**LATIHAN ATTACK & DEFENSE**

**[CYBER SECURITY]**

**Reja Revaldy F.**

**Rezka Norhafizah**

**ATTACK & DEFENSE**

[ATTACK 3](#_Toc85548047)

[FILE UPLOAD VULNERABILITY 3](#_Toc85548048)

[DIRECTORY BRUTEFORCE 5](#_Toc85548049)

[PHP COMMAND INJECTION 6](#_Toc85548050)

[RCE (REMOTE CODE EXECUTION) 7](#_Toc85548051)

[SHELL SPAWNING 8](#_Toc85548052)

[LOGIN 9](#_Toc85548053)

[PRIVILEDGE ESCALATION 11](#_Toc85548054)

[SQL INJECTION 12](#_Toc85548055)

[PASSWORD BRUTEFORCE 14](#_Toc85548056)

[DEFENSE 15](#_Toc85548057)

[REGISTER 15](#_Toc85548058)

[LOGIN 15](#_Toc85548059)

[FILE UPLOAD 16](#_Toc85548060)

[HIDDEN DIRLISTING & APACHE VERSION 17](#_Toc85548061)

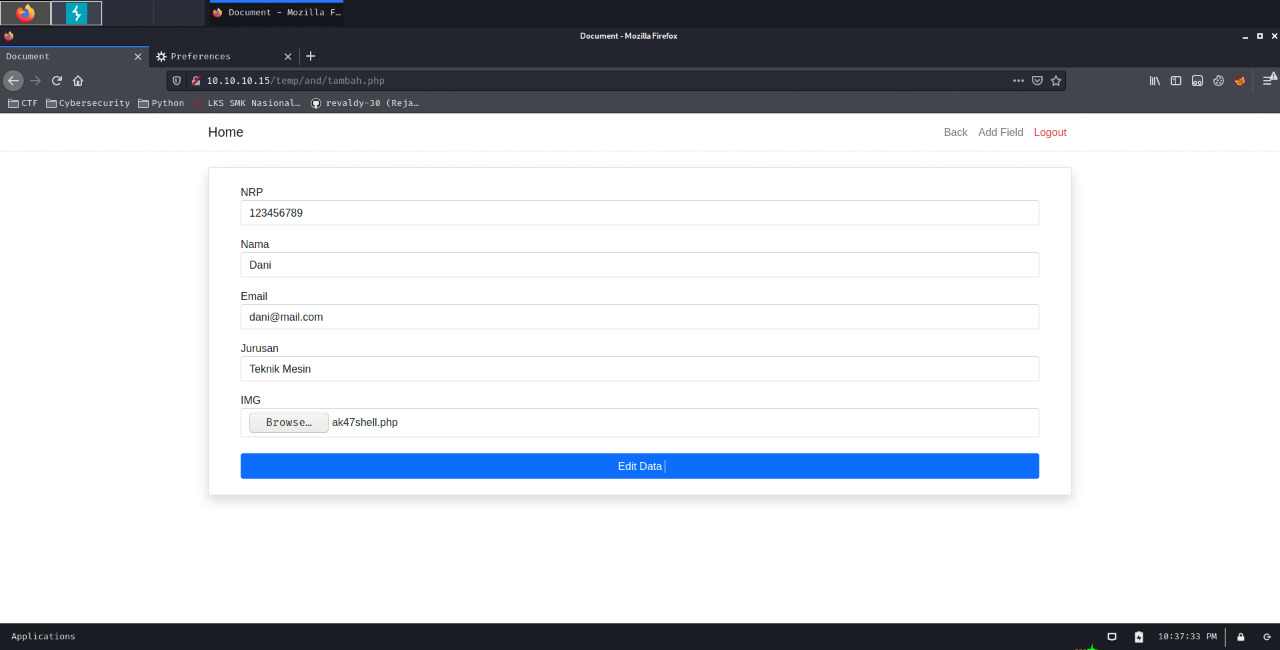
[CHANGE PERMISSION 19](#_Toc85548062)

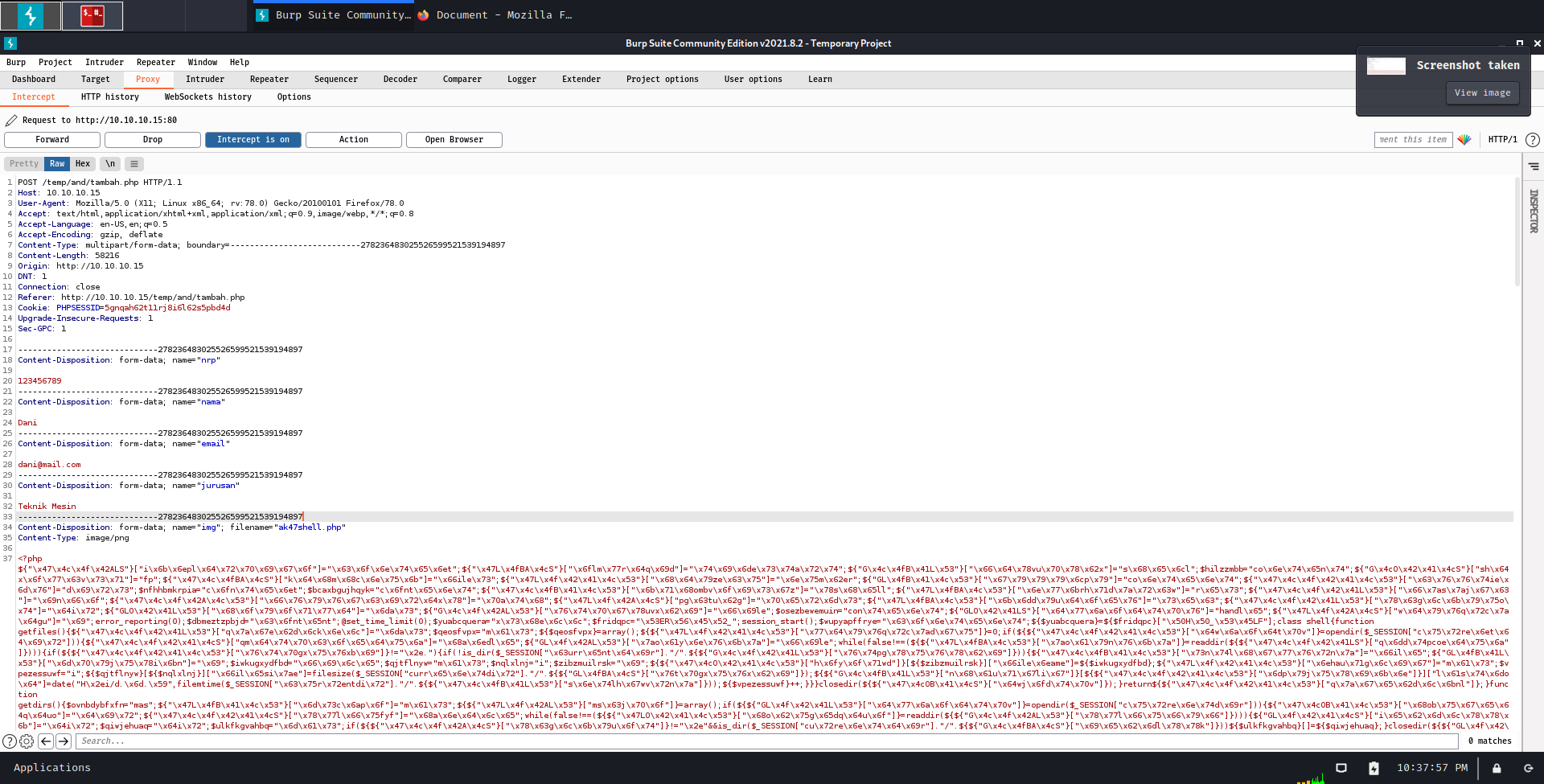
# ATTACK

## FILE UPLOAD VULNERABILITY

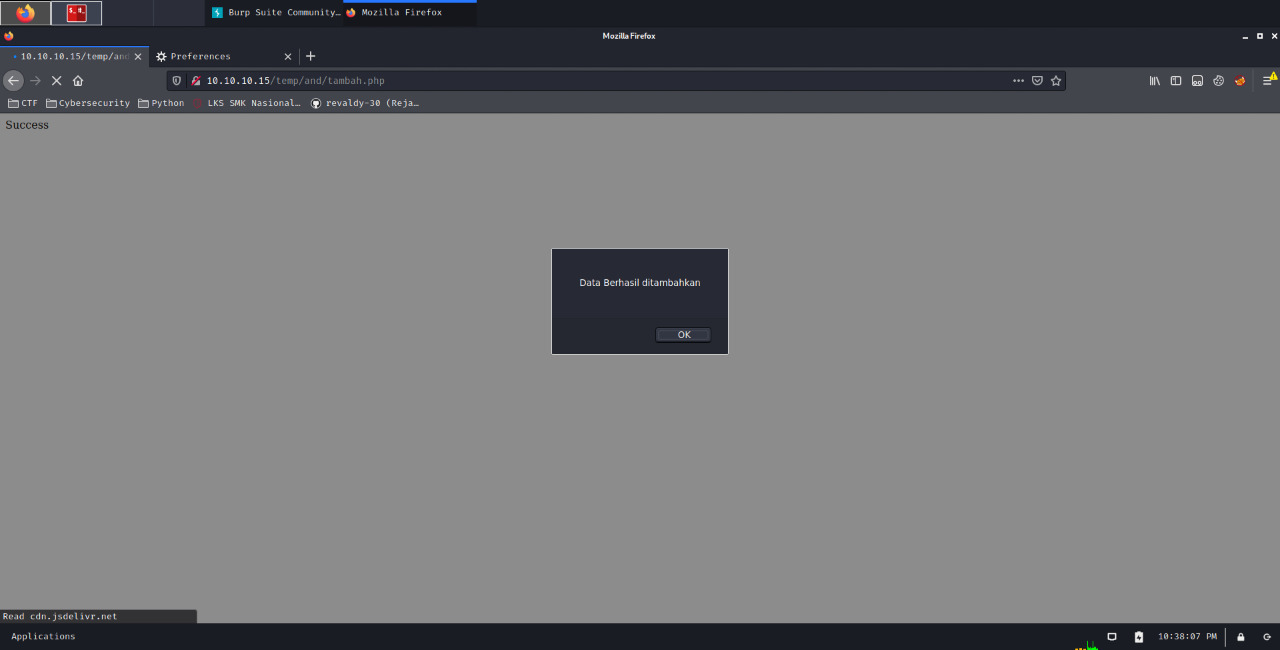
Di website ini, diberikan halaman untuk menambahkan data siswa ke database server dan disertakan form upload. Setelah kami coba, form upload ini ternyata hanya memperbolehkan file bertipe image.

