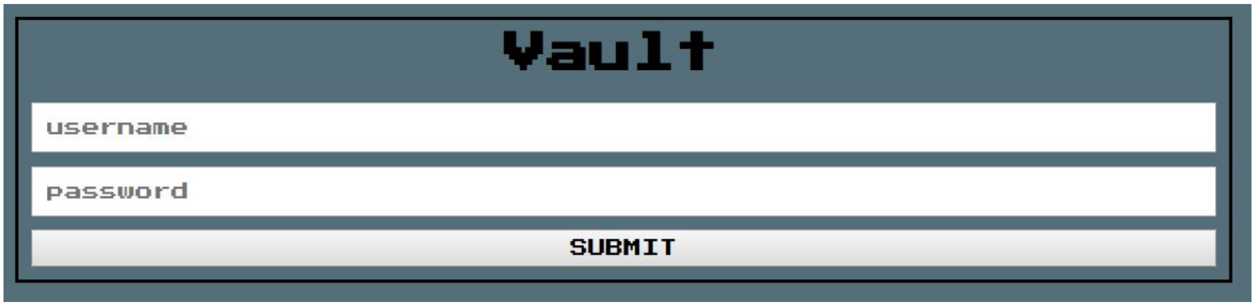
WEB: Vault

We are given the following web page:



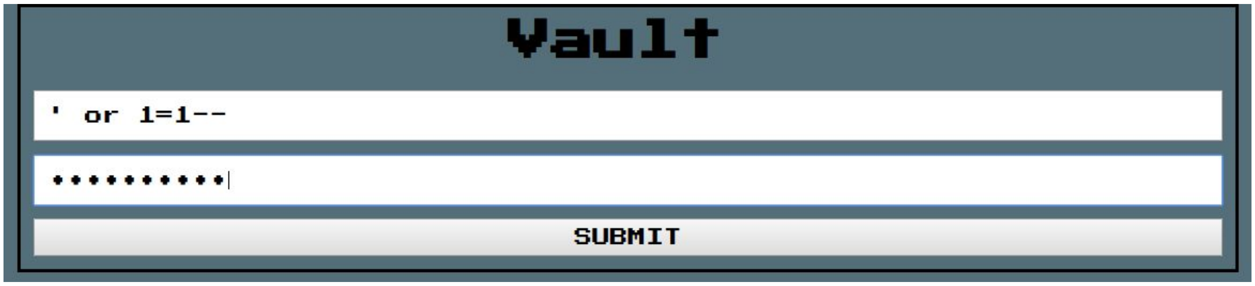
If we try to insert some random values, e.g., “test”, the application responds with a “Denied Access” page.

It seems that we need to guess correct credentials in order to reach the flag. A fair hypothesis is that the APP is using a database like system that handles the password. If we inspect the page we do not see any useful information that we can exploit.

As aforementioned, a fair hypothesis is that the system relies on a database, so what about SQL injection?

We can insert the SQL injection as following:

' or 1=1--



' or 1=1--

•••••••••••

With the following result:

ACCESS GRANTED

Nothing much to see here: if we follow the QR code we can’t find any flag. However, this time there are some cookies, and one of these contains the following url encoded string:

ZW5jcnlwdENURntpX0g0dDNfaW5KM2M3aTBuNX0%3D

After decoding it, we obtain the following:

ZW5jcnlwdENURntpX0g0dDNfaW5KM2M3aTBuNX0=

This is a base64, so we can decode it. If we decrypt it we obtain the flag:

encryptCTF{i_H4t3_inJ3c7i0n5}