

Forum: [Hack Forums](#)

Thread: [\[CYBERSEC SERIES #9 \] Password Cracking Explained: Hashes, Salts & Brute Force](#)

Mastercarder - June 7, 2026, 12:26 am

? Introduction

One of the biggest misconceptions in cybersecurity is that attackers can simply "see" your password after a database breach.

In reality, most services store password hashes rather than actual passwords.

Understanding how password cracking works helps explain why some passwords are compromised in seconds while others remain secure for years.

? What Is A Password Hash?

A hash is a one-way mathematical function that converts data into a fixed-length string of characters.

Code Password:
password123

Hash:
ef92b778baf771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
Key points:

- Easy to generate
- Extremely difficult to reverse
- Used to verify passwords without storing them directly

When you log in, the website hashes the password you enter and compares it to the stored hash.

If they match, access is granted.

? What Happens During A Data Breach?

Imagine a website gets compromised.

An attacker may obtain:

- Usernames

- Email addresses
- Password hashes

The attacker cannot immediately read the passwords.

Instead, they attempt to crack the stolen hashes offline by testing huge numbers of password guesses.

This allows attackers to test millions or even billions of guesses without interacting with the website itself.

? Dictionary Attacks

A dictionary attack uses large lists of common passwords.

Code password

password123

qwerty

letmein

welcome

football

dragon

Each password is hashed and compared against the stolen hashes.

If a match is found, the password is revealed.

This is why weak passwords are often cracked almost instantly.

? Brute Force Attacks

Brute force attacks systematically try every possible combination until the correct password is found.

The longer and more random the password becomes, the harder brute forcing becomes.

A password using uppercase letters, lowercase letters, numbers and symbols is significantly stronger than a short password using only lowercase letters.

Length is one of the most important factors in password security.

? What Are Rainbow Tables?

Rainbow tables are databases containing precomputed password hashes.

Instead of generating hashes during an attack, an attacker simply looks up the hash value.

This can dramatically speed up password recovery attempts.

Modern systems largely defend against this through salting.

? What Is Salting?

A salt is random data added to a password before hashing.

This ensures that two users with identical passwords still end up with completely different hashes.

Salting makes rainbow table attacks significantly less effective.

? Why Some Hashes Are Harder To Crack

Not all hashing algorithms are equal.

Older algorithms such as MD5 and SHA1 are considered outdated.

Modern systems often use:

- bcrypt
- scrypt
- Argon2

These algorithms are intentionally slow, making large-scale password cracking much more difficult.

? Real-World Example

User A:

Code password123

User B:

Code F7@9wL!2Qz#8TnP4

User A may be cracked almost immediately.

User B could require an impractical amount of computing power and time.

The attacker does not care who you are. They care how difficult your password is to guess.

? How To Protect Yourself

? Use long passwords

? Use unique passwords

? Enable Multi-Factor Authentication (MFA)

? Use a password manager

? Change passwords after known breaches

Avoid:

? Reusing passwords

? Names and birthdays

? Common words

? Predictable patterns

? Final Thoughts

Password cracking is not magic.

Most successful attacks rely on weak passwords, reused credentials and predictable human behaviour.

The strongest defence is a long, unique password combined with MFA.

A few extra characters can be the difference between being compromised in seconds and remaining secure for years.

CyberSec Series Progress

? Series #1

? Series #2

? Series #3

? Series #4

? Series #5

? Series #6

? Series #7

? Series #8

? Series #9

Series #10 Coming Soon

Pr0m3th3us - June 7, 2026, 12:33 am

Thank fuck someone made a TUT for this. Im working on a TUT right now (not this category) so i only skimmed over it, but i will be reading this in full tom and posting another response.

Mastercarder - June 7, 2026, 12:39 am

(Jun 7, 2026 12:33 AM)Pr0m3th3us Wrote: [\[CITE\]](#) Thank fuck someone made a TUT for this. Im working on a TUT right now (not this category) so i only skimmed over it, but i will be reading this in full tom and posting another response.

Appreciate it bro! Will be posting series 10 soon!

Hope it helps.

Edmond Dantes - June 7, 2026, 2:55 am

Another great tutorial mate, hope people take notes :)

Mastercarder - June 7, 2026, 3:05 am

(Jun 7, 2026 02:55 AM)Edmond Dantes Wrote: [\[CITE\]](#) Another great tutorial mate, hope people take notes :)

Thank you mate, appreciate the support. Glad you're finding the series useful. Still got a few more topics lined up, so hopefully there's something in each thread that helps people improve their security knowledge. ?

Pr0m3th3us - June 7, 2026, 2:30 pm

Interesting, i never knew about rainbow tables and salting....

Most of my pw's for import stuff are at minimum 13 characters, but some go up to 30. Caps, lowers, numbers, symbols...And yes i remember them..usually.

Dotexe - June 7, 2026, 2:43 pm

(Jun 7, 2026 02:30 PM)Pr0m3th3us Wrote: [\[CITE\]](#) Interesting, i never knew about rainbow tables and salting....

Most of my pw's for import stuff are at minimum 13 characters, but some go up to 30. Caps, lowers, numbers, symbols...And yes i remember them..usually.

You gotta be kidding me ..

Pr0m3th3us - June 7, 2026, 2:52 pm

(Jun 7, 2026 02:43 PM)Dotexe Wrote: [\[CITE\]](#) You gotta be kidding me ..

Nope. I have a method to my madness and its easy.

<https://hackforums.net/showthread.php?tid=6298403>

Dotexe - June 7, 2026, 3:08 pm

(Jun 7, 2026 02:52 PM)Pr0m3th3us Wrote: [\[CITE\]](#) Nope. I have a method to my madness and its easy.

