FRUITS

mongodb+srv://chall_solver:7VY1PoARhHMuCTpu@cluster0.crmz3.mongodb.net/Phishing?retryWrites=true&w=majority

Note
This URL is all you need.

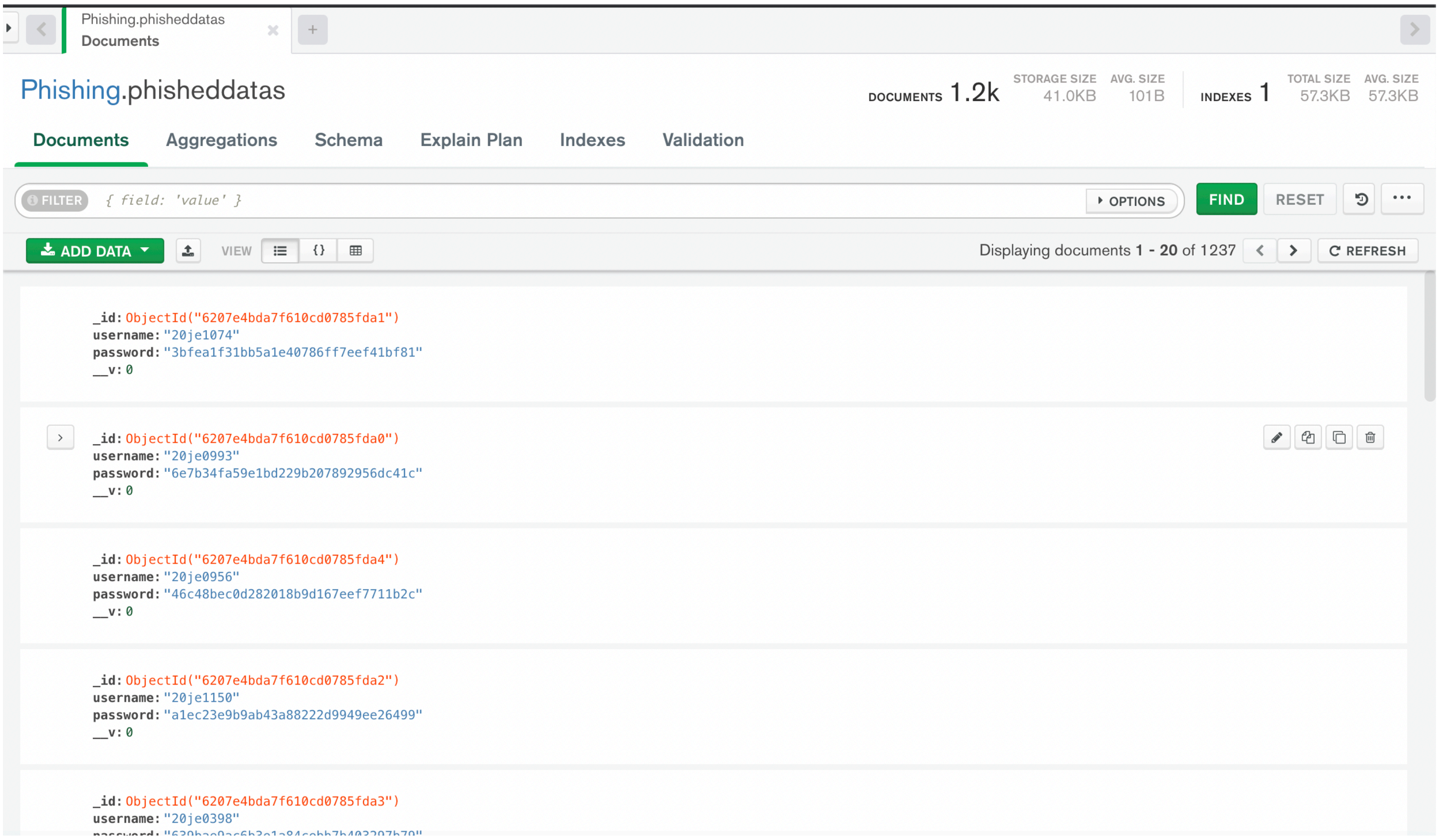
Description

There is a string given in the prompt which is used to connect to a database

Writeup

It is evident from the given url that the database is on MongoDB.
So I installed MongoDB Compass to connect.

