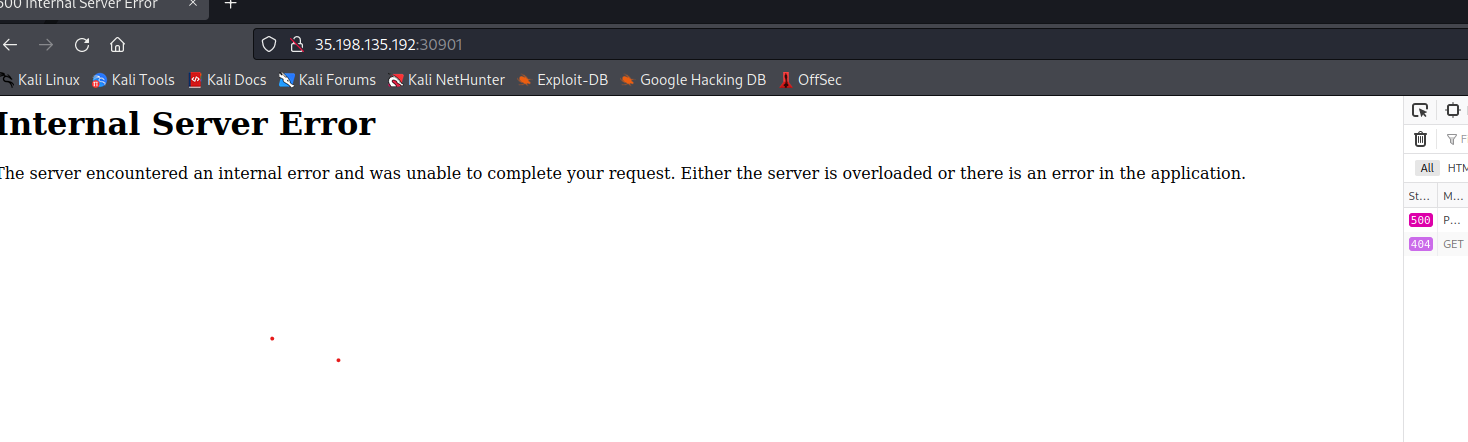
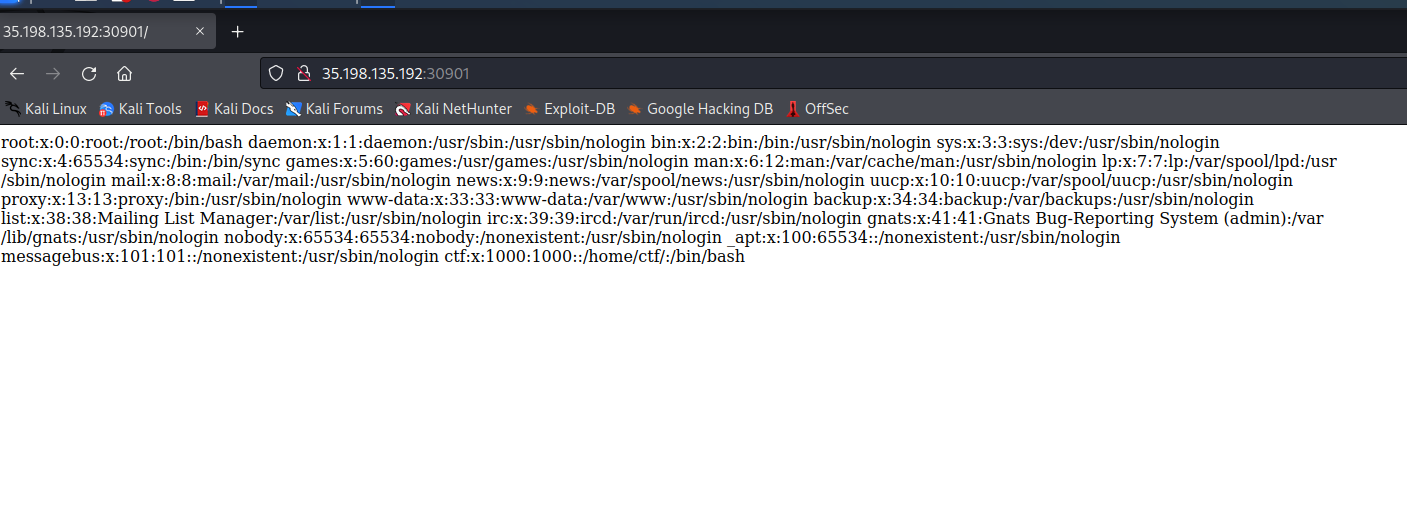
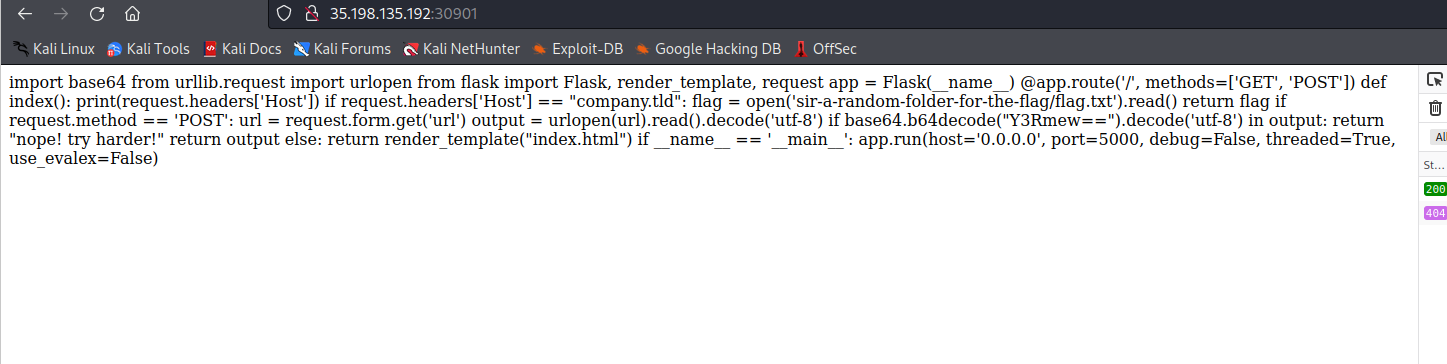
DAVIT KILADZE

