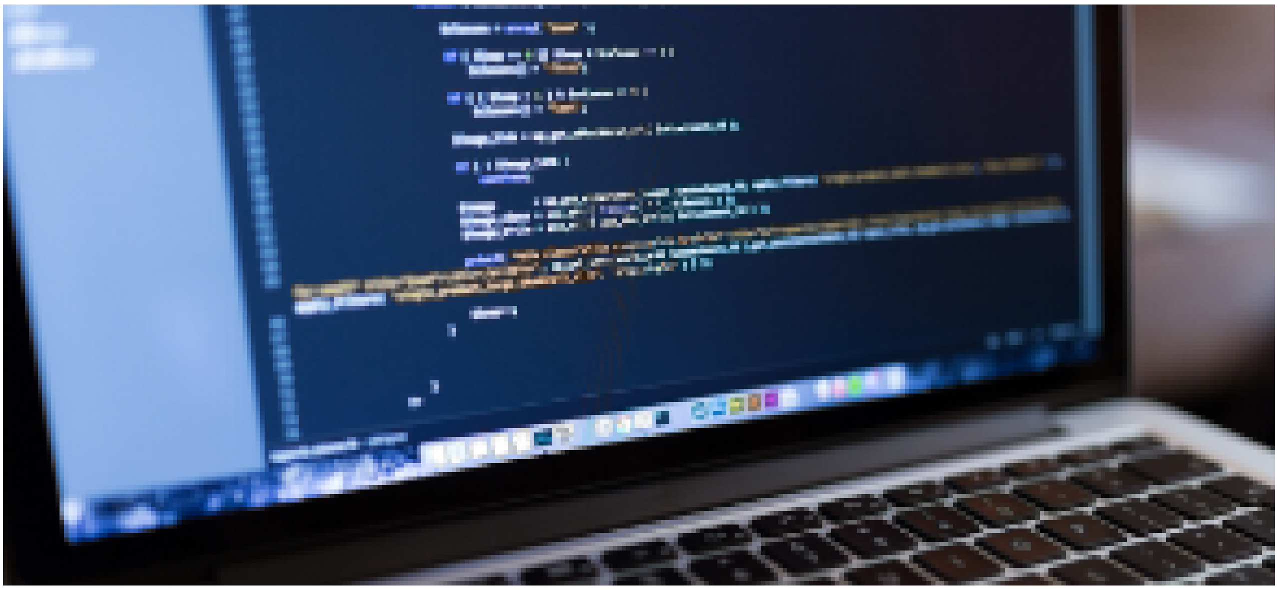
How to Decrypt MD5 Passwords in PHP?

infosecscout.com/decrypt-md5-php

Patrick Fromaget



If you are new in the MD5 world, you probably ask yourself how to decrypt MD5 passwords in PHP after encrypting them.
In this post, I'll show you how to do this, but you probably need an explanation about the MD5 algorithm before 🙂

The MD5 cryptographic algorithm is not reversible.
PHP can encrypt any word into MD5, but not decrypt an MD5 hash to retrieve the original word.
When using the MD5 algorithm to check passwords in PHP, we must have both side encrypted (the password typed and the password stored in the database).

I'll remind you what is the MD5 algorithm and why you can't reverse it to find the password.
Then I'll show you how to validate the password in your code (with PHP samples).
And finally, I'll show you how to use the MD5Online API to find lost passwords.

By the way, if you are interested in how MD5 decryption really works, I highly encourage you to take a look at my e-book "The Secrets of MD5 Decryption"here. It explains everything you need to know, going directly to the point with practical examples you can test on your computer. You don't need any hardware to get started, just a few tips I give in this book.

Download now

What is MD5?

MD5 encryption

MD5 is an algorithm that generates a 32 characters string (hexadecimal) for any word or phrase given in input.
You can even encrypt an entire file into a MD5 hash.

Here is an example:

```
MD5("MD5Online") = d49019c7a78cdaac54250ac56d0eda8a
```

Become a Cyber Security Expert!:
Enroll in the Complete Cyber Security Course now, and master online safety.
Learn to defeat hackers, protect privacy, and stay anonymous with over 50 hours of on-demand video.
If you are interested in the encryption algorithm, you can check the Wikipedia page.
But for the moment you just have to remember that there is an infinite possibility of input for a finite output possibilities (always 32 characters).

