

Misc - Eternal Loop

So it appears to be a zip file containing nested zip files,

```
[hacktheboxVM]-[00:20-11/10]-[/home/nq1p/HTB]
nq1p$ unzip Eternal\ Loop.zip Archive:  Eternal Loop.zip
[Eternal Loop.zip] 37366.zip password:
extracting: 37366.zip
[hacktheboxVM]-[00:20-11/10]-[/home/nq1p/HTB]
nq1p$
```

After some guessing I figure out the password for each zip file is the filename of the zip file it contains (minus the .zip).

```
[hacktheboxVM]-[00:21-11/10]-[/home/nq1p/HTB]
nq1p$ unzip 37366.zip
Archive:  37366.zip
[37366.zip] 5900.zip password:
skipping: 5900.zip                                incorrect password
[hacktheboxVM]-[00:21-11/10]-[/home/nq1p/HTB]
nq1p$ unzip 37366.zip
Archive:  37366.zip
[37366.zip] 5900.zip password:
password incorrect--reenter: %c
[hacktheboxVM]-[00:21-11/10]-[/home/nq1p/HTB]
nq1p$ unzip 37366.zip
Archive:  37366.zip
[37366.zip] 5900.zip password:
password incorrect--reenter:
password incorrect--reenter:
inflating: 5900.zip
[hacktheboxVM]-[00:21-11/10]-[/home/nq1p/HTB]
```

Presumably given the name the nest is deep enough that the challenge isn't meant to be solved manually.

So a script needs to be written to automate unzipping the zip folder.

Simple automation of shell commands like this should probably just be achieved with a bash/zsh script. Although a Python script could be written using an archiving library, etc.

General flow of the script would be:

1. unzip initial zip that contains the nest (password: hackthebox)
2. Read out contents of the zip

3. There is only one file, the next zip, grab the filename of that zip minus ".zip" at the end
4. Use that filename to unzip the zip
5. Repeat steps 2-4 with new zip until I suppose an error happens because there's no more zips to unzip?

Now to implement this into a bash script.

--Minor interlude later as I spend an hour setting up emacs, etc--

Alright, time to get started on this script. This is actually taking quite a bit of time to get started, reviewing cheatsheets, etc to remind myself of bash's syntax. It's not quite muscle memory like Python's is so I don't remember how functions work, etc. Another reason to do the script in Bash, it'd just be useful to get more familiar with Bash.

--Few minutes later--

Oh god, you refer to passed arguments in a function by their position and not a name, I hate Bash scripting already.

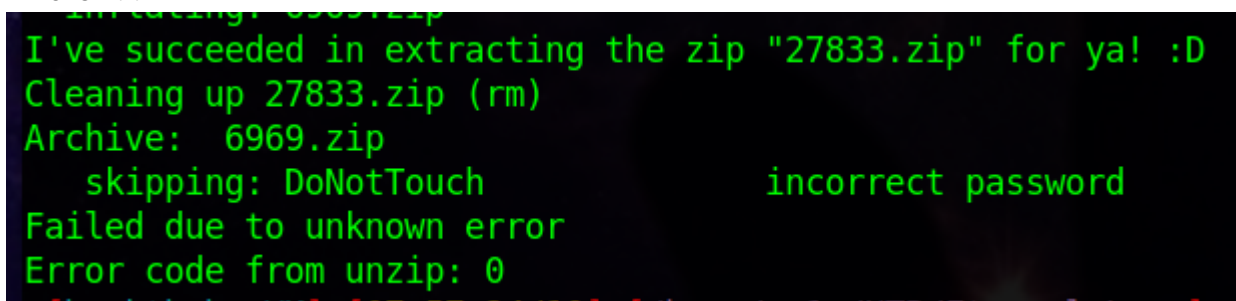
--A week or two later--

Well passed out, got too tired and then woke up sick, was sick for a week or two. So time to pick up from where I left off I suppose, read my notes, figure out what I meant to do to finish this script and then I should finally be done I suppose.

--An hour or two later--

Script's finally done!

And oh??



```
Extracting: 27833.zip
I've succeeded in extracting the zip "27833.zip" for ya! :D
Cleaning up 27833.zip (rm)
Archive:  6969.zip
  skipping: DoNotTouch                               incorrect password
Failed due to unknown error
Error code from unzip: 0
```

Uh. Tried manually extracting it with the usual, hackthebox, etc, that's not it.. hmm..

Welp! I think we're past the basic scripting stage, let's give brute force a shot I suppose, I've tried all the passwords fitting to the rule so far, "hackthebox", maybe even just the filename of the last zip.. Still nothing.

