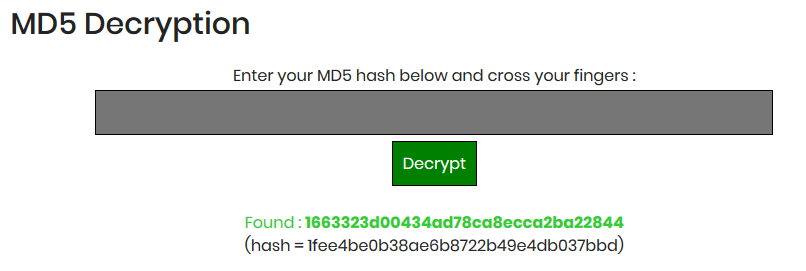
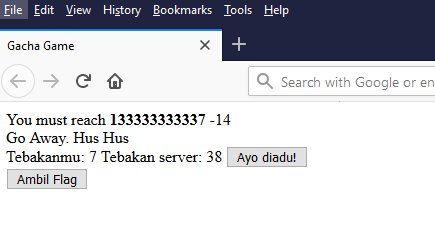
**Welcome To KKSI2019 [50 pts]**

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.



KKSI2019{1663323d00434ad78ca8ecca2ba22844}

**Tsunade Gambling Master [100 pts]**



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



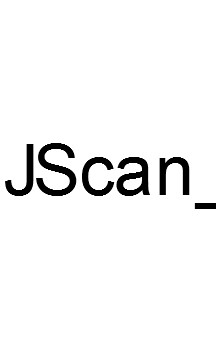
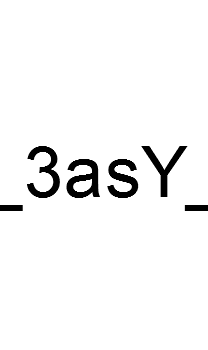
Kami menganalisis code javascript diatas dan mendapati 2 function yang membuat kami curiga yaitu funcion ready\_to\_serve() dan serve(t). Pada function ready\_to\_serve() nilai kembali fungsi tersebut adalah place\_flag.split(‘\_’) yang akan membagi place\_flag="Tr0ll1ng\_th3\_Us3r" menjadi 3 elemen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

KKSI2019{JScan\_3asY\_Tr0ll1nG}