

Forum:[Hack Forums](#)

Thread: [\[Info\]Types of Hashes\[Share\]](#)

Tainted Star - July 29, 2011, 10:59 am

I've seen many threads here on HF(In this category only) asking for kind of hash.
So , here it is.

Hope it's helpful to you all.

DES(Unix)

Example: IvS7aeT4NzQPM

Used in Linux and other similar OS.

Length: 13 characters.

Description: The first two characters are the salt (random characters; in our example the salt is the string "Iv"), then there follows the actual hash.

Notes: [1] [2]

Domain Cached Credentials

Example: Admin:b474d48cdfc4974d86ef4d24904cdd91

Used for caching passwords of Windows domain.

Length: 16 bytes.

Algorithm: MD4(MD4(Unicode(\$pass)).Unicode(strtolower(\$username)))

Note: [1]

MD5(Unix)

Example: \$1\$12345678\$XM4P3PrKBgKNnTaqG9P0T/

Used in Linux and other similar OS.

Length: 34 characters.

Description: The hash begins with the \$1\$ signature, then there goes the salt (up to 8 random characters; in our example the salt is the string "12345678"), then there goes one more \$ character, followed by the actual hash.

Algorithm: Actually that is a loop calling the MD5 algorithm 2000 times.

Notes: [1] [2]

MD5(APR)

Example: \$apr1\$12345678\$auQsX8Mvzt.tdBi4y6Xgj.

Used in Linux and other similar OS.

Length: 37 characters.

Description: The hash begins with the \$apr1\$ signature, then there goes the salt (up to 8 random characters; in our example the salt is the string "12345678"), then there goes one more \$ character, followed by the actual hash.

Algorithm: Actually that is a loop calling the MD5 algorithm 2000 times.

Notes: [1] [2]

MD5/phpBB3)

Example: \$H\$9123456785DAERgALpsri.D9z3ht120

Used in phpBB 3.x.x.

Length: 34 characters.

Description: The hash begins with the \$H\$ signature, then there goes one character (most often the

number '9'), then there goes the salt (8 random characters; in our example the salt is the string "12345678"), followed by the actual hash.

Algorithm: Actually that is a loop calling the MD5 algorithm 2048 times.

Notes: [1] [2]

MD5 Wordpress

Example: \$P\$B123456780BhGFYSIUqGyE6ErKErL01

Used in Wordpress.

Length: 34 characters.

Description: The hash begins with the \$P\$ signature, then there goes one character (most often the number 'B'), then there goes the salt (8 random characters; in our example the salt is the string "12345678"), followed by the actual hash.

Algorithm: Actually that is a loop calling the MD5 algorithm 8192 times.

Notes: [1] [2]

MySQL

Example: 606717496665bcba

Used in the old versions of MySQL.

Length: 8 bytes.

Description: The hash consists of two DWORDs, each not exceeding the value of 0x7fffffff.

MySQL5

Example: *E6CC90B878B948C35E92B003C792C46C58C4AF40

Used in the new versions of MySQL.

Length: 20 bytes.

Algorithm: SHA-1(SHA-1(\$pass))

Note: The hashes are to be loaded to the program without the asterisk that stands in the beginning of each hash.

RAdmin v2.x

Example: 5e32cceaafed5cc80866737dfb212d7f

Used in the application Remote Administrator v2.x.

Length: 16 bytes.

Algorithm: The password is padded with zeros to the length of 100 bytes, then that entire string is hashed with the MD5 algorithm.

MD5

Example: c4ca4238a0b923820dcc509a6f75849b

Used in phpBB v2.x, Joomla version below 1.0.13 and many other forums and CMS.

Length: 16 bytes.

Algorithm: Same as the md5() function in PHP.

md5(\$pass.\$salt)

Example: 6f04f0d75f6870858bae14ac0b6d9f73:1234

Used in WB News, Joomla version 1.0.13 and higher.

Length: 16 bytes.

Note: [1]

md5(\$salt.\$pass)

Example: f190ce9ac8445d249747cab7be43f7d5:12

Used in osCommerce, AEF, Gallery and other CMS.

Length: 16 bytes.

Note: [1]

md5(md5(\$pass))

Example: 28c8edde3d61a0411511d3b1866f0636

Used in e107, DLE, AVE, Diferior, Koobi and other CMS.

Length: 16 bytes.

md5(md5(\$pass).\$salt)

Example: 6011527690eddca23580955c216b1fd2:wQ6

Used in vBulletin, IceBB.

Length: 16 bytes.

Notes: [1] [3] [4]

md5(md5(\$salt).md5(\$pass))

Example: 81f87275dd805aa018df8befe09fe9f8:wH6_S

Used in IPB.

Length: 16 bytes.

Notes: [1] [3]

md5(md5(\$salt).\$pass)

Example: 816a14db44578f516cbaef25bd8d8296:1234

Used in MyBB.

Length: 16 bytes.

Note: [1]

md5(\$salt.\$pass.\$salt)

Example: a3bc9e11fddf4fef4deea11e33668eab:1234

Used in TBDev.

Length: 16 bytes.

Note: [1]

md5(\$salt.md5(\$salt.\$pass))

Example: 1d715e52285e5a6b546e442792652c8a:1234

Used in DLP.

Length: 16 bytes.

Note: [1]

SHA-1

Example: 356a192b7913b04c54574d18c28d46e6395428ab

Used in many forums and CMS.

Length: 20 bytes.

Algorithm: Same as the sha1() function in PHP.

sha1(strtolower(\$username).\$pass)

Example: Admin:6c7ca345f63f835cb353ff15bd6c5e052ec08e7a

Used in SMF.

