به نام خداوند بخشایشگر

آشنایی با هش و انواع آن

آشیانه دیجیتال سکیوریتی تیم

نویسنده : محمد جاویدان

تقدیم به تمامی دوستانم در سایت آشیانه و کتابناک

هش چیست؟

منظور از هش رمز گذاری روی متن هست و در اصل برای ساخته شده که وقتی که شما مدیر یک فروم هستید پسورد های کابران را بطور مستقیم نتونید ببینید و از آنها سو استفاده کنید اما برای اینکه سرور بتونه بفهمه که پسورد ها درست هستن یا نه از یه الگوریتم استفاده می کنه که برگشت پذیر نیست (هش).

برای اینکه منظورم را بهتر بفهمید یک مثال دیگه می زنم:

مثلا کاربر هنگام ثبت نام در سایت این اطلاعات را وارد کرده:

نام کاربری:M.hack

پسورد :123456

سرور این اطلاعات رو به این صورت ذخیره می کنه :

نام کاربری:M.hack

پسورد :e10adc3949ba59abbe56e057f20f883e

الان دیگه مدیر نمی تونه پسورد واقعی کاربر رو ببینه حالا کاربر برای لاگین کردن این اطلاعا رو وارد می کنه:

نام کاربری:M.hack

پسورد :123456

حالا سرور پسورد کاربر رو به صورت هش در میاره

md5(123456) --> e10adc3949ba59abbe56e057f20f883e

حالا اگه هش پسوردی که کاربر وارد کرده برابر هش پسورد کاربر موقع ثبت نام باشه کاربر وارد سایت می شه

انواع هش :

هش ها انواع مختلفی دارن که از معروف ترین اونا می شه به اشاره کرد به: md1,md2, md3,md4,md5

متداول ترین نوع هش md5 هست چون از سرعت و امنیت بالایی بر خورداره.

بعضی از هش دست نویس هستن و نمی شه الگوریتمشونو پیدا کرد که این امر کرک کردن هش ها رو غیر ممکن می کنه.

در اینجا لیستی از انواع هش ها و خصوصیاتشونو براتون می زارم:

]tedade harf]	[type]	[example [
004	CRC-16:	a8b6
004	CRC-16-CCITT:	aeb5
004	FCS-16: 9	e25
008	ADLER32: 27014	d02
008	CRC-32: 73	bb8c64
008	CRC-32B:	c2412435
008	GHash-32-3:	00002286

