Hashbrowns

Category: Cryptography, General Skills

Created: Nov 8, 2020 5:14 PM

Points: 50

Solved: Yes

Subjective Difficulty: 🔥

WriteUp:

Author: @Tibotix

🔍 Research:

We are given an MD5 hash The Details hints us that there is no salt included.

📝 Vulnerability Description:

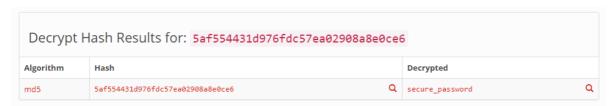When hashing a password without a salt, its likely that this hash is in an online database.

🧠 Exploit Development:

We use hashtoolkit to decrypt this hash.

🗝 Exploit Programm:

✳ Run Exploit:

Decrypt Hash Results for: 5af554431d976fdc57ea02908a8e0ce6

Algorithm	Hash		Decrypted	
md5	5af554431d976fdc57ea02908a8e0ce6	🔍	secure_password	🔍

FLAG: nactf{secure_password}

🗄 Summary / Difficulties:

📦 Further References:

🔨 Used Tools:

- Hashtoolkit

Notes:

-