Kemudian, kami menggunakan software burp suite untuk melakukan interception terhadap website, lalu kami upload shell dan dimodifikasi content type-nya menjadi image yang bertipe png :



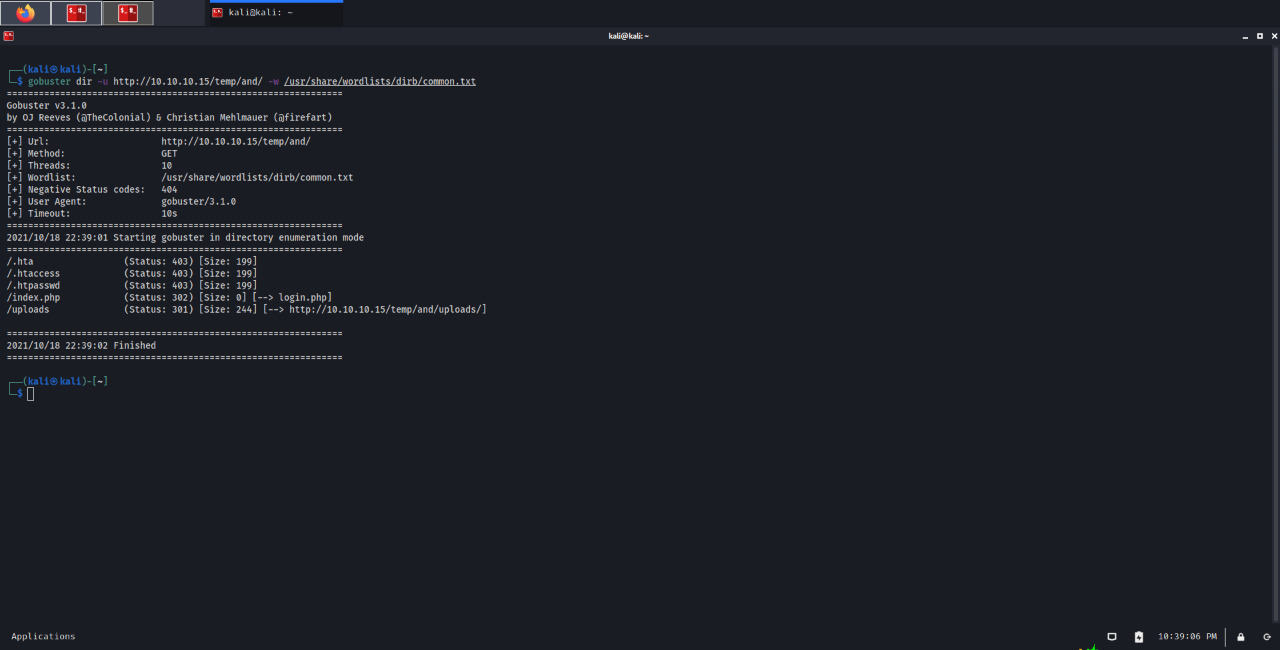


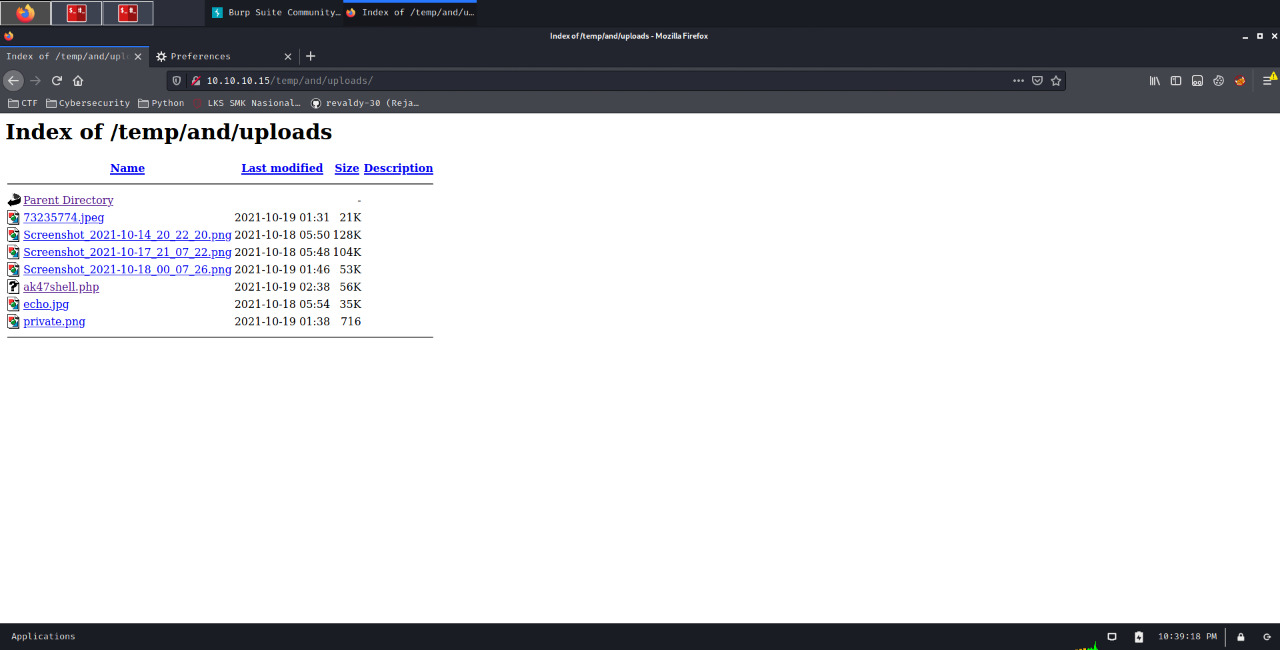
Maka, file yang telah kami modifikasi tadi berhasil diupload ke server :



## DIRECTORY BRUTEFORCE

Untuk mengetahui letak directory penyimpanan file yang diupload tadi, kami menggunakan gobuster dengan wordlist “common.txt” dan menemukan folder uploads :

