



**NAMA TIM : [Cyber Security Trunojoyo]**

|  |  |
| --- | --- |
| **Ketua Tim** | |
| **1.** | Wijanarko Putra Rajeb |
| **Member** | |
| **1.** | Muhamad Hendrik Wicaksono |
| **2.** | Muhammad Zaelani |

Universitas Trunojoyo Madura

KKSI 2019 UMUM - Surabaya

**Daftar Isi**

**Testing**

Testing [ 1 Point ] 2

**Misc**

Welcome To KKSI2019 [ 50 Point ] 3

**Forensics**

Login Trafic [ 50 Point ] 4

Read The Log [ 70 Point ] 6

Member Have Journal [ 70 Point ] 8

**Web**

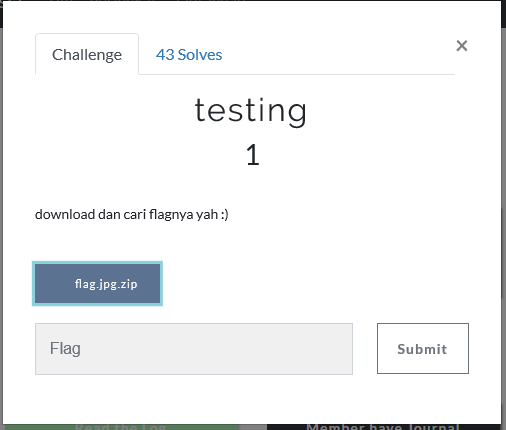
Tsunade Gambling Master [ 100 Point ] 11

Limited Eval [ 200 Point ] 13

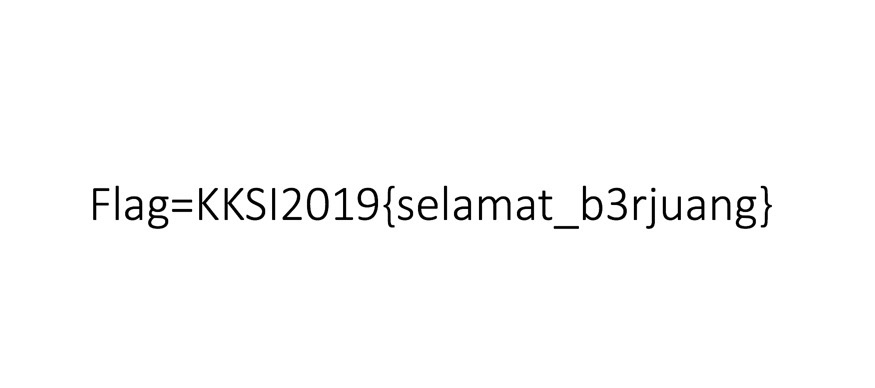
**Testing**

Testing [ 1 Point ]

Disediakan soal berikut:



Beserta file zip yang berisi flag.jpg berikut ini.

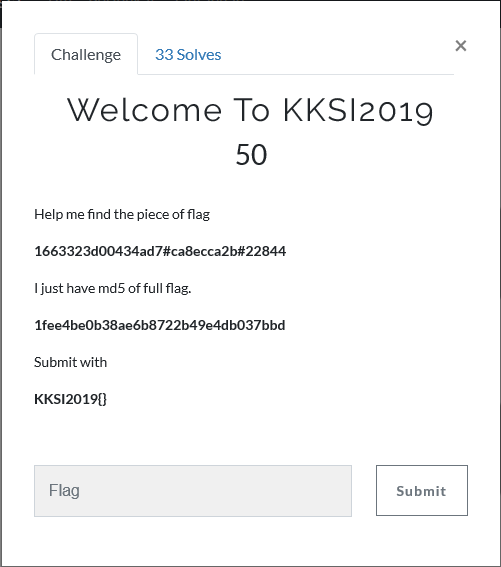


**FLAG : KKSI2019{selamat\_b3erjuang}**

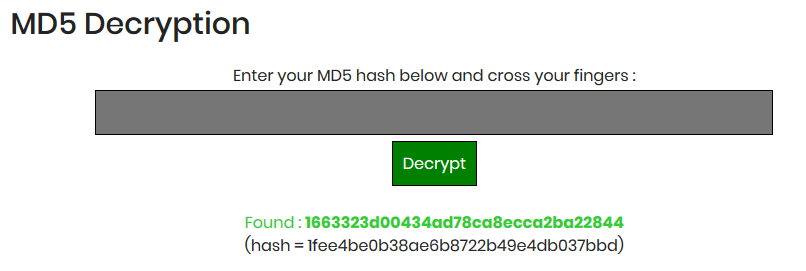
**Misc**

Welcome To KKSI2019 [ 50 Point ]

Disediakan soal berikut.



Disajikan flag yang tidak utuh dan hash md5 dari flag tersebut. Kami menggunakan md5 online decrypter <https://www.md5online.org> kemudian menginputkan hash md5 yang sudah ada dan keluar hasil decrypternya.

