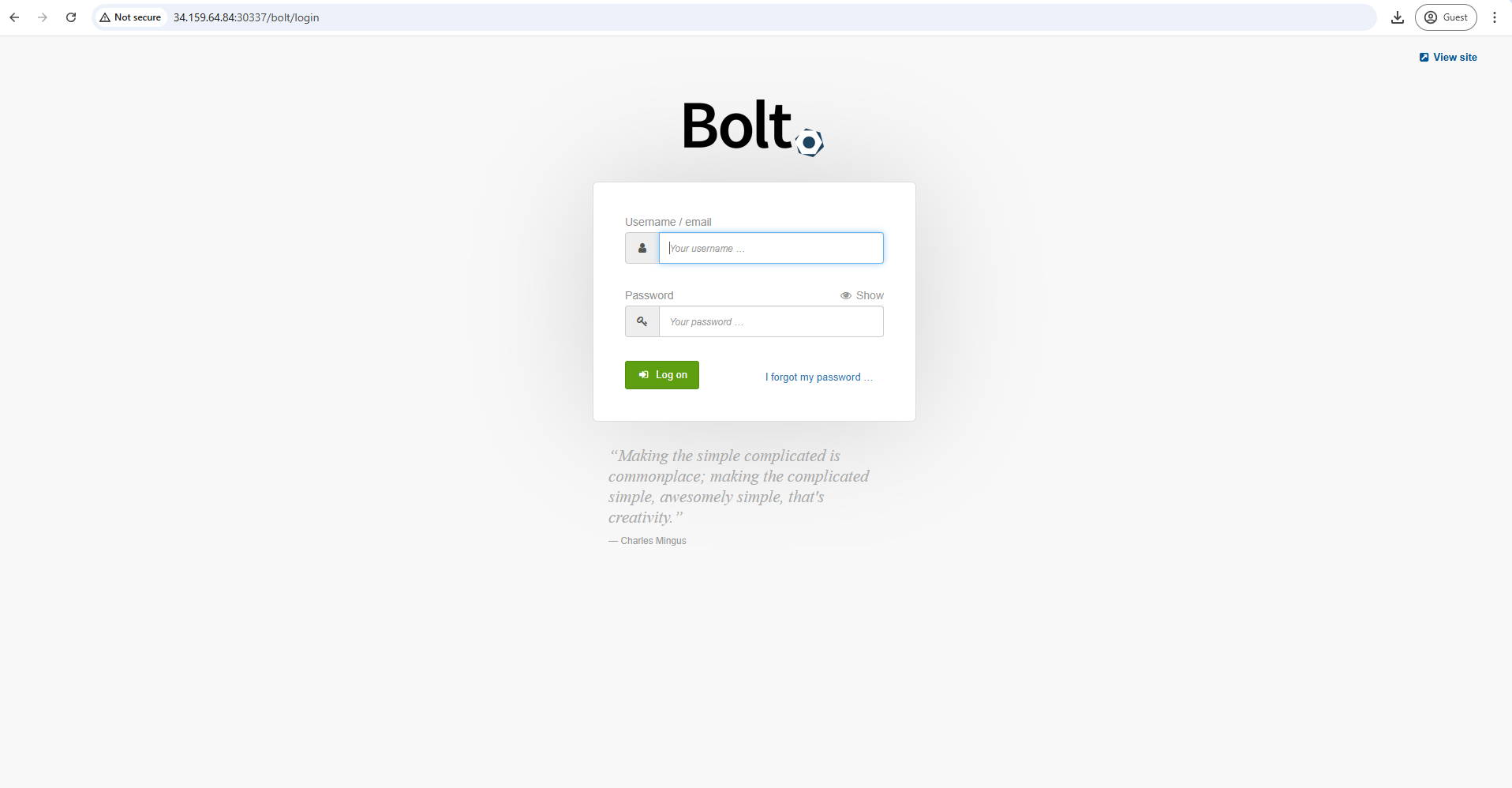
