Clash of Titan

Problem: Can you log into our application and retrieve the flag?

Given: nc 127.0.0.1 30003; logic file

Hint: There might be a collision in our logic.

Steps:

1) Understanding the given logic file:
- We see that there is a username and password required.
  -username = boko
  -password =
- More importantly we see that the password is encrypted with a hash function called pbkdf2sync. This is a function for computing a shasum of the password given. If you research this function you will find out that it is vulnerable because it produces the same hash for the password and the SHA hash of the same password. Read more to understand the flaw at https://www.chosenplaintext.ca/2015/10/08/pbkdf2-design-flaw.html

2) Connect to the server and try and log in. We try the username and password that we can see in the logic first. So, we pass the user name and password hash check. But, we hit the internal password check statement. This means "complexPasswordWhichContainsManyCharactersWithRandomSuffixeghjrjg" can pass the hash check.

```
prompt: username: boko
prompt: password: complexPasswordWhichContainsManyCharactersWithRandomSuffixeghj
rjg
You didn't try hard enough
```

3) Now we exploit the flaw of pbkdf2sync. We generate the SHA hash of the password with the following command. The command sends the password to the shasum program to compute the hash. Then, the xxd program converts the hash to the string "e6~n22k81<[p"k5hhV6*"

```
[qijun@glap crypto]$ echo -n 'complexPasswordWhichContainsManyCharactersWithRand
omSuffixeghjrjg' | shasum | xxd -r -p
e6~n22k81<[p"k5hhV6*[qijun@glap crypto]$
```

Now, let's try to get the flag...