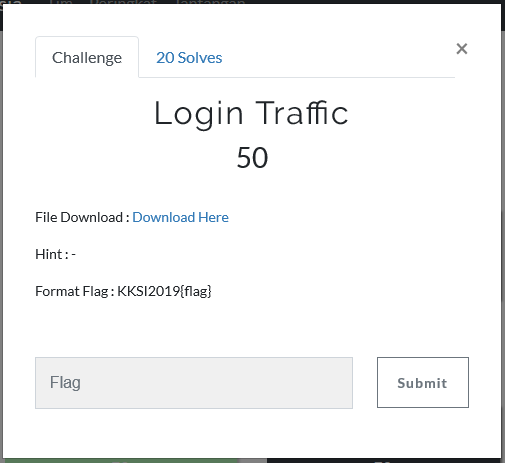


**FLAG : KKSI2019{1663323d00434ad78ca8ecca2ba22844}**

**Forensics**

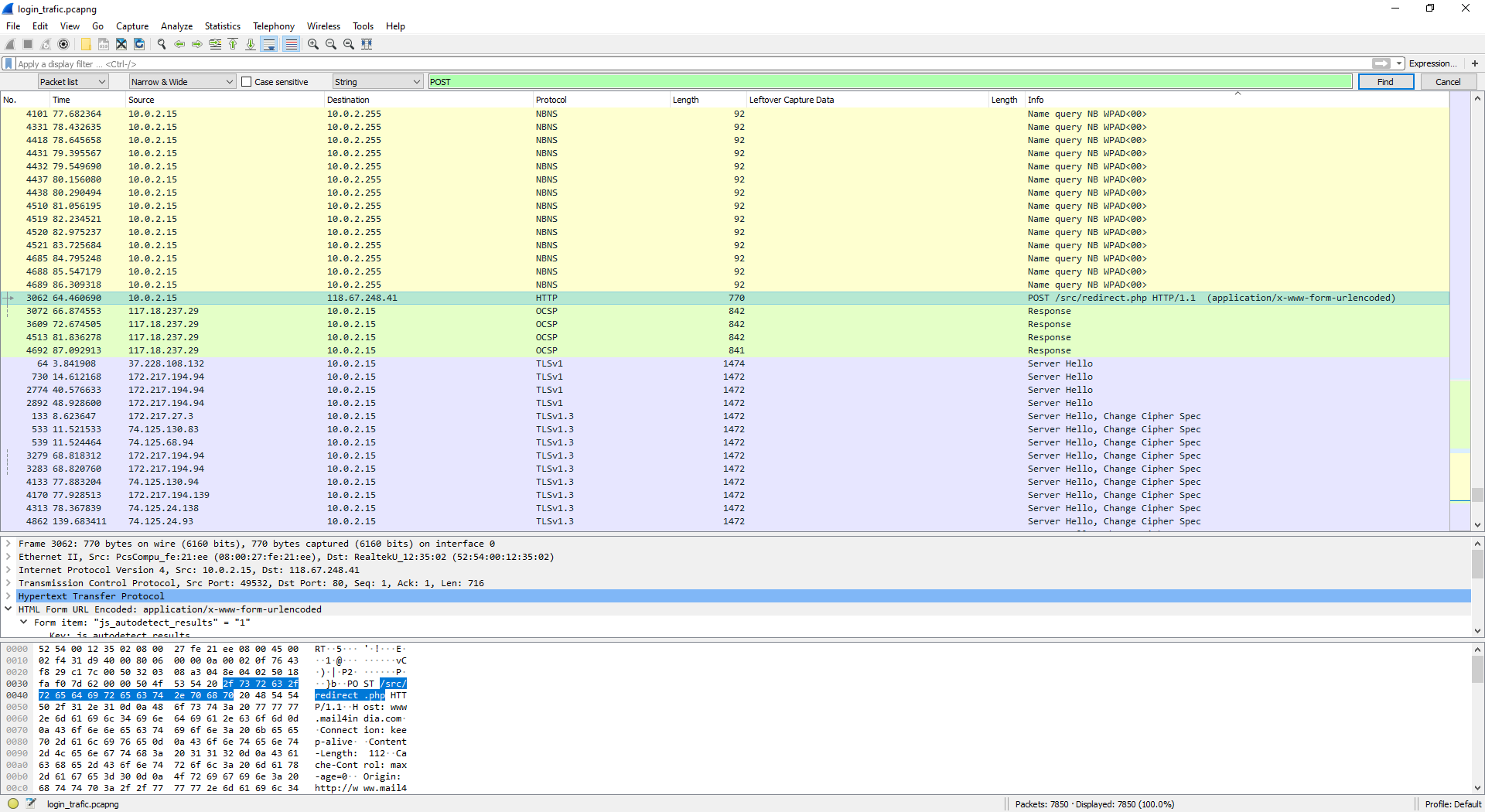
Login Trafic [ 50 Point ]

Disedikan Soal Berikut:

