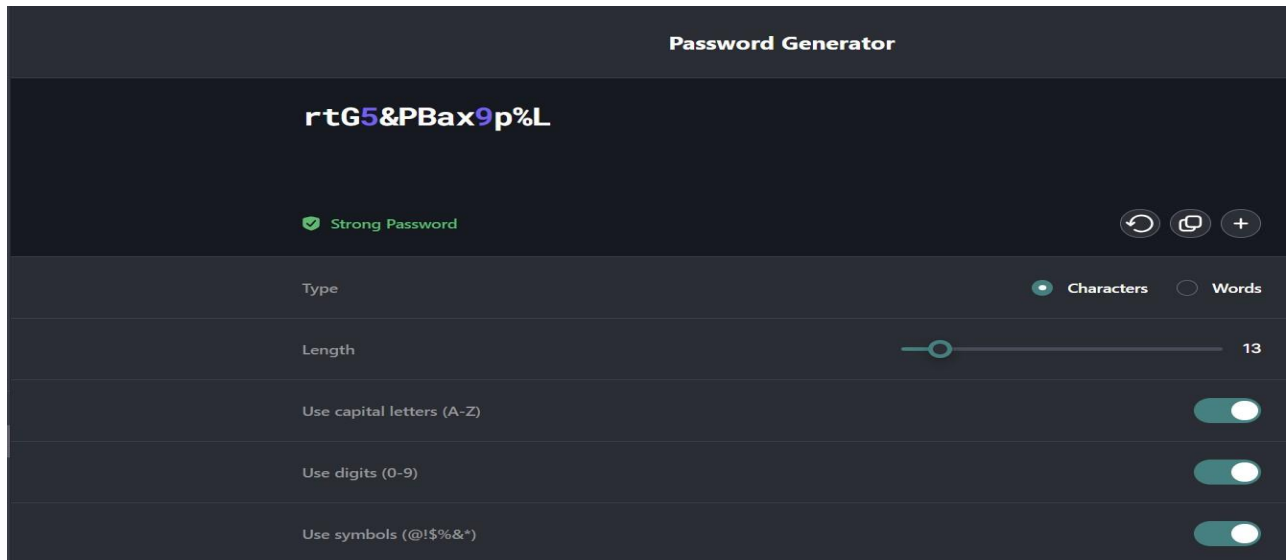


Password Security and Cryptographic Hashing Analysis

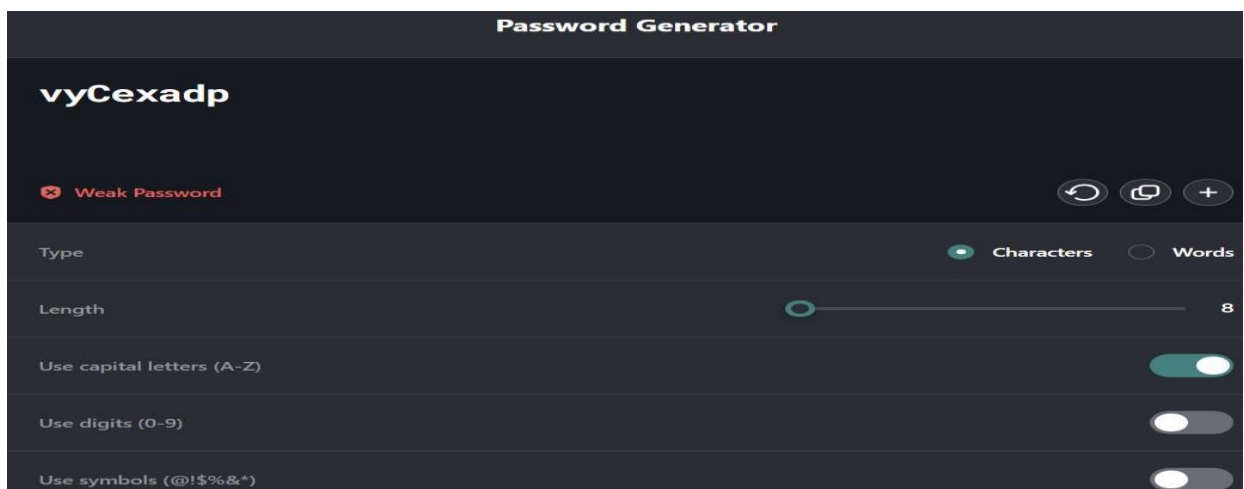
Core Concepts: Identity & Access Management (IAM), Cryptography, MD5 Hashing, Vulnerability Assessment, Security Awareness

Objective: Evaluated password entropy and cryptographic hashing vulnerabilities by generating, hashing, and cracking credentials to demonstrate the risks of weak access controls and the importance of secure password management.

Using a password security tool to generate highly complex combinations to establish a baseline for vulnerability testing. Creating a high-entropy password.



To show the versatility of the tool, a low-entropy credential has been displayed, demonstrating the risk of insufficient access control for hash cracking phase.



Password Security and Cryptographic Hashing Analysis

The results of both password strengths estimated time that is required for a brute-force showing how big of a difference would be for a strong password vises a weak password can be.

.....|

It would take a computer about
2 million years

.....

It would take a computer about
22 minutes

To simulate an offline compromised database scenario, MD5 cryptographic hashes were generated for both credentials for a vulnerability assessment.

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

rtG5&PBax9p%L

Generate →

Your String	rtG5&PBax9p%L	
MD5 Hash	a10f7702160df32b3a6d929336b3e1f5	Copy
SHA1 Hash	32e889c115f74f5b112ae5d2d459227bbece755f	Copy

MD5 Hash Generator

Use this generator to create an MD5 hash of a string:

vyCexadp

Generate →

Your String	vyCexadp	
MD5 Hash	2a350876ee99c1633b51f3796f38f119	<button>Copy</button>
SHA1 Hash	49137f7637c576d20afd907e381604a1adeb62d9	<button>Copy</button>

An offline hash cracking database is used to validate the MD5 hashes of both the weak and strong password to show the high-entropy has good resistance.

Proceeded!
1 hashes were checked: 0 found 1 not found

Pay professionals to decrypt your remaining lists
<https://hashes.com/en/escrow/view>

We can attempt to decrypt these hashes for free
Enter a valid email address and we will message you if w

Email

Email

SUBMIT

✖ Left:
? Hash Identifier

a10f7702160df32b3a6d929336b3e1f5

SEARCH AGAIN

Proceeded!
1 hashes were checked: 0 found 1 not found

Pay professionals to decrypt your remaining hashes
<https://hashes.com/en/escrow/view>

We can attempt to decrypt these hashes for free
Enter a valid email address and we will message you with the results.
Email

Email

SUBMIT

✖ Left:
? Hash Identifier

2a350876ee99c1633b51f3796f38f119

SEARCH AGAIN

A certificate of completion demonstrating proficiency of identifying malicious emails.



Security Insights & Conclusion

Having a password manager is a key component when it comes to generating and maintaining high-entropy credentials. It prevents old habits of using simple ineffective passwords.

You can improve the strength of MD5 hashing by using sharding, breaking up the information into puzzle like pieces. That does not make MD5 better, as it is still considered highly vulnerable. Also hashing still needs encryption.

The importance of checking links in potentially fraudulent emails is because you can catch obvious suspicions early. Hovering over a couple links in an email can reveal that they all lead to the same place, that raises red flags. As people are the new front line.