Graphical user interface, text

Description automatically generated

**Write-Up CTF KKST2021 Kategori Pelajar**

NAMA TIM : BornMatrix

INSTITUSI : SMKN 2 Banjarmasin

Senin, 11 Oktober 2021

**Ketua Tim**

1. Reja Revaldy .F.

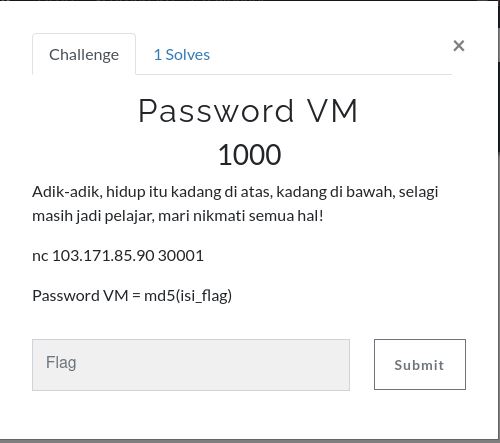
**Member**

1. Rezka Norhafizah

#### **MISC**

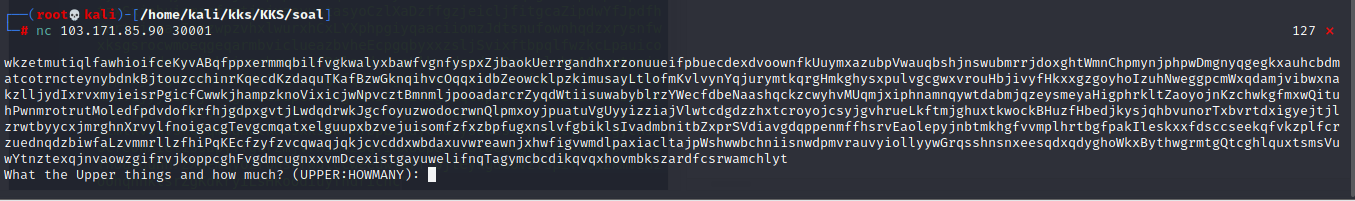
#### **[PASSWORD VM]**

**Soal**

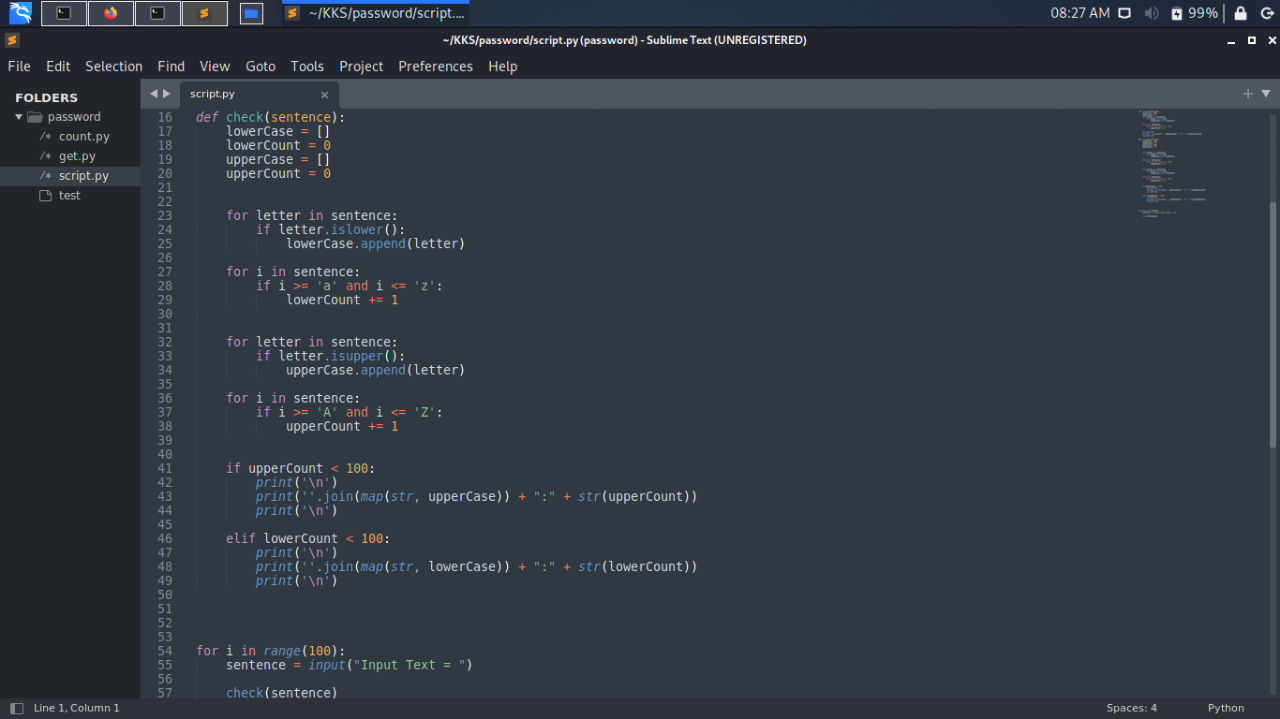


**Pembahasan**

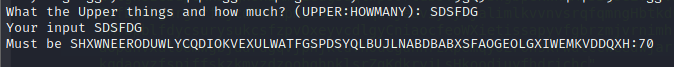
Setelah kami melakukan nc 103.171.85.90 30001 muncul pertanyaan yang di mana kita diminta untuk mencari uppercase dan lowercase beserta jumlahnya