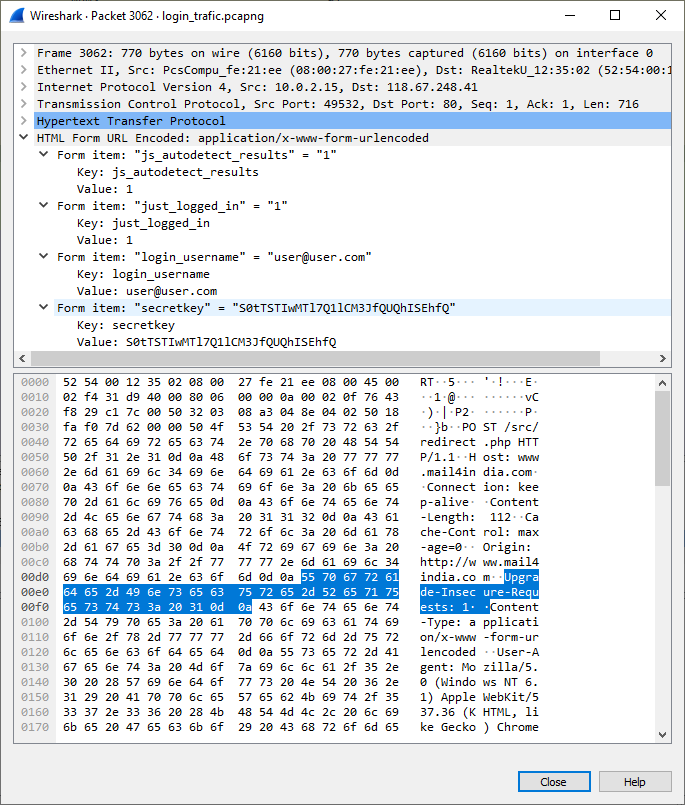


Dengan file **login\_trafic.pcapng**  dan Description: File Download : [Download Here](https://drive.google.com/file/d/1vlAgIsY7f5Z0NLnr0QIiZ74PuHA5DPIU" \o "https://drive.google.com/file/d/1vlAgIsY7f5Z0NLnr0QIiZ74PuHA5DPIU)

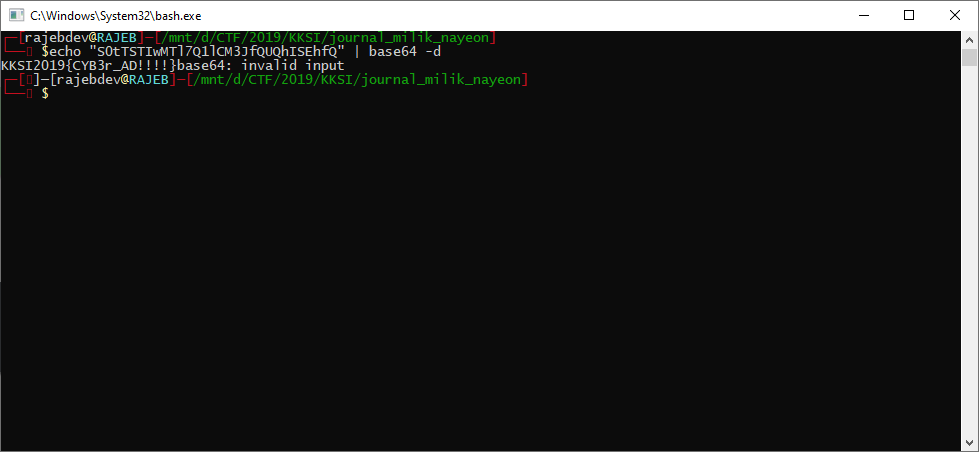
Dilakukan Analisa terhadap log tersebut menggunakan aplikasi WireShark, kami menemukan banyak sekali lalu lintas file. Namun tidak ada yang menarik dari semua file lalu lintas yang ada. Kami sempat berfikir sejenak. Kemudian kami ingat bahwa soal menunjukkan kata login dimana berarti biasanya sebuah login bisa menggunakan method GET atau POST. Setelah itu dilakukan pencarian log dengan string POST maka didapatkan sebuah baris log yang menunjukkan POST ke sebuah halaman.



Dari situ kami membuka log pada baris tersebut maka didapatkan tampilan data form html sebagai berikut.



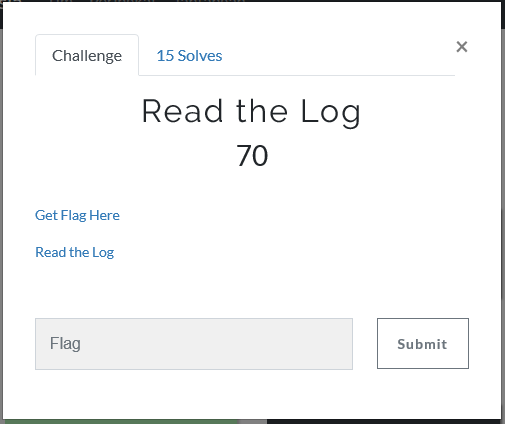
Terdapat Sebuah secretkey berupa base64 yang kami yakini sebagai flagnya. Maka setelah di decode didapakan flagnya.