So, the MD5 output is not unique, and you can’t reverse it.
But we’ll see in the next paragraph how the decryption works.

MD5 decryption

You must be saying, “If decryption is impossible, how does MD5Online work?”.

In fact, the good answer is:

- **There is no decryption algorithm, the function md5_decrypt() doesn’t exist**
- **But every encryption process gives the same result**

So, I now know that the MD5 hash corresponding to “MD5Online” is d49019c7a78cdaac54250ac56d0eda8a (previous part).
If someone asks me to decrypt this hash, I’m able to answer that there is a good chance that “MD5Online” is the encrypted word.

That is how the MD5 decryption tool is working on MD5Online.
We have a giant database of known MD5 hash, so we can find the result for a lot of hash.

The answer to your question is: no, it’s not really possible to decrypt MD5 passwords in PHP.
So, how can you validate user passwords if you can’t decrypt the database field?

How to validate MD5 passwords?

Theory

The MD5 algorithm is very fast.
So, you can use it where you want, without slowing down your website.

That’s why we were using MD5 to store passwords in a database.
And so to validate them, you can encrypt the input password, and check it with the database one.

The pseudo-code will look like this:

```
IF (MD5(INPUT_STRING) == DATABASE_PASSWORD)
THEN LOGIN()
```

I’ll show you in the next paragraph how to manage the two steps with PHP.

PHP/MySQL samples

Create a user account

The first step is to create a user account.
To do this, you need to create a database, with at least two fields: username and password.

For example, in MySQL, you can create something like this:

```
CREATE TABLE IF NOT EXISTS `users` (
  `username` varchar(32) NOT NULL,
  `password` varchar(32) NOT NULL,
  PRIMARY KEY (`username`)
)
```

The password will be MD5 encrypted, so it will always be 32 characters length.

To create a new user with PHP, you have to do something like that:

```
mysqli_query("INSERT INTO users (username, password)
VALUES ('".$_POST['username']."','".md5($_POST['password'])."'"));
```

You probably already done that, you just need to use the md5() function to encrypt the password.
I recommend using salt with MD5, but it’s not mandatory to understand the process.

Obviously, before that, you need to connect to your MySQL database server, probably clean the $_POST data, and create a form in HTML to register the user.
But we are not here for a basic PHP lesson 🙂

Validate the user password

Then come the part you didn’t know before reading this article.
In the login process, you need to compare the input password to the database password.

Here is what you can do:

```
$query = mysqli_query("SELECT * FROM users
WHERE username='".$_POST['username']."'
AND password='".md5($_POST['password'])."');

if(mysqli_num_rows($query)) {
   //connect
}
else {
   //bad password
}
```

So again, we’ll use the md5() function to encrypt the password before logging in the user.
We only check that the input password is the same as in the database.

At no time it is necessary to decrypt the password stored in the database.

How to finally decrypt passwords in PHP? (API)

If you still need to decrypt a high number of MD5 passwords for another reason that the one we have just seen, I have a solution for you.

MD5Online offer an API you can use in PHP (or with other languages) to send requests directly in our database
That way you can decrypt a lot of MD5 encrypted passwords automatically in PHP.

This is a paid service, if you are interested you will find more info on this page.

As soon as you have your VIP key, you can use this sample code:

```
<?php
$url = 'https://www.md5online.org/api.php';
$key = 'YOUR_VIP_KEY';

//manage your input here, from a form, a file or a database
$md5 = "d3c8e06e57cc1af7ebdba01427e62bc2";

$result = file_get_contents($url."?p=".$key."&h=".$md5);

//do your post action here, with the result
echo $result;
?>
```

I'll let you adding a loop, and maybe a query to get all the passwords at once from your database.
But you have here the minimal part to use the MD5Online API in PHP.

Conclusion

That's it, you now know how to decrypt MD5 passwords in PHP.
Or rather how to use them without decrypting them.

But I also give you a way to really decrypt them with the MD5Online API.
I hope you enjoy this article, feel free to share if it was helpful 🙂

Whenever you're ready for more security, here are things you should think about: