



GOODCRYPTOGRAPHY

5

7

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 AGAINST OFFLINE ATTACKS

SWITCH TO BRUTE-FORCE PROOF (== SLOWER) ALGORITHMS

- ▶ <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
- ▶ [https://en.wikipedia.org/wiki/Pepper_\(cryptography\)](https://en.wikipedia.org/wiki/Pepper_(cryptography))

INCREASE THE ENTROPY BY USING A PEPPER

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

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

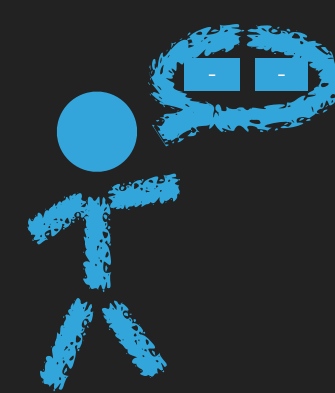
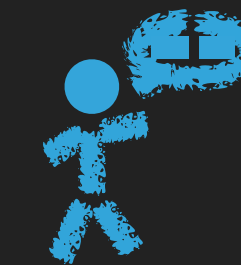
HASHES – EVEN SALTED – OFFER NO PROTECTION AGAINST OFFLINE ATTACKS

SWITCH TO BRUTE-FORCE PROOF (== SLOWER) ALGORITHMS

INCREASE THE ENTROPY BY USING A PEPPER

- <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
- [https://en.wikipedia.org/wiki/Pepper_\(cryptography\)](https://en.wikipedia.org/wiki/Pepper_(cryptography))

USER LOGIN: MIGRATE PASSWORDS



LOGIN

USER

PASSWORD

- Online migration of passwords to a new hashing scheme