**FLAG : KKSI2019{CYB3r\_AD!!!!}**

Read The Log [ 70 Point ]

Disediakan soal sebagai berikut.



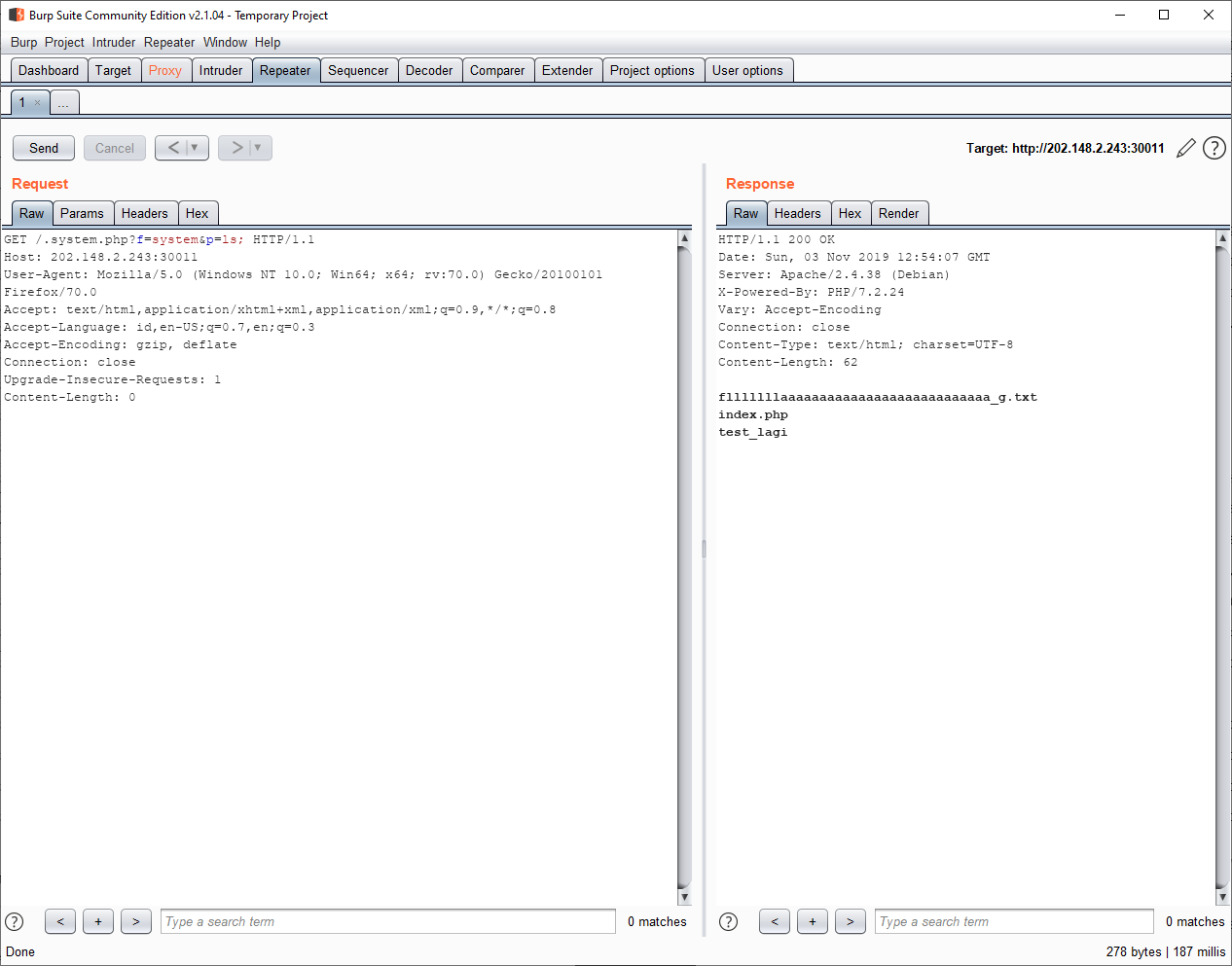
Description: [Get Flag Here](http://202.148.2.243:30011/" \o "http://202.148.2.243:30011/) [Read the Log](https://drive.google.com/file/d/1zujIwaWX3i9wcmCJX6nYT2o6xtwIWFOM)

Beserta file **access.log** yang berisi log dari sebuah lalu lintas access sebuah webiste.

