

Forum:[Hack Forums](#)

Thread: [CHALLENGE 65 hex chars UNKNOWN HASH - CAN YOU CRACK IT](#)

rob2k9 - December 30, 2014, 12:30 pm

ok so i hacked into a very popular website in fact one of the biggest if not the biggest in its feild

and the hash i got for the admins account is very unusual i have pasted it bellow

30b9aa9dadd02f3dd29bf3ba3a8714e9409c9109d0b78575af80158f157f62b0e

as you can see its just not normal lol

anyway let see how good the people are around here and see if anyone can crack this or get find out what kind it is

DavidSerbia - December 30, 2014, 12:35 pm

"OK so i hacked into this very very popular website"

- just lol

rob2k9 - December 30, 2014, 12:41 pm

(Dec 30, 2014 01:35 PM)DavidSerbia Wrote: [\[CITE\]](#) "OK so i hacked into this very very popular website"

- just lol

dont post if its not help full and google usernames before you say lol dude!

chick3nman - December 30, 2014, 12:49 pm

(Dec 30, 2014 01:30 PM)rob2k9 Wrote: [\[CITE\]](#) ok so i hacked into a very popular website in fact one of the biggest if not the biggest in its feild

and the hash i got for the admins account is very unusual i have pasted it bellow

30b9aa9dadd02f3dd29bf3ba3a8714e9409c9109d0b78575af80158f157f62b0e

as you can see its just not normal lol

anyway let see how good the people are around here and see if anyone can crack this or get find out what kind it is

This is a 260 bit hash. There is no hashing function that i am aware of that uses this bit length. This is either a custom system or you have produced an incorrect hash. This could be truncated or have extra characters, or you have have accidentally mixed the salt onto the hash without knowing.

rob2k9 - December 30, 2014, 1:03 pm

(Dec 30, 2014 01:49 PM)chick3nman Wrote: [\[CITE\]](#) This is a 260 bit hash. There is no hashing function that i am aware of that uses this bit length. This is either a custom system or you have produced an incorrect hash. This could be truncated or have extra characters, or you have have accidentally mixed the salt onto the hash without knowing.

the hash was taken directly from a msql db from under the table users and coulmm password the

hash is a perfect copy from the db and this site it is from is one of a kind there is no other site out there that uses their script so I am guessing it is custom coded so would the hashing system be maybe ?

I was thinking it may be maybe a weirdly splitted sha512 hash or some smaller hash like sha256/sha1/md5 with appended/prepended salt

but got no clue where to start from in terms of cracking it this has to be the best hashing system I have seen used on a public site considering places like Sony and stuff still use normal md5 and sha

DavidSerbia - December 30, 2014, 1:07 pm

He hacked into a "very popular website" and he does not know that this hash is 264 bit ... A TRUE HACKER ROFL

chick3nman - December 30, 2014, 1:38 pm

(Dec 30, 2014 02:07 PM)DavidSerbia Wrote: [\[CITE\]](#) He hacked into a "very popular website" and he does not know that this hash is 264 bit ... A TRUE HACKER ROFL

But....It's not 264 bit.... It's 260....

(Dec 30, 2014 02:03 PM)rob2k9 Wrote: [\[CITE\]](#) the hash was taken directly from a mysql db from under the table users and couldn't password the hash is a perfect copy from the db and this site it is from is one of a kind there is no other site out there that uses their script so I am guessing it is custom coded so would the hashing system be maybe ?

I was thinking it may be maybe a weirdly splitted sha512 hash or some smaller hash like sha256/sha1/md5 with appended/prepended salt

but got no clue where to start from in terms of cracking it this has to be the best hashing system I have seen used on a public site considering places like Sony and stuff still use normal md5 and sha
Can you create an account on the site with a known password and then get the hash for it? Or maybe dump the rest of the database so we can see the other hashes? I need more example material to determine how this was hashed.

rob2k9 - December 30, 2014, 1:46 pm

the db has over 316 thousand users I can try create an account and dump it and see what we get no problem and as for other accounts here is a few other hashes below

```
036fef7a35f9f3fa690641ba66b6f7b7595fdc0d81de411cc50ef77a8fea96246
4e9a4779356280e64a39b314153c719873fda49742ce85ae6119db4fadcf6c637
4e4a76cb9f520d5892020a1375ddac3258a4f8fda278c44d9c1fefb5dcf8601b4
e2b56df164c93b1e94ed59db6dd3dbf72adfa1a6db2870bd1133c327390fb9137
0c5511e2bc024809213d743d16f9c1585be613cb0a8673d7f03eafcc3ed085639
```

