

Forum:[Hack Forums](#)

Thread: [decrypt edmodo bcrypt hash](#)

ansjdnfiqnuaskdnfa45 - April 3, 2024, 6:02 am

I was wondering whether someone could help me decrypt this bcrypt hash from edmodo.

original:

\$826y4\$31226\$dObW2ZfmeO3TbFeh4Y0WcQc22O4T1c827Y7zfU6yaM2ucg9z0bbO77RBZsC9.v1
GSJXZSwrby9dlvmK

de-obfuscated:

\$2y\$12\$OWZmOTFhYWQ2OTc2YzUyMugzbO77RBZsC9.v1GSJXZSwrby9dlvmK

I've tried to use resources on this specific topic, although I've hit a wall with my understanding, and was wondering if I could receive some specific advice or help. Realistically how should one go about decrypting this hash? Thank you.

EDIT: the salt is 62481a9d9614a5d9798b74eaf6202c1b

account_ - April 3, 2024, 6:19 am

Running it now, whats your offer if I crack it?

ansjdnfiqnuaskdnfa45 - April 3, 2024, 6:31 am

(Apr 3, 2024 06:19 AM)account_ Wrote: [\[CITE\]](#) Running it now, whats your offer if I crack it?

I'm not sure on what is a fair price since I'm new, and I don't stand to gain any financial benefit from gaining the password.

Would 5 USD btc be a fair price? Happy to work. Thank you for the fast reply too.

account_ - April 3, 2024, 6:39 am

(Apr 3, 2024 06:31 AM)ansjdnfiqnuaskdnfa45 Wrote: [\[CITE\]](#) I'm not sure on what is a fair price since I'm new, and I don't stand to gain any financial benefit from gaining the password.

Would 5 USD btc be a fair price? Happy to work. Thank you for the fast reply too.

Ok, will let you know if I hit the bcrypt hash.

ansjdnfiqnuaskdnfa45 - April 3, 2024, 6:51 am

(Apr 3, 2024 06:39 AM)account_ Wrote: [\[CITE\]](#) Ok, will let you know if I hit the bcrypt hash.

Additionally, I have an eatstreet.com bcrypt hash. I am even less sure about how these work, but if you would like some additional info to work from (i.e. full name, emails associated) I can help with that, preferably privately.

\$2a\$12\$zZST.yUY.cecobzee3kx5OQP9dIU8ffDOdDBCh.R2zRykFCAUmpje

salt apparently is: 16

If you get both, then I'm more than happy to reimburse 5 USD for each.

EDIT: this eatstreet.com hash is concerning the same individual as the edmodo hash, but they have used a different email.

bitk1ng - April 3, 2024, 10:28 am

(Apr 3, 2024 06:02 AM)ansjdnfiquaskdnfa45 Wrote: [\[CITE\]](#) I was wondering whether someone could help me decrypt this bcrypt hash from edmodo.

original:

\$826y4\$31226\$dObW2ZfmeO3TbFeh4Y0WcQc22O4T1c827Y7zfU6yaM2ucg9z0bbO77RBZsC9.v1GSJXZSwrby9dlvmK

de-obfuscated:

\$2y\$12\$OWZmOTFhYWQ2OTc2YzUyMugzbO77RBZsC9.v1GSJXZSwrby9dlvmK

I've tried to use resources on this specific topic, although I've hit a wall with my understanding, and was wondering if I could receive some specific advice or help. Realistically how should one go about decrypting this hash? Thank you.

EDIT: the salt is 62481a9d9614a5d9798b74eaf6202c1b

(Apr 3, 2024 06:51 AM)ansjdnfiquaskdnfa45 Wrote: [\[CITE\]](#) Additionally, I have an eatstreet.com bcrypt hash. I am even less sure about how these work, but if you would like some additional info to work from (i.e. full name, emails associated) I can help with that, preferably privately.

\$2a\$12\$zZST.yUY.cecobzee3kx5OQP9dIU8ffDOdDBCh.R2zRykFCAUmpje

salt apparently is: 16

If you get both, then I'm more than happy to reimburse 5 USD for each.

EDIT: this eatstreet.com hash is concerning the same individual as the edmodo hash, but they have used a different email.