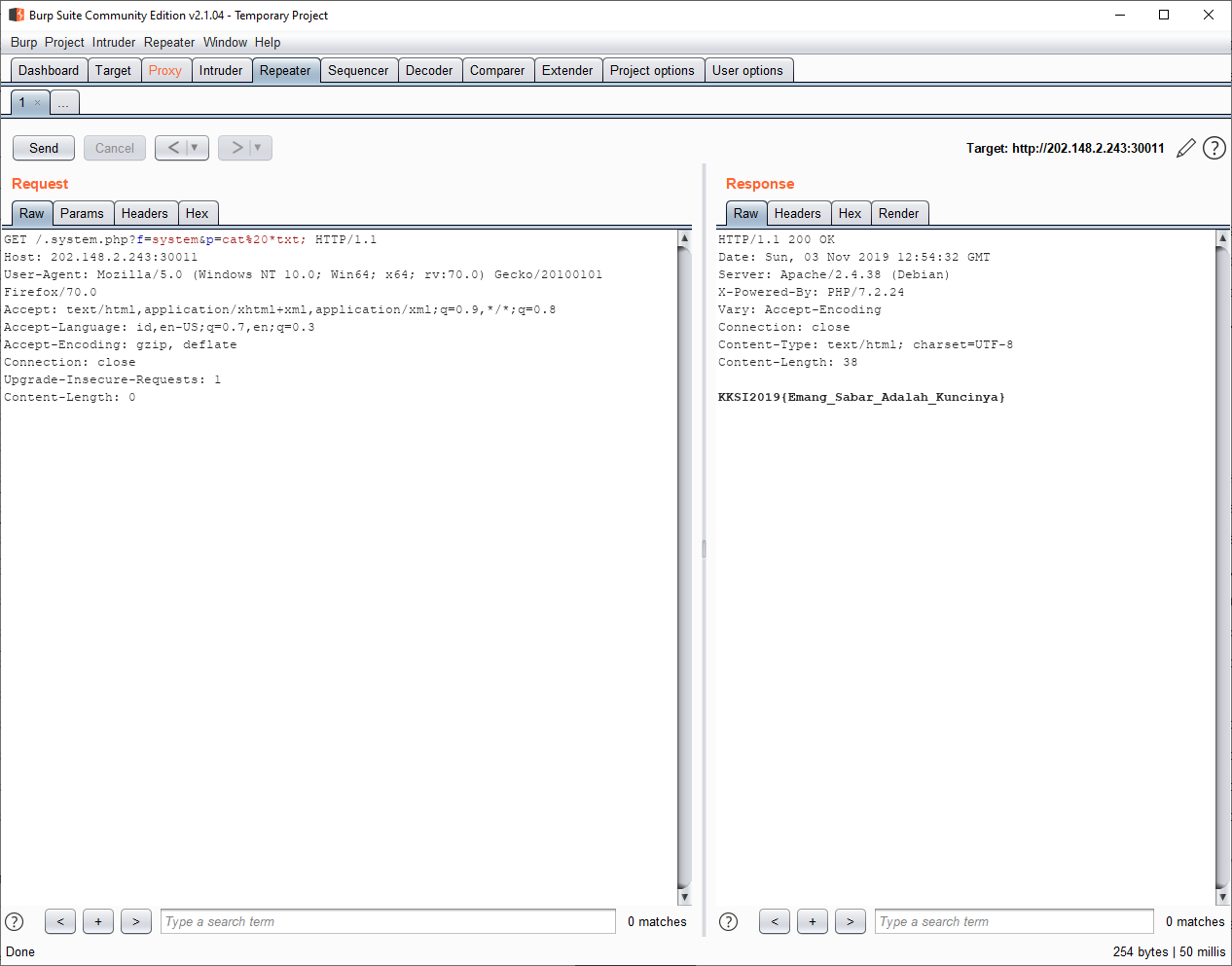
Dilakukan Analisa terhadap log tersebut. Log tersebut mengidentifikasi pengaksesan sebuah alamat atau url sebuah website dimana banyak mendapatkan respond. Pertama kami lakukan pencarian terhadap url dengan respond **200**. Dengan sabar kami meneliti satu persatu log yang ada. Kemudian ada yang menarik untuk kami yaitu sebuah log dengan parameter mirip seperti command linux (system, exec, id, dll). Sebagai berikut.



Kemudian kami lakukan pengiriman data menggunakan BurpSuite agar memudahkan kami. Kami mencoba menggati **id** dengan **ls (LS kecil)**. Maka didapatkan list directory yang ada.



Terdapat file flag dengan nama sangat panjang. Kemudian kami melakukan cat terhadap flag tersebut dengan mengganti **id** menjadi **cat%20\*txt**. Persen 20 berarti spasi. Maka kami mendapatkan flagnya.



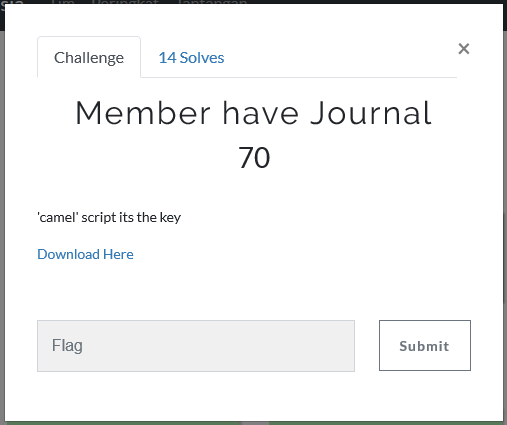
**FLAG : KKSI2019{Emang\_Sabar\_Adalah\_Kuncinya}**

Member Have Journal [ 70 Point ]

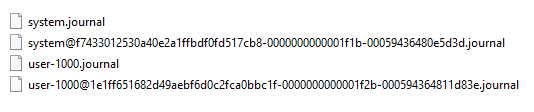
Disediakan soal berikut.