After connecting it looked something like this

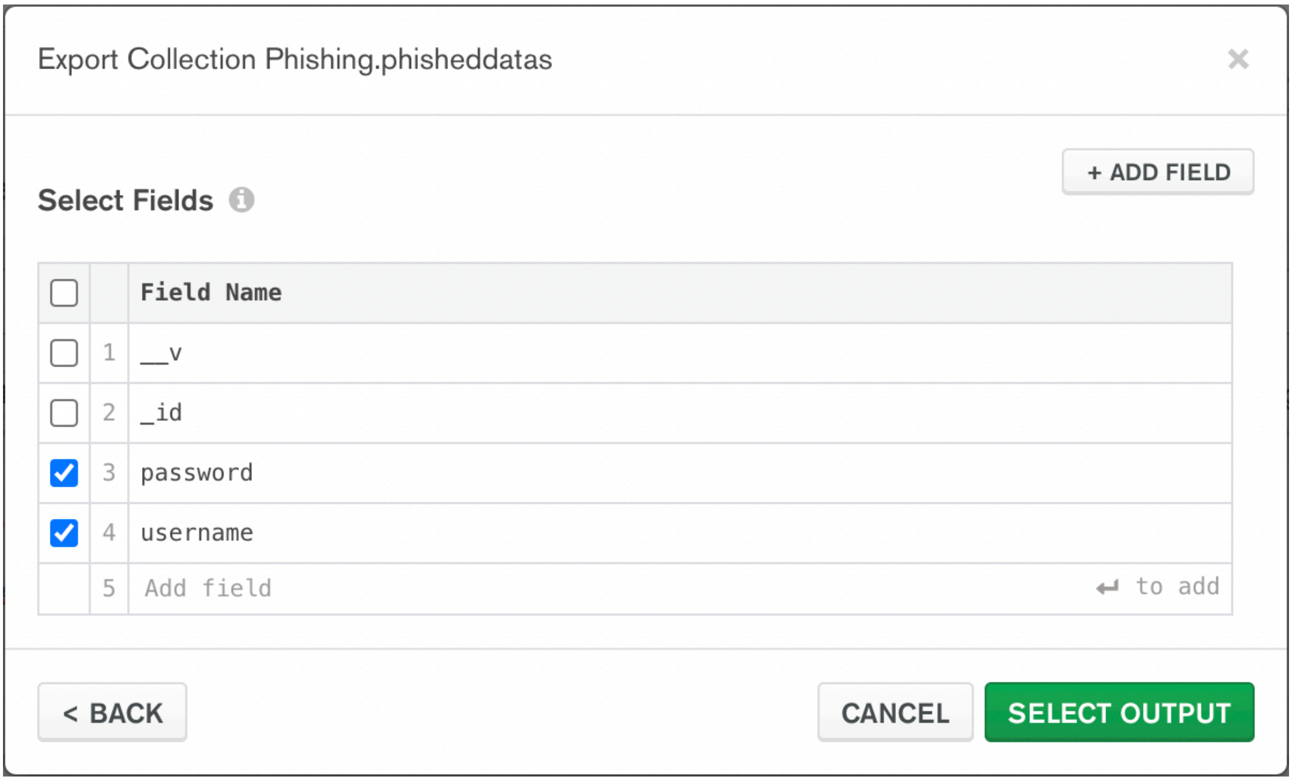


```
_id: ObjectId("6207e4bda7f610cd0785fda1")
username: "20je1074"
password: "3bfea1f31bb5a1e40786ff7eef41bf81"
__v: 0

_id: ObjectId("6207e4bda7f610cd0785fda0")
username: "20je0993"
password: "6e7b34fa59e1bd229b207892956dc41c"
__v: 0

_id: ObjectId("6207e4bda7f610cd0785fda4")
username: "20je0956"
password: "46c48bec0d282018b9d167eef7711b2c"
__v: 0

_id: ObjectId("6207e4bda7f610cd0785fda2")
username: "20je1150"
password: "a1ec23e9b9ab43a88222d9949ee26499"
__v: 0

_id: ObjectId("6207e4bda7f610cd0785fda3")
username: "20je0398"
password: "630bae9ac6b3e1a84cebb7b403297b79"
```

From the first glance it appears to be some data with username as admission number and Password as some MD5 hashed string.

When I checked first couple of passwords with this MD5 hash library it showed that the words are **gonna** and **never**.

