Forum:Hack Forums

Thread: How would you decrpyt an md5 salted but know the salt

Slasher - *April 20, 2010, 7:22 pm*

Hey, I was wondering since I need a salted one decrypted but I know the salt how would I go about decrypting it? Would I still need to brute force it or is there an easier online way?

Anyway here is the hash and salt.. if anyone wants to take a try at it

Spoiler (Click to View)93a8bbd88ecb986818af17831e86a62b salt : mx- : (its vBulletin)

romey007 - *April 20, 2010, 7:36 pm*

i dont know how it i am sorry

Slasher - *April 21, 2010, 11:31 am*

(Apr 20, 2010 07:36 PM)romey007 Wrote: *[CITE]* i dont know how it i am sorry
then why do you need to respond if you don't respond then I know that you don't know how...

symetrik - *April 21, 2010, 12:35 pm*

You'll still have to brute force, as it's still a hash. A salt is simply a way to make the hash harder to attack.

You simply append the salt to the hash, depending on how vBulletin does it.

Commonly, it's: salt+password
i.e., if the password was "panda", the password, salted, would look like:
mx-panda

vBulletin may do it differently, I've personally seen:
salt+password
password+salt
(salt+password)+salt

etc. Mainly possible ways.

To brute force it, write out a program in similar vein to this (although I can use this following code, you'll have to find a wordlist for yourself, and also... Python is slow.)
Code #! /usr/bin/env python

```
from hashlib import md5

def bruteForce(hashedWord, wordList, hashSalt, saltStyle):
    for word in wordList:
        hashed = md5(saltStyle.replace("salt", hashSalt).replace("hash", word))
        if hashed.hexdigest() == hashedWord:
            print "The word is %s." % word
            quit()

wordList = [word.rstrip() for word in open(raw_input("Absolute Path To Wordlist: "))
```

```
hashedWord = raw_input("Hash: ")
hashSalt = raw_input("Salt: ")
saltStyle = raw_input("\nExample of Salt Style: salthash OR salthashsalt OR hashsalt, etc.\nSalt Style: ")

bruteForce(hashedWord, wordList, hashSalt, saltStyle)
hashedWord is the hash, of course.
wordList is the path to your word list.
hash salt is the salt used.
salt style is the style in which the salt is used (let's just say it's salt+password, for this example)

When run:
Code symetrik$ python bruteForce.py
Absolute Path To Wordlist: /Users/rawr/Documents/wordlists/massive.txt
Hash: 93a8bbd88ecb986818af17831e86a62b
Salt: mx-

Example of Salt Style: salthash OR salthashsalt OR hashsalt, etc.
Salt Style: salthash
```

Slasher - *April 24, 2010, 3:27 pm*

Anyone else wanna give light on this?

account_ - *March 5, 2023, 11:26 am*

93a8bbd88ecb986818af17831e86a62b:mx-:shift2