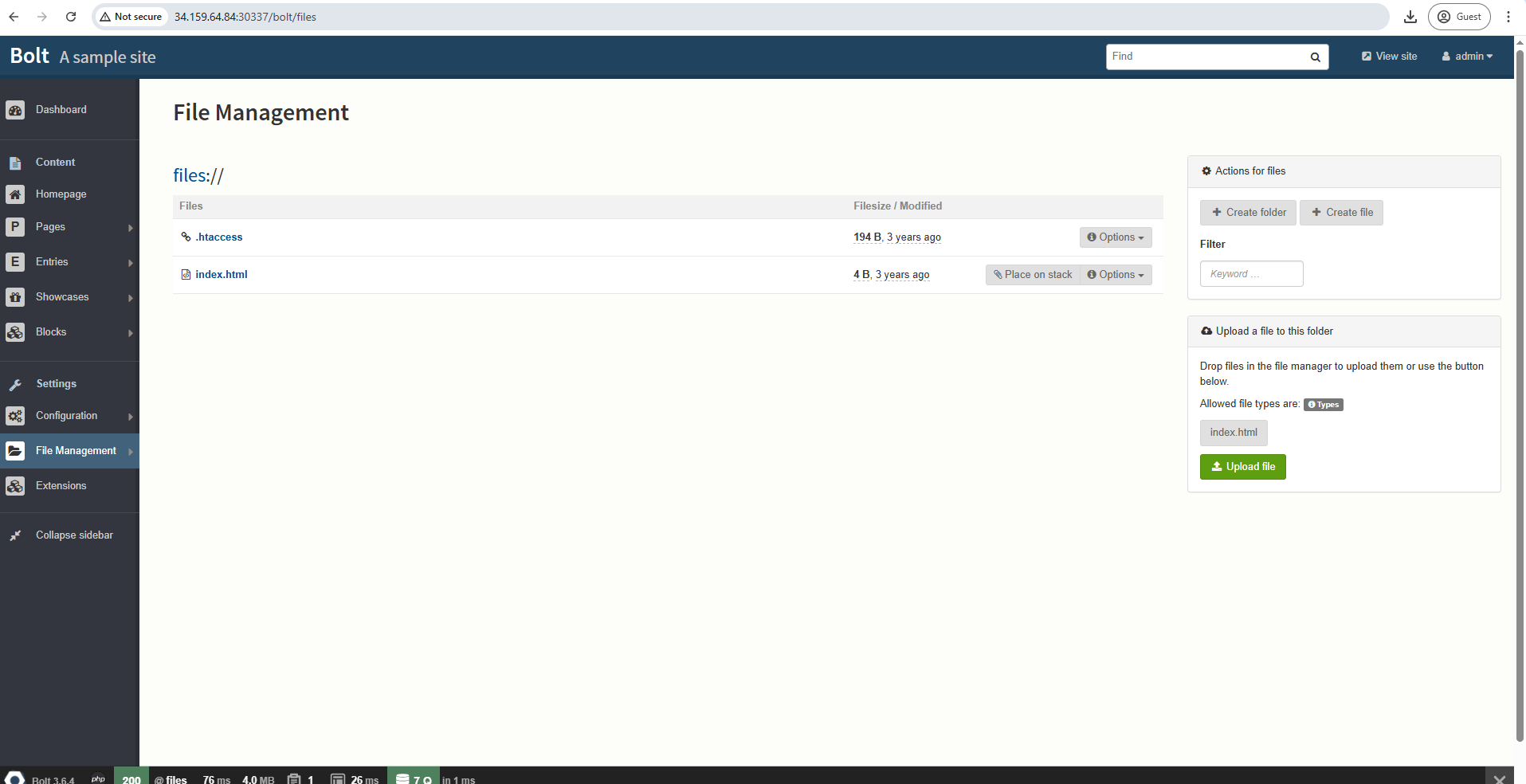
BOLT

