



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

1	Steps of attacks, snapshots, victim screen	2
2	Validity	5
3	Observed output in attacker PC, victim PC, and other related PC	5
4	Countermeasure	9

List of Figures

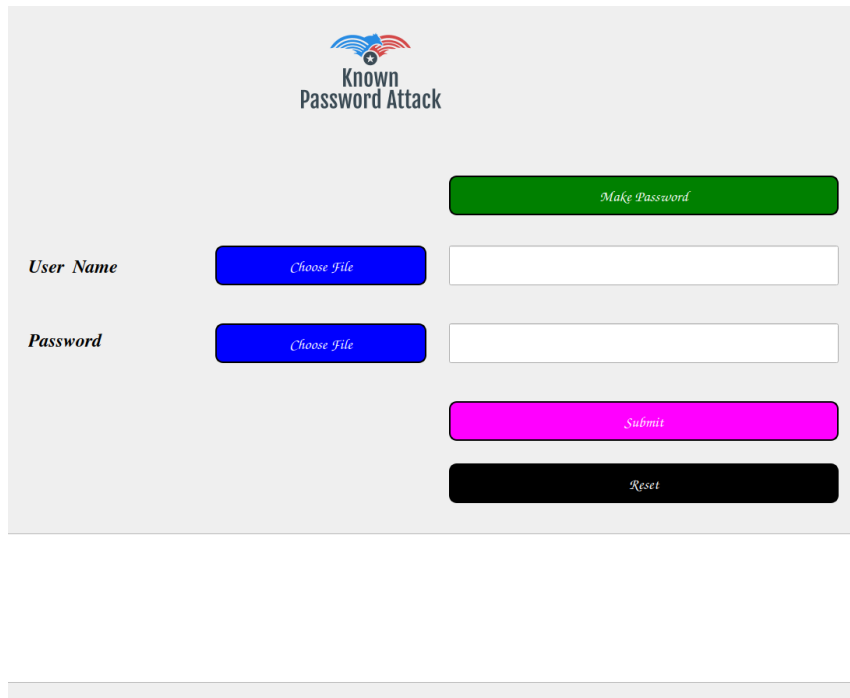
1	Attacker Screen	2
2	Victim screen	3
3	Server Database	4
4	Server Process	4
5	An attack using username and password	5
6	An attack using username and password file	6
7	An attack using username file and password	7
8	An attack using username file and password file	8
9	Making a strong password	10

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

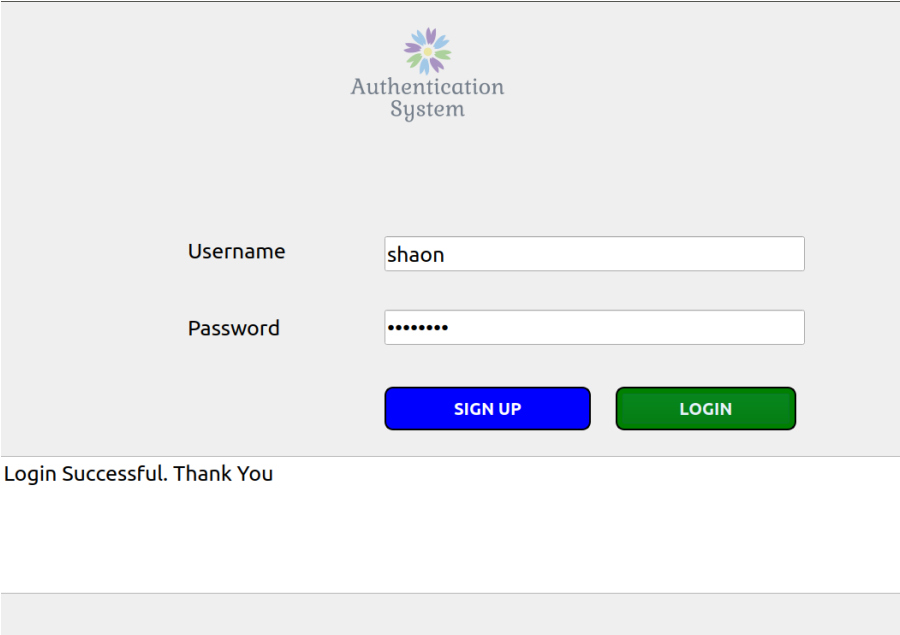
Attacker screen, Victim screen, Victim server, Victim server database are given below



The image shows a web application interface titled "Known Password Attack". At the top center is a logo with a blue and red bird-like icon above the text "Known Password Attack". Below the logo, there are several interactive elements: a green button labeled "Make Password" on the right; a row for "User Name" with a blue "Choose File" button and a text input field; a row for "Password" with a blue "Choose File" button and a text input field; a magenta button labeled "Submit" on the right; and a black button labeled "Reset" on the right. The entire interface is set against a light gray background.

Figure 1: Attacker Screen

Known Password Attack



The image shows a web-based authentication interface. At the top center is a logo consisting of a stylized flower with eight petals in various colors (blue, green, yellow, orange, red, purple, pink, and light blue). Below the logo, the text "Authentication System" is displayed in a serif font. The main area contains two input fields: "Username" with the value "shaon" and "Password" with masked characters ".....". Below these fields are two buttons: a blue "SIGN UP" button and a green "LOGIN" button. At the bottom of the form, a message reads "Login Successful. Thank You". The entire interface is set against a light gray background.

