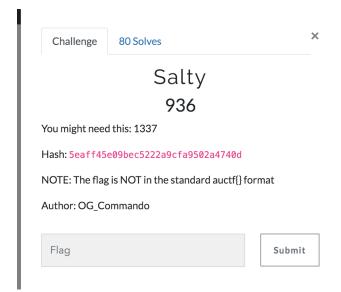
Saturday, March 7, 2020 12:16 PM



The hash length is 32 which suggests MD5 (a 128 bit hash). (32/2)*8 = 128

I found a tool in Kali called hash-identifier

They suggest the salt is 1337

I created a **hashfile** file with the hash in it.

To prepare for a brute force attack, I created a **mask** file with this:

I then tried to brute force with this:

~/bin/hashcat/hashcat -a 3 -m 0 -O hashfile mask

```
-a 3 ---> brute force
-m 0 ---> MD5
```

This will brute force all strings of length 1 to 5 with 1337 prefix or suffix. No joy.

Then I tried the rockyou.txt dictionary file with this rules file.

^7^3^3^1

This prepends 1337 to every word in the file:

hashcat remembers previous finds so clear this out using:

rm ~/bin/hashcat/hashcat.potfile

~/bin/hashcat/hashcat -m 0 -a 0 -O -r rules hashfile ../../rockyou.txt

-a 0 --> dictionary attack -m 0 --> MD5

yields: 5eaff45e09bec5222a9cfa9502a4740d:**1337treetop**

So the flag is: treetop

If that hadn't worked, I was gonna append 1337 with \$1\$3\$3\$7