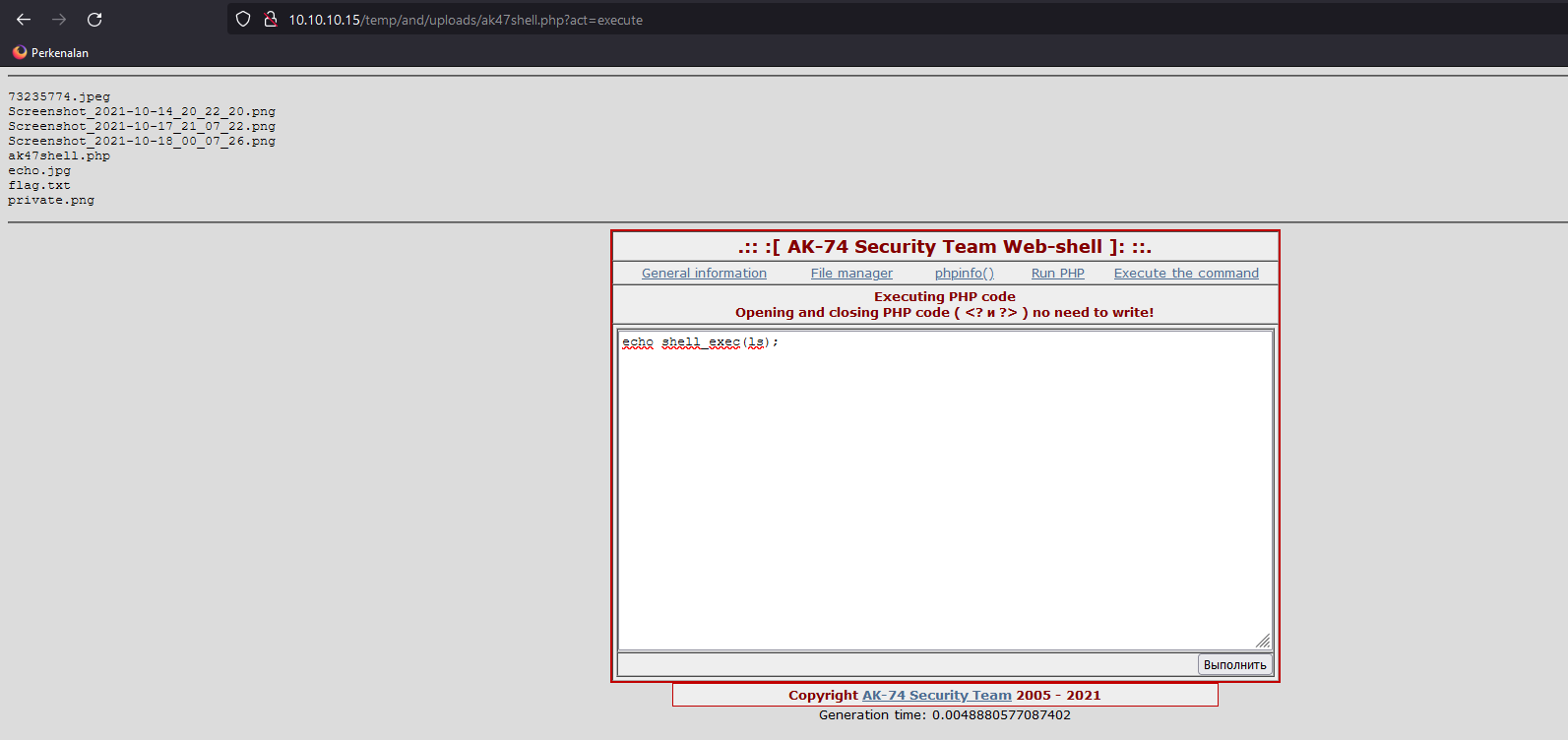




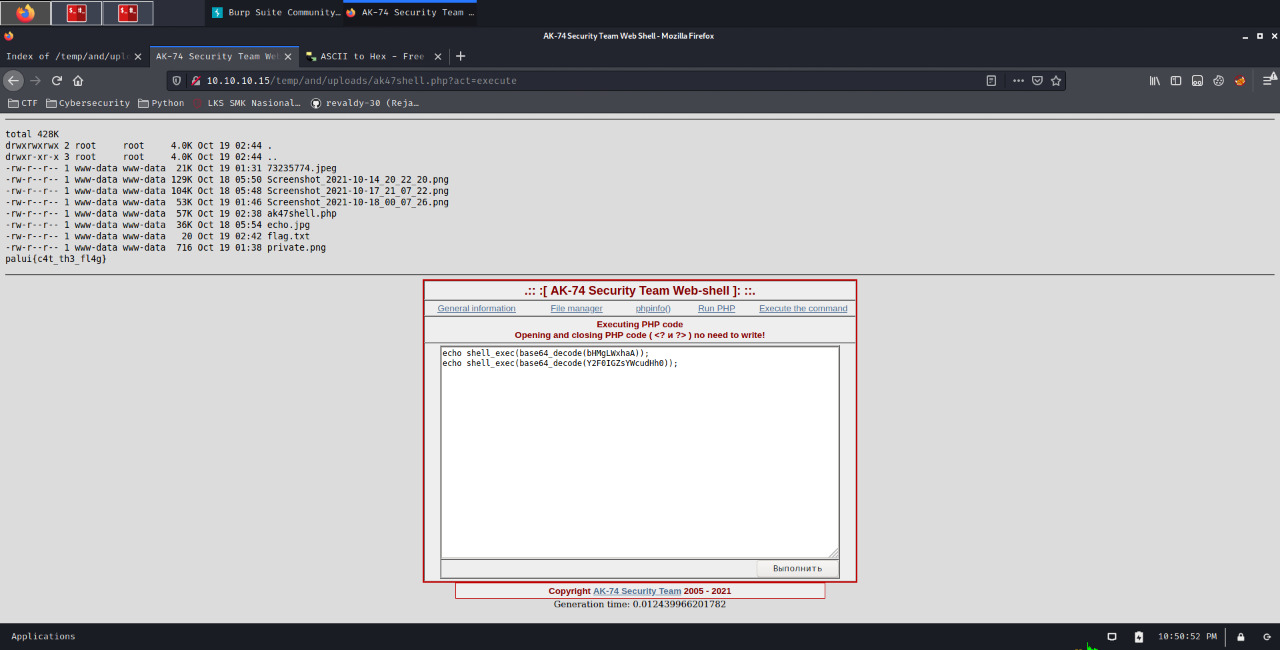
## PHP COMMAND INJECTION

Setelah itu, kami coba eksekusi shell tersebut dan berhasil. Di sini kami menggunakan reverse shell ak47 (source : <https://github.com/backdoorhub/shell-backdoor-list>).

Setelah itu, kami mencoba jalankan script php di shell tersebut untuk melakukan command injection terhadap server. Pertama-tama kami mencoba mengeksekusi command ls pada shell seperti pada gambar :

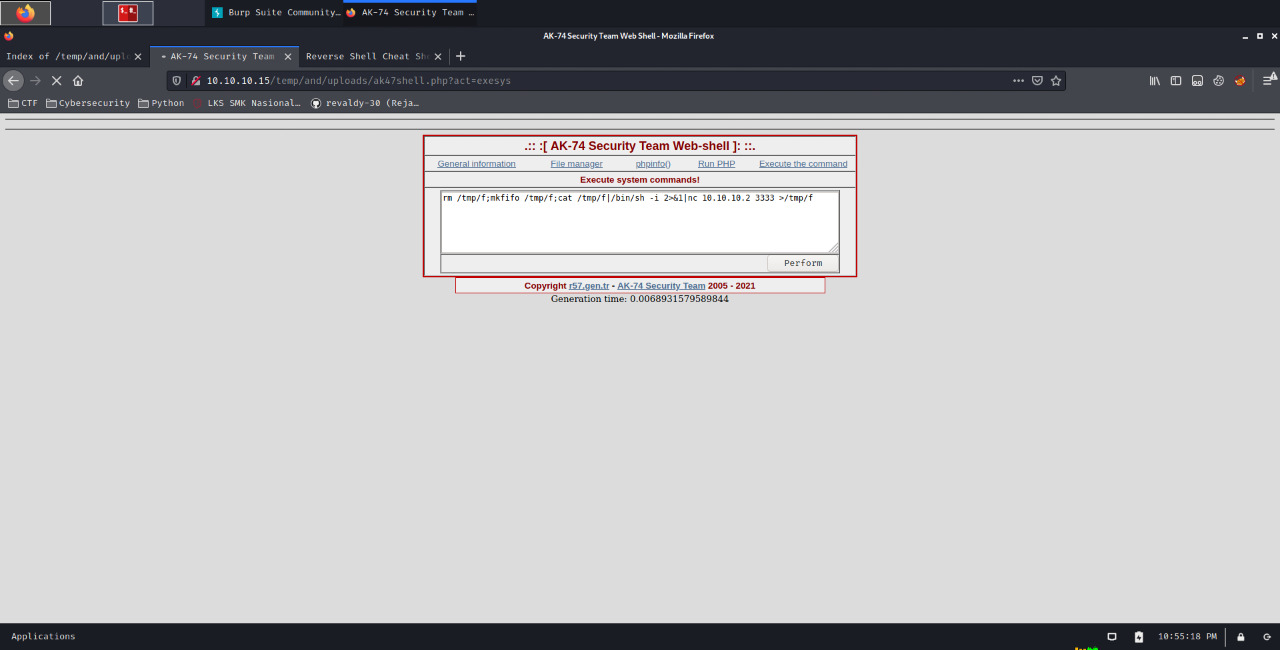


Di sini kami menemukan sebuah file flag dan kami mencoba untuk melihat apa isi dari file tersebut menggunakan perintah “cat flag.txt” tapi ternyata tidak bisa dieksekusi. Kemudian kami melakukan bypass pada command tersebut dengan cara base64 decode :

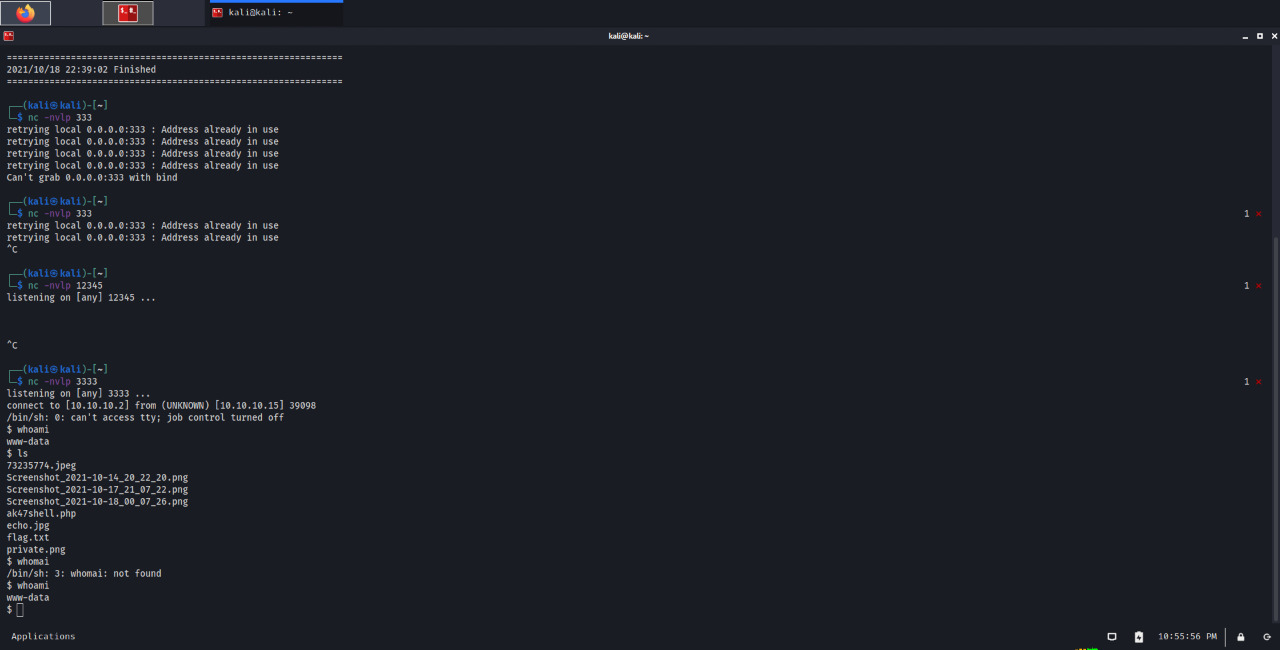


## RCE (REMOTE CODE EXECUTION)

Selanjutnya, kami mencoba melakukan RCE melalui nc di reverse shell :

