Bangladesh University of Engineering and Technology

Final Report on
Known Password Attack

Course Code: CSE 406

Course Name: Computer Security Sessional

Author:
Md Hasan Al Kayem

Student ID:
1505023

September 9, 2019

Contents

List of Figures

1 Steps of attacks, snapshots, victim screen

Here are very simple steps to attack. These are given below.

- Enter username, password or username text file and password file.
- click submit to attack
- click make password to get a strong password
- click reset to make reset the action

Attacker screen, Victim screen, Victim server, Victim server database are given below

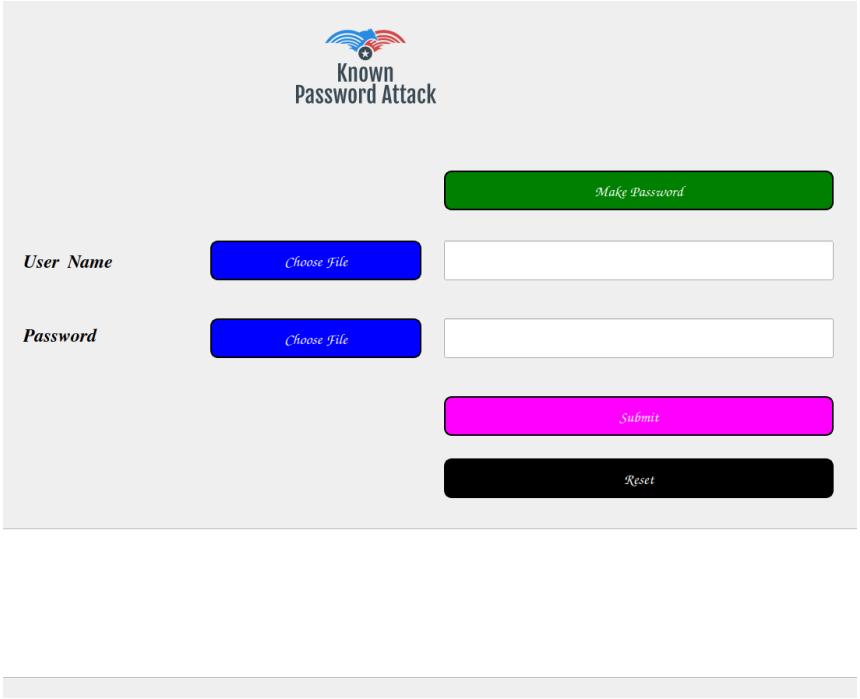

Figure 1: Attacker Screen

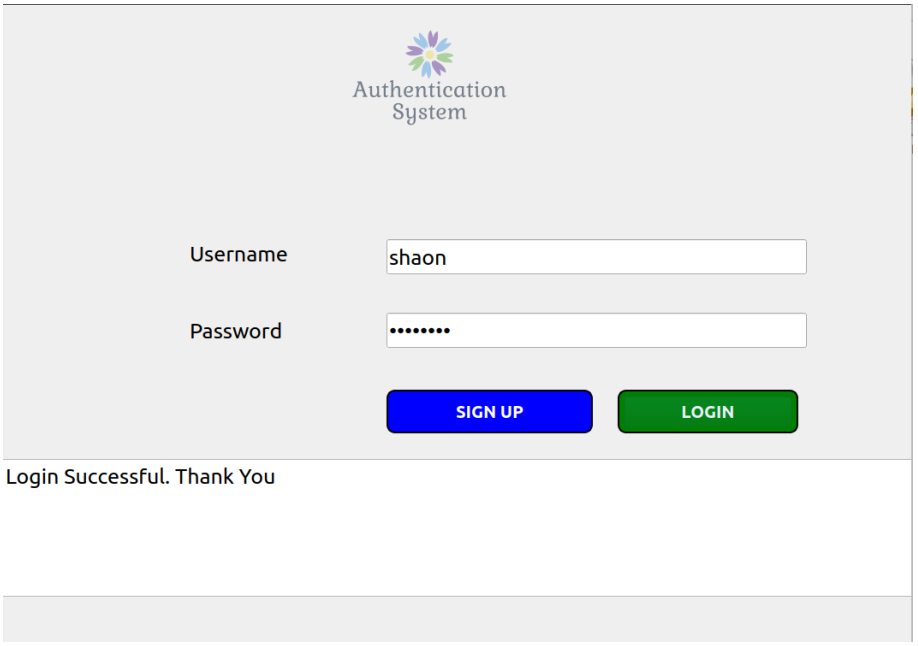

Figure 2: Victim screen

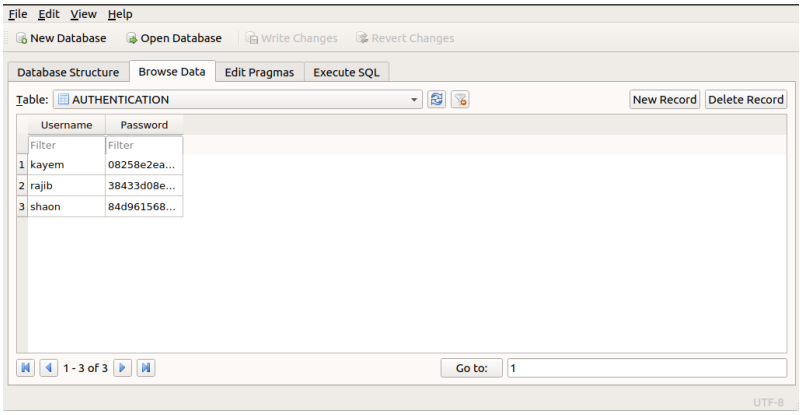

Figure 3: Server Database

```
received

b'login khaled 5f4dcc3b5aa765d61d8327deb882cf99'
data arived ... before encoding printing
b'login khaled 5f4dcc3b5aa765d61d8327deb882cf99'
after decoding printing ...
login khaled 5f4dcc3b5aa765d61d8327deb882cf99
['login', 'khaled', '5f4dcc3b5aa765d61d8327deb882cf99']
('khaled', '5f4dcc3b5aa765d61d8327deb882cf99')

received

Connected to : 127.0.0.1 : 53568
b'login shaon 84d961568a65073a3bcf0eb216b2a576'
data arived ... before encoding printing
b'login shaon 84d961568a65073a3bcf0eb216b2a576'
after decoding printing ...
login shaon 84d961568a65073a3bcf0eb216b2a576
['login', 'shaon', '84d961568a65073a3bcf0eb216b2a576']
('shaon', '84d961568a65073a3bcf0eb216b2a576')

received
```

Figure 4: Server Process

2 Validity

Here as I use username and password from common use, there is a big chance of matching in username and password combination. So with best guess if username and password become matched, it will surely confirm about this attack. So this attack will succeed.

3 Observed output in attacker PC, victim PC, and other related PC

As without knowing of victim and server PC, password is cracked by attacker. So here is only attacker PC with different combination of input and guessing password.

