

Forum:[Hack Forums](#)

Thread: [Let's crack the Tumblr database hashes. \(READREADREADO](#)

C0ldplay - June 12, 2016, 6:46 am

Alright I ain't stupid. I know that the hashes are HASH:SALT. And I also know that the leak ONLY contains the HASH part of it. But here's an idea, why can't we brute force the hash? I mean, let's assume that the SALT is only up to 5 characters. Theoretically, we could "brute force" the salt. How could this be done? simple.

Using "Cruch" to generate a 5 character list, (also includes 1,2,3,4) to get every possible salt. Then use a "combo" maker to use one or two test hashes, and use the two hashes with every single salt then use hashcat to attempt to crack them. If done, we could figure out how long the salts are and possibly bring us closer to cracking the hashes.

should i attempt this or is it retarded

TheTwitchTerror - June 12, 2016, 6:48 am

I don't know about this but yea attempt pls

J?ey - June 12, 2016, 6:53 am

sounds like it would take way more resources than what its worth...

C0ldplay - June 12, 2016, 6:54 am

(Jun 12, 2016 06:53 AM)J?ey Wrote: [\[CITE\]](#) sounds like it would take way more resources than what its worth...

It wouldn't take too long, on my set up I get around 60mil per second. Not too bad, wouldn't take too long.

Ooze - June 12, 2016, 6:54 am

Talk with Chick3man about this, it would be very difficult but you could make a good amount of money by selling the hashes.

I know I would pay

Evanescence - June 12, 2016, 6:56 am

Are these just Tumblr passwords? I don't see how they would be worth much.

Cryptography - June 12, 2016, 6:58 am

(Jun 12, 2016 06:56 AM)Evanescence Wrote: [\[CITE\]](#) Are these just Tumblr passwords? I don't see how they would be worth much.

Combo list for all social media accs, useful combos for cracking into OGs.

Evanescence - June 12, 2016, 7:03 am

(Jun 12, 2016 06:58 AM)Cryptography Wrote: [\[CITE\]](#) Combo list for all social media accs, useful combos for cracking into OGs.

Oh cool, sounds great. I think cracking these without the salt would take a really long time though.

C0ldplay - June 12, 2016, 7:05 am

(Jun 12, 2016 07:03 AM)Evanescence Wrote: [\[CITE\]](#) Oh cool, sounds great. I think cracking these without the salt would take a really long time though.

Yeah, which is why I decided to make this thread...

We can try to brute force the salts and see if we can figure out a formula for it.

joepvand - June 12, 2016, 7:05 am

(Jun 12, 2016 07:03 AM)Evanescence Wrote: [\[CITE\]](#) Oh cool, sounds great. I think cracking these without the salt would take a really long time though.

Thats why he is bruteforcing the salts right?

Evanescence - June 12, 2016, 7:10 am

(Jun 12, 2016 07:05 AM)rob_ert Wrote: [\[CITE\]](#) Yeah, which is why I decided to make this thread...

We can try to brute force the salts and see if we can figure out a formula for it.

Wouldn't you have to try each salt guess with each hash guess? I'm sorry if I'm asking stupid questions. I don't know exactly how this works and I'm tired as fuck.

Mr. Robot - June 12, 2016, 7:11 am

Your best bet is to look up an email for a user you know uses only one password, then go from there. Maybe examine a few that you can definitely say that's so and so's password then onwards march

(Jun 12, 2016 07:10 AM)Evanescence Wrote: [\[CITE\]](#) Wouldn't you have to try each salt guess with each hash guess? I'm sorry if I'm asking stupid questions. I don't know exactly how this works and I'm tired as fuck.

Different salts for different hashes love.

Evanescence - June 12, 2016, 7:17 am

(Jun 12, 2016 07:11 AM)Mr. Robot Wrote: [\[CITE\]](#) Your best bet is to look up an email for a user you know uses only one password, then go from there. Maybe examine a few that you can definitely say that's so and so's password then onwards march

Different salts for different hashes love.

Fuck, I wanna give you another rep so you can be at 1700 but I already gave you 3. ?

wpacracknet - June 22, 2016, 2:18 pm

(Jun 12, 2016 07:11 AM)Mr. Robot Wrote: [\[CITE\]](#) Different salts for different hashes love.

I did a part analysis on it and there are multiple matches with the same hashes. So it does seem like a static salt.

Sheeple - June 22, 2016, 2:20 pm

(Jun 12, 2016 07:11 AM)Mr. Robot Wrote: [\[CITE\]](#) Your best bet is to look up an email for a user you know uses only one password, then go from there. Maybe examine a few that you can definitely say that's so and so's password then onwards march

Different salts for different hashes love.

You cannot 100% say that the salts are different.

Many databases use static salts.

And I've seen sha's get salted with 15 digit salts so

Faith Connors - June 22, 2016, 8:33 pm

I mean if you're going through with this, I think you're batshit crazy but that's still awesome and I encourage you to pursue that goal. It'll be awesome in the end and you'll get a lot of recognition for sure.

Bellaquito123 - September 20, 2020, 7:01 pm

(Jun 12, 2016 06:46 AM)C0ldplay Wrote: [\[CITE\]](#) Alright I ain't stupid. I know that the hashes are HASH:SALT. And I also know that the leak ONLY contains the HASH part of it. But here's an idea, why can't we brute force the hash? I mean, let's assume that the SALT is only up to 5 characters. Theoretically, we could "brute force" the salt. How could this be done? simple.

Using "Cruch" to generate a 5 character list, (also includes 1,2,3,4) to get every possible salt. Then use a "combo" maker to use one or two test hashes, and use the two hashes with every single salt then use hashcat to attempt to crack them. If done, we could figure out how long the salts are and possibly bring us closer to cracking the hashes.

should i attempt this or is it retarded

So nobody get this done rights?

Kaos-Industries - November 26, 2020, 5:26 pm

(Sep 20, 2020 07:01 PM)Bellaquito123 Wrote: [\[CITE\]](#) So nobody get this done rights?
It doesn't seem so no