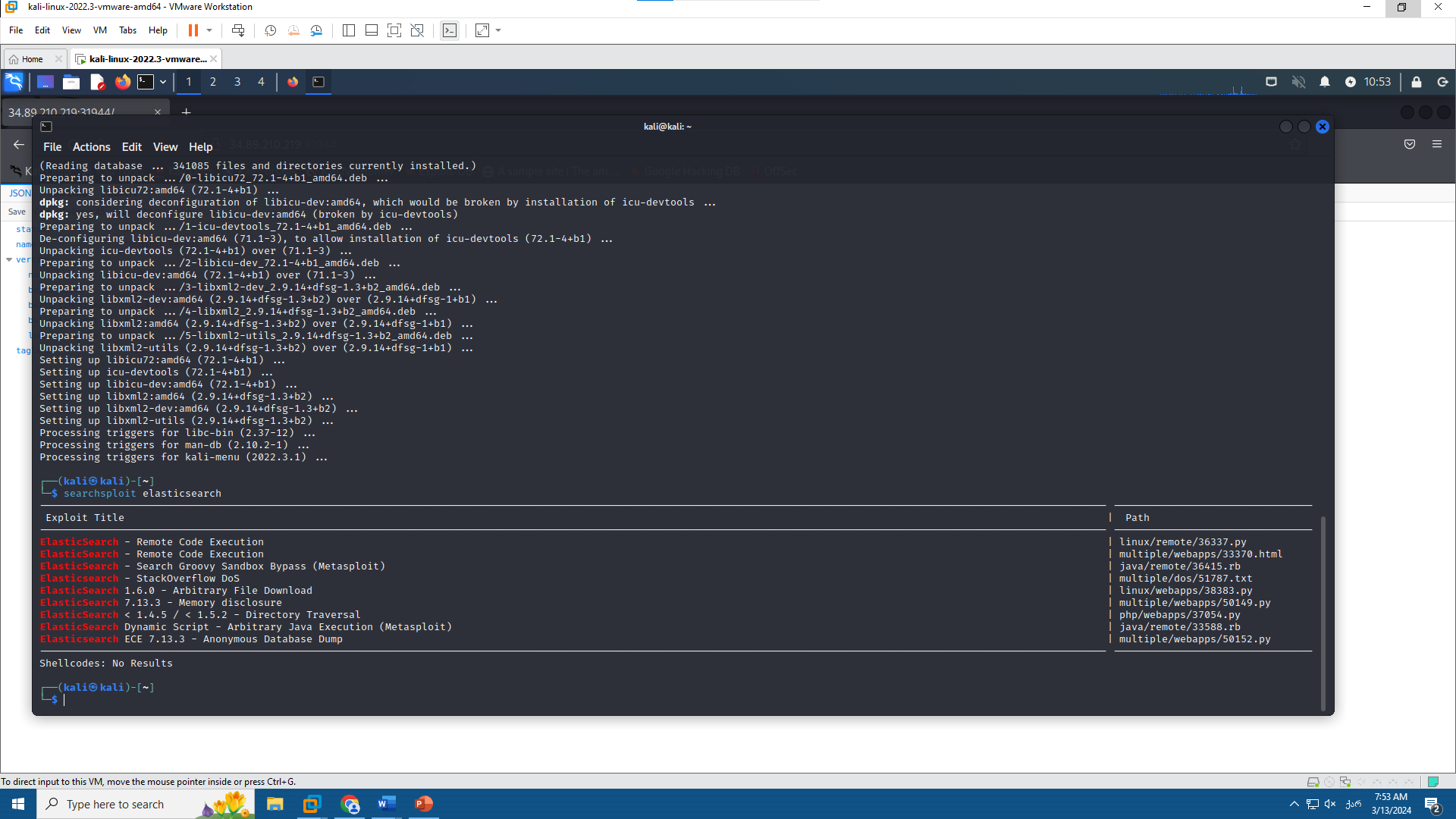
მაგალითად ერთერთი გვიჩვენებს რომელ php unit-თან გვაქვს საქმე. ამ ინფორმაციის გამოყენებით შეგვიძლია მოვიძიოთ მოცემული იუნითისთვის უკვე გამოვლენილი სისუსტეები. აღმოჩნდა რომ /vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php მოცემულ მისამართზე მიკითხვისას შეგვიძლია რექვესთში php ქომანდები გავატანოთ რომელიც შემდეგ სერვერზე გაეშვება. Burpsuite-ის გამოყენებით შესაძლებელია ამის გაკეთება. 