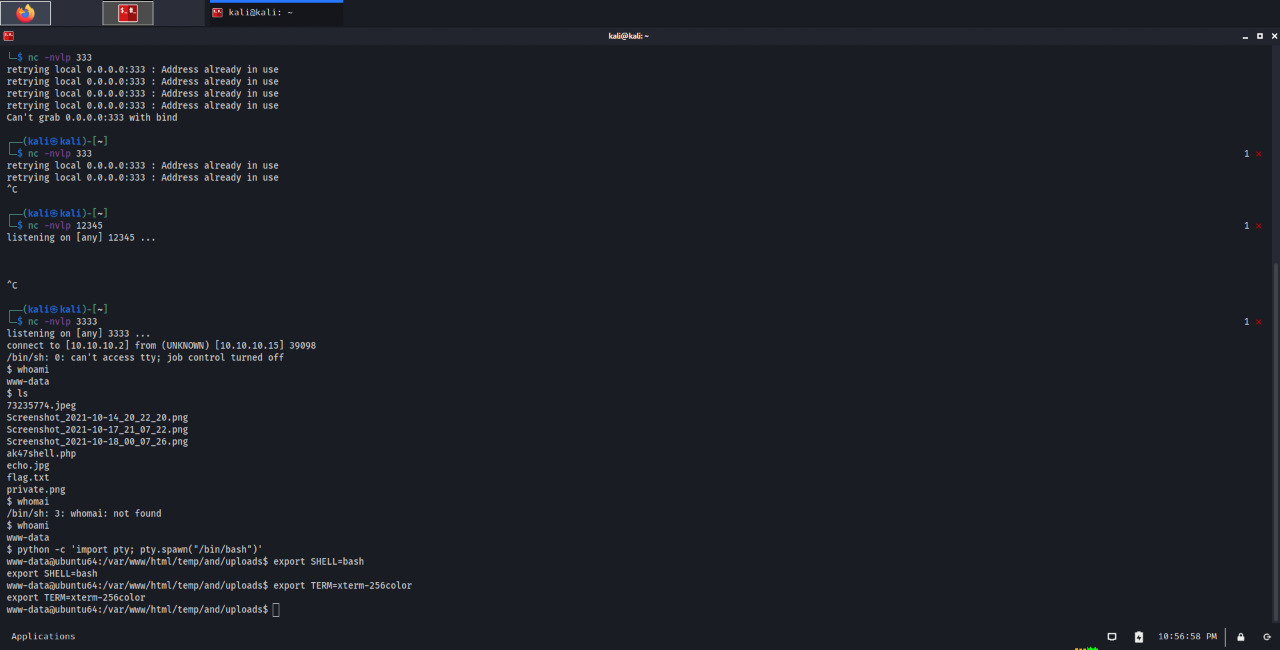


Kemudian kami jalankan agar bisa listen di port 3333 dan kami berhasil masuk ke server :



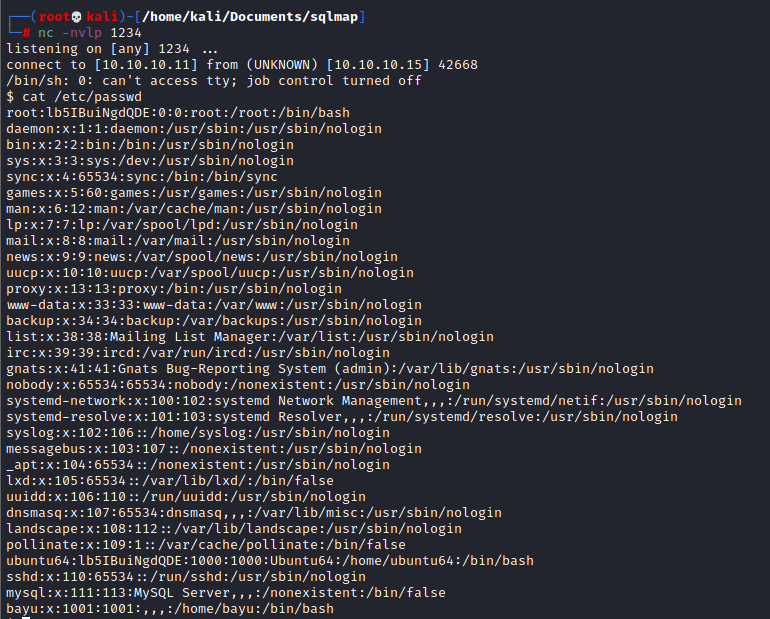
## SHELL SPAWNING

Kami menggunakan python untuk melakukan spawning bash :

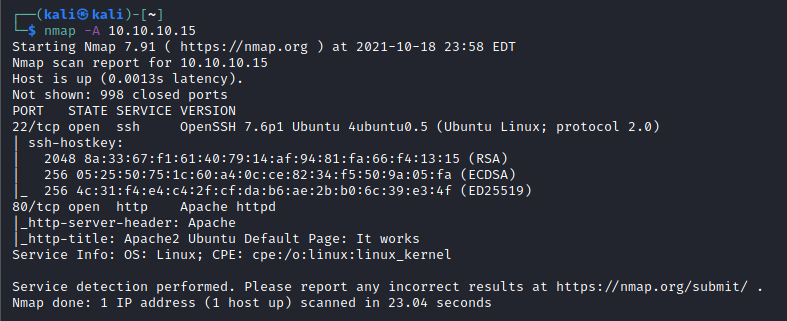


## LOGIN

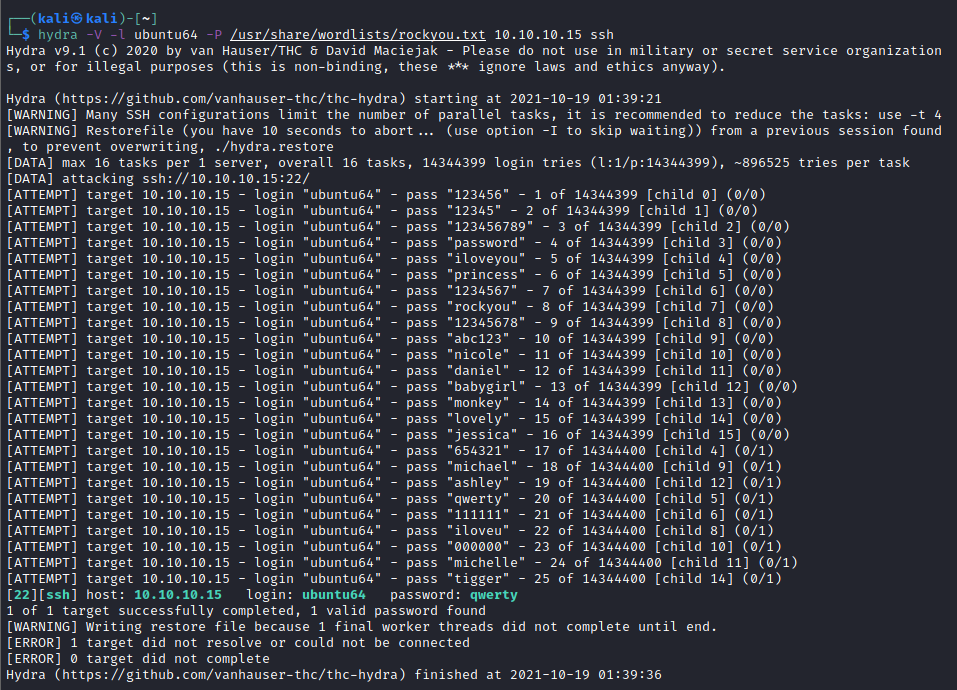
Setelah melakukan spawning bash kami mencoba untuk melihat user yang terdapat dalam server :



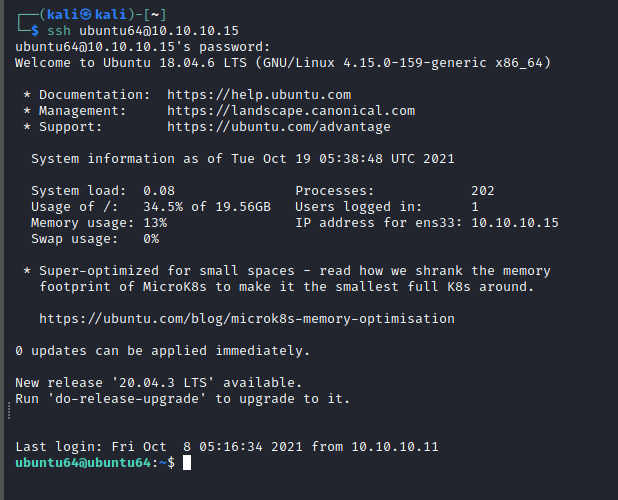
Didapat user selain root yaitu ubuntu64 dan bayu. Kemudian, kami coba scan menggunakan nmap untuk melihat port apa saja yang open :