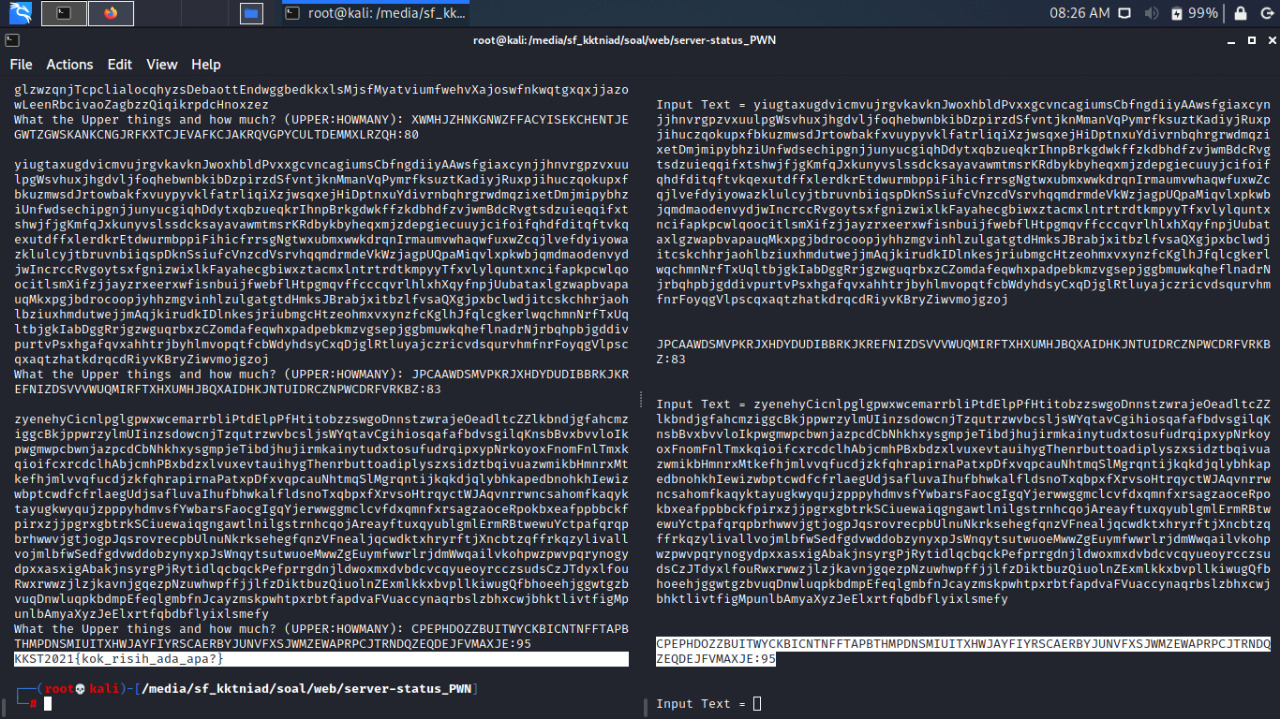


Selanjutnya, kami membuat script python sederhana yang di mana berisi program untuk mencari uppercase dan lowercase beserta jumlahnya

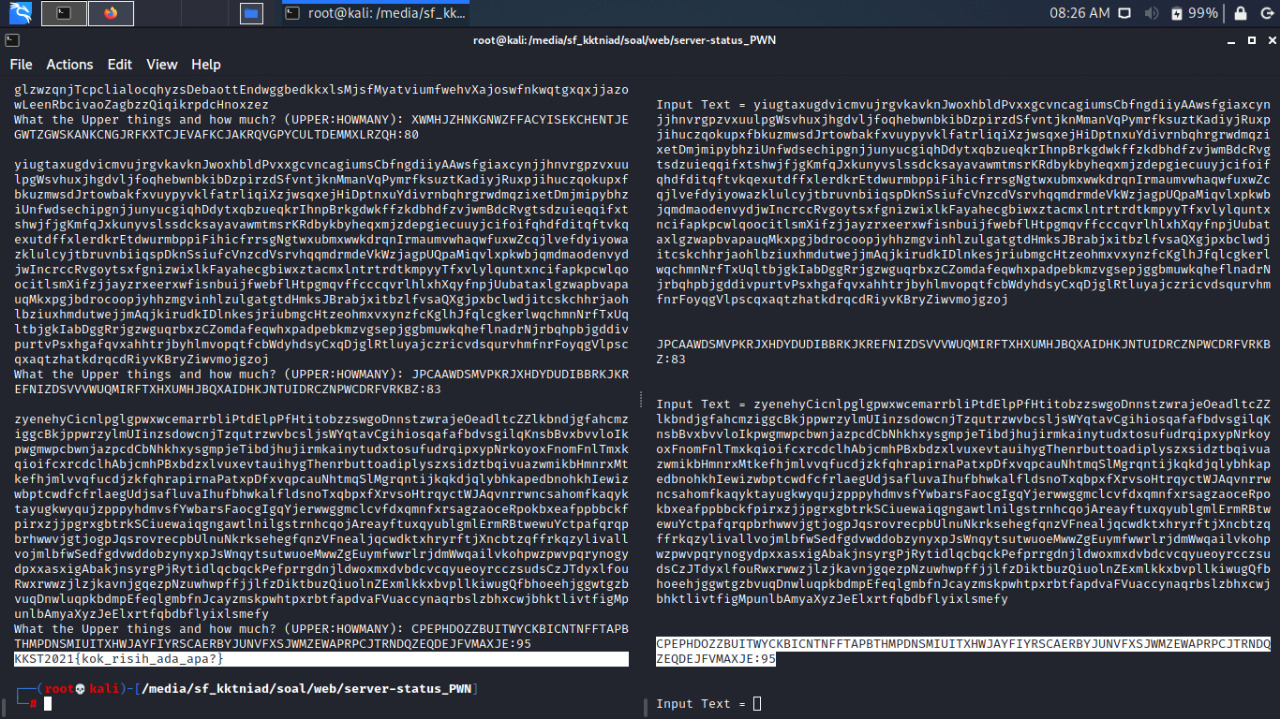


Kemudian kami input string yang dimunculkan oleh nc tersebut pada script python dan kami mendapatkan uppercase atau lowercase beserta jumlahnya yang diminta. Setelah itu, kami coba input ke soal dan didapat :





Dari hal tersebut, kami dapat menyimpulkan bahwa ketika kita menginput jawaban yang salah maka program akan memberitahu jawaban yang benar, dan ketika kita menginput jawaban yang benar maka program akan mengulangi hal yang sama yaitu menanyakan uppercase ataupun lowercase beserta jumlahnya. Selanjutnya, kami coba hal tersebut berulang kali dan didapat flag :

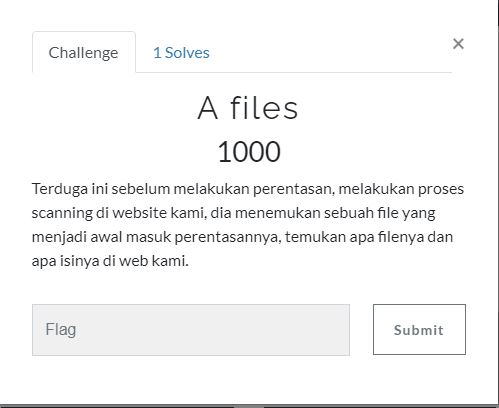


**FLAG = KKST2021{kok\_risih\_ada\_apa?}**

#### **FORENSIC**

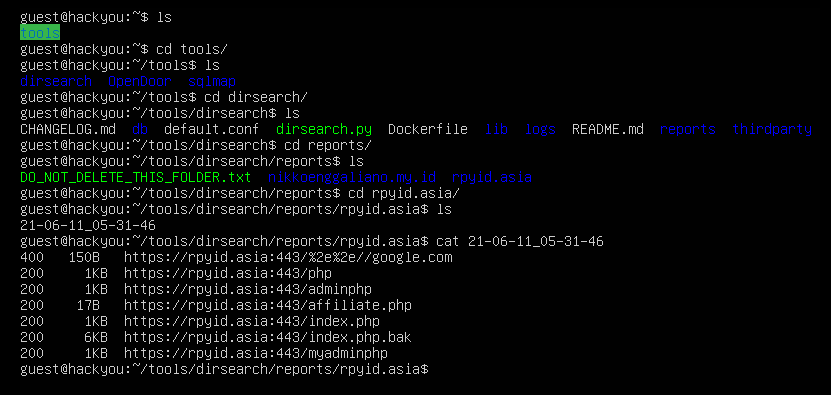
#### **[A FILE]**

**Soal**

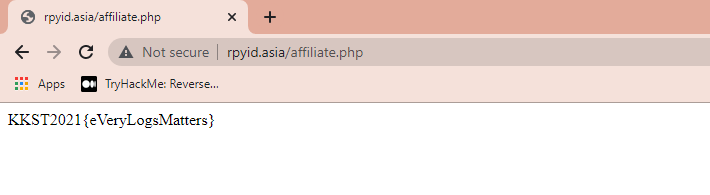
****

**Pembahasan**

Setelah didapat password untuk VM tadi, maka kami jalankan VM tersebut dan login sebagai guest. Selanjutnya kami coba ls untuk mengetahui folder apa saja yang terdapat pada user. Dan didapat :



Lalu, kami coba browsing <https://rpyid.asia> dan kami masukkan satu persatu file yang tertera di atas, untuk mengetahui file mana yang berisi flag, dan ternyata itu adalah affiliate.php :



**FLAG = KKST2021{eVeryLogsMatters}**

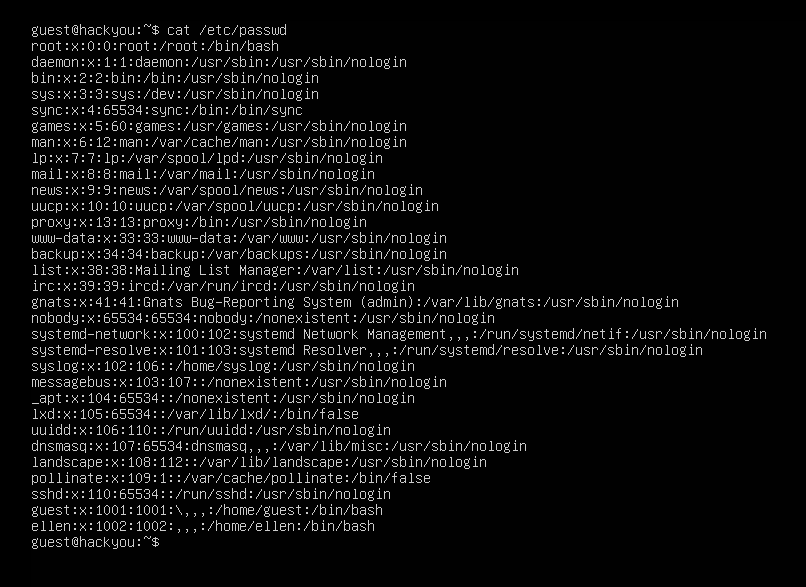
#### **[ANOTHER USER]**

**Soal**



**Pembahasan**

Pertama-tama kami melihat ke dalam file /etc/passwd untuk mencek apakah ada user selain guest :

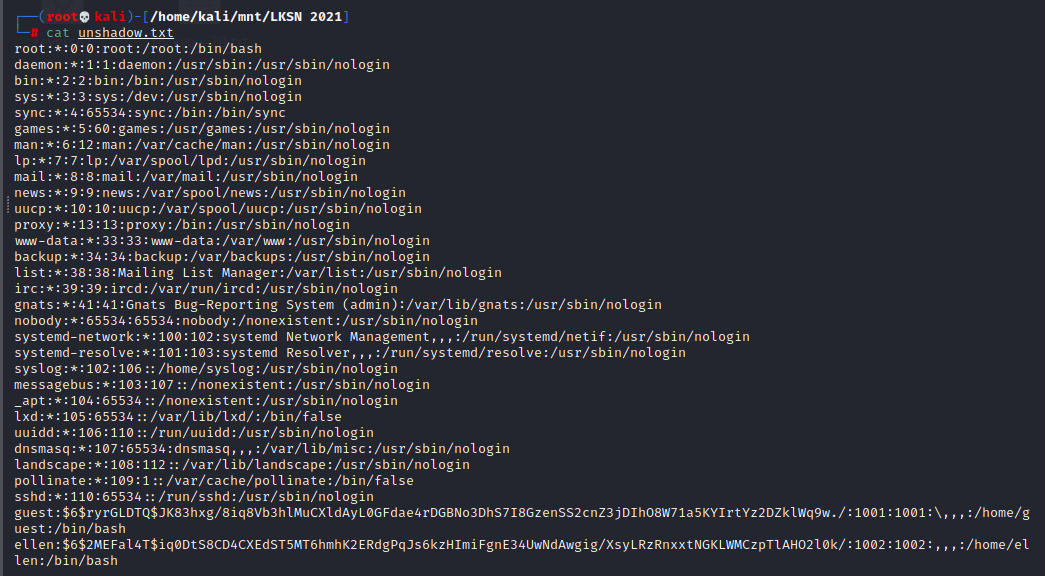
****

Seperti yang terlihat pada gambar, terdapat user lain selain guest, yaitu ellen. Selanjutnya, kami melihat ke dalam file /etc/shadow untuk mencek password yang digunakan oleh user.

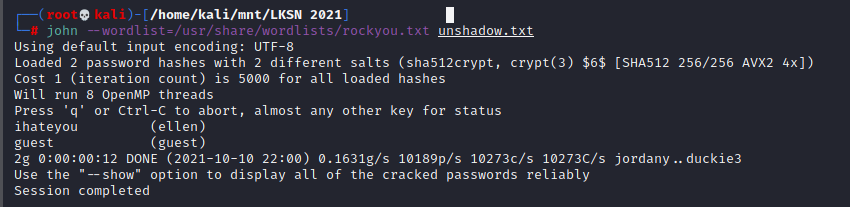


Terlihat bahwa password yang digunakan oleh user ellen ini diencrypt menggunakan algoritma SHA512. Kemudian kami mencoba crack password tersebut menggunakan john the ripper dan wordlist yang digunakan adalah rockyou.txt. Namun, sebelum itu kedua file tersebut harus di unshadow terlebih dahulu.





Setelah itu, langsung saja kami eksekusi menggunakan john the ripper :

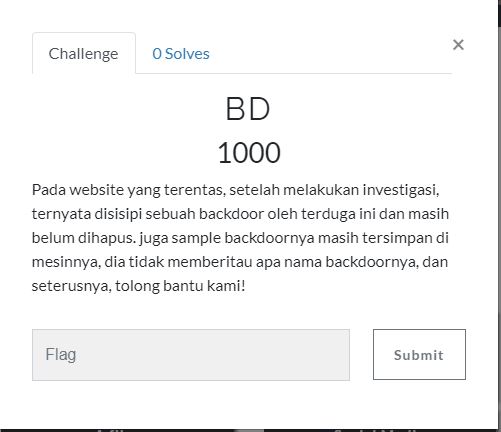


Dan didapat user selain guest yaitu ellen dengan password ihateyou.

