Hacking Adventures

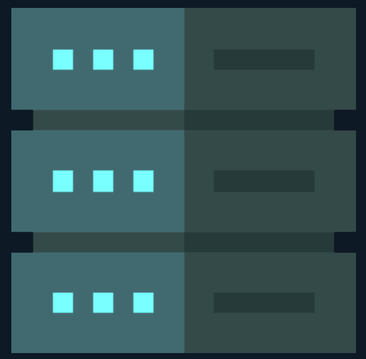
Preparation

- https://github.com/neXenio/hacking-adventures
- Branches:
  - kotlin/challenge-2
  - python/challenge-2
- DM me about pair programming partner and other languages

Goal for Today

- Crack the following password hashes
  - 6Rup8P8oJnxK98aXa8HhGROLdvws9xmgawl7rsh2E5E=
  - 0abdVS0D4YnJJ4b7l0RRr1
  - tt3L+UynOrLtxTN/r/nlDCXnl//QEdMhKEt+AR1hpTY

Storing Passwords



Password123456

Password123456

55251d1743e6...

Problems

601	11,808,233,683	114,647	222,842,049
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
268,765,495	Wattpad accounts

Recently added breaches

52,485	Wendy's accounts
90,655	SirHurt accounts
112,251	Fanpass accounts
22,424,472	Read Novel accounts
174,168	BlackBerry Fans accounts
348,302	OGUsers (2021 breach) accounts
188,089	Paragon Cheats accounts
1,580,249	PayHere accounts
305,470	Aimware accounts
63,451	Devil-Torrents.pl accounts

Source: cybernews.com

Problems

Latest breaches:

- 700 Thousand LinkedIn Accounts
- 500 Million Facebook Accounts
- 11 Thousand WeLeakInfo files

Largest breaches:

- 3.2 Billion Comb Accounts
- 1.4 Billion The BreachCompilation Accounts
- 500 Million Facebook Accounts

Source: haveibeenpwned.com

Problems

Billions of passwords leaked online from past data breaches

by **Lance Whitney** in **Security**
on June 9, 2021, 7:09 AM PDT

Dubbed RockYou2021, the list as revealed on a hacker forum contains 8.4 billion password entries, says CyberNews.

Source: techrepublic.com

Storing Passwords

- https://crackstation.net/hashing-security.htm
- Hash Functions
  - hash("hello") = 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
  - hash("hbllo") = 58756879c05c68dfac9866712fad6a93f8146f337a69afe7dd238f3364946366
  - hash("waltz") = c0e81794384491161f1777c232bc6bd9ec38f616560b120fda8e90f383853542
- Common Examples
  - MD5 (checksums)
  - SHA-256 (authentication, blockchain)
  - Argon2 (passwords)

Storing Passwords

user	hash	salt	timestamp	…
jane@doe.com	ca978112…	lorem	1256953732	
brad@majors.com	3e23e816…	ipsum	1653488378	
sandy@olsson.com	2e7d2c03…	dolor	1343045914	
arthur@dent.com	18ac3e73…	sit	1573651353	

- Dangers
  - No salt
  - Salt reuse
  - Small salt
  - Bad hash function
  - Bad password policies

Best Practices

- As a developer
  - use random salts with at least 32 bytes
  - use argon2
  - spend some time on a good password policy / show password strength
  - consider encrypting the hashes (relevant for 1M+ users)
  - password reset: use short-lived single-use tokens
  - offer MFA

Best Practices

- As a user
  - use a password manager
  - use MFA

Best Practices

- As a hacker (with access to hashed passwords)
  - use a combination of tactics
    - word lists of common passwords
    - password patterns such as WORD + DIGITS (e.g. password123456)
    - use Vari@T1on$ of words
  - use tools like hashcat, John the Ripper, crackstation.net
  - https://xkcd.com/792/