Terdapat dua port yang open di sini, yaitu port 22 dan port 80. Selanjutnya kami coba brute force menggunakan tools hydra dan memakai wordlist rockyou.txt :



Didapat passwordnya yaitu qwerty, lalu kami login melalui ssh :

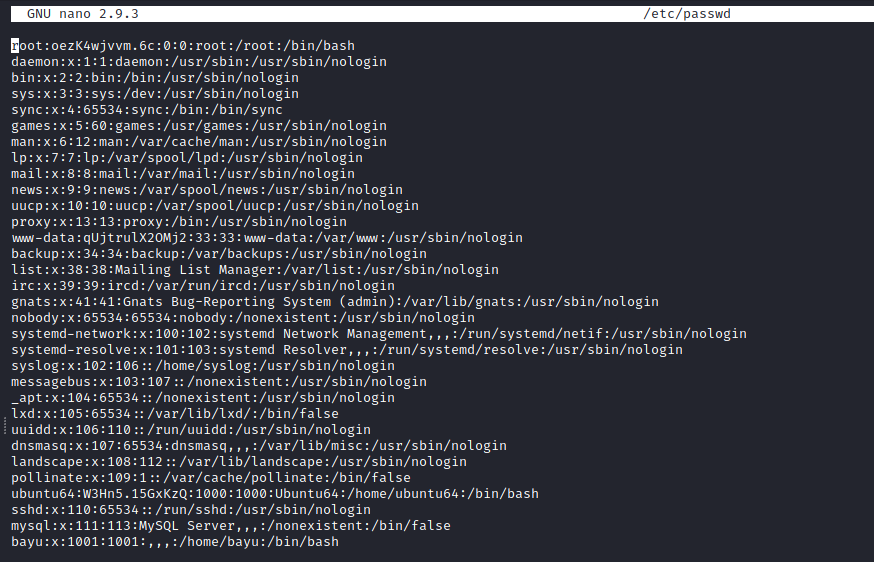


## PRIVILEDGE ESCALATION

Setelah berhasil login ke user, untuk masuk ke root kami mengubah password ke root-nya, yaitu dengan cara meng-generate password baru yaitu abcd :



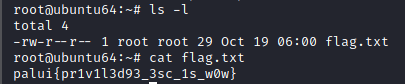
Selanjutnya, pada file /etc/passwd kami edit password untuk root-nya menjadi password baru yang sudah digenerate tadi dan kami simpan file nya :



Lalu, kami coba login ke root dan memasukkan password yang baru, kemudian berhasil :

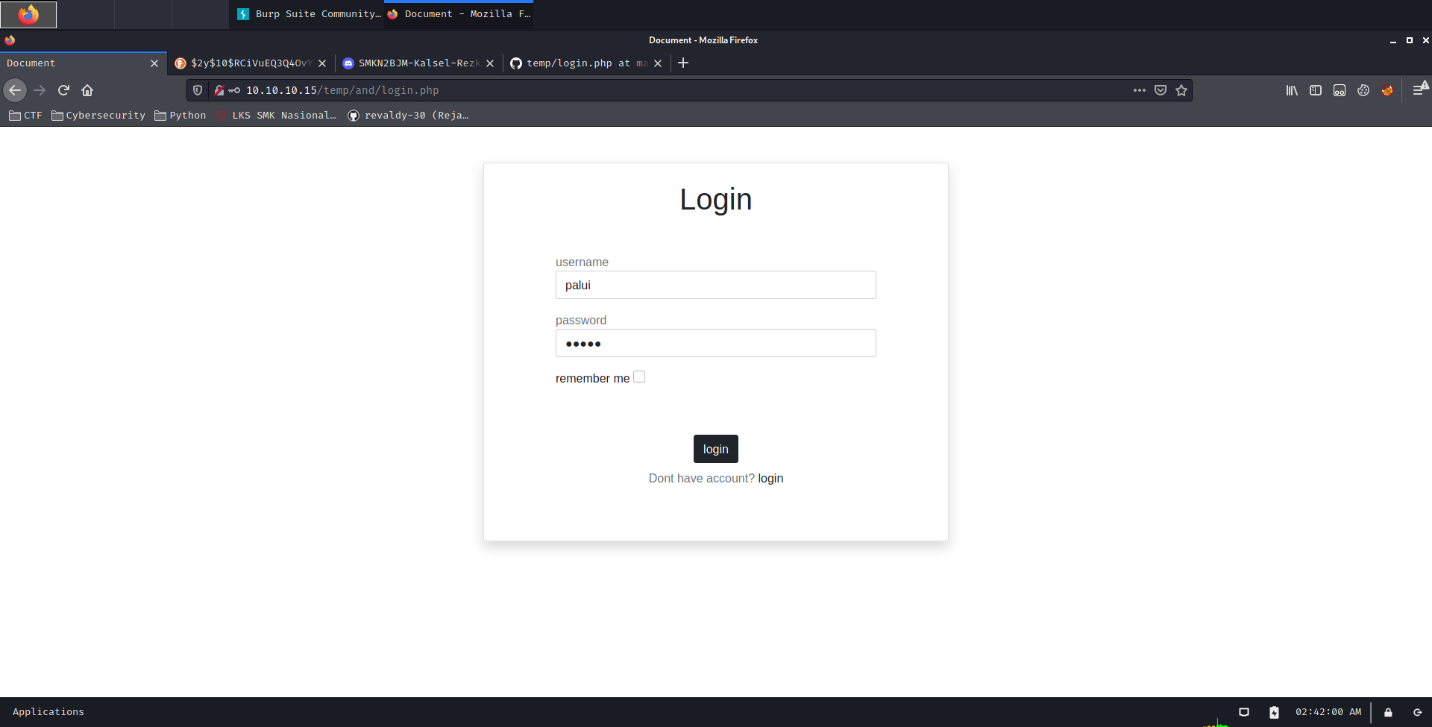


Terakhir, kami mencoba melihat file yang ada pada server dan didapat file yang berisi flag :

