Passwords

Bryan Hansen
twitter: bh5k
http://www.linkedin.com/in/hansenbryan

pluralsight
hardcore dev and IT training

Passwords


RADIO ORPHAN
19 35
ANNIE'S SS
H G T F U P A M Z N B L Y O
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
C Q X J D R W I E S V

MD5 Hash

- One of the original methods to encrypt
- <password-encoder hash="md5" />
- Need to update our database with new password
- Creating users is a little more difficult because of the hash
- secret = 5ebe2294ecd0e0f08eab7690d2a6ee69

BCrypt

- MD5 Hash is actually still quite weak
  - Google your MD5 hashed password and see what is returned
- Salt helps add security, but adds complexity
- BCrypt adds a salt with no extra configuration
- Password length is longer requiring us to increase column size

Summary

- MD5 Hash
- Salt
- MD5 vulnerabilities
- BCrypt