

HackThisCode / CTF-Writeups

Watch5

Star14

Fork9

<> Code

Issues 0

Pull requests 2


Projects 0

Pulse

Graphs

Branch: master CTF-Writeups / 2017 / EasyCTF / Genius / README.md

Find fileCopy path

 ValarDragon Minor modifications, and writeup Mane Event 0a65ce5 on Mar 22

1 contributor

57 lines (45 sloc) 2.27 KB

RawBlameHistory



# Genius

- 230 points
- Category: Cryptography
- Problem statement: Your boss told you that this [team](#) has come up with the cryptographic hash of the future, but something about their operation just seems a little fishy.
- Hint: No hint

Here's the site:



## GUESS

GOOD LUCK

Since they hinted at their hash being twice the strength of md5, I thought I'd just put it into [crackstation's](#) hash cracker, and see whats going on.

```
daaed60729d08bb180
b42dad5453b2128a32f6612b13ea5d9fef843bee79633652a6d6ae08e964609f00e883ab809346
226dff6887080fb68b
```

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

## Crack Hashes

Hash	Type	Result
8a7fca9234d2f19c8abfcd812971a26c8c510dcaefd5061b191ad41d8b57d0ce631f5074f94b32730d0c025f1d7aacd7	Unknown	Not found.
be1ab1632e4285edc3733b142935c60b90383bad42309f7f6850d2b4250a713d0b2d7a97350465a02554d29d92bfefaf	md5	like
be1ab1632e4285edc3733b142935c60b90383bad42309f7f6850d2b4250a713d0b2d7a97350465a02554d29d92bfefaf	md5	like
d64ddd0de1b187cd670783f5e28d681dd401ed3009d05ce4ef600d364a2c953e4cc801b880dddef59829a5ad08bd8a63	md5	ly_s
73d559bc117f816333174e918d0587de5cca214701dbe9ff7f42da7bccf074b811292b9d4dc398866ef95869b22b3941e	md5	ng_2
78635bc95eaa7662a2ddf3e3d45cf1084f4233d6c396e8a0e6fbf597d07b88178d03f3f7757bdbdaaed60729d08bb180	Unknown	Not found.
b42dad5453b2128a32f6612b13ea5d9fef843bee79633652a6d6ae08e964609f00e883ab809346226dff6887080fb68b	md5	have
b42dad5453b2128a32f6612b13ea5d9fef843bee79633652a6d6ae08e964609f00e883ab809346226dff6887080fb68b	md5	have

**Color Codes:** **Green:** Exact match, **Yellow:** Partial match, **Red:** Not found.

md5(like) = be1ab1632e4285edc3733b142935c60b The hash it was found in is

be1ab1632e4285edc3733b142935c60b90383bad42309f7f6850d2b4250a713d0b2d7a97350465a02554d29d92bfefaf

So I split the given hash into 32 char chunks, and than began brute forcing 4 byte strings with lowercase and UPPERCASE letters, `{ }`, and numbers. This gives us:

```
$ python3 geniusSolver.py
4cc801b880dddef59829a5ad08bd8a63      0_lo
d401ed3009d05ce4ef600d364a2c953e      0o00
1292b9d4c398666ef2f586b2b2b3941e      3_md
78635bc95eaa762a4bdfc3d4545cf108      5_we
8a7fca9234d2f19c8abfd812971a26c      0MG
```

```
90383bad42309f7f6850d2b4250a713d _LIT
5cca214701dbe9f7f42da7bccf074b81 _MAK
ef843bee79633652a6d6ae08e964609f _no_
0b2d7a97350465a02554d29d92bfefaf eral
b42dad5453b2128a32f6612b13ea5d9f have
00e883ab809346226dff6887080fb68b id34
8c510dcaefd5061b191ad41d8b57d0ce it_t
be1ab1632e4285edc3733b142935c60b like
d64ddd0de1b187cd670783f5e28d681d ly_s
73d559bc117f816333174e918d0587de ng_2
631f5074f94b32730d0c025f1d7aacd7 ook_
4f4233d6c396e8a0e6fbf597d07b8817 rrk_
8d03f3f7757bdbdaaed60729d08bb180 you_
OMG_it_took_like_LITerally_s0o000_long_2_MAK3_md5_werrk_you_have_no_id34
```

Putting that into the website's prompt gives a popup with the flag:

```
easyc{f{0UR_3nCRYpti0n_is_N0T_br0k3n_Ur_brok3n_6c5a390d}
```

Looks like no \$100000000000000 for us :( Pretty easy challenge however!

