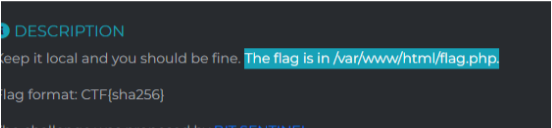
Alien-inclusion

რადგანაც პირდაპირ Description ში გვიწერია რომ flag მდებარეობს /var/www/html/flag/php



შესაბამისად POST Request ით შეგვიძლია მივიდეთ ფლაგამდე

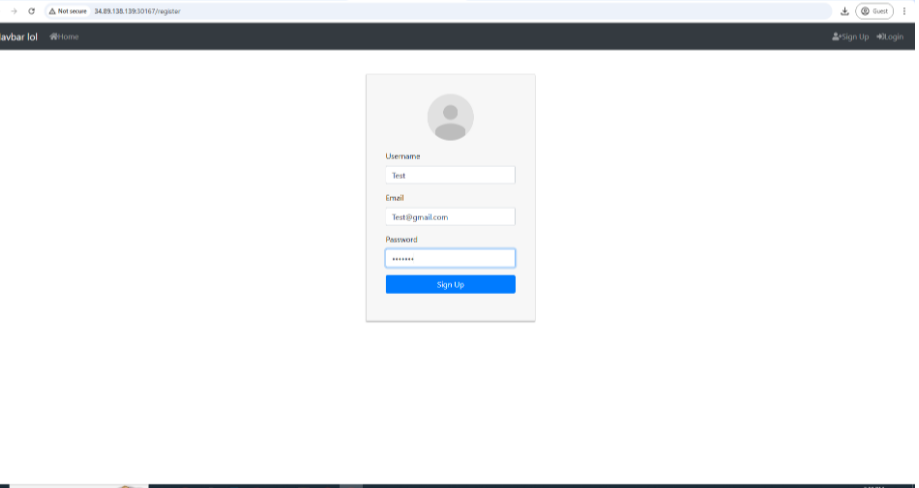
მარტივი ბრძანებით

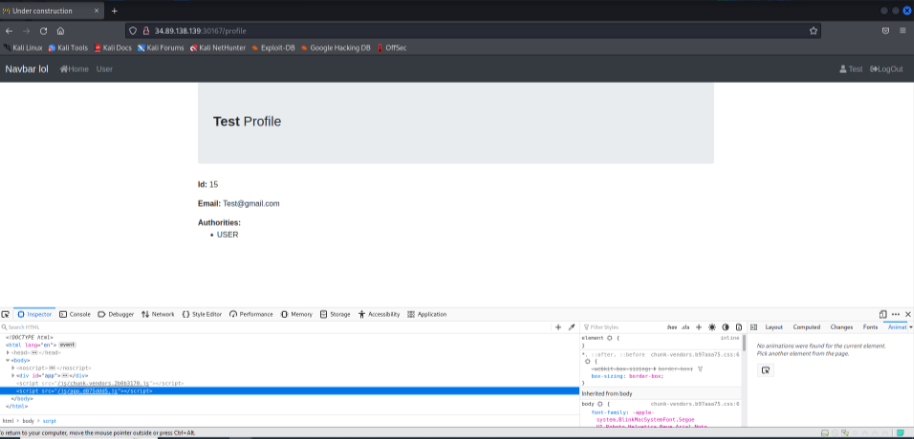
curl ‘http://34.107.26.201:30628/?start=1&’ -XPOST –data ‘start=flag.php’