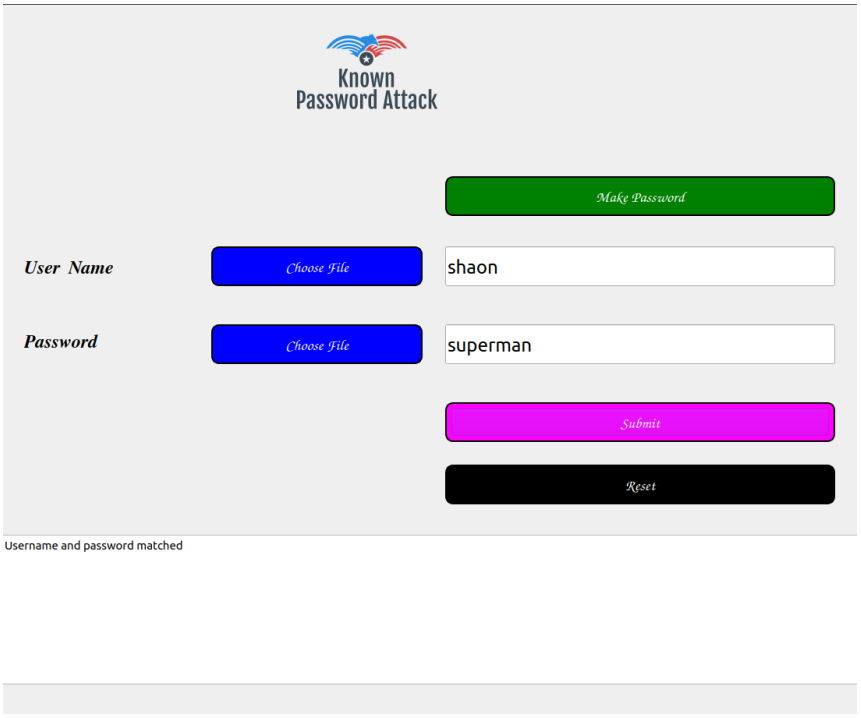

Figure 5: An attack using username and password

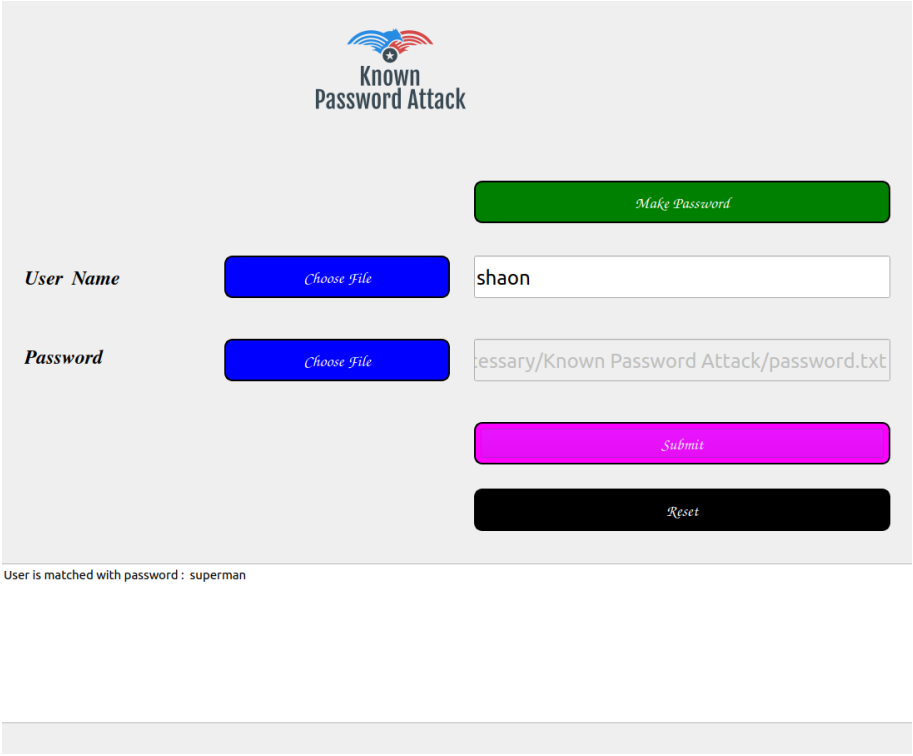

Figure 6: An attack using username and password file

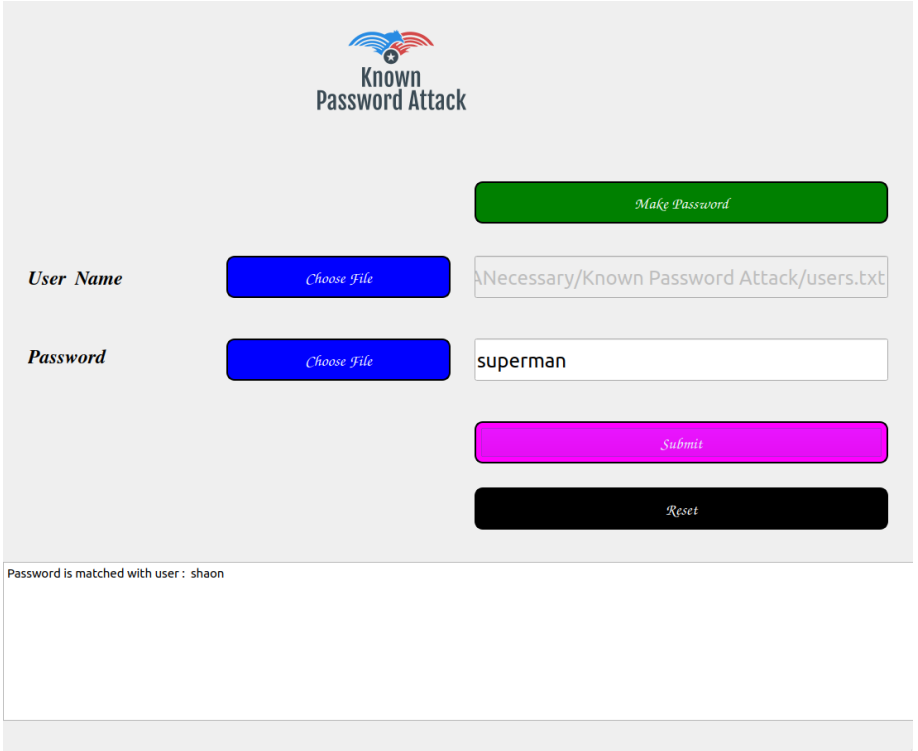

Figure 7: An attack using username file and password

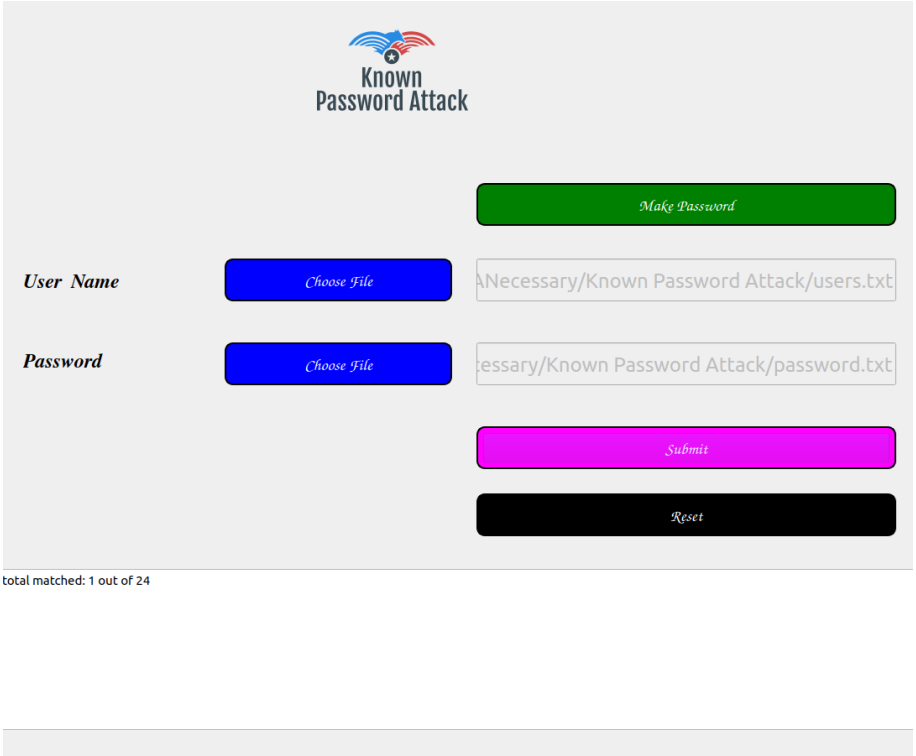

Figure 8: An attack using username file and password file