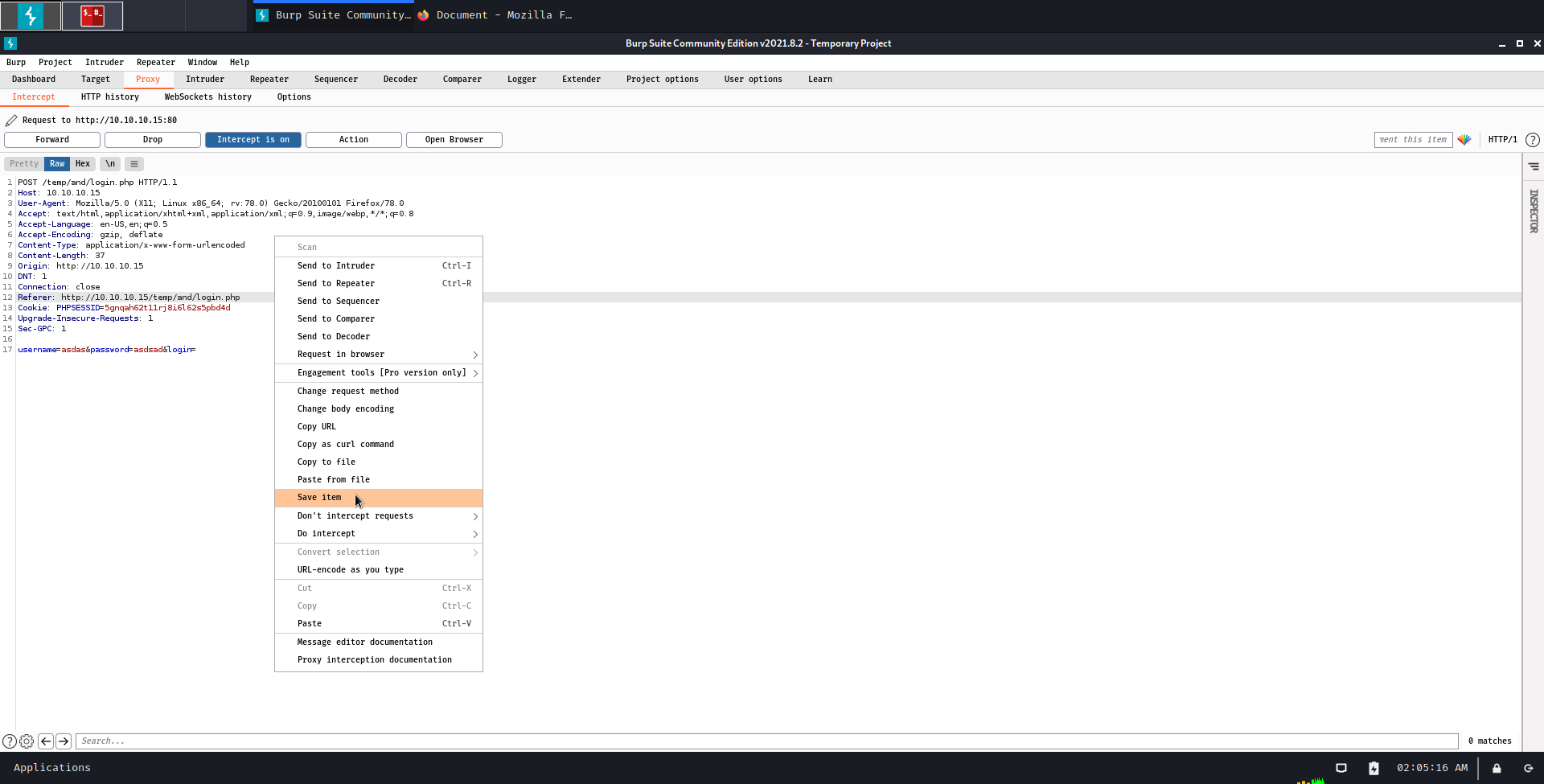


## SQL INJECTION

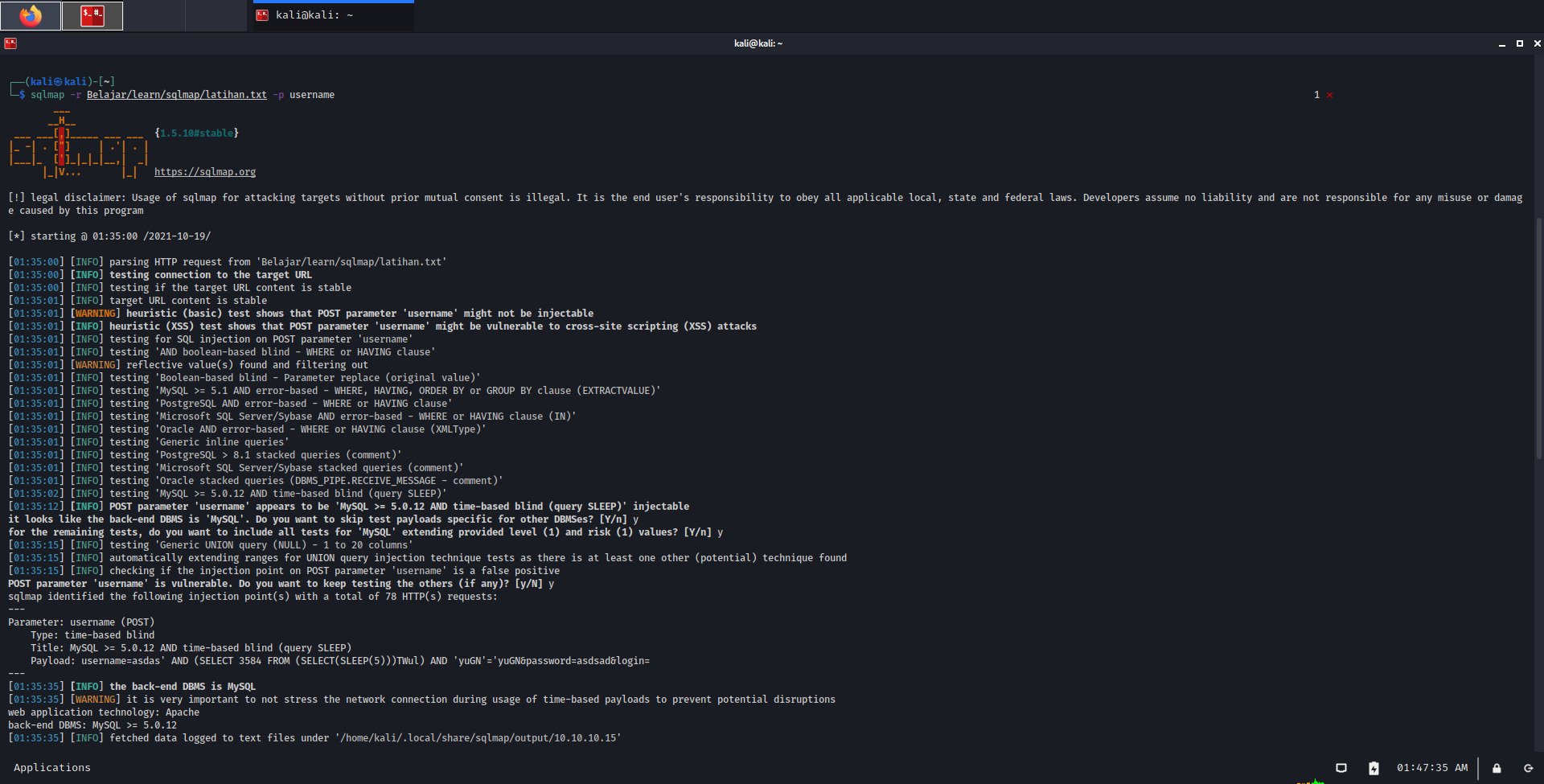
Di tampilan awal login, kami coba input sembarang karakter pada username dan password :



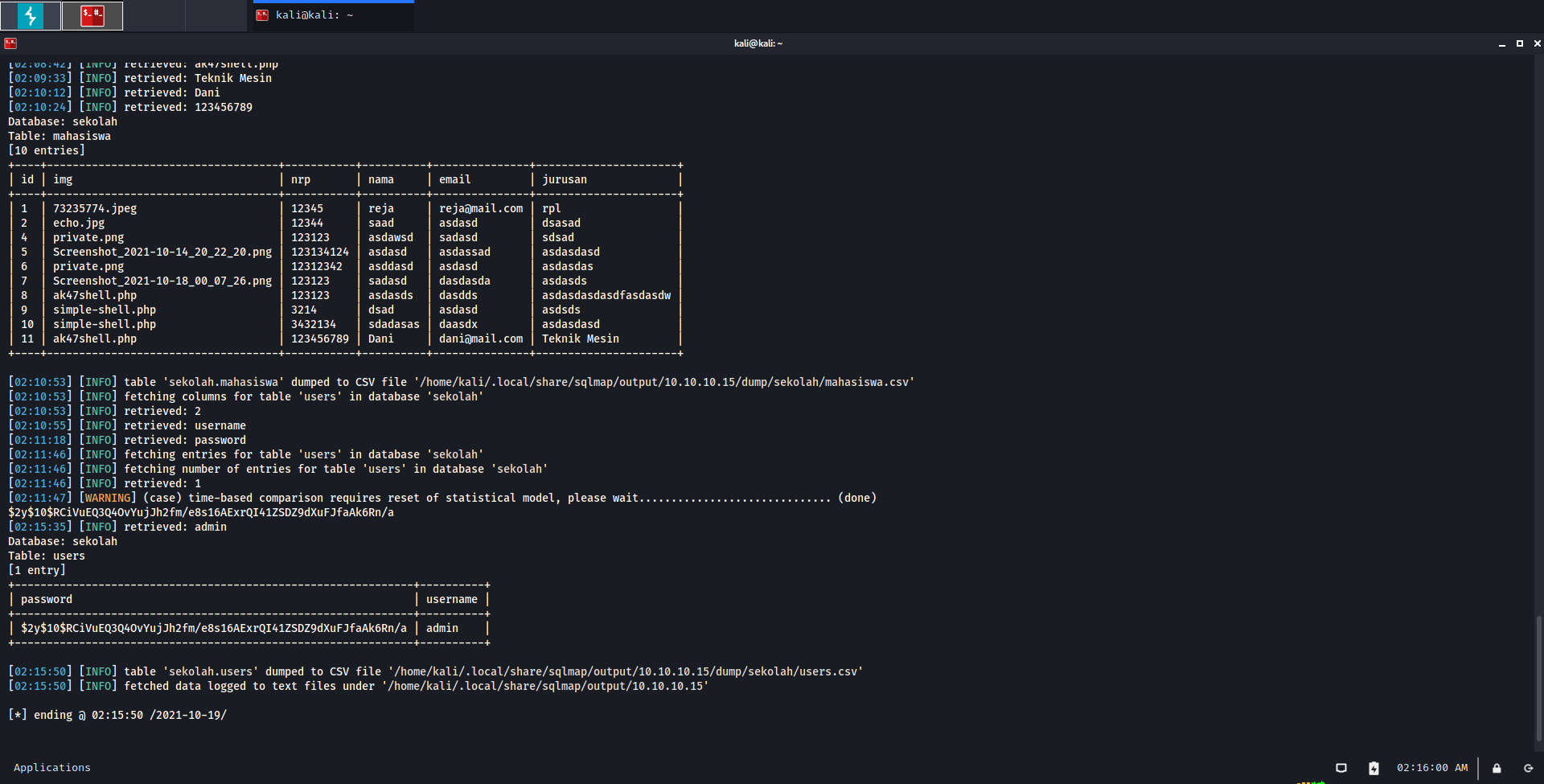
Lalu kami tangkap menggunakan burp suite dan request header yang ada kami simpan ke local agar kami bisa melakukan sql injection menggunakan sqlmap :



Setelah kami menggunakan sqlmap pada file yang sudah disimpan tadi, kami menemukan bahwa database tersebut vulnerable :



Selanjutnya, kami melakukan dump terhadap file tersebut untuk mengetahui isi dari database website tersebut :



