NAMA SEKOLAH : SMK NEGERI 2 BANDUNG

Selasa 14 Mei 2024

Ketua Tim :

Muhammad Akhtar Khawarizmi

Anggota Tim :

Harvi Muhammad Zakhir

CTF SOAL 5

IP : 192.168.10.225

Recon

Pada soal kali ini kita diberikan sebuah ip, pertama-tama mari kita lakukan recon dengan menggunakan tools nmap :

Exploit

Setelah kita scan, kita menemukan bahwa port 80 terbuka, maka mari kita coba masuk lewat browser :

Setelah menjelajahi website tersebut, saya menemukan bahwa kita dapat mengubah parameter yang berada di url /show :

Saya langsung mencoba meng-inject sql query ke dalam parameter tersebut :

192.168.10.225/show.php?id=1+order+by+1--+-

Namun ternyata tidak muncul, sayapun mencoba mencari url lain, akhirnya saya menemukan parameter ‘id’ pada /cat.php/

Saya pun mencoba meng-inject sql query ke dalam parameter tersebut :

:

Sayapun mencoba mengubah 192.168.10.225/show.php?id=1+order+by+1--+-

Dengan 192.168.10.225/show.php?id=1+order+by+n--+-, sampai sqlnya error :

Dengan begini bisa kita pastikan bahwa table dari website tersebut ada 4, setelah itu kita coba masukkan sql-inject :

-

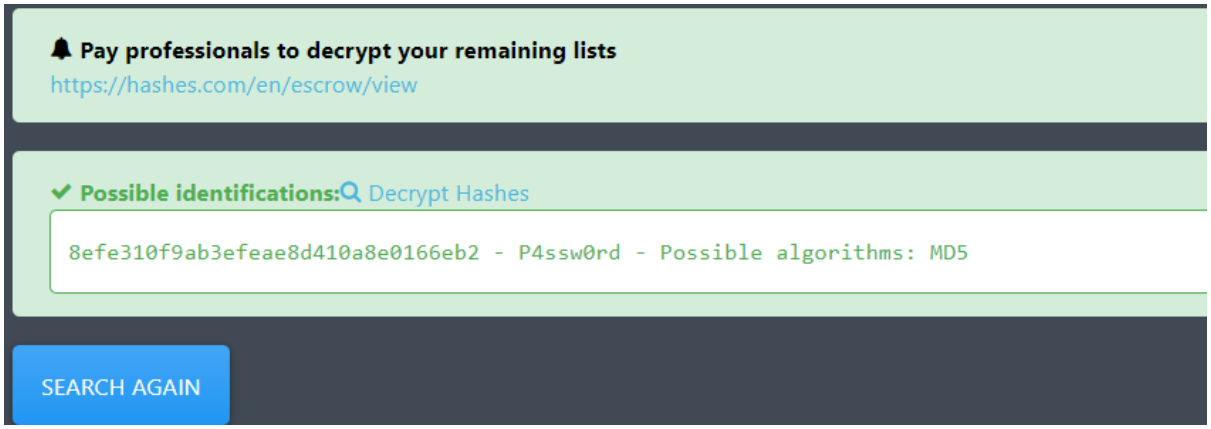
3+union+select+1,(select(@x)from(select(@x:=0x00),(select(0)from(information_schema.columns)where(table_schema=database())and(0x00)in(@x:=concat+(@x,0x3c62723e,table_name,0x203a3a20,column_name))))x),3,4--+-

Maka akan muncul semua tabel yang ada di website tersebut, dengan begitu kita coba mengambil value kolom ‘login’ dan ‘password’ dengan meng-inject query :