**FLAG = KKST2021{ellen:ihateyou}**

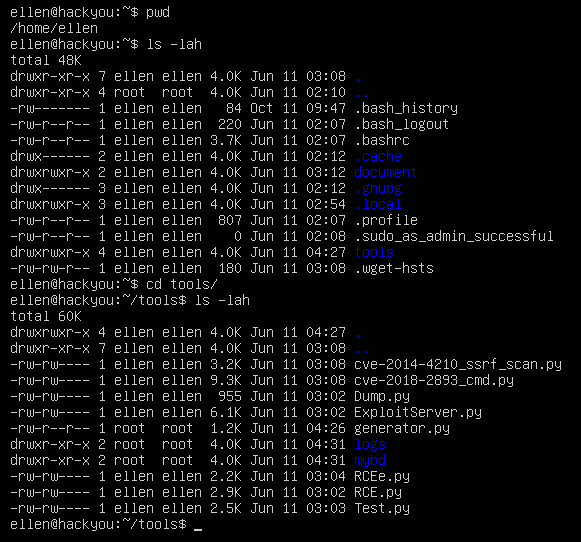
#### **[BD]**

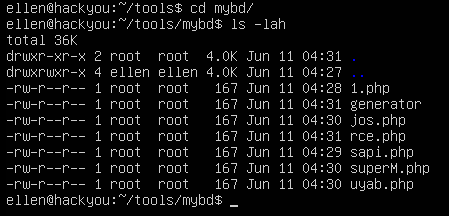
**Soal**

****

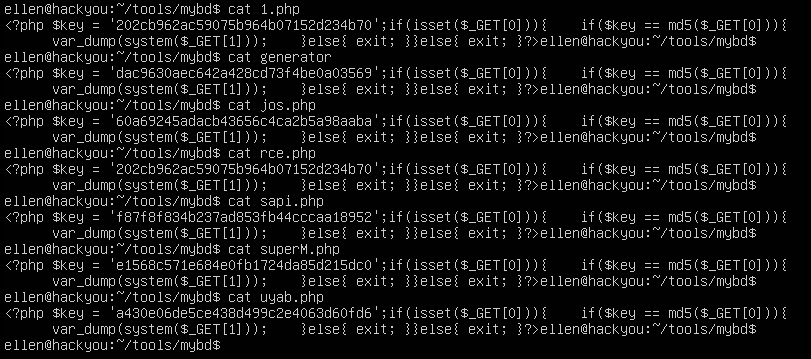
**Pembahasan**

Kami login menggunakan user ellen kemudian kami mendapatkan direktori mybd yang kami asumsikan ialah lokasi di mana backdoornya berada :

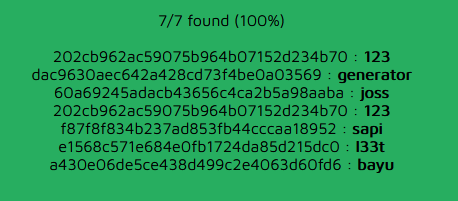




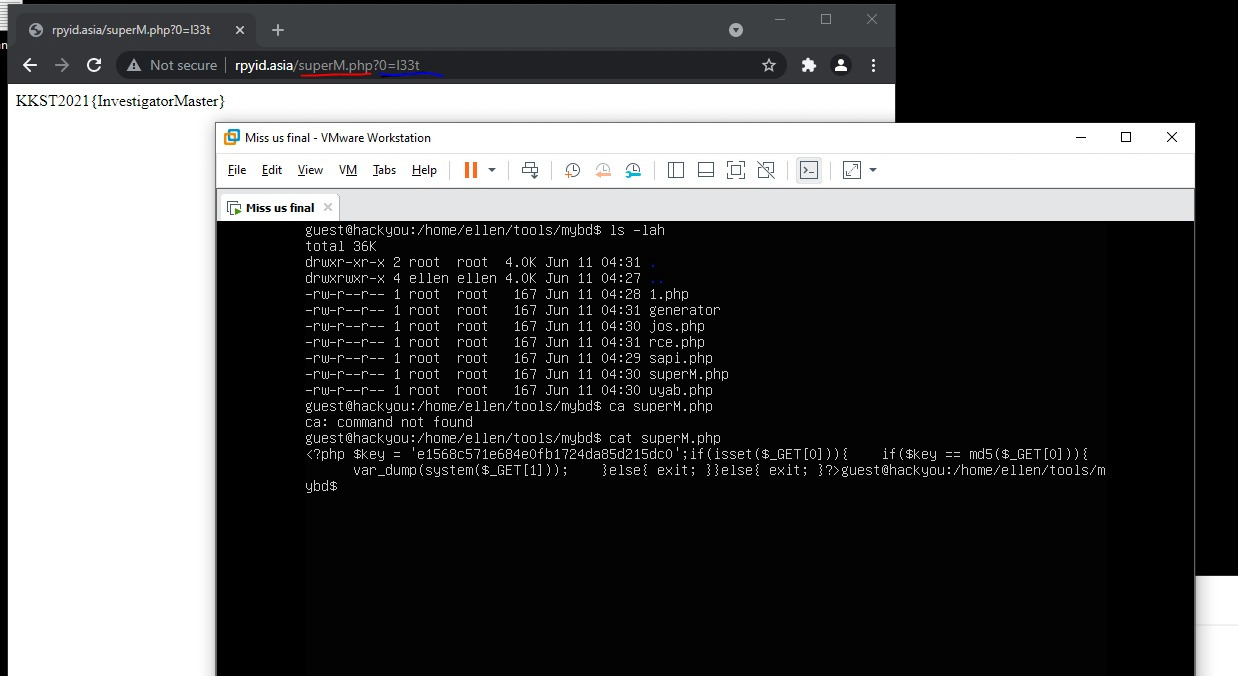
Selanjutnya, kami buka satu persatu file di atas dan didapat :



Terlihat bahwa key diencrypt menggunakan md5. Lalu, kami decrypt key tersebut satu persatu di <https://www.md5online.org/md5-decrypt.html> dan didapat :



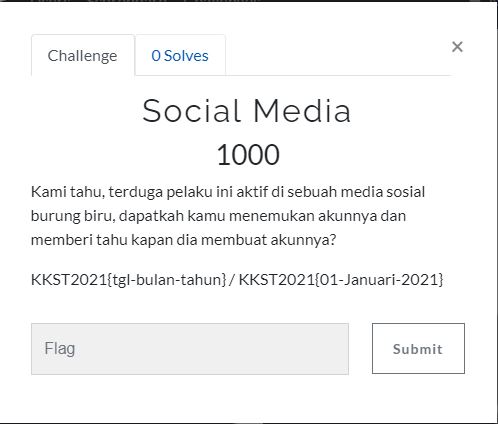
Lalu, kami buka kembali <https://rpyid.asia> dan kami buka satu persatu file backdoor nya dengan menyertakan key yang sudah didecrypt md5 tadi sebagai parameter. Hasilnya, file superM.php merupakan backdoor :