4 Countermeasure

There are some countermeasures of Known password attack such as One time password (OTP), making password stronger by using unbiased password. In my project I implemented strong password making which is a countermeasure for Known password attack.

Here I followed few rules of strong password which are

- 12 Characters or More
- Mixed and Matched Caps, Symbols, and Numbers
- No obvious substiturions
- Not in the Dictionary
- Does not contain names
- Does not contain phone or address numbers
- Unique

Here by clicking on makepassword button, one can get a strong and unbiased password for him which is quite hard to guess. So, it would be a countermeasure. Which is demonstrated in 9 .

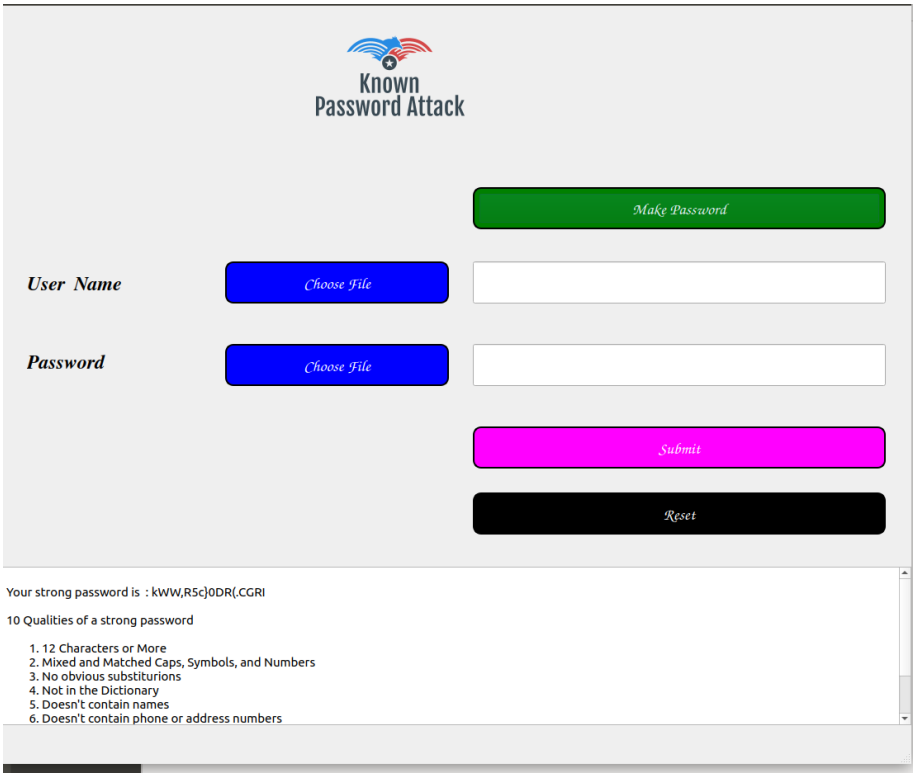

Figure 9: Making a strong password