008 GHash-32-5: 0001a9a6

009 Elf-32 141305404

013 DES (Unix): 9 ii.t8skwpdOc

016 MySQL: 7 cd2b5942be28759

024 Haval128 (Base64): nkDtiD+2PphdKZtAzaK48g==

024 MD2 (Base64): 2 oU7DT+I2ZswKDpp5t7Wuw==

024 MD4 (Base64): pEgBeq8h2FJfwQroeqZynQ==

024 MD5 (Base64): kAFQmDzST7DWlj99KOF/cg==

024 RipeMD128 (Base64):
wUoSGZxm5LqEY2sPaRRMdw==

024 SNEFRU128 (Base64): VT0GSJKCmaDyKidaAsg7EA==

024 Tiger128 (Base64):
8 ljB6IQUqypSerVB/8W4vw==

028 Haval160 (Base64):
sh6HbE05HiqJdmEUnYNXa1UwoIk=

028 RipeMD160 (Base64):
jrII9+BdmHqbBEqOmMawh/FaC/w=

028 SHA-1 (Base64):
qZk+NkcGgWq6PiVxeFDCbJzQ2J0=

028 Tiger160 (Base64):
8 ljB6IQUqypSerVB/8W4v5Nfe5U=

032 .md5(md5($pass)):
ec0405c5aef93e771cd80e0db180b88b

032 .md5(md5($pass).$salt):
ec0405c5aef93e771cd80e0db180b88b

032 .md5(md5($salt).md5($pass)):
6 b2e416060edbaa9d35302f13d3e1a6a

032 Domain Cached Credentials:
bdaff79a8c1ec80aeda2b713127459bb

032 Haval128 (HMAC):
9 e40ed883fb63e985d299b40cda2b8f2

032 Haval128_3: 9e40ed883fb63e985d299b40cda2b8f2

032 Haval128_4 cbeedc24a720eeebb519ebb74d150e29

032 Haval128_5
7 d12652903d058b5501e6875d9d202d7

032 Haval192 (Base64):
p7FMnvMJIxmw5147IL1X0YC/IHRWKeje

032 LM AAD3B435B51404EEAAD3B435B51404EE

032 MD2 (HMAC):
da853b0d3f88d99b30283a69e6ded6bb

032 MD2: da853b0d3f88d99b30283a69e6ded6bb

032 MD4 (HMAC):
a448017aaf21d8525fc10ae87aa6729d

032 MD4: a448017aaf21d8525fc10ae87aa6729d

032 MD5 (HMAC):
900150983 cd24fb0d6963f7d28e17f72

032 MD5: 900150983 cd24fb0d6963f7d28e17f72

032 NTLM:
e0fba38268d0ec66ef1cb452d5885e53

032 RipeMD128 (HMAC):
c14a12199c66e4ba84636b0f69144c77

032 RipeMD128:
c14a12199c66e4ba84636b0f69144c77

032 SNEFRU128 (HMAC):
553 d0648928299a0f22a275a02c83b10

032 SNEFRU128:
553 d0648928299a0f22a275a02c83b10

032 Tiger128 (HMAC):
f258c1e88414ab2a527ab541ffc5b8bf

032 Tiger128:
f258c1e88414ab2a527ab541ffc5b8bf

032 Tiger192 (Base64):
8 ljB6lQUqypSerVB/8W4v5Nfe5UcEylR

032 Windows-LM
631 FA8FFB4B946F9AAD3B435B51404EE

032 Windows-NTLM
88 D2888508C8106338D69F90E3AD49AA

034 MD5 (Unix):
1P2lE.rGp$SYCpUzBZjWRGKyMe/MbU00

037 MD5 (APR):
$apr1$ZSc84vgF$YiKqBzqnUskAPKeDWlN8/0

040 Haval160 (HMAC):
b21e876c4d391e2a897661149d83576b5530a089

040 Haval160:
b21e876c4d391e2a897661149d83576b5530a089

040 Haval160_3
7 da6a6938ac24f848f202e0ea7a3b5119eec2e6a

040 Haval160_4
6339 f7fe0cbb724619f251f21c2662940bf9a6c6

040 Haval160_5
e79dbb57d907135ba95e892719446164c05497aa

040 Haval224 (Base64):
W8lVIguiNGqUjShI7KN73V7KbsyntZS9MpI/qw==

040 MySQL v5.x:
0 d3ced9bec10a777aec23ccc353a8c08a633045e

040 RipeMD160 (HMAC):