**FLAG = KKST2021{InvestigatorMaster}**

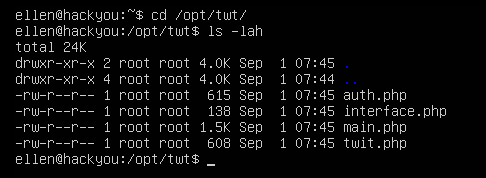
#### **[Social Media]**

**Soal**

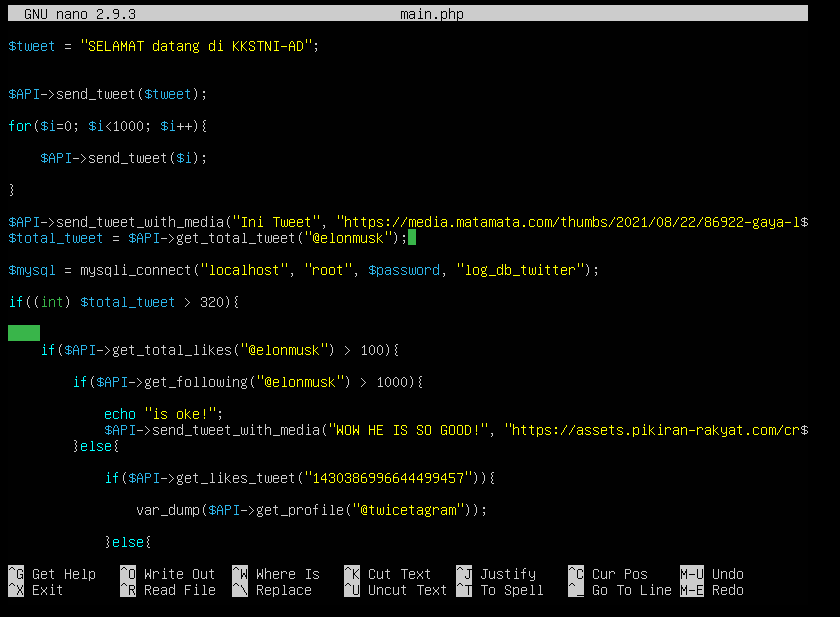
****

**Pembahasan**

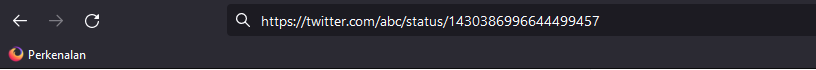
Dari soal, didapat hint bahwa pelaku aktif di social media burung biru yaitu twitter. Lalu, kami menemukan tools wrapper API pada direktori /opt/twt.