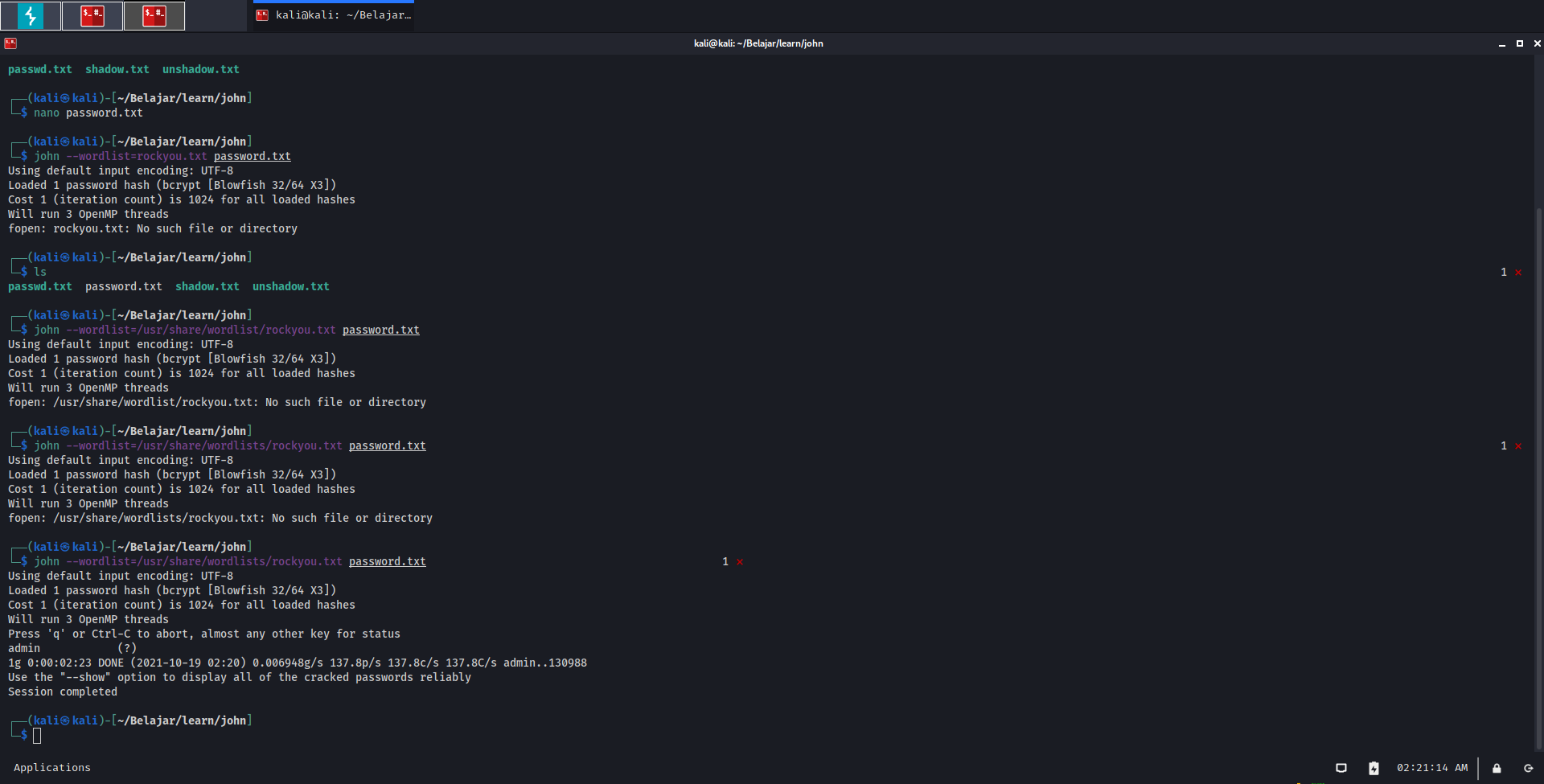
Terlihat pada gambar kami menemukan beberapa info berikut :

* Database : sekolah
* Table : mahasiswa
* Table : users

Value table bisa dilihat secara rinci pada gambar di atas.

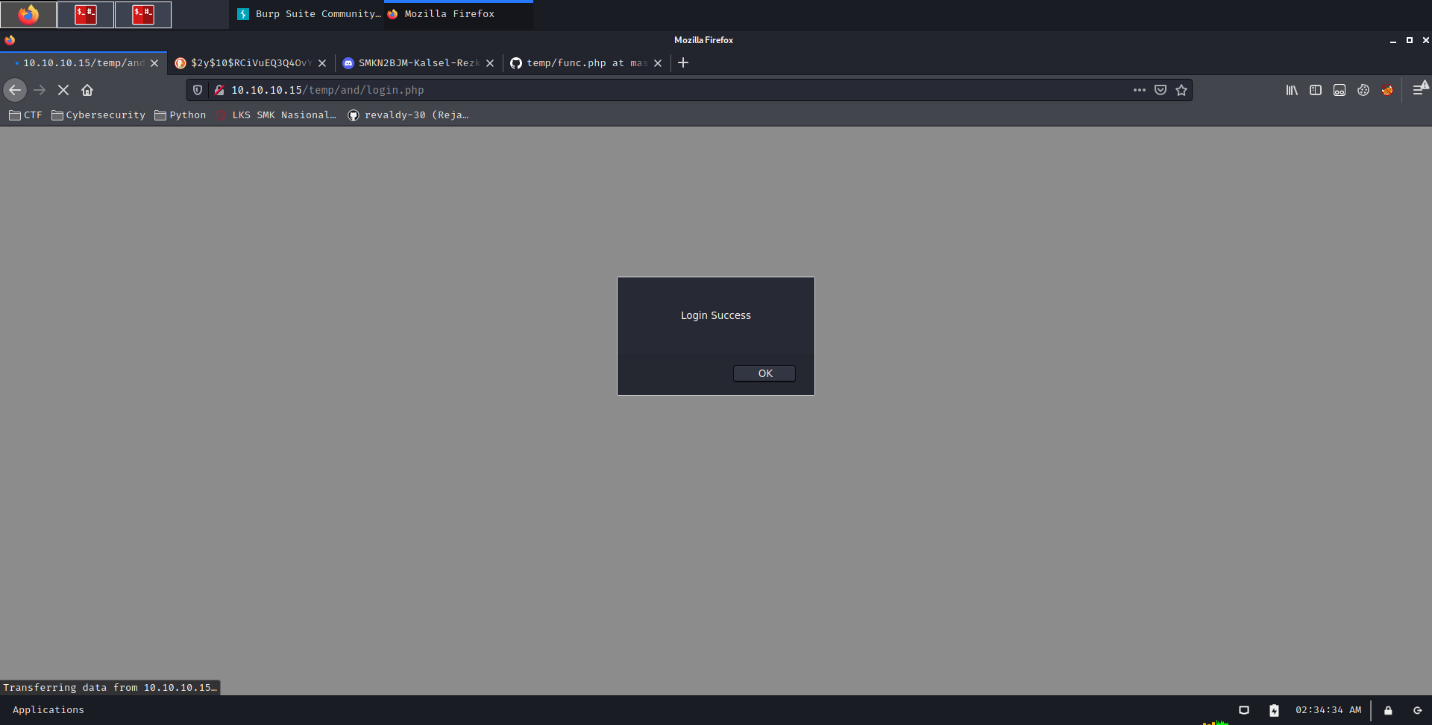
## PASSWORD BRUTEFORCE

Dari info hasil sql injection yang kami lakukan sebelumnya, kami menemukan table users dengan username “admin” dan password yang terenkripsi. Di sini langsung saja kami brute force menggunakan john the ripper dan wordlist “rockyou.txt” :



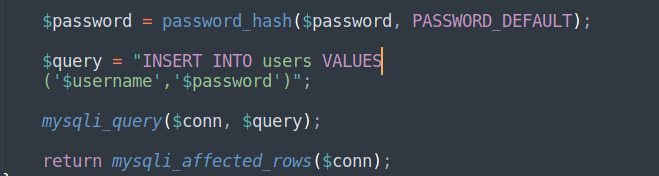
Dan ditemukan bahwa passwordnya adalah “admin”.

Lalu kami coba login menggunakan kredensial yang didapatkan :