I exported all these passwords into a .csv file.
There is an inbuilt feature in MongoDB Compass to export this.



Export Collection Phishing.phisheddatas ×

Select Fields

+ ADD FIELD

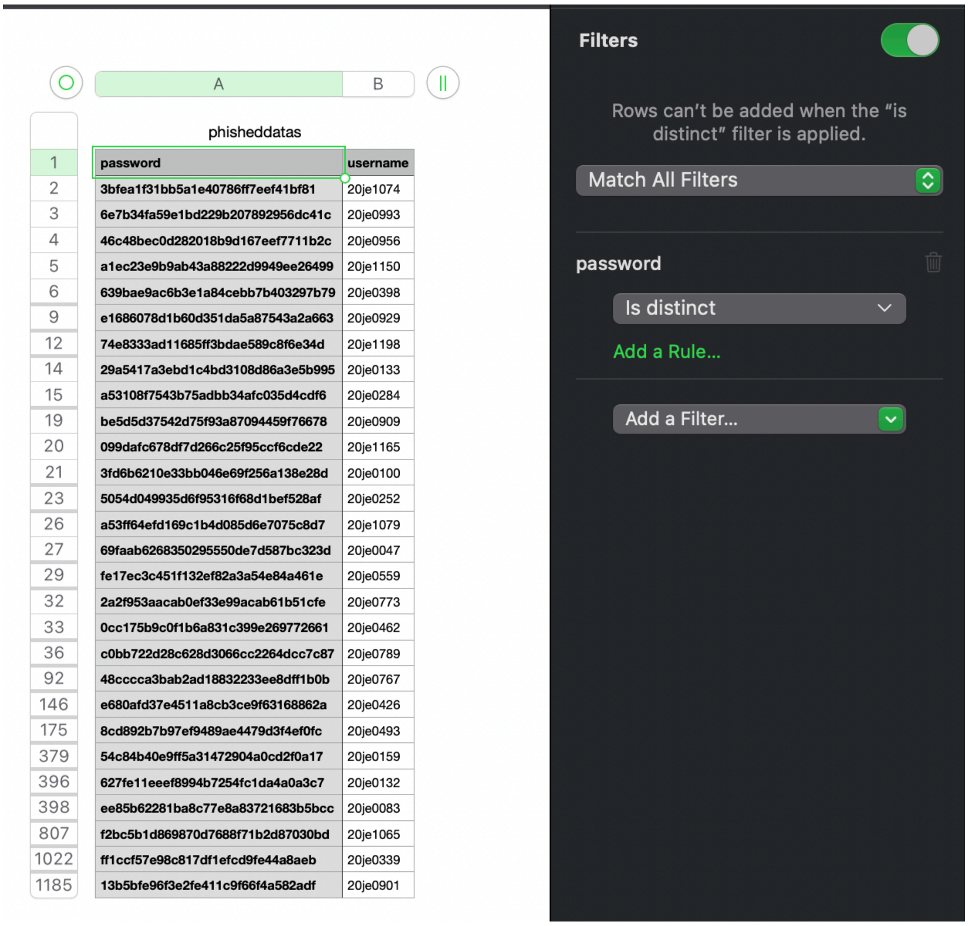
□		Field Name
□	1	__v
□	2	_id
☑	3	password
☑	4	username
	5	Add field ↵ to add

< BACK

CANCEL

SELECT OUTPUT

Then I filtered the data to show a hashed string only once.
It gives us these passwords…