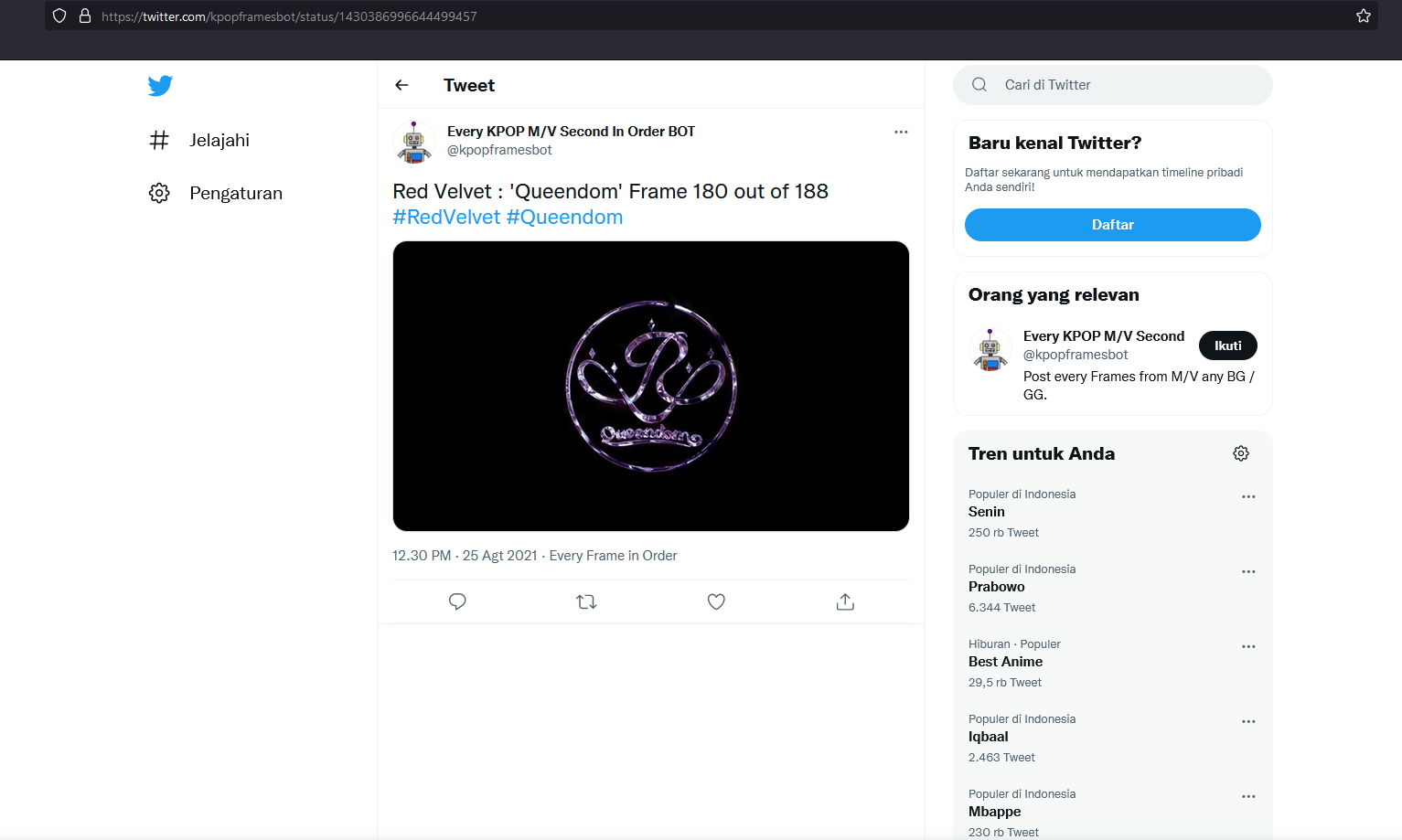


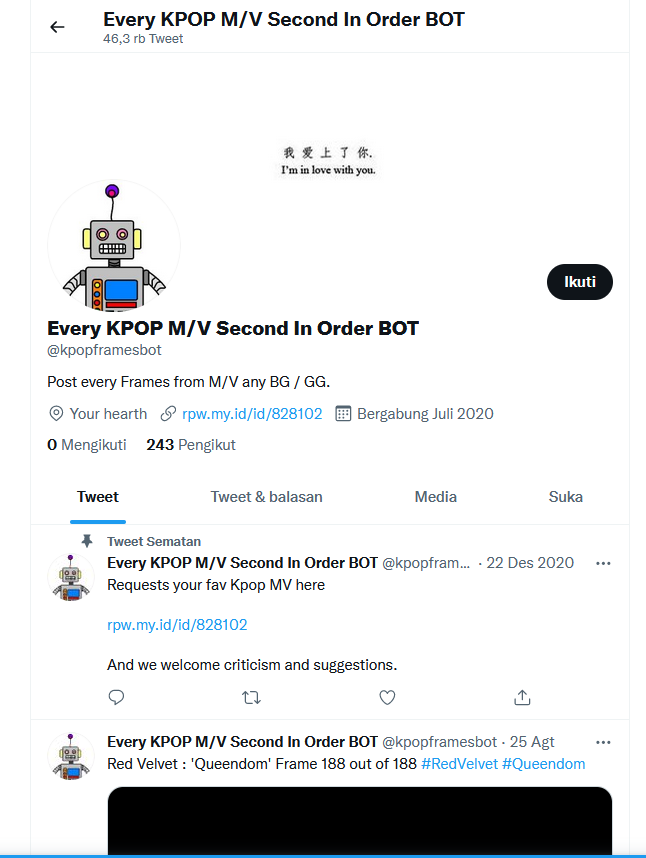
Setelah kami membuka file main.php terlihat bahwa ini merupakan script yang dibuat pelaku untuk mengambil like twitter dari seorang artis dan kemudian diarahkan ke id postingan twitter si pelaku. Di sini, kami mendapat id postingan twitter dari si pelaku yaitu 1430386996644499457 :



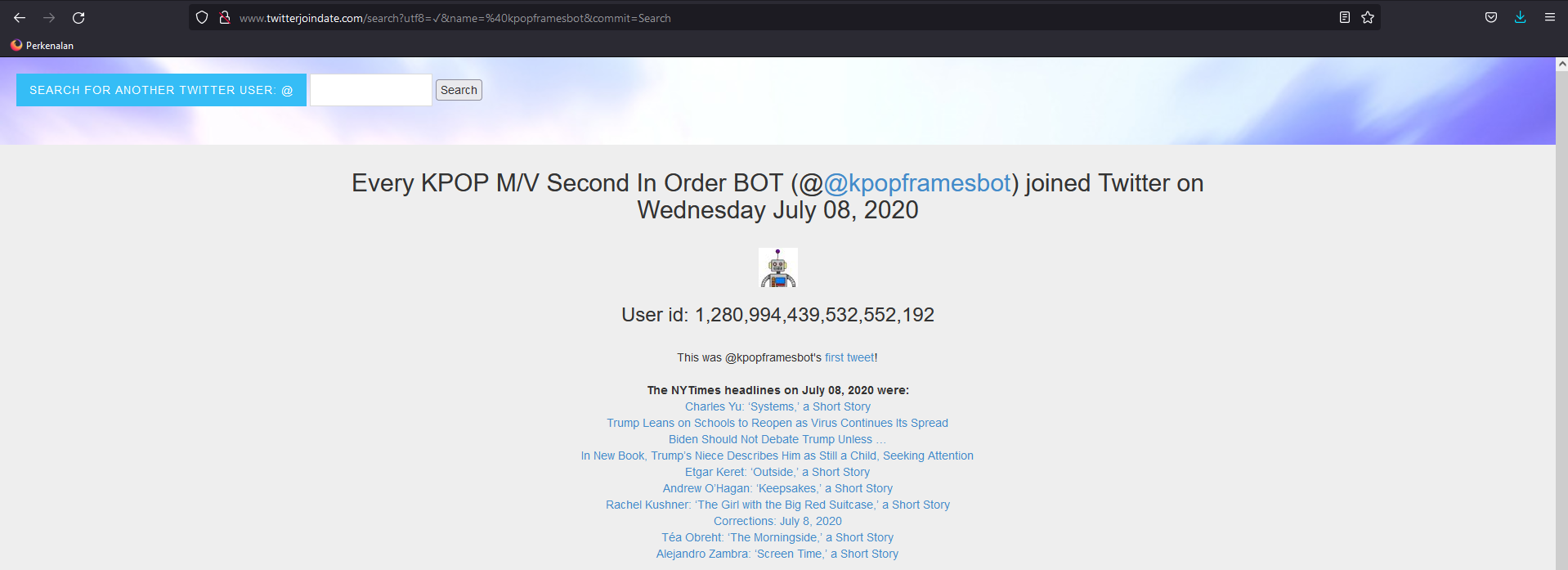
Karena kami tidak tahu user twitter nya apa, maka kami susun saja seperti berikut dan ternyata langsung diarahkan ke user lain :







Lalu, untuk mencari kapan akun tersebut bergabung kami masukkan user @kpopframesbot pada link <http://www.twitterjoindate.com/> dan didapat :



