# unixpasswordcracker

August 3, 2021

## 1 Sprint #3 - Unix Password Cracker

- Author: **César Freire**
- Date: **2021-08-04**

## 2 Objective

- Determin if a list of unix users as a week password by dictionary attack https://en.wikipedia.org/wiki/Dictionary_attack

## 3 References

- https://pt.wikipedia.org/wiki/SHA-2
- https://en.wikipedia.org/wiki/Rainbow_table

## 4 Sample Data

A sample data was obtanin by Mr. C with password: `123456`

```
webmaster:$6$123456$37mxvJGRzjWxgD3HYl.bKq4aUXrcYV8mkOpxmqg8ARv3t9ke5ZM/
NBbwTkx1FDcnLhrOX3jQc6L/NKAohhQJn/:15915:0:99999:7:::
```

## 5 File Format

- **Username** : It is your login name.
- **Password** : It is your encrypted password. The password should be minimum 8-12 characters long including special characters, digits, lower case alphabetic and more. Usually password format is set to `$id$salt$hashed`

The `$id` is the algorithm used On GNU/Linux as follows:

| id | type |
|---|---|
| 1 | MD5 |
| $2a$ | Blowfish |
| $2y$ | Blowfish |
| 5 | SHA-256 |
| 6 | SHA-512 |

# 6 Crypt Lib example

[8]:

```
import crypt

line ='webmaster:$6$123456$37mxvJGRzjWxgD3HYl.bKq4aUXrcYV8mk'\
      '0pxmqg8ARv3t9ke5ZM/NBbwTkx1FDcnLhr0X3jQc6L/NKAohhQJn/:' \
      '15915:0:99999:7:::'

line_split = line.split(':')
print(line_split)
hash_ = line_split[1]

password = input('password:')
result = crypt.crypt(password, hash_)
if result == hash_:
    print('Password found for webmaster')
else:
    print('Password no found for webmaster')
```

```
['webmaster', '$6$123456$37mxvJGRzjWxgD3HYl.bKq4aUXrcYV8mk0pxmqg8ARv3t9ke5ZM/NBb
wTkx1FDcnLhr0X3jQc6L/NKAohhQJn/', '15915', '0', '99999', '7', '', '', '']
```

```
password: 123456
```

```
Password found for webmaster
```

## 6.1 Workflow

1. Create a script that read all lines from `linux_passwd_sample.txt` amd calls a function for every line
2. Create a function that test a line of hash and tests every password from `top_worst_passwords.txt`
3. If a crypted password mathes th hash output the username and password.
   Example: `Found password for user webmaster = 123456`
4. If the password canot be found just output a simple dot '.'

## 6.2 Improvements

- limit the number of lines in sample file
- limit the number of attempts in passwords file
- Calculate how mutch time will take to finish job base on first line
- Update remain time at regular intervals
- Give some feedback if user wants to debug

## 6.3 Question ?

Does any user as a week password? Who?

[ ]:

```
# code goes here
```