

Forum:[Hack Forums](#)

Thread: [50\\$ md5 hash](#)

NiNJAA - October 20, 2025, 1:02 pm

MD5 HASH

62780599eda3dca7fc2d0641e2ffa95d

NiNJAA - October 20, 2025, 1:05 pm

(Oct 20, 2025 01:03 PM)Tyr Wrote: [\[CITE\]](#) Testing lookup paths for hash on cracking sites. Will update.

This is some hacker's website hash; I don't think it will be in any public database.

Tyr - October 20, 2025, 1:07 pm

(Oct 20, 2025 01:05 PM)NiNJAA Wrote: [\[CITE\]](#) This is some hacker's website hash; I don't think it will be in any public database.

It's not. I can look into this later if someone doesn't already get to ya :) best of luck bud

Assuming you are using rockyou.txt, ye?

NiNJAA - October 20, 2025, 1:11 pm

(Oct 20, 2025 01:07 PM)Tyr Wrote: [\[CITE\]](#) It's not. I can look into this later if someone doesn't already get to ya :) best of luck bud

Assuming you are using rockyou.txt, ye?

i dont try anything if someone crack i pay for it

HerrWinston - October 20, 2025, 1:53 pm

Been running my dehasher for about 40 minutes now, maybe i will get the answer sooner or later lmao, there arent ANY hints perchance right? atleast length or something

onlineuser | D3RFER - October 20, 2025, 2:14 pm

Rockyou is not gonna get you any results, or anyone that attempts, you heard it here first.

Tyr - October 20, 2025, 7:46 pm

(Oct 20, 2025 02:14 PM)onlineuser | D3RFER Wrote: [\[CITE\]](#) Rockyou is not gonna get you any results, or anyone that attempts, you heard it here first.

I agree. Going around just blasting rockyou rarely works today.

Yes, it's dated and limited and people now have stronger passwords & passphrases: people increasingly use longer passphrases and password managers, which aren't covered by rockyou. The big issue is how modern hashing slows attackers: bcrypt/Argon2/PBKDF2 intentionally make each guess expensive, so a cheap dictionary gives you little advantage. Wordlists are your best friend though either way, this was kind of the message I was hinting at.

rockyou is useful for quick demos, though.

ClickAds - October 20, 2025, 8:00 pm

(Oct 20, 2025 07:46 PM)Tyr Wrote: [\[CITE\]](#) I agree. Going around just blasting rockyou rarely works

today.

Yes, it's dated and limited and people now have stronger passwords & passphrases: people increasingly use longer passphrases and password managers, which aren't covered by rockyou. The big issue is how modern hashing slows attackers: bcrypt/Argon2/PBKDF2 intentionally make each guess expensive, so a cheap dictionary gives you little advantage. Wordlists are your best friend though either way, this was kind of the message I was hinting at.

rockyou is useful for quick demos, though.

Rockyou is more of a classic for quick tests or CTFs, but in real-world scenarios, modern hashing and password habits make it almost obsolete. Custom or hybrid wordlists tuned for the target are way more effective now.

DramaKing - October 20, 2025, 8:03 pm

(Oct 20, 2025 07:46 PM)Tyr Wrote: [\[CITE\]](#) I agree. Going around just blasting rockyou rarely works today.

Yes, it's dated and limited and people now have stronger passwords & passphrases: people increasingly use longer passphrases and password managers, which aren't covered by rockyou. The big issue is how modern hashing slows attackers: bcrypt/Argon2/PBKDF2 intentionally make each guess expensive, so a cheap dictionary gives you little advantage. Wordlists are your best friend though either way, this was kind of the message I was hinting at.

rockyou is useful for quick demos, though.

Yeah, Chrome even checks passwords against a built-in wordlist now. This hash is MD5, so I was able to blast through the largest wordlist that I could find + rules. Nada.

Tyr - October 20, 2025, 8:06 pm

(Oct 20, 2025 08:00 PM)ClickAds Wrote: [\[CITE\]](#) Rockyou is more of a classic for quick tests or CTFs, but in real-world scenarios, modern hashing and password habits make it almost obsolete. Custom or hybrid wordlists tuned for the target are way more effective now.

Correct. Nice addition. I see you're somewhat new here. Would love to see more posts about this stuff from you in the future. :)

ClickAds - October 20, 2025, 8:07 pm

(Oct 20, 2025 08:06 PM)Tyr Wrote: [\[CITE\]](#) Correct. Nice addition. I see you're somewhat new here. Would love to see more posts about this stuff from you in the future. :)

I'm still learning from the discussions here but definitely planning to share more insights as I dig deeper into these topics.

onlineuser | D3RFER - October 20, 2025, 8:09 pm

(Oct 20, 2025 08:03 PM)DramaKing Wrote: [\[CITE\]](#) Yeah, Chrome even checks passwords against a built-in wordlist now. This hash is MD5, so I was able to blast through the largest wordlist that I could find + rules. Nada.

Exactly.

Chrome amongst many other services checks passwords against a built-in wordlist.

Would be easier to make a wordlist based on the target in this particular situation.
Some information gathering + custom wordlist = way better chances

Tyr - October 20, 2025, 8:09 pm

(Oct 20, 2025 08:07 PM)ClickAds Wrote: [\[CITE\]](#) I'm still learning from the discussions here but definitely planning to share more insights as I dig deeper into these topics.

Well I do sincerely hope you learn something here and hope you enjoy your time learning! See you around.

NiNJAA - *October 20, 2025, 8:13 pm*

(Oct 20, 2025 01:53 PM)HerrWinston Wrote: [\[CITE\]](#) Been running my dehasher for about 40 minutes now, maybe i will get the answer sooner or later lmao, there arent ANY hints perchance right? atleast length or something i dont know any hint

hint is

this hash HACKER SERVER

freya33 - *October 21, 2025, 11:40 pm*

good comments

NiNJAA - *October 22, 2025, 4:54 am*

(Oct 21, 2025 11:40 PM)freya33 Wrote: [\[CITE\]](#) good comments
???

Tyr - *October 22, 2025, 7:14 pm*

(Oct 21, 2025 11:40 PM)freya33 Wrote: [\[CITE\]](#) good comments
You are a good comment.

onlineuser | D3RFER - *October 23, 2025, 9:25 pm*

(Oct 21, 2025 11:40 PM)freya33 Wrote: [\[CITE\]](#) good comments
Just why. Like why even bother