Password Security

LA GitHub Field Day 2018

JonLuca De Caro

You've been lied to

The average American has been conditioned to use passwords that are easy for computers to guess, but hard for humans to remember

Let's walk through an average user's password selection process:

- Pick a password: mittens (their cat's name)
- Need a capital: Mittens
- Need a special char: Mitten$
- Need a num: Mitten$1

Overall complexity?

8 characters.

Time to crack on an average desktop with a modern GPU?

9 hours

(for salted md5 - unsalted? Instantaneously)

And those numbers are just with brute force attempts!

A lot of these issues are just due to developers storing their passwords using weak hashing methods, right?

- In reality, *9.1%* of all passwords show up in the Top 1000 Common Passwords List
- The password "123456" accounts for ~1% of all passwords
- Small variations in the most common passwords will drastically reduce cracking times

And regaardless, there are still some pretty bad developers writing code

- Still use SHA1
- Still use MD5
- Store passwords in plaintext (see: 000webhost)

- Now, this is an audience of good developers, right?
- You'll use PBKDF2 with HMAC-SHA512 with 1,000,000 iterations and a 1024-bit salt.

But is cracking a password the only attack?

Password Reuse

- Password reuse is actually a much more suble issue.
- Most people use the same password for different sites, or small variations of it

A *lot* of sites have been hacked.

- LinkedIn
- MySpace
- Uber
- Equifax

Chances are good that someone has used that same password before - trying it and common variations has an extremely high success rate

The crazy part?

- A lot of these are hacked databases are public
- And they have been cracked (dehashed)
- And they're relatively small (16.1M passwords/GB)

Just to see how easy this was, I spent about an afternoon collating data from different sources, writing a parser, and inserting them into a database overnight

The result?

- 450GB of text
- 240GB MongoDB
- 4.2 *Billion* usernames and passwords

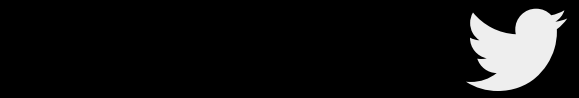
Demo

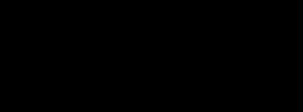
Connect to `0xDEADBEEF` and navigate to 169.254.100.154

Conclusion

- Increasing password entropy is the only way to have a secure password - make it long and random
- Use a password manager (although that might just be kicking the can down the road)
- Cycle your passwords often

Questions?

 @jonlucadecaro

 jonluca

 @jonluca