-

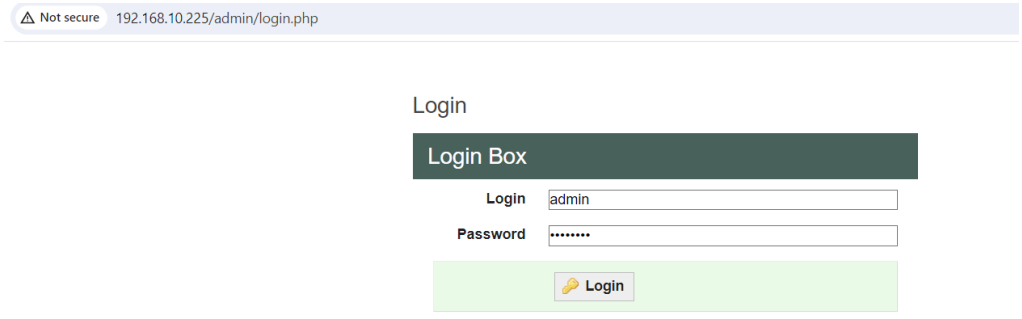
3+union+select+1,/*!50000(SELECT+GROUP_CONCAT(login,0x3a,password+SEPARATOR+0x3c62723e)+FROM+users)*/,3,4--+-

Maka kita berhasil mendapatkan data dari username & juga passwordnya, namun password tersebut mungkin sudah di hash, kita coba cari value aslinya :

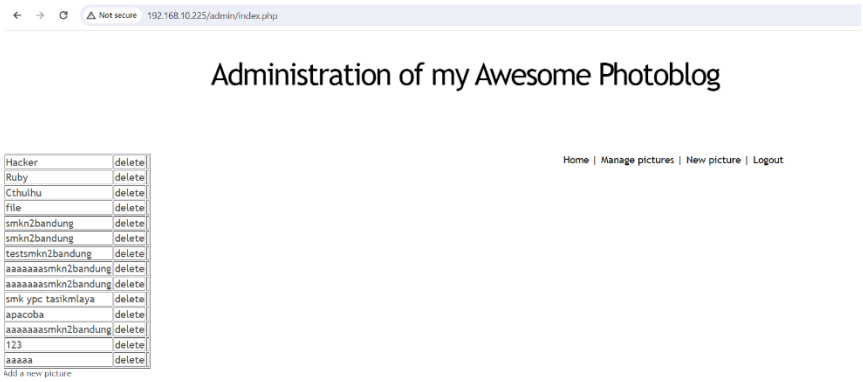


Maka kita berhasil mendapatkan passwordnya yaitu : P4ssw0rd

Setelah itu mari kita coba login menggunakan kredensial :
Login = admin & Password = P4ssw0rd

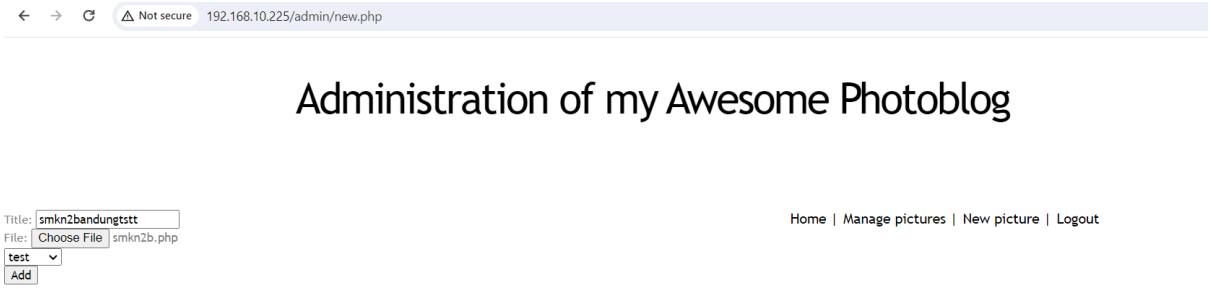


Maka kita berhasil Login sebagai admin :

