Lab: elastic

მითითებულ IP მისამართზე შესვლისას, ეკრანზე მოცემული შედეგით საკმაოდ დიდი ინფრომაციის მიღება შეიძლება.

A computer code on a white background

Description automatically generated

ვიღებთ ინფორმაციას ვერსიის შესახებ. ამ შემთხვევაში ვხედავთ რომ გამოყენებულია 1.3.4 ვერსია. ამიტომ ვეძებ ცნობილ სისუსტეებს elastic ვერსია 1.3.4 ზე. ინტერნეტში ძებნის შედეგად გადავაწყდით Arbitrary file read CVE. ამაზე exploit შეგვიძლია ვიპოვოთ [**CVE-2015-5531- Arbitrary file Vulnerability**](https://github.com/nixawk/labs/blob/master/CVE-2015-5531/exploit.py)**.** ამ exploit-ის გამოყენებისთვის უნდა გავუშვათ შემდეგი ბრძანება: python3 exploit\_elastic.py IPIPIP /etc/passwd დაბრუნებულ შედეგში ჩანს ჩვენი CTF.