8 eb208f7e05d987a9b044a8e98c6b087f15a0bfc

040 RipeMD160:
8 eb208f7e05d987a9b044a8e98c6b087f15a0bfc

040 SHA-0:
58 f00fa5db65ab4ba2551f77d9b575f41a805ae0

040 SHA-1 (HMAC):
a9993e364706816aba3e25717850c26c9cd0d89d

040 SHA-1:
a9993e364706816aba3e25717850c26c9cd0d89d

040 SHA224 (Base64):
Iwl9IjQF2CKGQqR3vaJVsyqtvOS9oLP342ydpw==

040 Tiger160 (HMAC):
f258c1e88414ab2a527ab541ffc5b8bf935f7b95

040 Tiger160:
f258c1e88414ab2a527ab541ffc5b8bf935f7b95

044 Haval256 (Base64):
hpnx4zhNBbKoSwMmk+K29G34WhOlDZOAjWh0u4+56Gw=

044 RipeMD256 (Base64):
r71uIoudjLvO9cotA+bboQrAvH3L5GgOHkLS6XVFm2U=

044 SHA256 (Base64):
ungWv48Bz+pBQUDeXa4iI7ADYaOWF3qctBD/YfIAFa0=

044 SNEFRU256 (Base64):
fQMyBWR6KvPcgzn2yyVkPDPrxiLTKXnEthKwLEkDAxs=

048 Haval192 (HMAC):
a7b14c9ef3092319b0e75e3b20b957d180bf20745629e8de

048 Haval192:
a7b14c9ef3092319b0e75e3b20b957d180bf20745629e8de

048 Haval192_4
e014185fbb9f19faba90dab14c25c34275cdd3e362775c65

048 Haval195_5
f36196ce912fbb5959948043f8248de2a92f74ab4a549b44

048 Tiger192 (HMAC):
f258c1e88414ab2a527ab541ffc5b8bf935f7b951c132951

048 Tiger192:
f258c1e88414ab2a527ab541ffc5b8bf935f7b951c132951

048 Tiger2
afd7ce60de4799388c88898d708b649d228fc06accecbbb6

056 Haval224 (HMAC):
5 bc955220ba2346a948d2848eca37bdd5eca6ecca7b
594bd32923fab

056 Haval224:
5 bc955220ba2346a948d2848eca37bdd5eca6ecca7b
594bd32923fab

056 Haval244_3
e29a8c16b58e57ebbfd22ddf169e04ffc0136c3452af1
9093fc1c4d0

056 Havan244_4
a29f04a725e5a700f1e388239564e5a3d7f22f302036
5bf4f9bc1d36

056 RipeMD320 (Base64):
3 kwBswVPiTCnnQmuc46SMB5aFwhb7/3BuNEWcT5
0+C+pQtZM28RoLQ==

056 SHA224 (HMAC):
23097 d223405d8228642a477bda255b32aadbce4bd
a0b3f7e36c9da7

056 SHA224:
23097 d223405d8228642a477bda255b32aadbce4bd
a0b3f7e36c9da7

060 Blowfish
2a05$abcdefghijklmnopqrstuu5s2v8.iXieOjg/.AyS
BTTZIIVFJeBui

064 GOST R34.11-94:
f3134348c44fb1b2a277729e2285ebb5cb5e0f29c975
bc753b70497c06a4d51d

064 Haval256 (HMAC):
8699 f1e3384d05b2a84b032693e2b6f46df85a13a50
d93808d6874bb8fb9e86c

064 Haval256:
8699 f1e3384d05b2a84b032693e2b6f46df85a13a50
d93808d6874bb8fb9e86c

064 Haval256_3
48 ab01f979cf2da92fda1e865ffa315ebb112d1ffe750
38089ef73b4abb181cc

064 Haval256_4
a22c64a107bf9118f8b22470e4daa0e7eb08dbad9f7e
4d35dcf409ec40292a75

064 Haval256_5
5 b25f8d944429aad67775eec490272dc21ca5631488
f227ef5efd25b30f91a72

064 Panama
e6d3cb945bb3583cf4262033ad99d24166d7d1a321d
ada9cb23efd021ab07694

064 RipeMD256 (HMAC):
afbd6e228b9d8cbbcef5ca2d03e6dba10ac0bc7dcbe4
680e1e42d2e975459b65

064 RipeMD256:
afbd6e228b9d8cbbcef5ca2d03e6dba10ac0bc7dcbe4