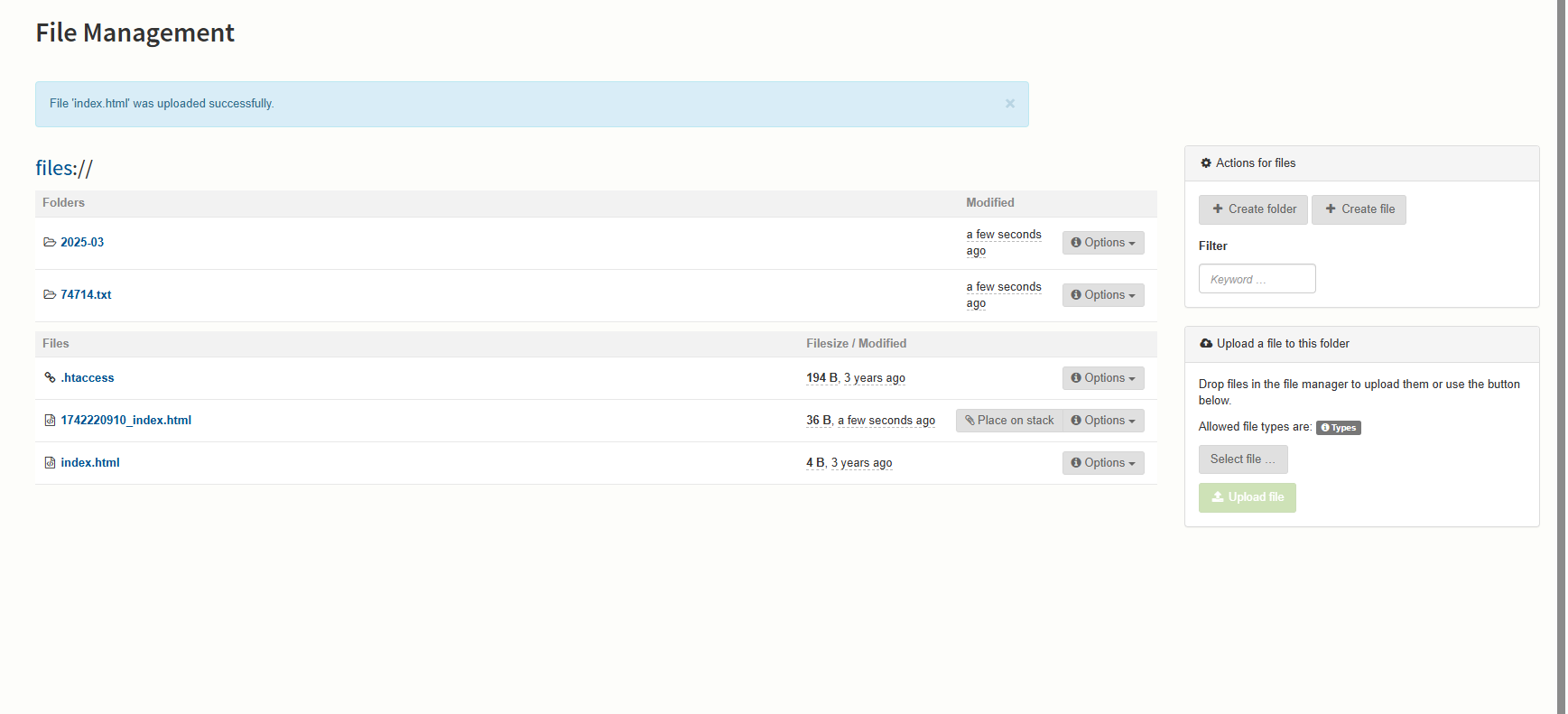
რადგანაც ლაბის აღწერას ქვია BOLT ვივარაუდე რომ ეს არის ბოლტ ზე აწყობილი საიტი შესაბამისად პირდაპირ ლოგინ ფეიჯზე გადავედი და ბრუტფორსით გადავუყევი სავარაუდო დაუცველი პაროლების და იუზერნემებს