chick3nman - December 30, 2014, 1:51 pm

(Dec 30, 2014 02:46 PM)rob2k9 Wrote: [\[CITE\]](#) the db has over 316 thousand users I can try create an account and dump it and see what we get no problem and as for other accounts here is a few other hashes below

```
036fef7a35f9f3fa690641ba66b6f7b7595fdc0d81de411cc50ef77a8fea96246
4e9a4779356280e64a39b314153c719873fda49742ce85ae6119db4fadcf6c637
4e4a76cb9f520d5892020a1375ddac3258a4f8fda278c44d9c1fefb5dcf8601b4
e2b56df164c93b1e94ed59db6dd3dbf72adfa1a6db2870bd1133c327390fb9137
0c5511e2bc024809213d743d16f9c1585be613cb0a8673d7f03eafcc3ed085639
```

So, since these are so close to 256 bits in length, I'm assuming something along the lines of appended/prepended salt like you. Although it is still possible these are 260 bit hashes of a custom/unknown algorithm.

rob2k9 - December 30, 2014, 1:56 pm

(Dec 30, 2014 02:51 PM)chick3nman Wrote: [\[CITE\]](#) So, since these are so close to 256 bits in length, I'm assuming something along the lines of appended/prepended salt like you. Although it is still possible these are 260 bit hashes of a custom/unknown algorithm.

ok well i just created an account on the site and am redumping the db to my ext hardrive and will look threw for the user account wen done and postback wen i have it

crazyycast13 - December 30, 2014, 2:11 pm

First of all, congrats on the hack.

Second of all, could you pm me the encryption algorithm when you login to the site? If not, set up a custom packet capture with wireshark to figure out what is sent from your computer. If it is changed in any way, we can have a start by figuring out how it's initially encrypted.

rob2k9 - December 30, 2014, 3:08 pm

(Dec 30, 2014 03:11 PM)crazyycast13 Wrote: [\[CITE\]](#) First of all, congrats on the hack.

Second of all, could you pm me the encryption algorithm when you login to the site? If not, set up a custom packet capture with wireshark to figure out what is sent from your computer. If it is changed in any way, we can have a start by figuring out how it's initially encrypted.

i will download wiresharck and set that up now as for the algorithem i cant see source code of files on server as it seems locked down tight was hard enough to get db access my connection keeps getting booted

crazyycast13 - December 30, 2014, 3:31 pm

(Dec 30, 2014 04:08 PM)rob2k9 Wrote: [\[CITE\]](#) i will download wiresharck and set that up now as for the algorithem i cant see source code of files on server as it seems locked down tight was hard enough to get db access my connection keeps getting booted

Your home IP or are you getting dcd from the network?

Pretty sure there's a way to see the login script on your side since the password should be encrypted on your side. It's more of a question of whether or not more stuff is done to the has server-side.

If we know what gets sent there and the database, we might be able to crack it.

rob2k9 - December 30, 2014, 3:45 pm

well right now i am at home and i use a us private vpn wen connecting out

crazyycast13 - December 31, 2014, 7:59 pm

(Dec 30, 2014 04:45 PM)rob2k9 Wrote: [\[CITE\]](#) well right now i am at home and i use a us private vpn wen connecting out

Any updates? Managed to figure out anything interesting?

rob2k9 - January 3, 2015, 12:43 pm

(Dec 31, 2014 08:59 PM)crazyycast13 Wrote: [\[CITE\]](#) Any updates? Managed to figure out anything interesting?

i created an account the password is tinytot and i dumped the account and this is the hashed password for that account

5d5d7868bfa264f04d8710d8b41279bf68ba101e16998826279ab263a06bdfb3c

VladimirDracula - January 3, 2015, 1:27 pm

(Dec 30, 2014 04:31 PM)crazyycast13 Wrote: [CITE](#) Your home IP or are you getting dcd from the network?

Pretty sure there's a way to see the login script on your side since the password should be encrypted on your side. It's more of a question of whether or not more stuff is done to the has server-side.

If we know what gets sent there and the database, we might be able to crack it.
wat? the password isnt getting encrypted its getting hashed. also, the hashing takes place server side not client side.

Forezza - January 3, 2015, 1:37 pm

Personally, I would guess that it is just a truncated SHA512 / Whirlpool hash that is salted as not many people bother to add the salt onto the end of the hash as they have to split it later. If they are manipulating the length of the hash, then they may be manipulating the password in some other way prior e.g. Rounds of MD5, reversing the password, etc. There are pretty much endless possibilities.