680e1e42d2e975459b65

064 SHA256 (HMAC):
ba7816bf8f01cfea414140de5dae2223b00361a39617
7a9cb410ff61f20015ad

064 SHA256:
ba7816bf8f01cfea414140de5dae2223b00361a39617
7a9cb410ff61f20015ad

064 SHA384 (Base64):
ywB1P0WjXou1oD1pmsZQBycsMqsO3tFjGotgWkP/
W+2AhgcroefMI1i67KE0yCWn

064 SNEFRU256 (HMAC):
7 d033205647a2af3dc8339f6cb25643c33ebc622d32
979c4b612b02c4903031b

064 SNEFRU256:
7 d033205647a2af3dc8339f6cb25643c33ebc622d32
979c4b612b02c4903031b

080 RipeMD320 (HMAC):
de4c01b3054f8930a79d09ae738e92301e5a17085be
ffdc1b8d116713e74f82fa942d64cdbc4682d

080 RipeMD320:
de4c01b3054f8930a79d09ae738e92301e5a17085be
ffdc1b8d116713e74f82fa942d64cdbc4682d

088 SHA512 (Base64):
3 a81oZNherrMQXNJriBBMRLm+k6JqX6iCp7u5ktV05
ohkpkqJ0/BqDa6PCOj/uu9RU1EI2Q86A4qmslPpUyknw
==

088 WHIRLPOOL (Base64):
TiRIpMb0hrsWtlYsc7QCC/MEPjpzG85yGuGzA9l+bUx
xge69tsV+J30ONJVxFMvWx5f8nZXYtYLSJSkgdtTu9Q==

096 SHA384 (HMAC):
cb00753f45a35e8bb5a03d699ac65007272c32ab0ed
ed1631a8b605a43ff5bed8086072ba1e7cc2358baeca134
c825a7

096 SHA384:
cb00753f45a35e8bb5a03d699ac65007272c32ab0ed
ed1631a8b605a43ff5bed8086072ba1e7cc2358baeca134
c825a7

128 SHA512 (HMAC):
ddaf35a193617abacc417349ae20413112e6fa4e89a9
7ea20a9eeee64b55d39a2192992a274fc1a836ba3c23a3f
eebbd454d4423643ce80e2a9ac94fa54ca49f

128 SHA512:
ddaf35a193617abacc417349ae20413112e6fa4e89a9
7ea20a9eeee64b55d39a2192992a274fc1a836ba3c23a3f
eebbd454d4423643ce80e2a9ac94fa54ca49f

128 WHIRLPOOL (HMAC):
4 e2448a4c6f486bb16b6562c73b4020bf3043e3a731
bce721ae1b303d97e6d4c7181eebdb6c57e277d0e34957
114cbd6c797fc9d95d8b582d225292076d4eef5

128 WHIRLPOOL:
4 e2448a4c6f486bb16b6562c73b4020bf3043e3a731
bce721ae1b303d97e6d4c7181eebdb6c57e277d0e34957
114cbd6c797fc9d95d8b582d225292076d4eef5

128 Whirlpool-0
7 f96ffa1c0f666d48f0cd1a25a3fc274fa95cef46551a2
b14513611be585f3b6588ae547a36be1802044be542f5b
530811084293cf9c77710397b84039d8c16d

128 Whirlpool-1
d0f4ff160916bb8fa1da40b3ad9b4fb9be1af2cf65f1e
5230d71f0ca4a426ba928e02ecdf1e001a41a53487443f6
5ae4a82d3e5d5b5b04e12fbf3d11f851f46b

128 Whirlpool-2
aa0be12a59790d8d54b1ee11b3230cb4a29a99060e
7b4fd5303c510264247b2e26b5d6a1c2543325de464117
08ba1e75a23c1083c71cacbcba36ae10ded61d5e

ADLER32: long: 8 only numbers and lowercase <g

Blowfish long: 60 only numbers, lowercase, Uppercase.,/ ,
starts with $2a$, sign 7 from left is$

CRC-16: long: 4 only numbers and lowercase <g

CRC-16-CCITT: long: 4 only numbers and lowercase <g

CRC-32: long: 8 only numbers and lowercase <g

CRC-32B: long: 8 only numbers and lowercase <g

DES (Unix): long: 13 lowecase, uppercase, numbers, / and.