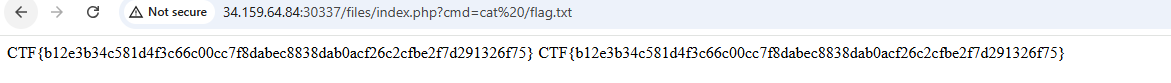
რამაც გაამართლა და admin:password ით შევედით ადმინის ფეიჯზე



ადმინით ავტორიზაციისას ვხედავთ რომ შეგვიძლია ფაილების ატვირთვა სადაც ვეცდებით შევუშვათ ჩვები კოდი <?php echo system($\_GET['cmd']);?>



რომელიც ხედავთ რომ წარმატებით გაეშვა index.html ით (რადგან .პჰპ ით არ ეშვებოდა)

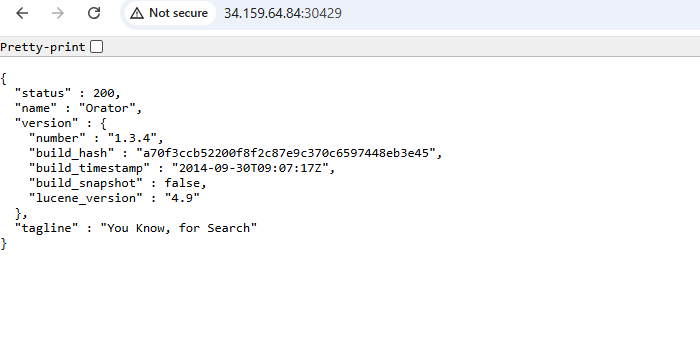
შემდეგ გადავიყვანთ rename ით index.php ლინკზე გადასვლისას ლინკს დავუმატებთ cmd=cat /flag.txt 

და ვხედავთ რომ ფლაგი გმაოიტანა

CTF{b12e3b34c581d4f3c66c00cc7f8dabec8838dab0acf26c2cfbe2f7d291326f75}

Elastic

რადგანაც ლაბს elastic ქვია ვივარაუდებთ რომ ეს საიტი არის elastic search ი საიტზე გადასვლისას ვხედავთ ვერსიასაც შესაბამისად გავუყვებით ამ ვერსიას და დავგუგლავთ მოწყვლადობებს