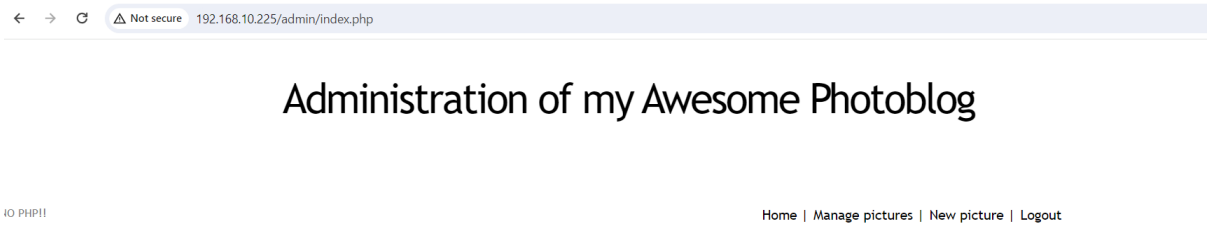


Post Exploit

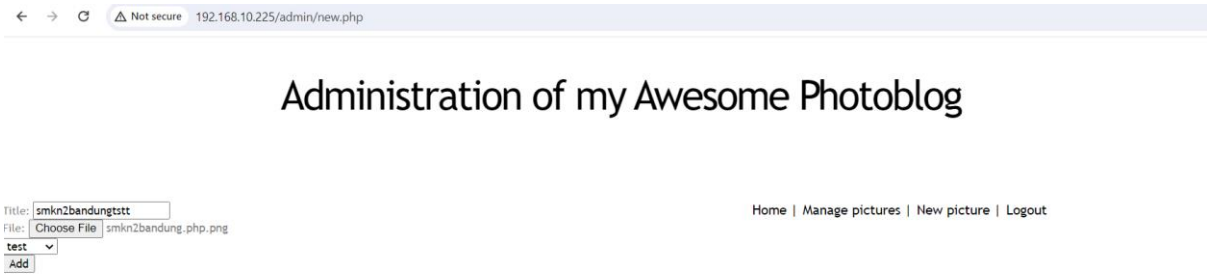
Karena disini tujuannya mengupload Shell Backdoor, maka saya coba mengupload file dengan ekstensi .php :



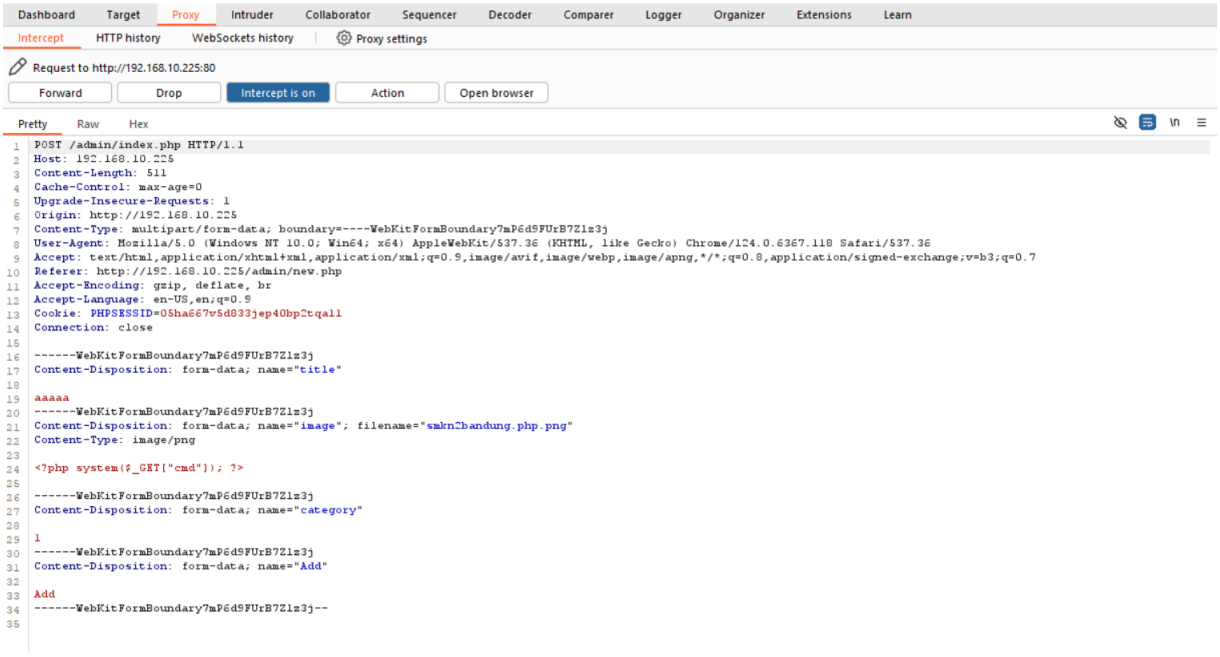
Namun server menolak file yang saya upload (NO PHP):



Maka saya mencoba melakukan tempering data dengan mengubah ekstensi menjadi .php.png :