შეგვიძლია სხვადასხვა ბრძანებების გაშვებით შევამოწმოთ ფაილები და დირექტორიები სერვერზე და აღმოვაჩენთ ფლაგ.ტხტ ფაილს რომელსაც ამ ქომანდით გავხსნით

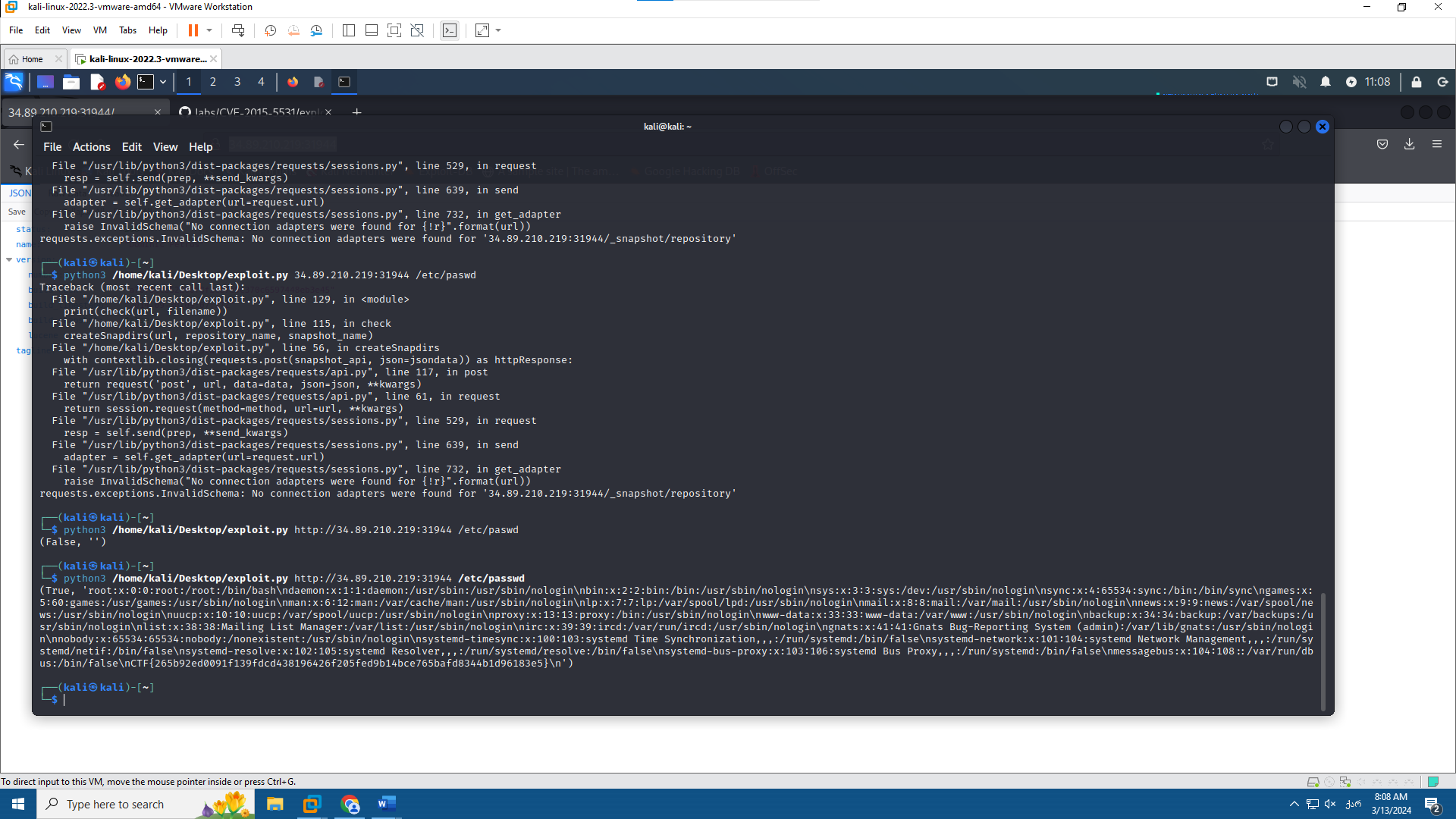


**Lab:** [**http://34.89.210.219:31944/**](http://34.89.210.219:31944/) **(elastic) *(მაქსიმუმ 6 ქულა)***

საიტზე შესვლისას მთავარ გვერდზე გამოჩენილია სენსიტიური ინფორმაცია ვერსიის შესახებ რაზეც შეგვიძლია კვლავ მოვძებნოთ რა სისუსტეებია ამ ვერსიაში აღმოჩენილი.



არსებული ხელსაწყოების გამოყენებით შეიძლება ვნახოთ კონკრეტული სისუსტეები და საჩვენოდ გამოვიყენოთ. ონლაინ არსებული მზა ექსპლოიტის გამოყენებით უბრალოდ მისამართს გადავცემთ დაწერილ სკრიპტს და ფლაგს დააბრუნებს.



შოთა ლაფაჩი, ოთხშაბათი 18:00