phisheddatas

	A	B
1	password	username
2	3bfea1f31bb5a1e40786ff7eef41bf81	20je1074
3	6e7b34fa59e1bd229b207892956dc41c	20je0993
4	46c48bec0d282018b9d167eef7711b2c	20je0956
5	a1ec23e9b9ab43a88222d9949ee26499	20je1150
6	639bae9ac6b3e1a84cebb7b403297b79	20je0398
9	e1686078d1b60d351da5a87543a2a663	20je0929
12	74e8333ad11685ff3bdae589c8f6e34d	20je1198
14	29a5417a3ebd1c4bd3108d86a3e5b995	20je0133
15	a53108f7543b75adbb34afc035d4cdf6	20je0284
19	be5d5d37542d75f93a87094459f76678	20je0909
20	099dafc678df7d266c25f95ccf6cde22	20je1165
21	3fd6b6210e33bb046e69f256a138e28d	20je0100
23	5054d049935d6f95316f68d1bef528af	20je0252
26	a53ff64efd169c1b4d085d6e7075c8d7	20je1079
27	69faab6268350295550de7d587bc323d	20je0047
29	fe17ec3c451f132ef82a3a54e84a461e	20je0559
32	2a2f953aacab0ef33e99acab61b51cfe	20je0773
33	0cc175b9c0f1b6a831c399e269772661	20je0462
36	c0bb722d28c628d3066cc2264dcc7c87	20je0789
92	48cccca3bab2ad18832233ee8dff1b0b	20je0767
146	e680afd37e4511a8cb3ce9f63168862a	20je0426
175	8cd892b7b97ef9489ae4479d3f4ef0fc	20je0493
379	54c84b40e9ff5a31472904a0cd2f0a17	20je0159
396	627fe11eeef8994b7254fc1da4a0a3c7	20je0132
398	ee85b62281ba8c77e8a83721683b5bcc	20je0083
807	f2bc5b1d869870d7688f71b2d87030bd	20je1065
1022	ff1ccf57e98c817df1efcd9fe44a8aeb	20je0339
1185	13b5bfe96f3e2fe411c9f66f4a582adf	20je0901

Filters

Rows can't be added when the "is distinct" filter is applied.

Match All Filters

password

Is distinct

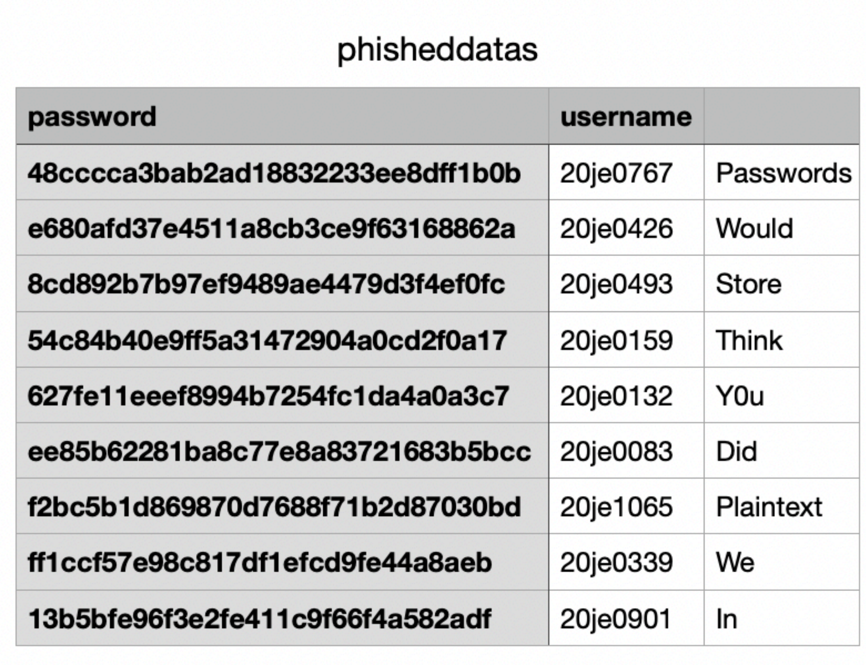
Add a Rule…

Add a Filter…

When we supply these passwords to the above mentioned library we get the words

As we have seen most of them are words from “**Never Gonna Give You Up**”

So when take out those words we get this…



phisheddatas

password	username	
48cccca3bab2ad18832233ee8dff1b0b	20je0767	Passwords
e680afd37e4511a8cb3ce9f63168862a	20je0426	Would
8cd892b7b97ef9489ae4479d3f4ef0fc	20je0493	Store
54c84b40e9ff5a31472904a0cd2f0a17	20je0159	Think
627fe11eeef8994b7254fc1da4a0a3c7	20je0132	Y0u
ee85b62281ba8c77e8a83721683b5bcc	20je0083	Did
f2bc5b1d869870d7688f71b2d87030bd	20je1065	Plaintext
ff1ccf57e98c817df1efcd9fe44a8aeb	20je0339	We
13b5bfe96f3e2fe411c9f66f4a582adf	20je0901	In

Rearranging those words we get the required flag

DID Y0U THINK WE WOULD STORE PASSWORDS IN PLAINTEXT