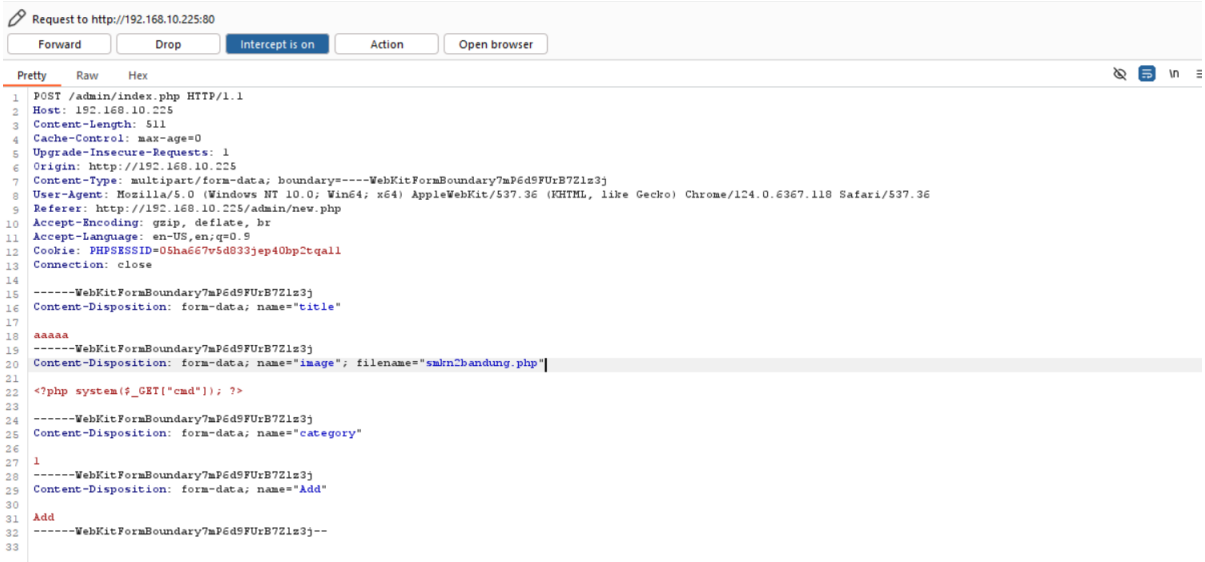
Setelah itu saya intercept request terlebih dahulu di burpsuite :



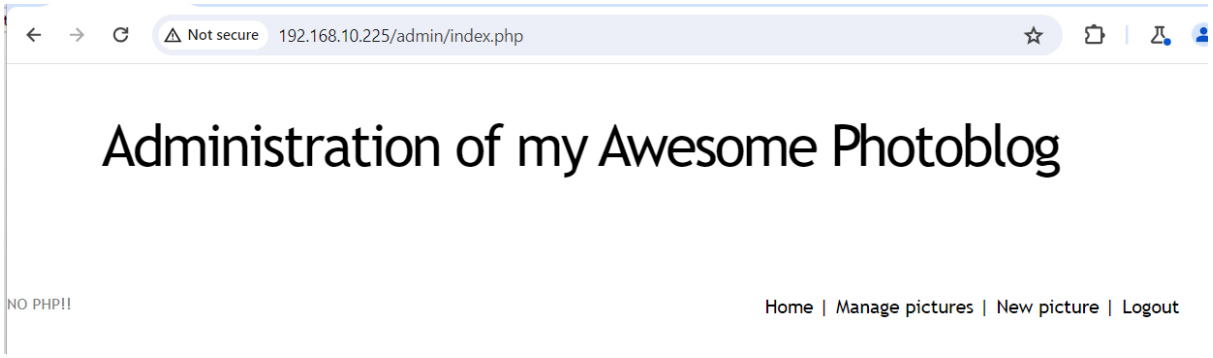
Lalu mengubah :
ekstensi yang awalnya .php.png menjadi .php

Content-Typenya pada data image saya hapus

Header Accept juga saya hapus :



Setelah itu saya klik forward, namun ternyata website masih menolak file yang saya upload :



Saat pengerjaan soal saya cukup sampai sini dikarenakan waktu habis, tapi saya masih terpikirkan bagaimana jika ekstensi bukan dirubah menjadi .php melainkan .pHP, apakah website masih menolak?