**FLAG = KKST2021{08-Juli-2020}**

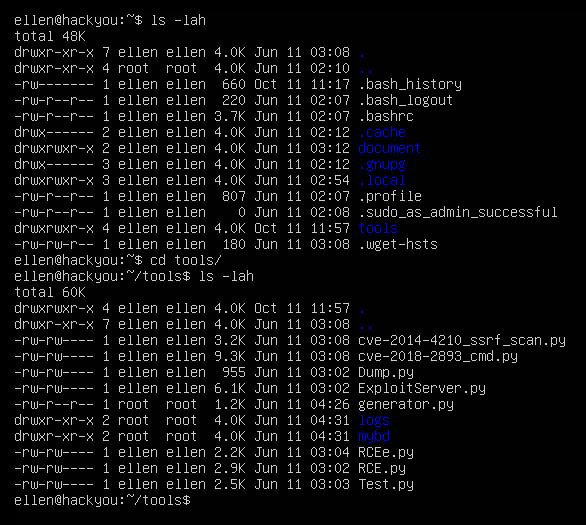
#### **[CVE]**

**Soal**

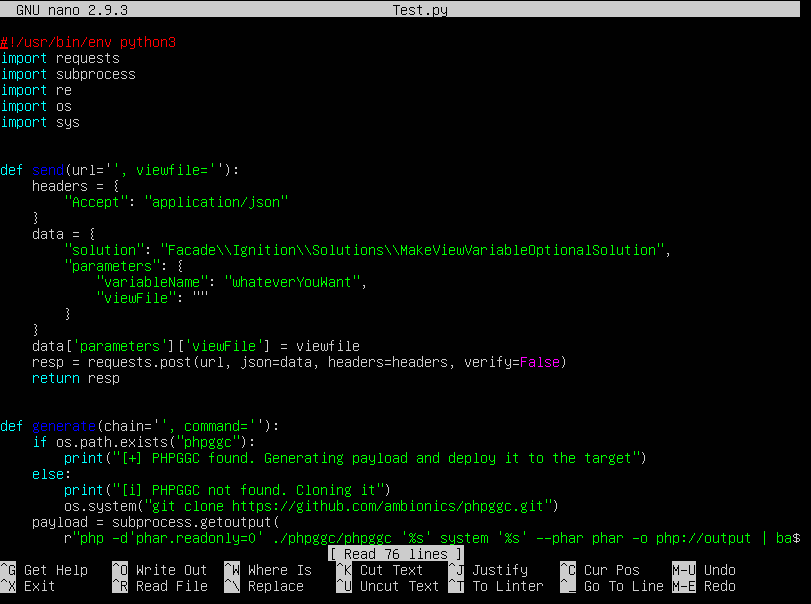
****

**Pembahasan**

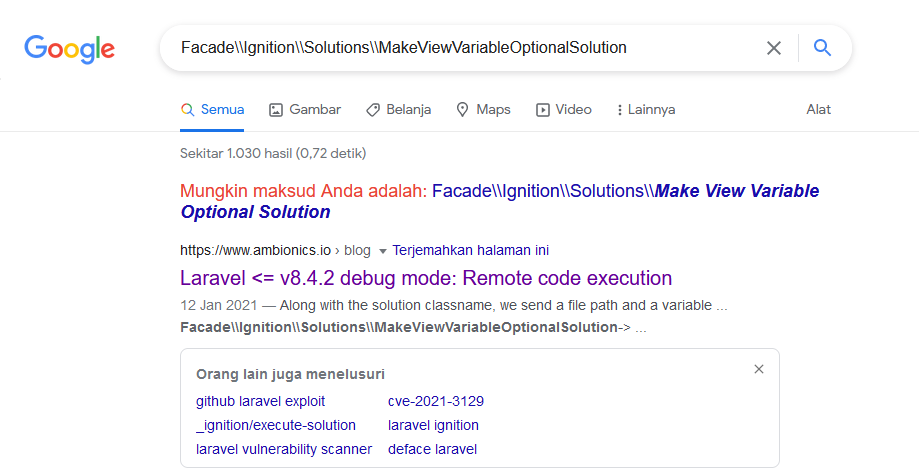
Di dalam folder tools, kami menemukan beberapa file exploit seperti berikut :



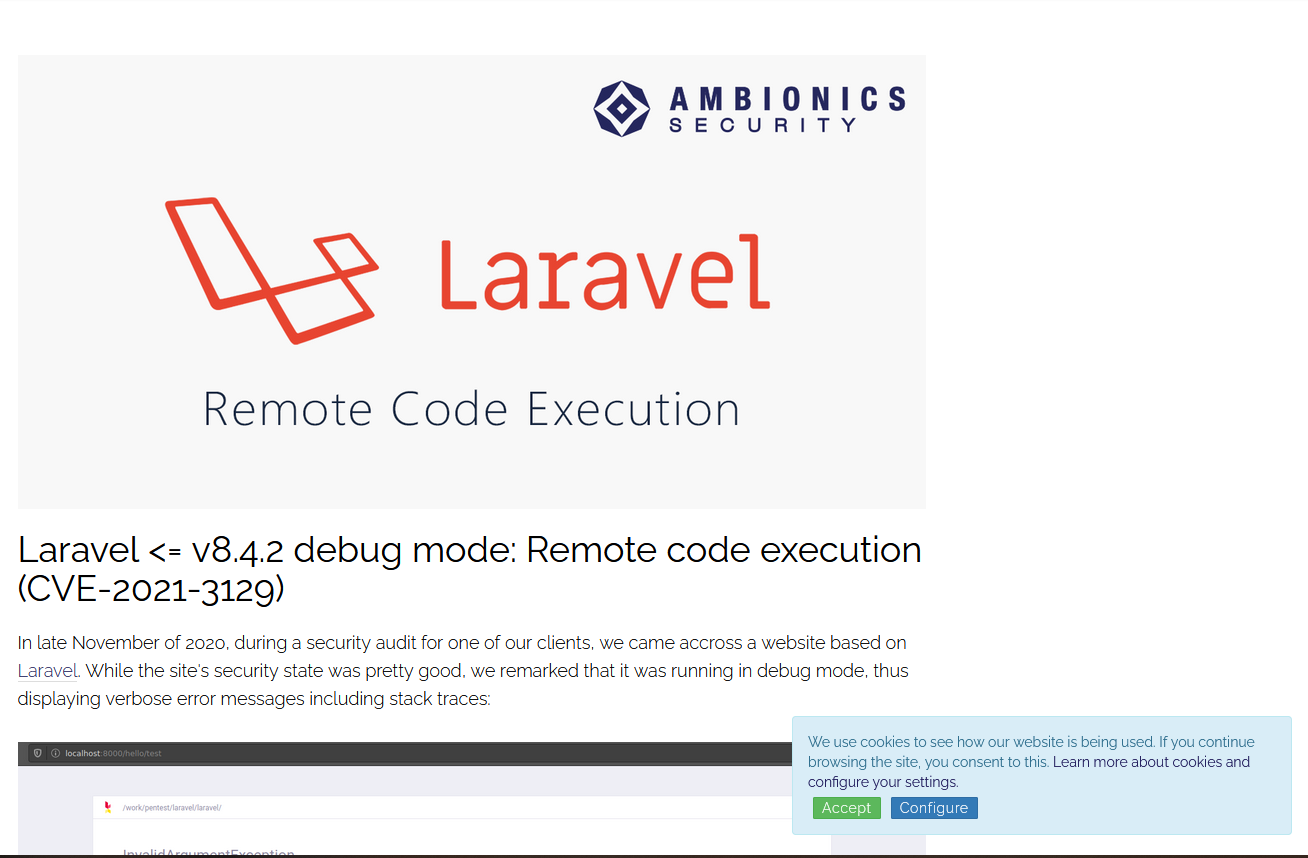
Sesuai hint yang diberikan yaitu bahasa pemrograman yang dipakai adalah PHP lalu kami mengambil kesimpulan bahwa CVE yang digunakan adalah CVE yang berhubungan dengan PHP. Kemudian, kami menemukan hal yang menarik pada isi file Test.py :



Setelah kami search di google “Facade\\Ignition\\Solutions\\MakeViewVariableOptionalSolution” ternyata benar itu merupakan CVE dari Laravel (framework PHP) :



Kemudian didapat nomor CVE-nya :