Description: 'camel' script its the key

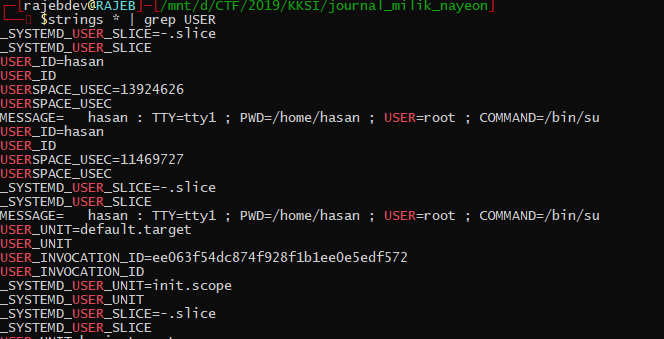
[Download Here](https://drive.google.com/file/d/1T0vPrGpO9mi69rTBEiQ2Emnl0z8pBAVU)



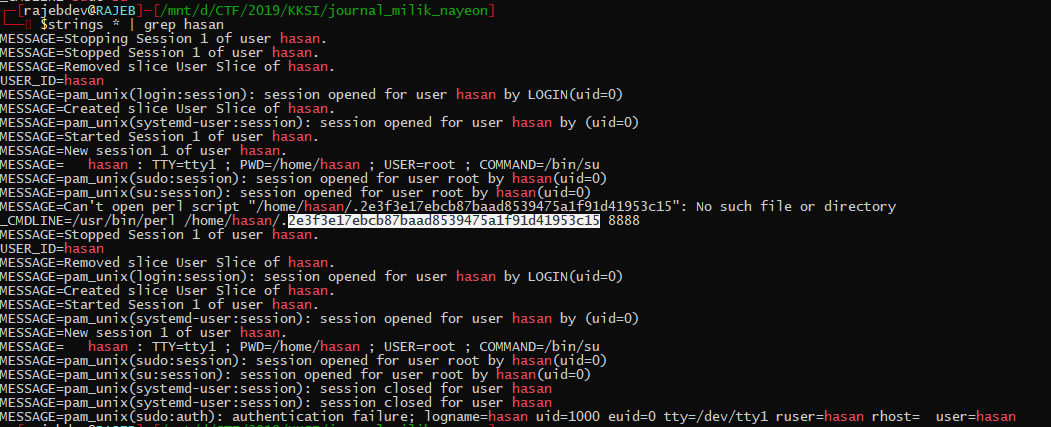
Beserta beberapa file dengan extensi journal.



Kami sempat bingung dengan file journal tersebut. Kemudian kami melakukan pencarian di google dan didapakan jikalau file journal tersebut merupakan sebuah track record dari sebuah file system. Kemudian seperti biasa kami melakukan kebiasan melakuka strings grep. Setelah berfikir agak keras, kami sadar biasanya jika ada soal dengan log file system flagnya tidak jauh dari user yang ada di dalam file system tersebut. Maka kami memutusakan untuk mencari dengan menggunakan strings dan grep. Pertama kami mencari strings yang ada dengan filter grep USER maka didapatkan hasil sebagai berikut.



Pada gambar diatas terlihat bahwa ada user hasan. Kemudian kami melakukan strings grep dengan filter grep hasan. Maka didapakan hasil sebagai berikut.



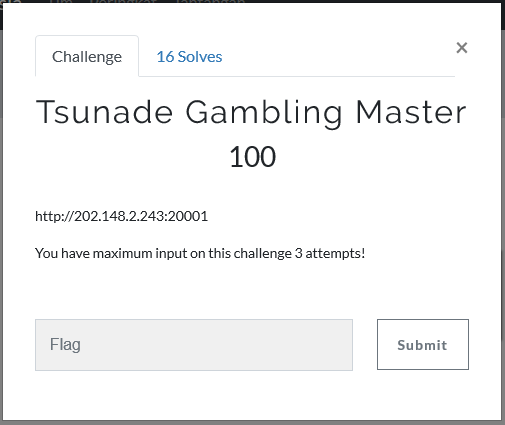
Dari hasil strings grep diatas. Karena tidak ada hal yang jelas seperti password. Kami melihat ada beberapa string hexadecimal yang sama, kami menduga bahwa itu merupakan flagnya. Maka kami memutuskan bahwa string hexa tersebut merupakan flagnya. Setelah kami coba inputkan ternyata benar. Maka flagnya adalah.

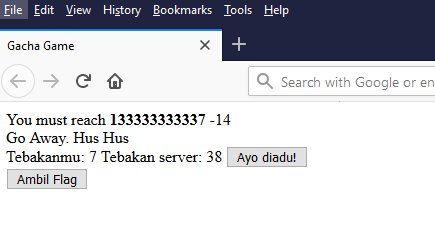
**FLAG : KKSI2019{2e3f3e17ebcb87baad8539475a1f91d41953c15}**

**Web**

Tsunade Gambling Master [ 100 Point ]

Disedikan soal berikut.





