VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

ENSURING PASSWORD SECURITY: A COMPREHENSIVE GUIDE TO AUDITING THE HASHING PROCESS

Under the guidance of:
Prof. Dr. THANGA MARIAPPAN L
Course: ISAA
Slot: F1

Team members:
Lokesh Kumaran R- 20MIS0052
Bavya I- 20MIS0060
Kaushik M- 20MIS0306

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

ABSTRACT:

Auditing the different hashing schemes in password storage is a fundamental aspect of safeguarding digital security. This research review covers the important elements of password security, such as the selection of robust hashing algorithms, appropriate work factors, and the strength of the encryption for given password.

Ensuring password policies that promote strong, complex passwords, and encryption of password transmission are vital components. Security audits, monitoring, and compliance with industry standards serve as additional layers of protection. Regular evaluations, user education, and an incident response plan collectively contribute to a robust system, guarding against unauthorized access and data breaches, and promoting secure and reliable authentication.

This paper provides a review of mostly used password-hashing schemes in todays world and their efficiency.

INTRODUCTION :

One such measure is the use of cryptographic hashing schemes, which transform user passwords into irreversible, fixed-length strings of characters. These hash values are stored on servers instead of plain-text passwords, enhancing security by making it more challenging for adversaries to reverse-engineer the original passwords. Nevertheless, not all hashing schemes are created equal. They vary in terms of security, computational cost, and resistance to attacks.

The objective of this research paper is to conduct a comprehensive audit of different hashing schemes used in password security, examining their strengths, weaknesses, and suitability for protecting sensitive user data. We will compare and contrast popular hashing algorithms such as algorithms like MD5 and SHA and framework dependant based security.

CHALLENGES :

- Evolving Threat Landscape:
- Usability vs. Security Trade-off:
- Regulatory Compliance:
- Interdisciplinary Collaboration:
- Quantum Computing Threat:
- Scalability:
- User Education and Behavior:
- Ethical Considerations:
- Cross-Platform Compatibility:
- Privacy Concerns:

ALGORITHMS USED :

- Md5.
- Sha1
- Sha 256
- Sha 512
- Django framework:
- bcrypt

AUDITING PROCESS :

1. Collect Passwords:
2. Assess Password Policies:
3. Generate Wordlist:
4. Select Brute-Force Tools:
5. Crack Passwords:
6. Measure Success Rate:
7. Analyse Password Complexity:
8. Recommend Improvements:
9. Educate Users
10. Monitor and Respond to Anomalies:

EXPERIMENT:DEMO

```
C:\Users\KAUSHIK MADAN\Downloads\hashcat-6.2.6\hashcat-6.2.6>hashcat.exe -m 0 demo.txt -a 3 -1 ?l  ?1?1?1?1?1?1?1?1
hashcat (v6.2.6) starting

OpenCL API (OpenCL 2.1 ) - Platform #1 [Intel(R) Corporation]
============================================================
* Device #1: Intel(R) UHD Graphics, 1536/3187 MB (796 MB allocatable), 32MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

```
1a1dc91c907325c69271ddf0c944bc72:pass

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 1a1dc91c907325c69271ddf0c944bc72
Time.Started.....: Sun Nov 05 19:17:57 2023 (0 secs)
Time.Estimated...: Sun Nov 05 19:17:57 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: ?1?1?1?1 [4]
Guess.Charset....: -1 ?l, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  6417.9 kH/s (0.15ms) @ Accel:128 Loops:26 Thr:32 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 26624/456976 (5.83%)
Rejected.........: 0/26624 (0.00%)
Restore.Point....: 0/17576 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-26 Iteration:0-26
Candidate.Engine.: Device Generator
Candidates.#1....: sari -> xmgg

Started: Sun Nov 05 19:17:53 2023
Stopped: Sun Nov 05 19:17:59 2023
```

EXPERIMENT RESULTS :

	method	Hash function	key	Port number	Time to retrieve
1	Md5	dc06698f0e2e75751545455899adccc3	pass@123	0	12days 2hours
2	Sha1	ba97b1cf397425a852d1316d10787b1d97b5bc85	pass@123	1400	21days 22hours
3	Sha256	d97086919b6522e13ba9b46c04902c38372102218a4b3ef2f45ac2a80e9fd240	pass@123	100	47days 21hours
4	Sha512	419b199de5751e4ac1e1ed5e601007331344f75d5939829ebfef895353e76ec95d14be93ecbc51e59f80d64e949379bbdfb52df7d93dd967676ab389ae173b84	pass@123	1700	230days 13hours
5	Django	pbkdf2_sha256$390000$E1AQCq34JRR1BKAxz0eFan$u3+pPwvXA9hHtL+RPt3nu2MBaPqi7t86K8tt32zbRNg=	pass@123	10000	>10 years
6	bcrypt	$2a$04$Pk/zPHTy2GHRw8a5H3rEmennu2raAIiyq/7u741TaVSi.9uEHoRBq	pass@123	3200	>10 years

FUTURE WORK:

1. Develop precise metrics to quantify the security of hashing schemes, such as their resistance to attacks and computational requirements for password cracking.
2. Investigate hybrid hashing schemes that combine multiple algorithms to improve security and examine their real-world performance.
3. Post-Quantum Cryptography: Investigate post-quantum cryptographic methods to mitigate the risks posed by quantum computing.
4. Password-less and User-Centric Authentication: Investigate password-less and user-centric authentication methods, as well as usability, security, and adoption considerations.

CONCLUSION:

The comparative analysis of different hashing schemes in the context of password security underscores the importance of selecting the right cryptographic technique to safeguard user credentials and sensitive data.

As the digital landscape continues to evolve, and with the ever-present threat of cyberattacks, the choice of a hashing scheme is a critical decision that has profound implications for overall system security.

Our examination of various hashing schemes like legacy algorithms like MD5 and SHA-1, has revealed significant disparities in security, performance, and adaptability to emerging threats.

THANK YOU