



JENNER AREN



7

3

User	Algorithm	Hash
SCOTT	MD5(MD5)	3959dc9...
...	PURE HASH CONSIDERED HARMFUL	

Even consumer grade graphic cards calculates giga-
hashes (2^{30}) per second.

HASHES – EVEN SALTED – OFFER NO PROTECTION

SWITCH TO BRUTE-FORCE PROOF SCHEMES

- ▶ <https://www.troyhunt.com/our-password-hashing-has-no-clothes/>
- ▶ <https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40>
- ▶ <http://cynosureprime.blogspot.de/2017/08/320-million-hashes-exposed.html>
- ▶ https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

User	Algorithm	Hash
SCOTT	MD5(MD5)	3959dc9...
...	PURE HASH CONSIDERED HARMFUL	
...		...

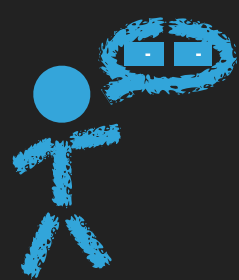
Even consumer grade graphic cards calculates giga-hashes (2^{30}) per second.

HASHES – EVEN SALTED – OFFER NO PROTECTION

SWITCH TO BRUTE-FORCE PROOF SCHEMES

- ▶ <https://www.troyhunt.com/our-password-hashing-has-no-clothes/>
- ▶ <https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40>
- ▶ <http://cynosureprime.blogspot.de/2017/08/320-million-hashes-exposed.html>
- ▶ https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

USER LOGIN: MIGRATE PASSWORDS



LOGIN

USER

PASSWORD

- ▶ Online migration of passwords to a new hashing scheme

Already migrated?

VALIDATE PASSWORD

CONTINUE LOGIN

YES

NO

HASH PWD WITH
NEW ALGORITHM

STORE NEW HASH

Migrate passwords to new hashing scheme at login time