Subject: how can i turn my serial hash back into a serial?
Posted by Distrbd21 on Wed, 02 Mar 2011 09:12:02 GMT
View Forum Message <> Reply to Message

my friend found my old serial hash on a server and i was wondering if i could turn the hash into my serial again.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by reborn on Wed, 02 Mar 2011 09:36:44 GMT
View Forum Message <> Reply to Message

Not likely very easy, some would even say it's impossible.
Besides, I don't think detailing how to do it would be a great idea. People already have huge databases of serials, all it would take is for someone to reverse them all and serial banning for XWIS would be rendered useless.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by danpaul88 on Wed, 02 Mar 2011 13:32:39 GMT
View Forum Message <> Reply to Message

The whole point of a hash is that you CANNOT convert it back into the original string. Each hash output has infinite possible inputs which could have created it.

The only way to turn a hash back into the source string is using rainbow tables of known values, but since a serial number is not something like 'hi this is your serial' it is, for all intents and purposes, impossible.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by halo2pac on Sun, 06 Mar 2011 05:45:03 GMT
View Forum Message <> Reply to Message

danpaul88 wrote on Wed, 02 March 2011 08:32for all intents and purposes, impossible.

Even brute forcing it would take a few years, and you don't know its straight numbers, or double md5'd/ which would take a super computer 4 years/.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by Gen_Blacky on Mon, 07 Mar 2011 04:30:13 GMT
View Forum Message <> Reply to Message

halo2pac wrote on Sat, 05 March 2011 22:45danpaul88 wrote on Wed, 02 March 2011 08:32for

all intents and purposes, impossible.

Even brute forcing it would take a few years, and you don't know its straight numbers, or double md5'd/ which would take a super computer 4 years/.

How do you brute force a serial hash into a serial lols you would never know when the next character is correct.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by saberhawk on Mon, 07 Mar 2011 04:56:55 GMT
View Forum Message <> Reply to Message

Gen_Blacky wrote on Sun, 06 March 2011 23:30halo2pac wrote on Sat, 05 March 2011 22:45danpaul88 wrote on Wed, 02 March 2011 08:32for all intents and purposes, impossible.

Even brute forcing it would take a few years, and you don't know its straight numbers, or double md5'd/ which would take a super computer 4 years/.

How do you brute force a serial hash into a serial lols you would never know when the next character is correct.

<really long number representing the serial so far> + 1, etc etc until it matches the hash?

Subject: Re: how can i turn my serial hash back into a serial?
Posted by danpaul88 on Mon, 07 Mar 2011 18:15:36 GMT
View Forum Message <> Reply to Message

Also, why is this in the MOD forum? It's clearly nothing to do with creating mods for Renegade.

Based on the Renegade serial length and using the numbers 0 - 9 for each of the 20 digits, there are 10^20 possible combinations.

Or, to put it another way

10000000000000000000

Good luck brute forcing that.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by halo2pac on Wed, 09 Mar 2011 01:36:39 GMT

View Forum Message <> Reply to Message

Actually you can bruteforce a 12 digit md5 hash in a few dats time on a i7. and if you have applications that run cross network aka slave server bruteforcers you can crack that with a hundred computers in a couple days.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by danpaul88 on Wed, 09 Mar 2011 14:14:27 GMT
View Forum Message <> Reply to Message

halo2pac wrote on Wed, 09 March 2011 01:36Actually you can bruteforce a 12 digit md5 hash in a few dats time on a i7. and if you have applications that run cross network aka slave server bruteforcers you can crack that with a hundred computers in a couple days.

Except a renegade serial is 20 digits and who said it was an MD5 hash? For all we know it could be SHA-1, or double MD5 or even a combination of different hashes ran one after the other.

Also, in order to brute force something you need a method to programatically determine if the input which produced the required hash was ACTUALLY the original input. Since multiple inputs produced the same hash you can easily wind up 'brute forcing' completely the wrong value unless you have some way to validate the result.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by Sladewill on Wed, 09 Mar 2011 22:17:01 GMT
View Forum Message <> Reply to Message

Who says its even a well known hash, they could of easily written there own hash which is pretty simple to do.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by Olaf van der Spek on Sat, 19 Mar 2011 23:54:29 GMT
View Forum Message <> Reply to Message

danpaul88 wrote on Wed, 09 March 2011 15:14
Except a renegade serial is 20 digits and who said it was an MD5 hash? For all we know it could be SHA-1, or double MD5 or even a combination of different hashes ran one after the other.

Also, in order to brute force something you need a method to programatically determine if the input which produced the required hash was ACTUALLY the original input. Since multiple inputs produced the same hash you can easily wind up 'brute forcing' completely the wrong value unless you have some way to validate the result.
It's 22 digits of which 4 can be calculated. That's 10^18 or about 2^60 combinations.

Finding out the used hash algorithm itself isn't the hard part.

60 bits might be a bit too much for existing rainbow based attacks.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by Jerad2142 on Thu, 11 Aug 2011 18:32:02 GMT
View Forum Message <> Reply to Message

Guess you have to screw around with the installer until you can figure out where the code is that generates the hash and then run it backward.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by danpaul88 on Fri, 12 Aug 2011 08:50:22 GMT
View Forum Message <> Reply to Message

Jerad Gray wrote on Thu, 11 August 2011 19:32Guess you have to screw around with the installer until you can figure out where the code is that generates the hash and then run it backward.

No such thing as running a hashing function 'backwards', it's a one way process. Since each output can be generated from an infinite number of inputs it's impossible for any function to simply take a hash value, lets say 'hbq3tgh423uhj35', and turn it back into the exact input that generated that hash, which could be (for example) '1234', but could also be (as another example) 'lol games' or 'Perl is awesome'.

Brute forcing or rainbow tables are the only ways (that I know of) to turn a hash back into the original value and even then it's impossible to be 100% accurate as it's basically guess work and relies upon recognizing common words in the input used to generate the hash or the input being in a known, fixed format which even then there might not be a unique input matching that format to produce each hash.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by halo2pac on Wed, 17 Aug 2011 03:25:51 GMT
View Forum Message <> Reply to Message

The game technically takes your numeric serial and hashes it some how. Either by md5 or some wol-ish hack of the md5 function. either way...if theres a way in theres a way out.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by Gen_Blacky on Wed, 17 Aug 2011 03:53:59 GMT
View Forum Message <> Reply to Message

You need to find the way in before you can find your way out

Subject: Re: how can i turn my serial hash back into a serial?
Posted by danpaul88 on Wed, 17 Aug 2011 08:07:18 GMT
View Forum Message <> Reply to Message

halo2pac wrote on Wed, 17 August 2011 04:25The game technically takes your numeric serial and hashes it some how. Either by md5 or some wol-ish hack of the md5 function. either way...if theres a way in theres a way out.

HASH abc = 1234
HASH def = 1234
HASH hij = 1234

So, if I give you the hash 1234, tell me what input produced it with 100% accuracy based on the table above. Here's a clue: it's impossible. That's the whole POINT of a hashing function.

Encryption is two way (can be decrypted), hashing is one way and a hash cannot be unhashed programatically without additional information about the original input to the hash function and even then is simply a best guess.

Subject: Re: how can i turn my serial hash back into a serial?
Posted by reborn on Wed, 17 Aug 2011 09:11:49 GMT
View Forum Message <> Reply to Message

Demonstrating how banning by serial hash could end up banning more than the intended client.

There's a really interesting topic that 0x90 made about APGAR decryption. It has no practical application implications, but is still quite facinating.