Disajikan sebuah web sederhana ‘Gacha Game’. Kami melakukan analisis terhadap source code dari situs tersebut. Kami mendapatkan script JavaScript sebagai berikut:



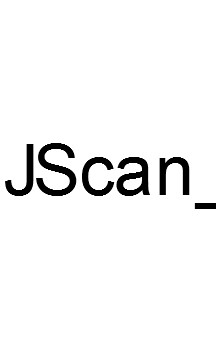
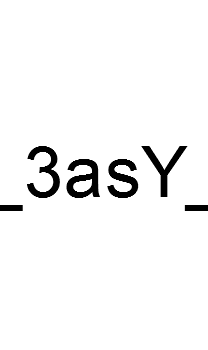
Kami menganalisis code javascript diatas dan mendapati 2 function yang membuat kami curiga yaitu funcion ready\_to\_serve() dan serve(t). Pada function ready\_to\_serve() nilai kembali fungsi tersebut adalah place\_flag.split(‘\_’) yang akan membagi place\_flag="Tr0ll1ng\_th3\_Us3r" menjadi 3 elemen yaitu ‘Tr0ll1ng’,’ th3’,’ Us3r’. Kemudian pada function serve(t) kami mendapati fungsi tersebut untuk membuat link yang menuju gambar dalam server sebagai berikut:

<img src=’./fl4g/Tr0ll1ng.png’>

<img src=’./fl4g/th3.png’>

<img src=’./fl4g/Us3r.png’>

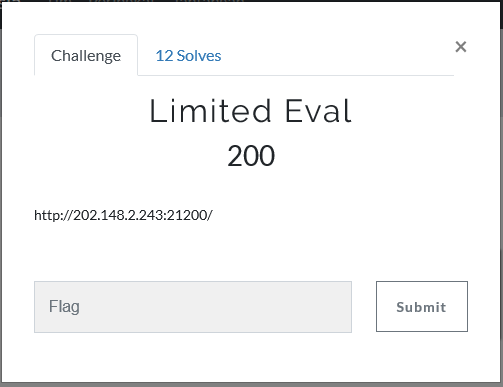
Ketika kami mencoba mengaksesnya hasilnya 3 gambar sebagai berikut:

**FLAG : KKSI2019{JScan\_3asY\_Tr0ll1nG}**

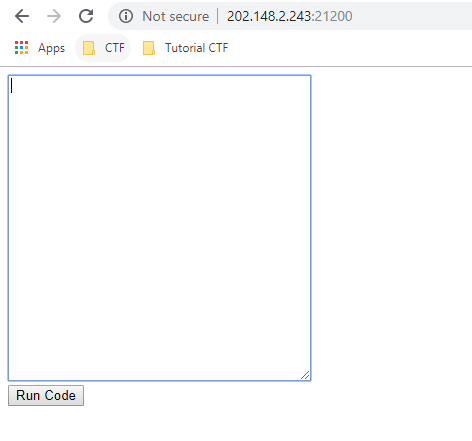
Limited Eval [ 200 Point ]

Disedikan soal berikut.