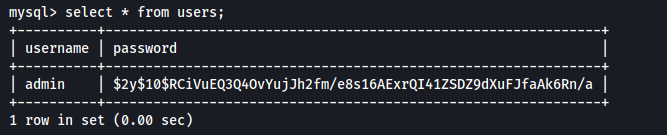


# DEFENSE

## REGISTER

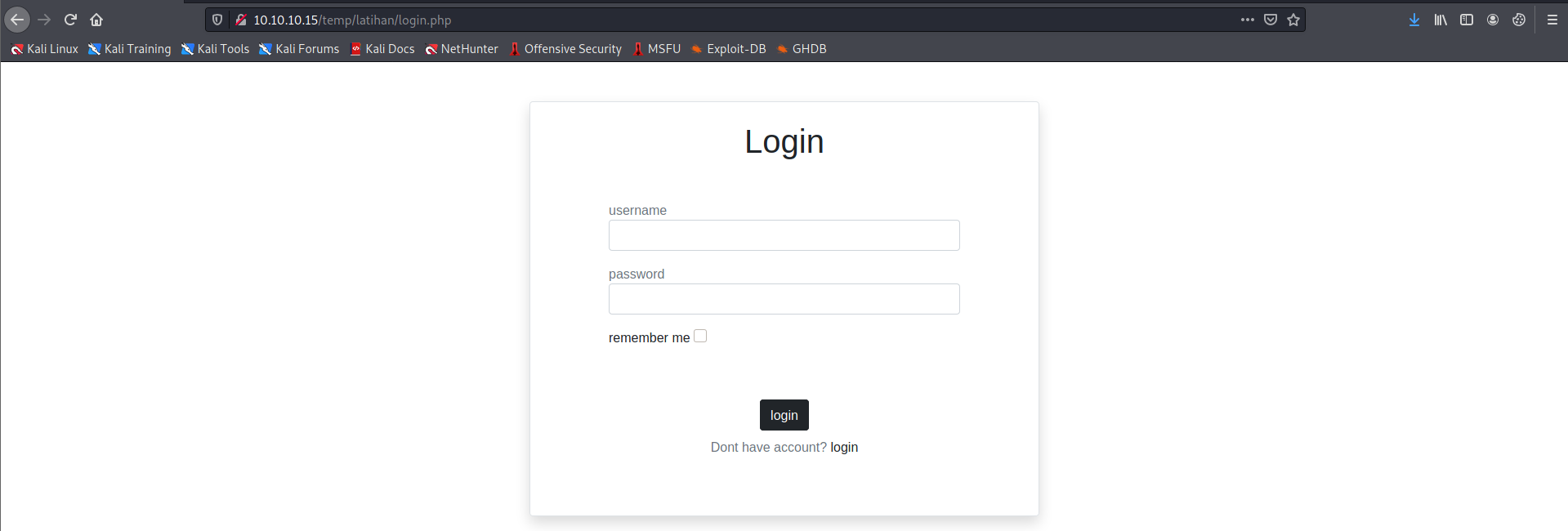


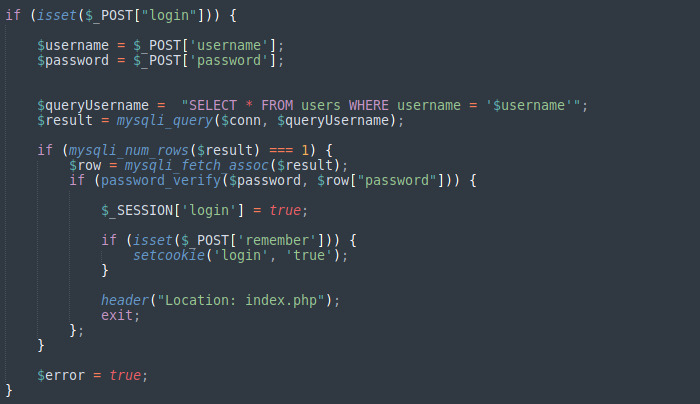
Untuk bagian register, kami melakukan enkripsi terhadap password yang dibuat, sehingga jika orang melakukan exploit terhadap database server maka yang akan dilihatnya adalah hasil encrypt dari password :



## LOGIN

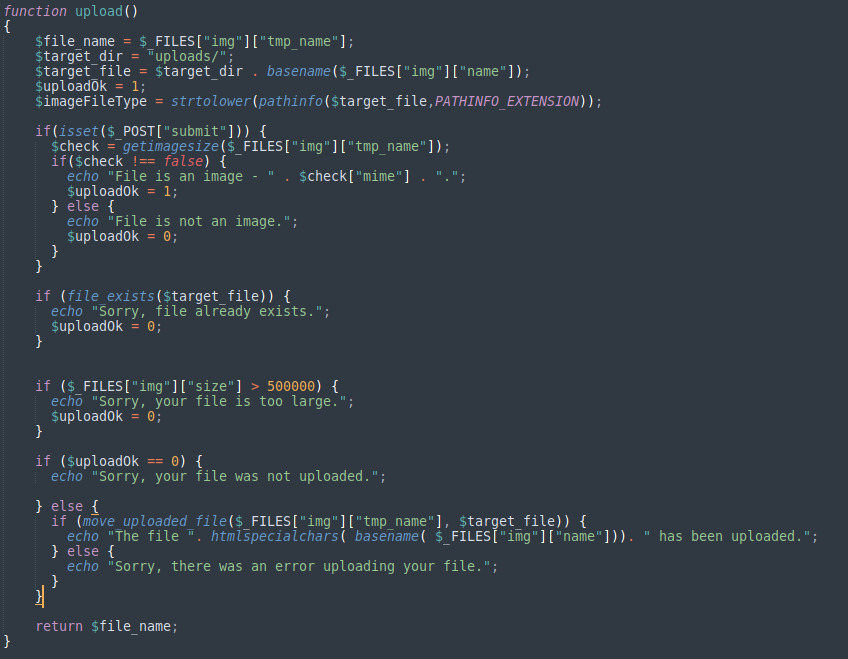
Untuk sisi login kami melakukan pengecekan terhadap password yang diinputkan dengan password yang ada di database, sehingga jika password yang dimasukkan benar maka akan berhasil login, begitu pula sebaliknya.





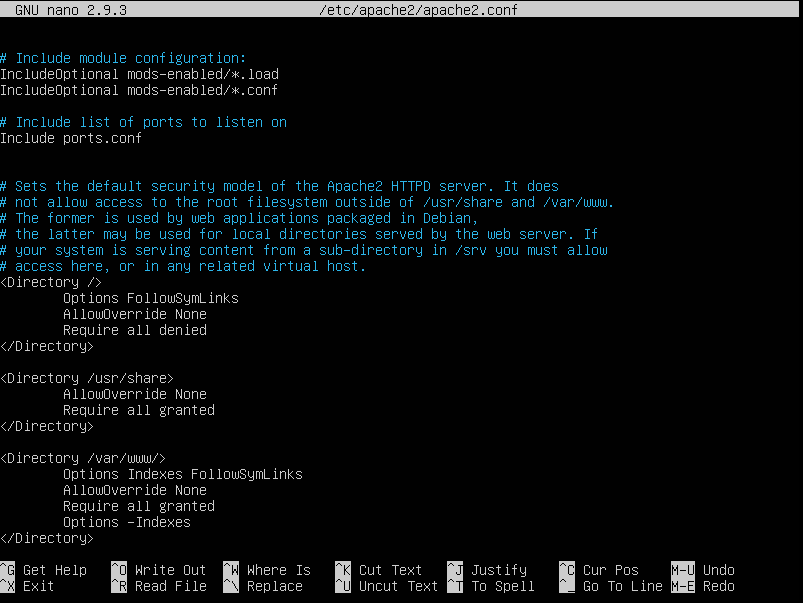
## FILE UPLOAD

Di bagian file upload, kami hanya mengizinkan file yang diupload berupa gambar dan ukuran file yang diupload dibatasi yaitu maksimal berukuran 0,5 Mb.

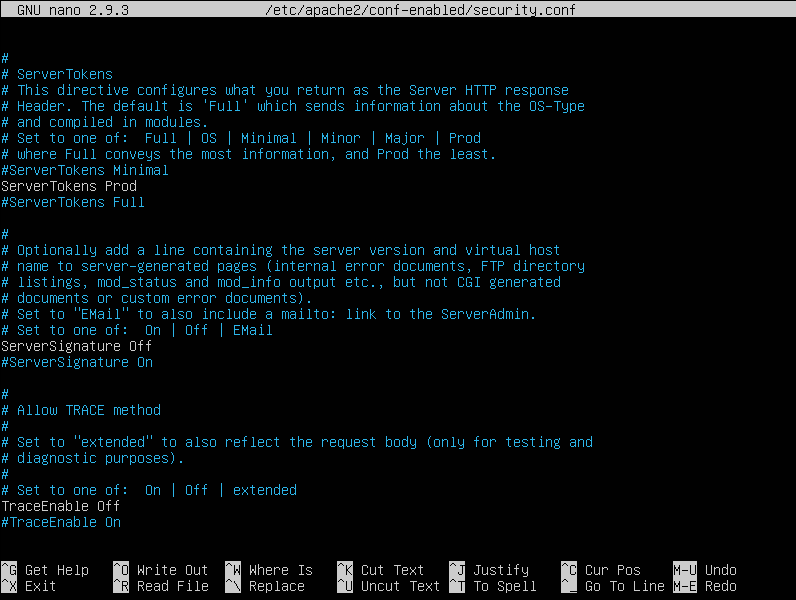


## HIDDEN DIRLISTING & APACHE VERSION

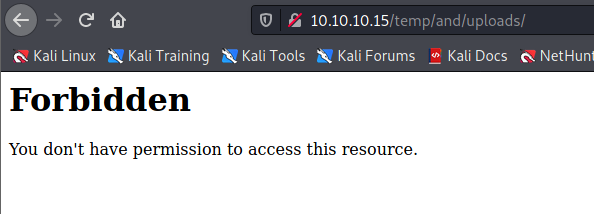
Di sisi keamanan server, kami menyembunyikan content directory listing dan versi apache nya. Untuk menyembunyikan content dirlisting, kami mengedit file /etc/apache2/apache2.conf dan menambahkan “Options -Indexes” seperti pada gambar :



Setelah itu, untuk menyembunyikan versi apache yang digunakan, kami mengedit file /etc/apache2/conf-enabled/security.conf di bagian ServerTokens yang semula “OS” menjadi “Prod” dan ServerSignature yang semula “On” menjadi “Off” :

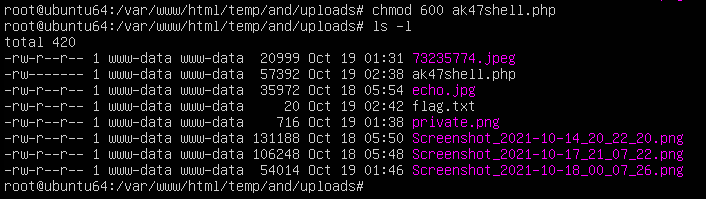


Setelah itu, kami restart apache nya dengan mengetik perintah “/etc/init.d/apache2 restart” dan kami coba jalankan kembali website dan berhasil dilakukan :



## CHANGE PERMISSION

Untuk bagian change permission, kami mengubah hak akses shell menjadi 600 sehingga selain owner tidak akan ada user lain yang bisa membaca atau mengeksekusi shell tersebut :



Selain itu, kami juga mengubah hak akses untuk file /etc/passwd dan file /etc/shadow menjadi 600, sehingga selain user root tidak akan ada user lain yang bisa melihat isi file :

