

Forum:[Hack Forums](#)

Thread: [How to make a password/key not readable?](#)

pms - June 24, 2019, 7:55 am

hi,

I want to make a simple gui that does this :

This is where i want the user to enter their key, that they could have gotten from me in real life. But to see the key, the user could easily read the source code right? Thats what i dont want them to be able to do. How do i sort of encrypt this (key = "what ever key") to something unreadable in the source code.

If i was a bit bad explaining, sorry, please ask me questions if needed.

Kallu609 - June 24, 2019, 9:11 am

You need to generate hash for the password. Here is example using hashlib:

pms - June 24, 2019, 10:23 am

(Jun 24, 2019 09:11 AM)Kallu609 Wrote: [\[CITE\]](#) You need to generate hash for the password. Here is example using hashlib:

Oh wow thats a cool function, ill try it out. Thank you.

michalmonday - June 24, 2019, 10:48 am

I don't get how this is going to help with the described problem...

The user can still modify the python code, including the "==" secret_hash" check. What you'd need is a server that will be running all the time, server that is supposed to receive the username/password (possibly encrypted) that will allow to download the desired content/application/python-code hidden from unauthorized people.

FoxBlood - June 24, 2019, 10:50 am

(Jun 24, 2019 10:23 AM)pms Wrote: [\[CITE\]](#) Oh wow thats a cool function, ill try it out. Thank you. Using just sha256 for hashing the password it's not the best way, there are many websites that provides databases with sha256. I recommend to combine those algorithms, maybe add a secret string into password like this:

```
sha512(sha256(password) + 'mysecretstring')
```

lolwtf - June 24, 2019, 5:05 pm

Rule of thumb: client-side validation can be hacked/manipulated.

Your question "How to make my source not readable" can be rephrased as "How can I obfuscate my source". You can do that, but smart people will still be able to modify your GUI to pass the password validation. In addition, how well you will be able to obfuscate your source also depends on the programming language that you will be using.

Please note that if you choose to go this route and do server-side authentication, the (protected) data can be reverse engineered as well.

(Jun 24, 2019 10:50 AM)FoxBlood Wrote: [\[CITE\]](#) Using just sha256 for hashing the password it's not the best way, there are many websites that provides databases with sha256. I recommend to combine those algorithms, maybe add a secret string into password like this:
sha512(sha256(password) + 'mysecretstring')
Use bcrypt. It is an industry standard.