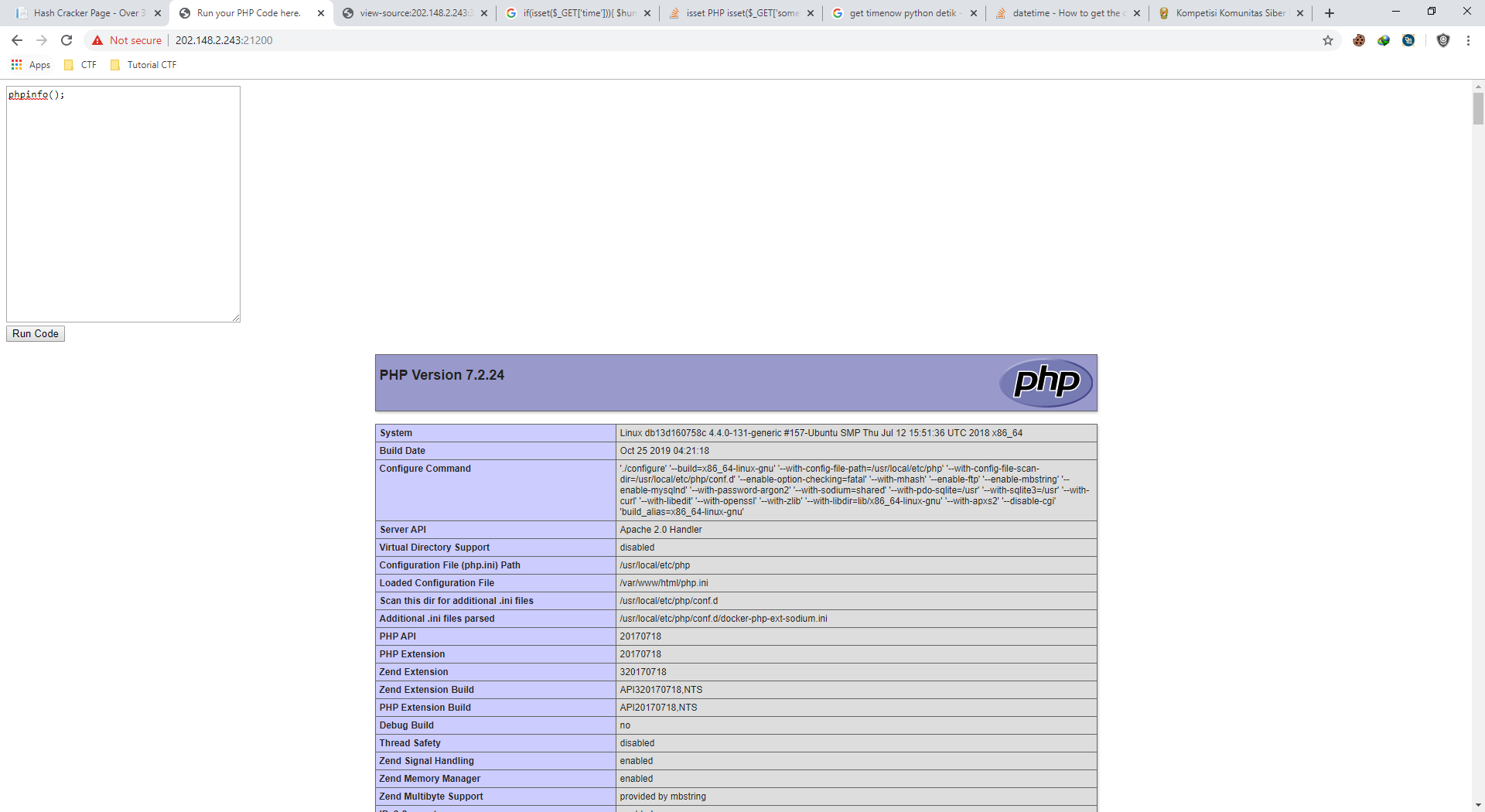


Description: <http://202.148.2.243:21200/>

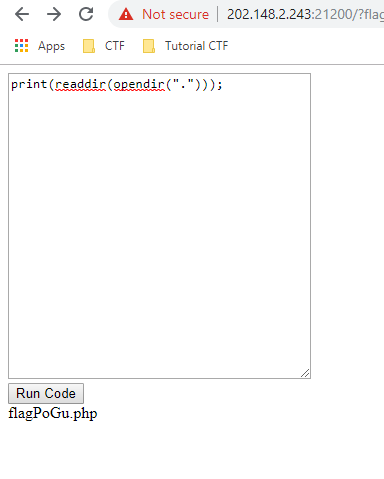
Diberikan tampilan web sebagai berikut.



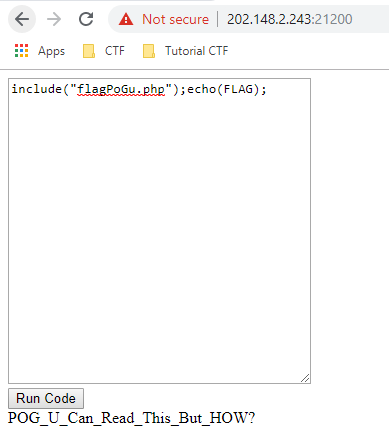
Menurut kami soal merupakan hint dasarnya, yaitu eval code dimana setiap kode yang kita input maka akan dijalankan seperti script php. Namun karena limited maka sudah pasti tidak semua code bisa dijalankan. Kami mencoba mempelajari PHP eval code. Maka seperti biasa dilakukan percobaan echo(1+2) maka ouput akan muncul 3. Ya seperti dugaan. Kemudian kami mencoba menginputkan phpinfo(); maka didapatkan hasil sebagai berikut.



Dari situ kami banyak mengetahui apa saja fungsi yang di disable. Maka kami mencoba beberapa fungsi atau code yang biasa digunakan. Ternyata include bisa dijalankan. Maka kami mencoba melakukan include file online injection kami. Namun ternyata url dan include terlalu panjang. Otomatis kami berfikir keras, mencari di google referensinya. Kami mencari cara untuk membaca directory yang ada untuk melihat file apa sajakah. Kemudian kami menemukan cara menggunakan **scandir** namun ternyata scandir didisable juga. Kemudian kami mencoba adiknya yaitu opendir, ternyata tidak di block, maka harus ditemani oleh readdir untuk membaca dir yang diopen tadi. Kemudian kami menyusun code pendek sebagai berikut. Maka dihasilkan.



Terlihat bahwa ada file flagPogu.php. Kemudian kami lakukan include dan melakukan echo(FLAG);. Hal ini kami lakukan melihat hampir semua code untuk memanggil sebuah FLAGnya. Maka didapakan hasil.



Maka didapatkan flagnya.

**FLAG : KKSI2019{POG\_U\_Can\_Read\_This\_But\_HOW?}**