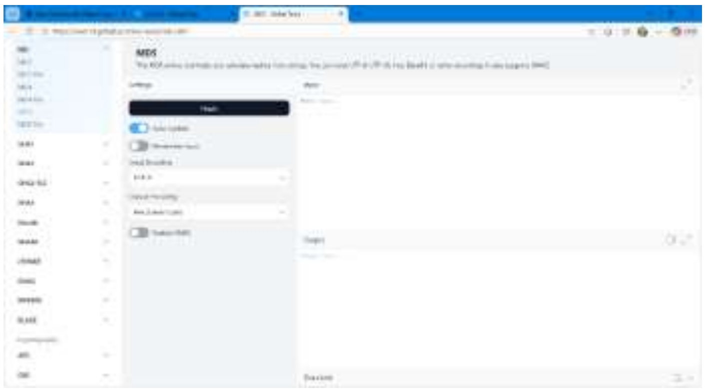
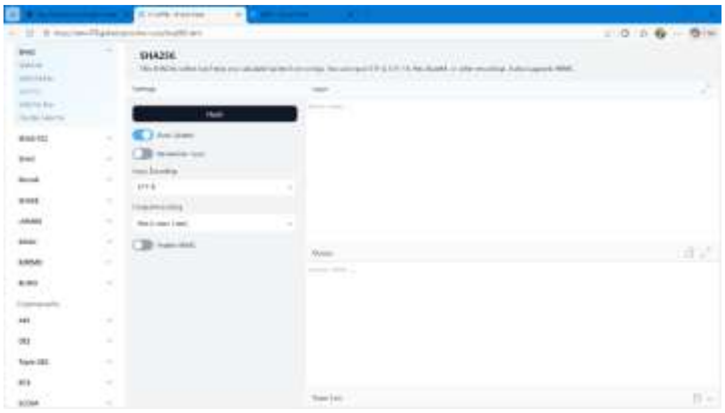
SCREENSHOTS

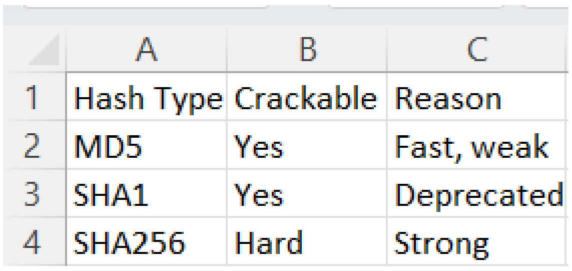
Hash generation MD5



Hash generation SHA



Comparison table



	A	B	C
1	Hash Type	Crackable	Reason
2	MD5	Yes	Fast, weak
3	SHA1	Yes	Deprecated
4	SHA256	Hard	Strong

Security Analysis

Why Weak Hashes Are Dangerous

Weak hash algorithms are dangerous because they can be cracked very quickly using modern hardware such as GPUs. Algorithms like MD5 and SHA-1 produce predictable outputs, making them vulnerable to brute-force and dictionary attacks. Attackers can pre-compute large databases of hashes (rainbow tables) and instantly match stolen hashes to original passwords. Once cracked, attackers can gain unauthorized access to user accounts, sensitive data, and systems. Weak hashes also fail to protect users if a database is breached. This puts both individuals and organizations at serious security risk.

Why MD5 and SHA-1 Should Not Be Used

MD5 and SHA-1 are considered obsolete due to known cryptographic weaknesses. MD5 can be cracked within seconds using freely available tools, and SHA-1 has been officially broken through collision attacks. These algorithms are extremely fast, which actually helps attackers try millions of password guesses per second. Many cybersecurity standards and organizations no longer recommend their use. Using MD5 or SHA-1 for password storage violates modern security best practices and can lead to data breaches. Secure systems must use stronger hashing algorithms designed specifically for passwords.

Where Attackers Use Hash Cracking

Attackers commonly use hash cracking after stealing password databases from compromised websites or applications. These databases usually store passwords in hashed form, which attackers then attempt to crack offline. Hash cracking is also used in data breaches, leaked credential dumps, and dark web marketplaces. Cybercriminals use cracked passwords for account takeover, identity theft, phishing, and credential-stuffing attacks. Ethical hackers and security professionals also use hash cracking in controlled environments to test system security. This helps organizations identify weak password practices and improve defenses.

Prevention Techniques

Salting

Salting is the process of adding a random value to a password before hashing it. This ensures that even identical passwords produce different hashes. Salting prevents attackers from using rainbow tables effectively. Each user has a unique salt, making mass cracking extremely difficult. Salting is a basic but essential security measure for password protection.

Peppering

Peppering adds a secret value to the password before hashing, similar to salting, but the pepper is stored separately from the database. Even if attackers steal the database, they cannot crack the hashes without knowing the pepper. Peppering adds an extra layer of security beyond salting. It significantly increases the difficulty of successful password cracking attacks.

---

bcrypt

bcrypt is a password hashing algorithm designed to be slow and computationally expensive. Its slowness makes brute-force attacks impractical. bcrypt also automatically includes salting, improving security further. It is widely used in modern web applications for secure password storage. bcrypt adapts to increasing computing power by allowing configurable cost factors.

Argon2

Argon2 is a modern and highly secure password hashing algorithm. It is resistant to GPU and ASIC-based attacks. Argon2 allows fine control over memory usage, time cost, and parallelism. It is currently recommended as one of the best algorithms for password hashing. Many security experts consider Argon2 the future standard for password protection.

Rate Limiting

Rate limiting restricts the number of login attempts within a specific time period. This prevents attackers from repeatedly trying different passwords. Even if strong hashes are used, rate limiting protects systems from online brute-force attacks. It helps detect suspicious behavior and improves overall system security. Rate limiting is an important defense mechanism in authentication systems.