DCC long: 32 only numbers and lowercase <g

Elf-32: long: 9 only numbers

FCS-16: long: 4 only numbers and lowercase <g

GHash-32-3: long: 8 only numbers and lowercase <g

GHash-32-5: long: 8 only numbers and lowercase <g

GOST R34.11-94: long: 64 only numbers and lowercase <g

Haval128_3: long: 32 only numbers and lowercase <g

Haval128_4: long: 32 only numbers and lowercase <g

Haval128_5 long: 32 only numbers and lowercase <g

Haval128 (Base64): long: 24 only numbers, lowercase, Uppercase, + ,/,., ends on==

Haval128 (HMAC): long: 32 only numbers and lowercase <g

Haval160: long: 40 only numbers and lowercase <g

Haval160_3: long: 40 only numbers and lowercase <g

Haval160_4: long: 40 only numbers and lowercase <g

Haval160_5: long: 40 only numbers and lowercase <g

Haval160 (Base64): long: 28 only numbers, lowercase, Uppercase, + ,/,., ends on=

Haval160 (HMAC): long: 40 only numbers and lowercase <g

Haval192: long: 48 only numbers and lowercase <g

Haval192 (Base64): long: 32 only numbers, lowercase, Uppercase.,/, + ,

Haval192_4: long: 48 only numbers and lowercase <g

Haval195_5: long: 48 only numbers and lowercase <g

Haval192 (HMAC): long: 48 only numbers and lowercase <g

Haval224: long: 56 only numbers and lowercase <g

Haval224 (Base64): long: 40 only numbers, lowercase, Uppercase, + ,/,., ends on==

Haval244_3: long: 56 only numbers and lowercase <g

Havan244_4:long: 56 only numbers and lowercase <g

Haval256_5: long: 64 only numbers and lowercase <g

Haval224 (HMAC): long: 56 only numbers and lowercase <g

Haval256: long: 64 only numbers and lowercase <g

Haval256 (Base64): long: 44 only numbers, lowercase, Uppercase, + ,/,., ends on==

Haval256_3: long: 64 only numbers and lowercase <g

Haval256_4: long: 64 only numbers and lowercase <g

Haval256 (HMAC): long: 64 only numbers and lowercase <g

Haval256_3: long: 64 only numbers and lowercase <g

MD2: long: 32 only numbers and lowercase <g

MD2 (Base64): long: 24 only numbers, lowercase, Uppercase, + ,/,., ends on==

MD2 (HMAC): long: 32 only numbers and lowercase <g

MD4: long: 32 only numbers and lowercase <g

MD4 (Base64): long: 24 only numbers, lowercase, Uppercase, + ,/,., ends on==

MD4 (HMAC): long: 32 only numbers and lowercase <g

MD5: long: 32 only numbers and lowercase <g

MD5 (HMAC): long: 32 only numbers and lowercase <g

MD5 (Base64): long: 24 only numbers, lowercase, Uppercase, + ,/,., ends on==

MD5 (APR): long: 37

$apr1$ZSc84vgF$YiKqBzqnUskAPKeDWlN8/0

starts with $apr1$, sign 15 from left is$

numbers, lowercase, Uppercase, . and/

MD5 (Unix): long: 34

1P2lE.rGp$SYCpUzBZjWRGKyMe/MbU00

starts with 1, sign 12 from left is$

MySQL: long: 16 only numbers and lowercase <g

MySQL v5.x: long: 40 only numbers and lowercase <g

NTLM: long: 32 only numbers and lowercase <g

PANAMA long: 64 only numbers and lowercase <g

RipeMD128: long: 32 only numbers and lowercase <g

RipeMD128 (Base64): long: 24 only numbers, lowercase, Uppercase, + ,/,., ends on==

RipeMD128 (HMAC): long: 32 only numbers and lowercase <g

RipeMD160: long: 40 only numbers and lowercase <g

RipeMD160 (Base64): long: 28 only numbers, lowercase, Uppercase, + ,/,., ends on=

