CHALLENGE NAME

CSAW 2021 CTF

USERNAME

Crack Me

233

Can you crack this? Your hash: `a60458d2180258d47d7f7bef5236b33e86711ac926518ca4545ebf24cdc0b76c`. Your salt: the encryption method of the hash. (So if the hash is of the word `example`, you would submit `flag{example}` to score points.) UPDATE Friday 9PM: To streamline your efforts we would like to give you some more details about the format for the hash encryption method. An example: if you think the hash is RIPEMD-128, use `ripemd128` for the salt.

2021-09-10

Contents

Crack Me

Writeup by: OreoByte

Team: OnlyFeet

Writeup URL: GitHub

```
1  Can you crack this? Your hash:
      a60458d2180258d47d7f7bef5236b33e86711ac926518ca4545ebf24cdc0b76c.
      Your salt: the encryption method of the hash. (So if the hash is of
      the word example, you would submit flag{example} to score points.)
      UPDATE Friday 9PM: To streamline your efforts we would like to give
      you some more details about the format for the hash encryption
      method. An example: if you think the hash is RIPEMD-128, use
      ripemd128 for the salt.
```

Here's the Hash

What Hash is This?

hashid -m A60458d2180258d47d7f7bef5236b33e86711ac926518ca4545ebf24cdc0b76c
OR Hash Analyzer

Cracking a Salted Hash with Hashcat

```
1  # Command Usage: hashcat -m 1420 <hash>:<salt> /usr/share/wordlists/
      rockyou.txt
2  $ hashcat -m 1420
      A60458d2180258d47d7f7bef5236b33e86711ac926518ca4545ebf24cdc0b76c:
      sha256 /usr/share/wordlists/rockyou.txt
```

```
1  $ hashcat -m 1420
      A60458d2180258d47d7f7bef5236b33e86711ac926518ca4545ebf24cdc0b76c:
      sha256 /usr/share/wordlists/rockyou.txt  --show
2  a60458d2180258d47d7f7bef5236b33e86711ac926518ca4545ebf24cdc0b76c:sha256
      :cathouse
```

Victory

Submit the flag and claim the points:

`flag{cathouse}`