**FLAG = KKST2021{CVE-2021-3129}**

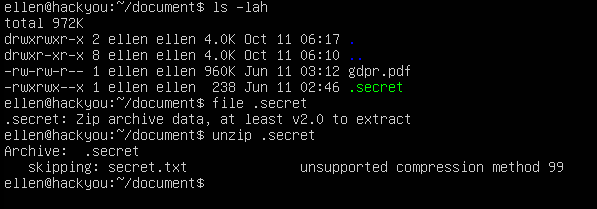
#### **[Secret Files]**

**Soal**

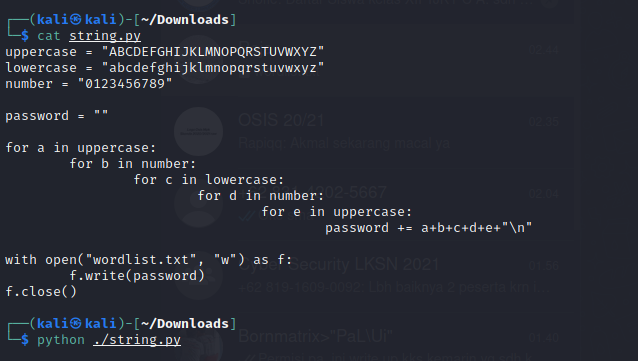
****

**Pembahasan**

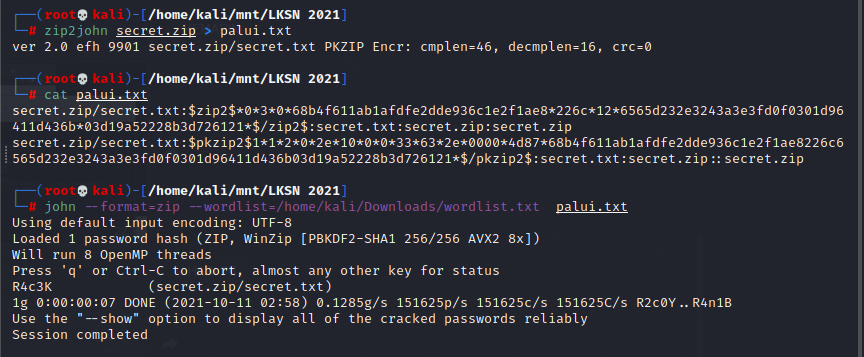
Awalnya, kami menemukan file dengan nama .secret sesuai yang diinformasikan oleh hint soal pada direktori /document. Lalu, kami coba analisis ternyata file tersebut adalah file zip yang mengandung file secret.txt :

****

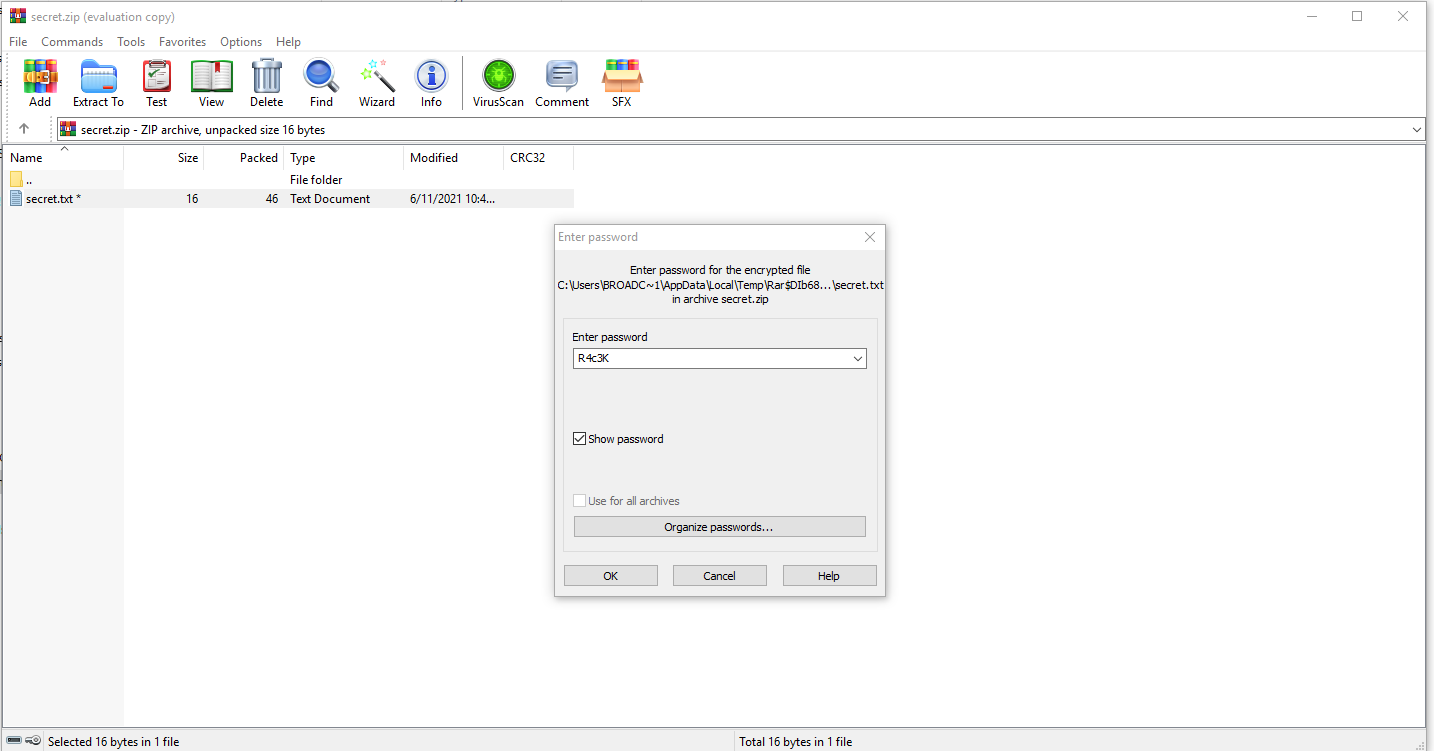
Kemudian, file zip tersebut kami copy ke local untuk memudahkan kami membruteforce file tersebut. Selanjutnya, karena pada soal diberi hint password terdiri dari 5 karakter (karakter pertama dan terakhir merupakan uppercase, karakter ketiga merupakan lowercase, dan sisanya merupakan angka) kami membuat script untuk meng-generate wordlist untuk bruteforce password.

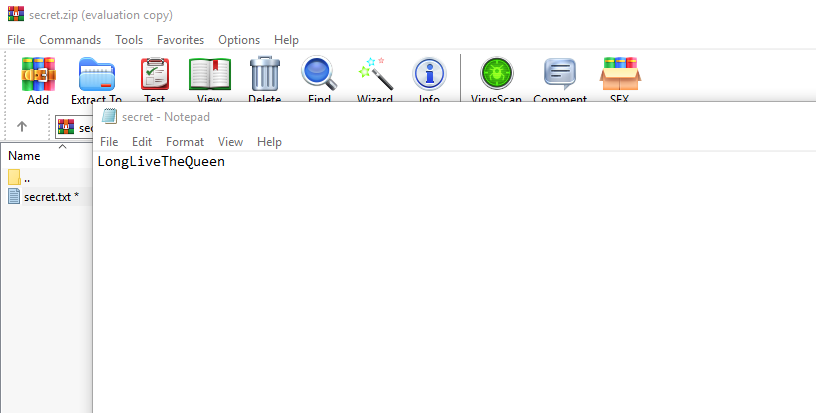


Selanjutnya, kami jalankan script tersebut dan didapat wordlist sesuai dengan hint yang diberikan. Setelah itu, kami menggunakan John The Ripper dan wordlist yang sudah di-generate tadi untuk membruteforce passwordnya :



Didapat passwordnya yaitu R4c3K, langsung saja kami ekstrak filenya dan didapat :



****

**FLAG = KKST2021{LongLiveTheQueen}**