Authentication System

Username

Password

[SIGN UP](#) [LOGIN](#)

Login Successful. Thank You

Figure 2: Victim screen

Known Password Attack

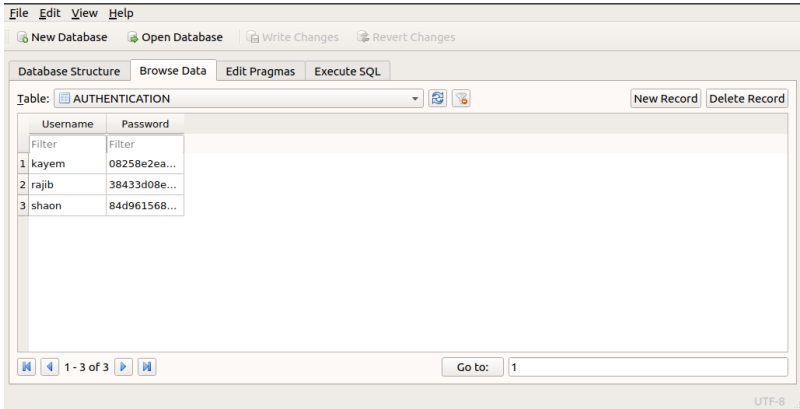


Figure 3: Server Database



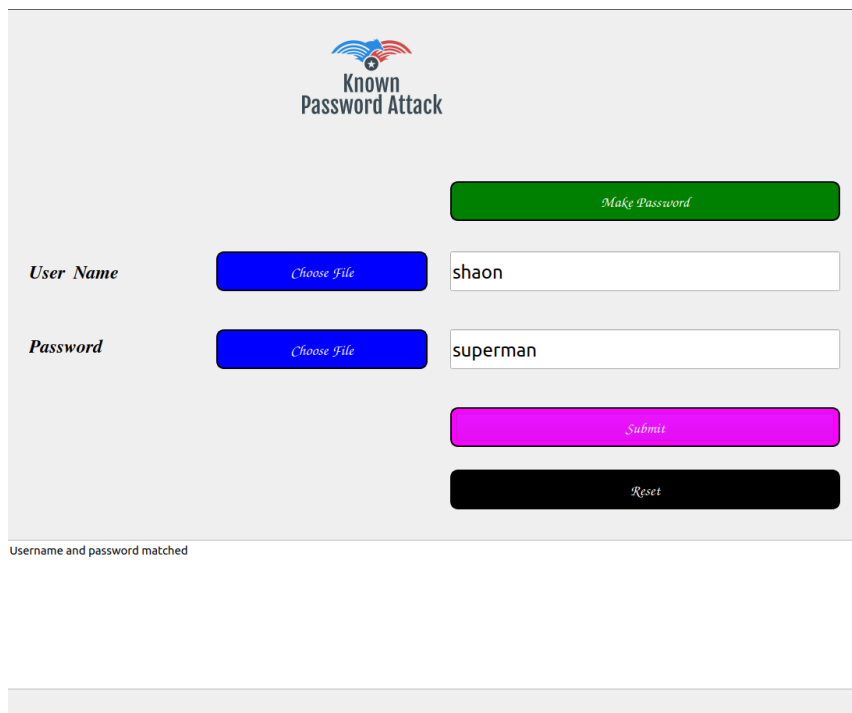
Figure 4: Server Process

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.



The screenshot displays a web interface for a 'Known Password Attack'. At the top center is a logo with a stylized 'K' and 'P' in blue and red, followed by the text 'Known Password Attack'. Below the logo, there are two main input sections. The first section is for 'User Name', featuring a blue button labeled 'Choose File' and a text input field containing 'shaon'. The second section is for 'Password', featuring a blue button labeled 'Choose File' and a text input field containing 'superman'. To the right of these input fields, there are three buttons: a green button labeled 'Make Password', a pink button labeled 'Submit', and a black button labeled 'Reset'. At the bottom of the interface, a message reads 'Username and password matched'.

Figure 5: An attack using username and password

Known Password Attack



Known Password Attack

User Name

Choose File

Password

Choose File

Make Password

Submit

Reset

Password is matched with user : shaon

Figure 7: An attack using username file and password

Known Password Attack



Known Password Attack

User Name

Choose File

A\necessary/known Password Attack/users.txt

Password

Choose File

essary/known Password Attack/password.txt

Make Password

Submit

Reset

total matched: 1 out of 24

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 substitutions
- 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 .

Known Password Attack

Known
Password Attack

User Name

Choose File

Password

Choose File

Make Password

Submit

Reset

Your strong password is : kWW,R5cJ0DR(CGRI

10 Qualities of a strong password

1. 12 Characters or More

2. Mixed and Matched Caps, Symbols, and Numbers

3. No obvious substitutions

4. Not in the Dictionary

5. Doesn't contain names

6. Doesn't contain phone or address numbers

Figure 9: Making a strong password