To make a few points clear:

This is your hash:

\$2y\$12\$OWZmOTFhYWQ2OTc2YzUyMugzbO77RBZsC9.v1GSJXZSwrby9dlvmK

1. \$2y\$ indicates the bcrypt algorithm version.
2. \$12\$ is the cost factor, and 12 within bcrypt is very good.
3. "OWZmOTFhYWQ2OTc2YzUyM" - this is the salt
4. "ugzbO77RBZsC9.v1GSJXZSwrby9dlvmK" - this is the hashed password.

Cracking this without any clues as to who owns this password is going to take minimum several weeks even with good hardware. Don't waste your time and energy on this unless you're willing to pay several thousands. The fact you didn't even know that the salt was included should tell you that what you are doing (or trying to do) is far beyond your capabilities.

ansjdnfiquaskdnfa45 - April 3, 2024, 3:34 pm

(Apr 3, 2024 10:28 AM)bitk1ng Wrote: [\[CITE\]](#) To make a few points clear:

This is your hash:

\$2y\$12\$OWZmOTFhYWQ2OTc2YzUyMugzbO77RBZsC9.v1GSJXZSwrby9dlvmK

1. \$2y\$ indicates the bcrypt algorithm version.
2. \$12\$ is the cost factor, and 12 within bcrypt is very good.
3. "OWZmOTFhYWQ2OTc2YzUyM" - this is the salt
4. "ugzbO77RBZsC9.v1GSJXZSwrby9dlvmK" - this is the hashed password.

Cracking this without any clues as to who owns this password is going to take minimum several weeks even with good hardware. Don't waste your time and energy on this unless you're willing to pay several thousands. The fact you didn't even know that the salt was included should tell you that what you are doing (or trying to do) is far beyond your capabilities.

Thank you for your thorough explanation. I acknowledge it is far beyond my capabilities which is why I made a post asking if someone could help me familiarize myself. I've seen posts in the past determine the salt the way I did it, a bit like the blind leading the blind. Regardless though I apologise if for flooding the board with another low quality post, I guess I was quite desperate and should've done more due diligence.

account_ - April 4, 2024, 7:39 am

<https://hashes.com/en/tools/verified?accessKey=b59dfb6f94>

Found \$2y\$12\$OWZmOTFhYWQ2OTc2YzUyMugzbO77RBZsC9.v1GSJXZSwrby9dlvmK

DramaKing - April 4, 2024, 8:10 am

Must have been a pretty weak password as I believe bcrypt is GPU-resistant or just very complex. I wouldn't consider cost 12 to be good, seems pretty common.

account_ - April 4, 2024, 8:31 am

(Apr 4, 2024 08:10 AM)DramaKing Wrote: [\[CITE\]](#) Must have been a pretty weak password as I believe bcrypt is GPU-resistant or just very complex. I wouldn't consider cost 12 to be good, seems pretty common.

The length of the pw is MD5 length.

Sent contract for the hash OP, just letting you know.

ansjdnfiquaskdnfa45 - April 5, 2024, 1:13 am

(Apr 4, 2024 08:31 AM)account_ Wrote: [\[CITE\]](#) The length of the pw is MD5 length.

Sent contract for the hash OP, just letting you know.

Thank you sir, I will accept the contract and send through the bitcoin as soon as I get the currency. My bank has recently slowed down transactions to exchanges so it may take me 24 hours to get back to you which is when I'll accept the contract and send through the amount straight after (if that is general etiquette).

Also if you want to keep running that other hash, the offer is still on the table for the other 5 USD.

account_ - April 5, 2024, 1:49 am

(Apr 5, 2024 01:13 AM)ansjdnfiquaskdnfa45 Wrote: [\[CITE\]](#) Thank you sir, I will accept the contract and send through the bitcoin as soon as I get the currency. My bank has recently slowed down transactions to exchanges so it may take me 24 hours to get back to you which is when I'll accept the contract and send through the amount straight after (if that is general etiquette).

Also if you want to keep running that other hash, the offer is still on the table for the other 5 USD.

Thanks for letting me know.

bitk1ng - April 13, 2024, 7:16 am

(Apr 4, 2024 07:39 AM)account_ Wrote: [\[CITE\]](#) Found
\$2y\$12\$OWZmOTFhYWQ2OTc2YzUyMugzbO77RBZsC9.v1GSJXZSwrby9dlvmK
Very good.

How many hashes did you check?

account_ - April 13, 2024, 7:27 am

(Apr 13, 2024 07:16 AM)bitk1ng Wrote: [\[CITE\]](#) Very good.

How many hashes did you check?