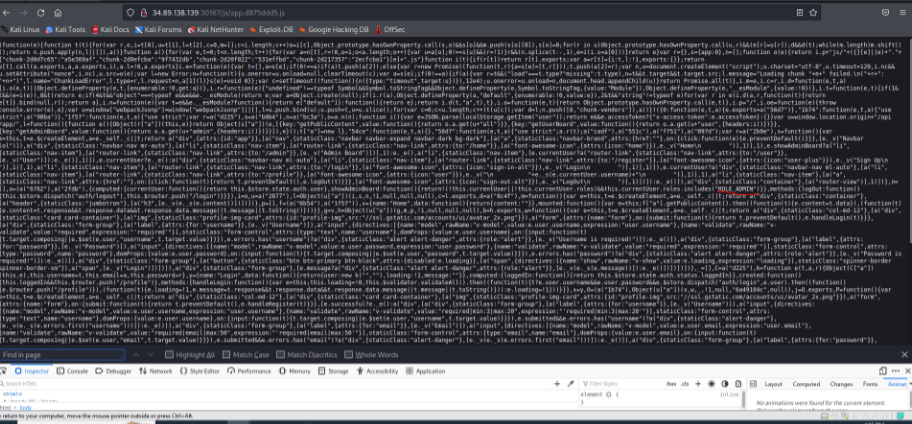


Under-construction

პირველ რიგში ვქმნით ექაუნთს



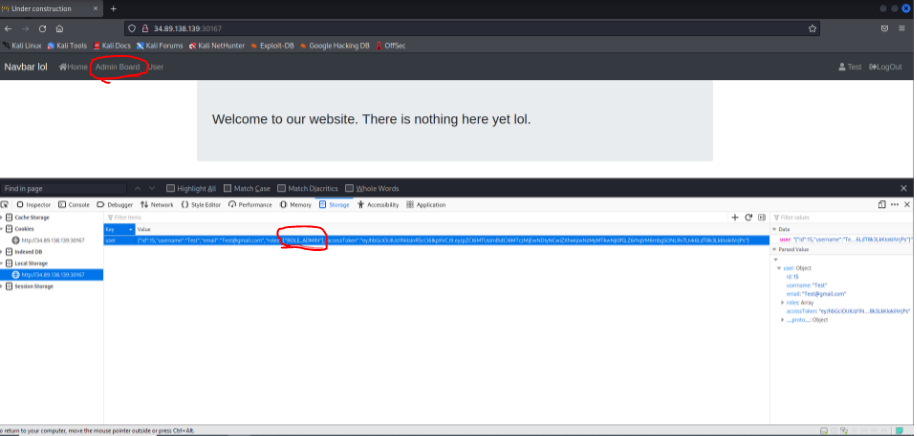
დაlogინების შემდეგ ინსპექტორში ვხედავთ შემდეგ მისამართს 

ამURL ის შემოწმებისას წავაწყდებით ასეთ რაღაცას: არსებობს როლი ROLE\_ADMIN და USER რომელიც ჩვენ გაგვაჩნია

შემდეგ Local Storage იდან თუ საკუთარ თავს USER როლის მაგივრად მივცემთ ROLE\_ADMIN

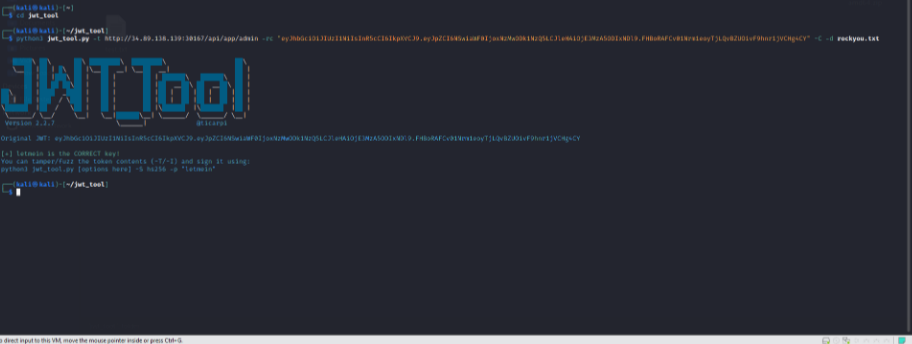
და დავარესტარტებთ საიტს დავინახავთ რომ გამოგვიჩდნებდა ახალი ღილაკი Admin Board

ნავიგაციის ველზე



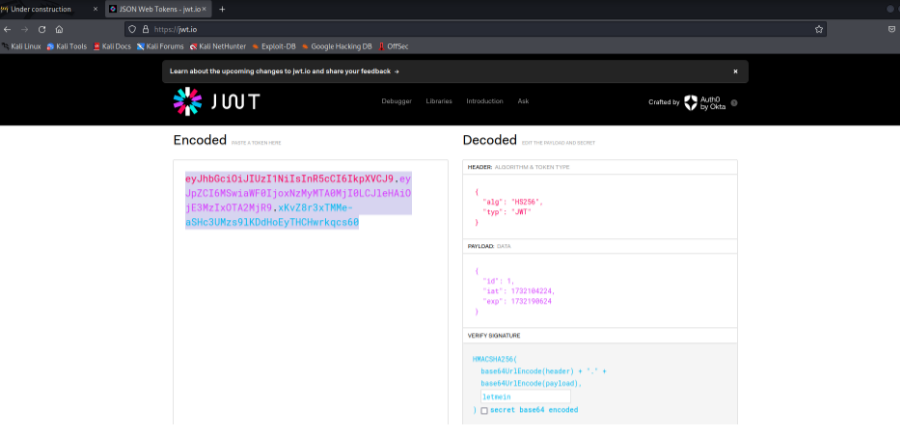
შემდეგ JWT\_tool ის,Rockyou listით და ჩვენი Token ის მეშვეობით ვიგებთ რა არის Secret

Key რომელიც როგორც JWT\_Tool მა გვითხრა არის letmein



რადგან უკვე გვაქვს ტოკენი და Secret ასევე ვიცით რომ რადგან ჩვენ ვართ ID:15 ადმინი

უნდა იყოს ID:1



ვცვლით IDს ,ტოკენს ვარესტარტებთ ადმინის dashboards და გვხდება ფლაგი