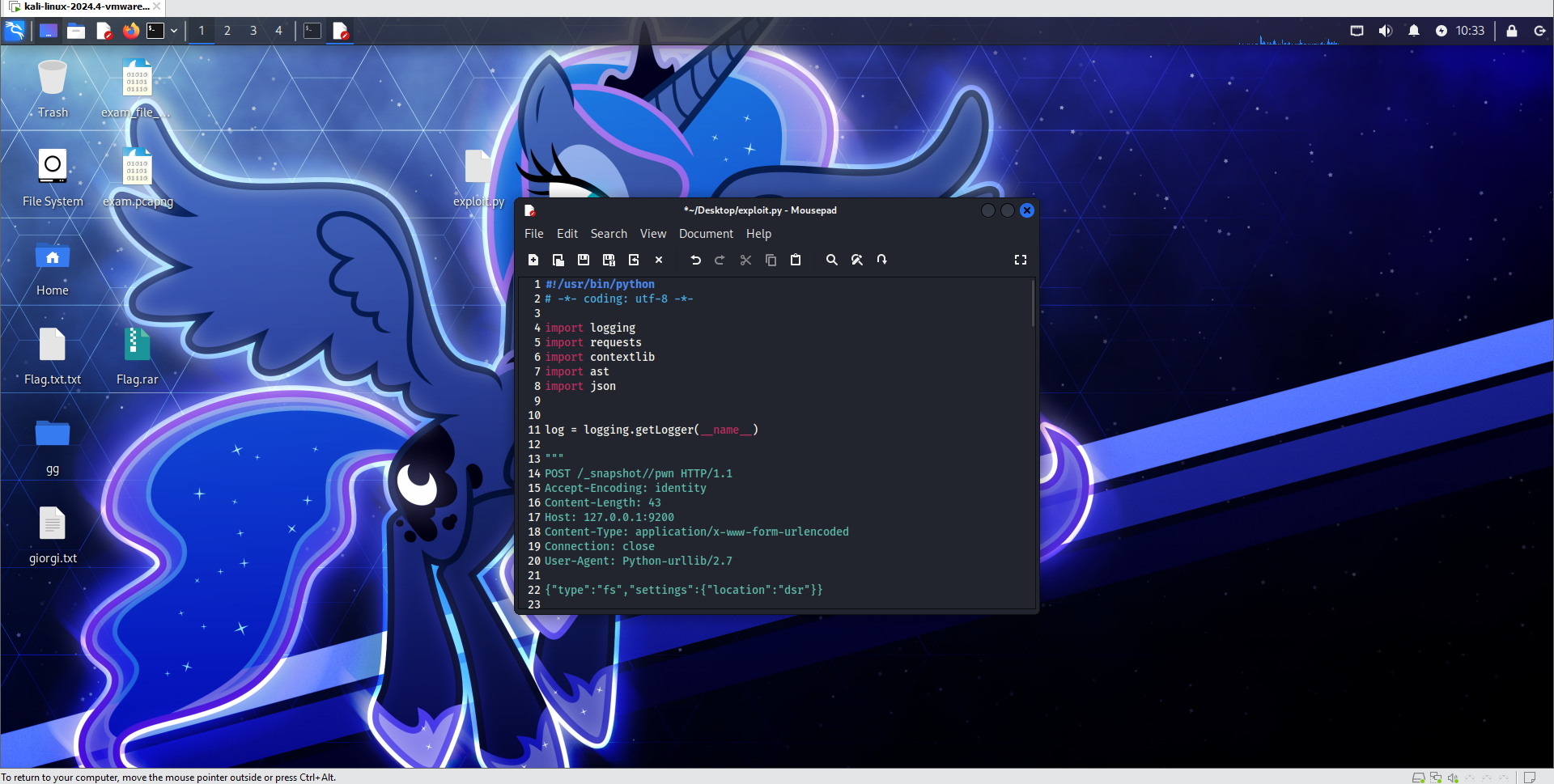


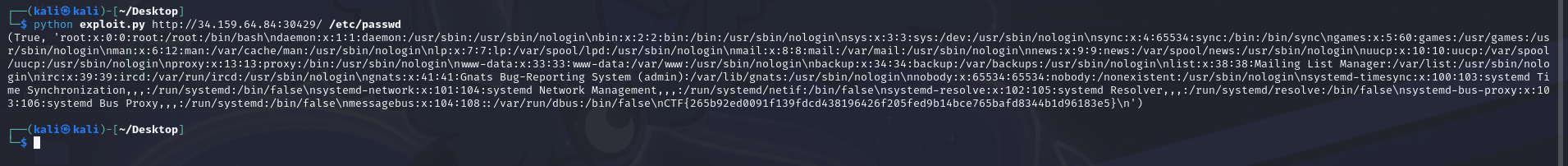
Elastic 1.3.4 Vulnerability CVE ს ის დაგუგვლისას ამომიგდო ერთი საინტერესო ვულნერაბილითი რომელსაც გამოვიყენებთ

**CVE-2015-5531- Arbitrary file Vulnerability**

ასევე დაგუგვლით ვიპოვე ამ ვულნერაბილითის ექსპლოითი github ზე

<https://github.com/nixawk/labs/blob/master/CVE-2015-5531/exploit.py>

რომელსაც ჩავაკოპირებთ ჩვენს კალიში და იქიდან გავუშვებთ



და ვიპოვით ფლაგსაც

CTF{265b92ed0091f139fdcd438196426f205fed9b14bce765bafd8344b1d96183e5}