Length: 20 bytes.

Note: [1]

sha1(\$salt.sha1(\$salt.sha1(\$pass)))

Example: cd37bfbf68d198d11d39a67158c0c9cddf34573b:1234

Used in Woltlab BB.

Length: 20 bytes.

Note: [1]

SHA-256(Unix)

Example: \$5\$12345678\$jBWLgeYZbSvREnuBr5s3gp13vqiKSNK1rkTk9zYE1v0

Used in Linux and other similar OS.

Length: 55 characters.

Description: The hash begins with the \$5\$ signature, then there goes the salt (up to 8 random characters; in our example the salt is the string "12345678"), then there goes one more \$ character, followed by the actual hash.

Algorithm: Actually that is a loop calling the SHA-256 algorithm 5000 times.

Notes: [1] [2]

SHA-512(Unix)

Example:

\$6\$12345678\$U6Yv5E1IWn6mEESzKen42o6rbEmFNLIq6Ik9X3reMXY3doKEuxrcDohKUx0Oxf44aeTixGEjssvtT1aKyZHjs

Used in Linux and other similar OS.

Length: 98 characters.

Description: The hash begins with the \$6\$ signature, then there goes the salt (up to 8 random characters; in our example the salt is the string "12345678"), then there goes one more \$ character, followed by the actual hash.

Algorithm: Actually that is a loop calling the SHA-512 algorithm 5000 times.

Notes: [1] [2]

Notes:

[1] Since the hashing requires not only a password but also a salt (or a user name), which is unique for each user, the attack speed for such hashes will decline proportionally to their count (for example, attacking 100 hashes will go 100 times slower than attacking one hash).

[2] The hash is to be loaded to the program in full, to the "Hash" column - the program will automatically extract the salt and other required data from it.

[3] The ':' character can be used as salt; however, since it is used by default for separating hash and salt in PasswordsPro, it is recommended that you use a different character for separating fields; e.g., space.

[4] Salt can contain special characters - single or double quotes, as well as backslash, which are preceded (after obtaining dumps from MySQL databases) by an additional backslash, which is to be removed manually. For example, the salt to be loaded to the program would be a'4 instead of a\4, as well as the salts a"4 instead of a\"4 and a\4 instead of a\\4.

Also , Description of algorithms of some hashing modules in PasswordsPro:

SHA-1(Django) = sha1(\$salt.\$pass)

Example: sha1\$12345678\$90fbbcf2b72b5973ae42cd3a19ab4ae8a1bd210b

12345678 is salt (in the hexadecimal format)

90fbbcf2b72b5973ae42cd3a19ab4ae8a1bd210b is SHA-1 hash.

SHA-256(Django) = SHA-256(\$salt.\$pass)

Example:

sha256\$12345678\$154c4c511cbb166a317c247a839e46cac6d9208af5b015e1867a84cd9a56007b

12345678 is salt (in the hexadecimal format)

154c4c511cbb166a317c247a839e46cac6d9208af5b015e1867a84cd9a56007b is SHA-256 hash.

SHA-384(Django) = SHA-384(\$salt.\$pass)

Example:

sha384\$12345678\$c0be393a500c7d42b1bd03a1a0a76302f7f472fc132f11ea6373659d0bd8675d04e12d8016d83001c327f0ab70843dd5

12345678 is salt (in the hexadecimal format)

c0be393a500c7d42b1bd03a1a0a76302f7f472fc132f11ea6373659d0bd8675d04e12d8016d83001c327f0ab70843dd5 is SHA-384 hash.

SHA-1(ManGOS) = sha1(strtoupper(\$username).':'.\$pass)

SHA-1(ManGOS2) = sha1(\$username.':'.\$pass)

MD5(Custom) = '=='.md5(md5(md5(\$pass).md5(\$pass).md5(\$pass).md5(\$pass)))

NOTE:I DID NOT WRITE IT , JUST SHARING IT.I DON'T TAKE CREDITS FOR THIS.

HaxOr? - July 29, 2011, 11:01 am

LOOOOL...I posted same thread while ago

<https://hackforums.net/showthread.php?tid=1393830>

Stage6 - July 29, 2011, 11:01 am

its actually a nice share brother <3

Thanks

eriko00 - July 29, 2011, 11:02 am

Thanks man, nice work. +rep

Captain Crunch - July 29, 2011, 11:03 am

You basically copied Haxors thread....

Tainted Star - July 29, 2011, 11:04 am

(Jul 29, 2011 11:01 AM)? ? x O r ? Wrote: [\[CITE\]](#) LOOOOL...I posted same thread while ago

<https://hackforums.net/showthread.php?tid=1393830>

Lol , Sorry.

Didn't know.

It's my first share though.

@Stage6 , glad you liked it :) .

????? - July 29, 2011, 11:07 am

wow i like this sharing !! Spoiler [\(Click to View\)](#) thank you so much

Virus24 - July 29, 2011, 11:07 am

Thanks for the share :) Would be good for some including me (Sorta) :3

Tainted Star - July 29, 2011, 11:14 am

Quote:You basically copied Haxors thread....

Btw , i dint took information from HF.

I had no idea if ever it was posted earlier (i checked it via HF Search Page , say , around starting of this month.

eriko00,Sam4 and Virus24,

Thanks for the vouches.

razor1911 - July 29, 2011, 11:17 am

Wtf, you both leeched it form same place LOL

Tainted Star - July 29, 2011, 11:21 am

Well , as i said , i am not taking any credits for this.

and yes , it's from the same place.