<https://hackforums.net/showthread.php?tid=6298403>

I was talking about rainbow tables and salting

Mastercarder - June 7, 2026, 3:12 pm

(Jun 7, 2026 02:30 PM)Pr0m3th3us Wrote: [\[CITE\]](#) Interesting, i never knew about rainbow tables and salting....

Most of my pw's for import stuff are at minimum 13 characters, but some go up to 30. Caps, lowers, numbers, symbols...And yes i remember them..usually.

A lot of people don't realise the difference.

Rainbow tables are basically huge precomputed databases of password hashes. If a database stores passwords without proper salting, attackers can often look up the hash instead of having to crack it from scratch.

Salting adds a unique random value to every password before it's hashed, which makes rainbow tables practically useless. It's one of those simple security measures that makes a massive difference.

Atleast you learned something today!

(Jun 7, 2026 03:08 PM)Dotexe Wrote: [\[CITE\]](#) I was talking about rainbow tables and salting
You'd be surprised as to how many people have no idea lol!

DeathPenalty666 - June 7, 2026, 4:00 pm

There is a great tricks to skip brutng too. When you have enough info you can generally contact support with the famous ^my account have been hacked,^ and ^my phone number was ip, i am tlaking with the support right now^ ... They usually ask you name order number date and purchase id (If its purchase related) in most case if you create a similar email, with a ip matching the account you can take it over in like 5min! Dumb af but you can save a lot of time.

Can salting be used for hacking of saved credidential for a game? I have a game instaled on 3 different pc and the 3 have totally different hashed password.

Mastercarder - June 7, 2026, 4:04 pm

(Jun 7, 2026 04:00 PM)DeathPenalty666 Wrote: [\[CITE\]](#) There is a great tricks to skip brutng too. When you have enough info you can generally contact support with the famous ^my account have been hacked,^ and ^my phone number was ip, i am tlaking with the support right now^ ... They usually ask you name order number date and purchase id (If its purchase related) in most case if you create a similar email, with a ip matching the account you can take it over in like 5min! Dumb af but you can save a lot of time.

Can salting be used for hacking of saved credidential for a game? I have a game instaled on 3 different pc and the 3 have totally different hashed password.

Good point on the support angle, but that's more of a social engineering weakness than a password weakness. If support can be convinced to hand over an account, it doesn't matter how strong the password is.

As for your question, yes. Salting is specifically designed to stop identical passwords from producing identical hashes. That's why the same game account installed on different PCs can show completely different password hashes even when the underlying password is the same.

DeathPenalty666 - June 7, 2026, 4:14 pm

(Jun 7, 2026 04:04 PM)Mastercarder Wrote: [\[CITE\]](#) Good point on the support angle, but that's more of a social engineering weakness than a password weakness. If support can be convinced to hand over an account, it doesn't matter how strong the password is.

As for your question, yes. Salting is specifically designed to stop identical passwords from producing identical hashes. That's why the same game account installed on different PCs can show completely different password hashes even when the underlying password is the same.

Lovely i learned something interesting today!!! thanks you

Mastercarder - June 7, 2026, 5:04 pm

(Jun 7, 2026 04:14 PM)DeathPenalty666 Wrote: [\[CITE\]](#) Lovely i learned something interesting today!!! thanks you
Anytime boss.?

Love to hear that. Always happy to help bro

Pr0m3th3us - June 7, 2026, 5:10 pm

(Jun 7, 2026 03:08 PM)Dotexe Wrote: [\[CITE\]](#) I was talking about rainbow tables and salting
Sorry, i don't keep up with the Joneses

(Jun 7, 2026 03:12 PM)Mastercarder Wrote: [\[CITE\]](#) A lot of people don't realise the difference.

Rainbow tables are basically huge precomputed databases of password hashes. If a database

stores passwords without proper salting, attackers can often look up the hash instead of having to crack it from scratch.

Salting adds a unique random value to every password before it's hashed, which makes rainbow tables practically useless. It's one of those simple security measures that makes a massive difference.

Atleast you learned something today!

You'd be surprised as to how many people have no idea lol!

Its always the simple things in tech that make the most difference in my experience, i'm going to do some research into who came up with that, and how. I like looking into the background of things like that. Thanks!

Mastercarder - June 7, 2026, 5:16 pm

(Jun 7, 2026 05:10 PM)Pr0m3th3us Wrote: [\[CITE\]](#) Sorry, i don't keep up with the Joneses

Its always the simple things in tech that make the most difference in my experience, i'm going to do some research into who came up with that, and how. I like looking into the background of things like that. Thanks!

Anytime bro! Doesn't a cost to teach people and learn new things.

Stanley - June 8, 2026, 1:57 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

Mastercarder - June 17, 2026, 2:37 pm

Spent a lot of time on this part of the series. Hope people learned something. Enjoy!

????????c? - July 24, 2026, 5:11 pm

```
\$wp$2y$10\$mxZL4/wCFdf9SjjH33A.f.EPpwGQzxqf.Vn4.yfF5XUSfs5KwFtBS
$P$BVXwZoQpxyOmqlgn/ygM3Lnv3IL/Js1
$P$BVOZPpXurDgRvueMIE.LkRMLQB6ktf0
$P$BcYzxvYVvP7IF1UTFEUjzV8wskHHBG/
$P$ByQEkrslxTABKHRQBmClwxLLntuU2r0
$P$BQEZY3spwRVGUDvfU0COquQz.gsgXa0
\$wp$2y$10\$3GxbukAXBs7EfgwajstQK..VGISrYkAB7n7fgQMrznii7OBIrMlHo
```

\$1000 if they manage to crack one