RipeMD160 (HMAC): long: 40 only numbers and lowercase <g

RipeMD256: long: 64 only numbers and lowercase <g

RipeMD256 (Base64): long: 44 only numbers, lowercase, Uppercase, + ,/,., ends on=

RipeMD256 (HMAC): long: 64 only numbers and lowercase <g

RipeMD320: long: 80 only numbers and lowercase <g

RipeMD320 (Base64): long: 56 only numbers, lowercase, Uppercase, + ,/,., ends on==

RipeMD320 (HMAC): long: 80 only numbers and lowercase <g

SHA-0: long: 40 only numbers and lowercase <g

SHA-1: long: 40 only numbers and lowercase <g

SHA-1 (Base64): long: 28 only numbers, lowercase, Uppercase, + ,/,., ends on=

SHA-1 (HMAC): long: 40 only numbers and lowercase <g

SHA224: long: 56 only numbers and lowercase <g

SHA224 (Base64): long: 40 only numbers, lowercase, Uppercase, + ,/,., ends on==

SHA224 (HMAC): long: 56 only numbers and lowercase <g

SHA256: long: 64 only numbers and lowercase <g

SHA256 (Base64): long: 44 only numbers, lowercase, Uppercase, + ,/,., ends on=

SHA256 (HMAC): long: 64 only numbers and lowercase <g

SHA384: long: 96 only numbers and lowercase <g

SHA384 (Base64): long: 64 only numbers, lowercase, Uppercase.,/, + ,

SHA384 (HMAC): long: 96 only numbers and lowercase <g

SHA512: long: 128 only numbers and lowercase <g

SHA512 (Base64): long: 88 only numbers, lowercase, Uppercase, + ,/,., ends on==

SHA512 (HMAC): long: 128 only numbers and lowercase <g

SNEFRU128: long: 32 only numbers and lowercase <g

SNEFRU128 (Base64): long: 24 only numbers, lowercase, Uppercase, + ,/,., ends on==

SNEFRU128 (HMAC): long: 32 only numbers and lowercase <g

SNEFRU256: long: 64 only numbers and lowercase <g

SNEFRU256 (Base64): long: 44 only numbers, lowercase, Uppercase, + ,/,., ends on=

SNEFRU256 (HMAC): long: 64 only numbers and lowercase <g

Tiger2: long: 48 only numbers and lowercase <g

Tiger128: long: 32 only numbers and lowercase <g

Tiger128 (Base64): long: 24 only numbers, lowercase, Uppercase, + ,/,., ends on==

Tiger128 (HMAC): long: 32 only numbers and lowercase <g

Tiger160: long: 40 only numbers and lowercase <g

Tiger160 (Base64): long: 28 only numbers, lowercase, Uppercase, + ,/,., ends on=

Tiger160 (HMAC): long: 40 only numbers and lowercase <g

Tiger192: long: 48 only numbers and lowercase <g

Tiger192 (Base64): long: 32 only numbers, lowercase, Uppercase

Tiger192 (HMAC): long: 48 only numbers and lowercase <g

WHIRLPOOL: long: 128 only numbers and lowercase <g

WHIRLPOOL (Base64): long: 88 only numbers, lowercase, Uppercase, + ,/,., ends on==

WHIRLPOOL (HMAC): long: 128 only numbers and lowercase <g

Whirlpool-0: long: 128 only numbers and lowercase <g

Whirlpool-1: long: 128 only numbers and lowercase <g

Whirlpool-2: long: 128 only numbers and lowercase <g

md5(md5($pass)): long: 32 only numbers and lowercase <g

md5(md5($pass).$salt): long: 32 only numbers and lowercase <g

md5(md5($salt).md5($pass)): long: 32 only numbers and lowercase <g

Windows-LM: long: 32 only numbers and Uppercase <G

Windows-NTLM: long: 32 only numbers and Uppercase <G

در سری بعدی با آموزش کرک انواع هش در خدمت شما خواهم بود

با تشکر