Cracked the one you quoted.

bitk1ng - April 13, 2024, 7:29 am

(Apr 13, 2024 07:27 AM)account_ Wrote: [\[CITE\]](#) Cracked the one you quoted.
Yes i know.

Seems my belief of how hard bcrypt is was incorrect or outdated. I Think you misunderstood the question. How many attempts did you need to find it? I know bcrypt is pretty strong against bruteforce so thats why i am asking.

account_ - April 13, 2024, 7:39 am

(Apr 13, 2024 07:29 AM)bitk1ng Wrote: [\[CITE\]](#) Yes i know.

Seems my belief of how hard bcrypt is was incorrect or outdated. I Think you misunderstood the question. How many attempts did you need to find it? I know bcrypt is pretty strong against bruteforce so thats why i am asking.
It was the length of a md5 hash.

shoot12384812 - August 16, 2024, 9:21 pm

(Apr 13, 2024 07:39 AM)account_ Wrote: [\[CITE\]](#) It was the length of a md5 hash.
can you please try this edmodo hash? i will pay 3usd litecoin

\$826y4\$31226\$dNbD2RfmeO3Tble24Z0Gclcw2N4j1M847N7jfd6laY2OcJ9h0RbGIIa4AOdJJIKp0K
gyfAR6WAsNBzS:47b8443227ca69c52b54ac294f6f9d05

dobroy_000 - August 17, 2024, 5:52 am

(Aug 16, 2024 09:21 PM)shoot12384812 Wrote: [\[CITE\]](#) can you please try this edmodo hash? i will pay 3usd litecoin

\$826y4\$31226\$dNbD2RfmeO3Tble24Z0Gclcw2N4j1M847N7jfd6laY2OcJ9h0RbGIIa4AOdJJIKp0K
gyfAR6WAsNBzS:47b8443227ca69c52b54ac294f6f9d05

my brothers and sisters in law, stop asking others to crack passwords, its 2024, you can just go online or download tools like john to crack them

account_ - August 17, 2024, 8:12 am

(Aug 16, 2024 09:21 PM)shoot12384812 Wrote: [\[CITE\]](#) can you please try this edmodo hash? i will pay 3usd litecoin

\$826y4\$31226\$dNbD2RfmeO3Tble24Z0Gclcw2N4j1M847N7jfd6laY2OcJ9h0RbGIIa4AOdJJIKp0K
gyfAR6WAsNBzS:47b8443227ca69c52b54ac294f6f9d05

Running it now, will let you know if I hit it.

DramaKing - August 17, 2024, 8:57 am

I gave it a try, but hashcat was giving me 200+ days for rockyou2021. \$3 wouldn't even begin to cover the cost. Only thing that I would try against bcrypt is a well-targeted wordlist.

account_ - August 18, 2024, 12:28 pm

(Aug 16, 2024 09:21 PM)shoot12384812 Wrote: [\[CITE\]](#) can you please try this edmodo hash? i will pay 3usd litecoin

\$826y4\$31226\$dNbD2RfmeO3Tble24Z0Gclcw2N4j1M847N7jfd6laY2OcJ9h0RbGIIa4AOdJJIKp0K
gyfAR6WAsNBzS:47b8443227ca69c52b54ac294f6f9d05

No luck with the hash.

SovietBastard - August 19, 2024, 5:37 am

(Aug 17, 2024 08:57 AM)DramaKing Wrote: [\[CITE\]](#) I gave it a try, but hashcat was giving me 200+ days for rockyou2021. \$3 wouldn't even begin to cover the cost. Only thing that I would try against bcrypt is a well-targeted wordlist.

this sounds like a lot of days

evilkitty156 - August 27, 2024, 7:16 am

Will someone help me understand how you are supposed to use hashcat to crack these, like which specific parameters? I totally get that you have an obfuscated bcrypt hash which is normally 3200, but the addition of the salt makes it so that it doesn't recognize the hash for processing. Is there an additional crack that needs performed against the salt??

EDIT:

It looks like removing the 2nd character for 32 characters from obfuscation and then running -m 25600 (bcrypt md5) can crack it without the need for the salt? Is the salt useless?

sbr5136014 - March 24, 2025, 8:46 pm

Can you crack me the following hash

\$5\$ITbH0ajjskN0/wAz\$ciO18PktNP9x4qkPhPXsfw0wlegJa3EkWfpm2rXY885