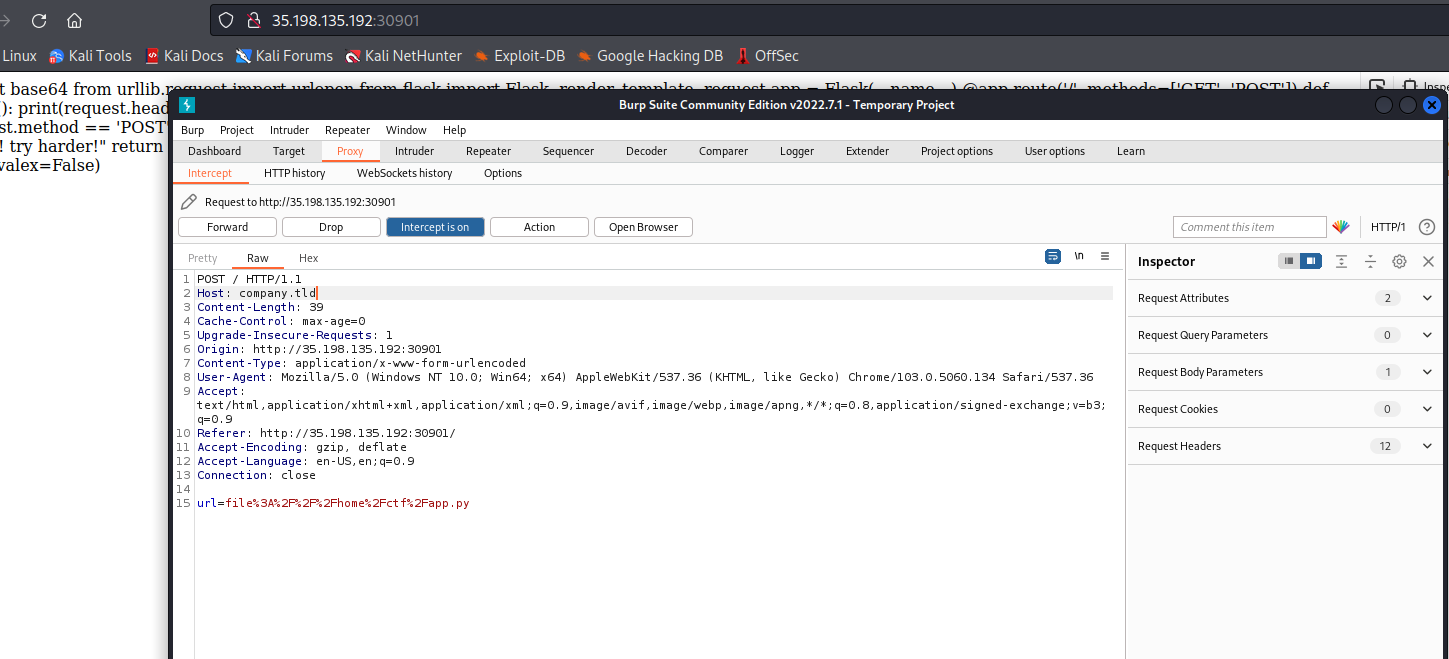
1.Ultra Crawl

თავდაპირველად ველში გავუშვი url facebook.com, სერვერმა დაგვიბრუნა შიდა ერრორი,

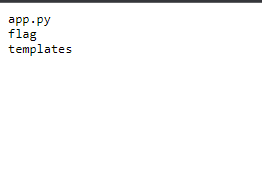


ახლა გავტესტავ LOCAL FILE INCLUSION მოწყვლადობას, გასატესტად გამოვიყენებ მარტივ ფეილოადს: <file:///etc/passwd>: 

აქედან გამომდინარე, საქმე გვაქვს local file inclusion მოწყვლადობასთან, ჩვენ შეგვიძლია დავინახოთ /home/ctf ბოლოში, რაც მიგვანიშნებს იმაზე რომ ctf ფოლდერის არის home ფოლდერში,ამიტომ შეგვიძლია გავუშვათ რამდენიმე ფაილოად რათა გავარკვიოთ თუ რა ენაზეა გაშვებული სერვერი, საცდელი მაგალითებია index.php, index.py, app.php,app.py, აქედან იმუშავა ბოლო ფაილმა: 

აქ გადავაწყდი ასეთ პირობას if request.headers['Host'] == "company.tld": flag = open('sir-a-random-folder-for-the-flag/flag.txt')., აქედან გამოდმინარე შეგვიძლია გამოვიყენოთ burp suite ან curl, რათა მოვახერხოთ ჰეადერების ჩანაცვლება და შესაბამისი პარამეტრის გადაცემა ჰეადერებშ რათა იმუშაოს ამ პირობამ, მე გამოვიყენებ ბურპ სუიტს,  ჰოსტის ადგილას უნდა ჩავწეროთ სურათზე ასახული ტექსტი რათა სერვერის კოდმა შეასრულოს კონრკეტული პირობა რის მიხედვითაც უკან დაგვიბრუნებს ფლაგს, დაგვიბრუნა პასუხი ctf{d8b7e522b0ab04101e78ab1c6ff68c4cb2f30ce9d4427d4cd77bc19238367933}

2. PING STATION

უპირველეს ყოფლისა ველში ვუთითებ იმას რაც წერია, იპ მისამართი, მაგალითად 8.8.8.8, სერვერი გვიბრუნებს შიდა ერრორ, ახლა ვცდი გაგზავნას იგივე იპ მი სამართის თმცაღა გავუშვებ command injection-ს 8.8.8.8; ls, ამან დამიბრუნა პასუხი :  რაც ნიშნავს იმას რომ მივაგენით ფლაგს

, ახლა გავუშვებ კომმანდს რომ წავიკითხო ფლაგი, 8.8.8.8; cat flag, დამიბრუნა ECSC{b1c0bc8e5e1b4c81199ad3c41bef8b69bea3ab86ecfb08c211d90ace0ff98df3} პასუხი, რაც იმას ნიშნავს რომ საიტი გავტეხეთ, იმისათვის რომ command line injection -ისგან თავი დავიცვათ ტექსტი უნდა გაიფილტროს front is an back is მხარეს, არუნდა შეიცავდეს ||, &&, ; და $() ოპერატორებს ტექსტი,