



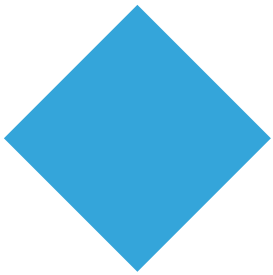
JENNER

Migrate passwords to new hashing scheme at login time



USER LOGIN: MIGRATE PASSWORDS





CONTINUE LOGIN



LOGIN

PASSWORD

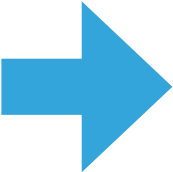
USER



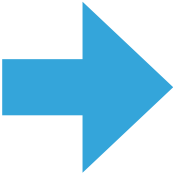




VALIDATE PASSWORD



**HASH PWD WITH
NEW ALGORITHM**



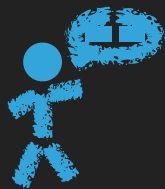
STORE NEW HASH



► **Online migration of passwords
to a new hashing scheme**

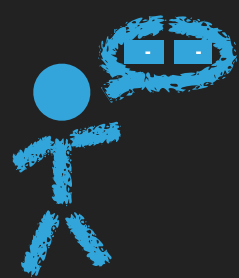


USER LOGIN: MIGRATE PASSWORDS



User	Algorithm	Hash	Last Login
SCOTT	PBKDF2(PWD)	3959dc9...	Now
PETER	MD5(PWD)	...	2 years ago
...	MD5(PWD)	...	4 months ago
...	MD5(PWD)
...	MD5(PWD)
...	MD5(PWD)

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