--15 minutes later--

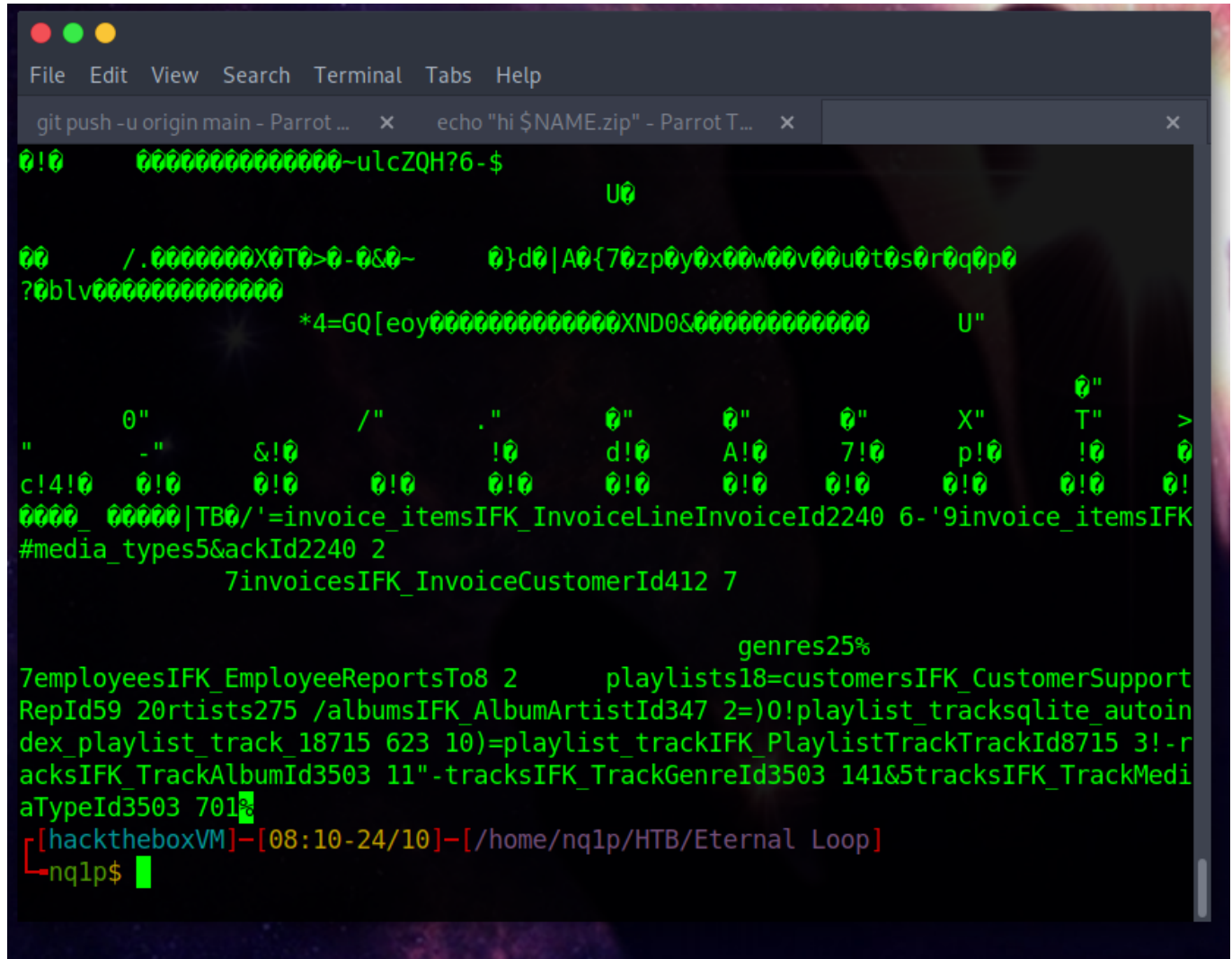
Huh! Yea, would you look at that.

```
[hacktheboxVM]-[08:07-24/10]-[/home/nqlp/HTB/Eternal Loop]
nqlp$ fcrackzip -u 6969.zip -D -p /usr/share/wordlists/rockyou.txt

PASSWORD FOUND!!!!: pw == letmeinplease
[hacktheboxVM]-[08:09-24/10]-[/home/nqlp/HTB/Eternal Loop]
```

Alright, fantastic, just got to manually unzip this now and.. I'm done?

Ah, fantastic, it's a, uh something, but not a text file with the flag, that's for sure.



```
File Edit View Search Terminal Tabs Help
git push -u origin main - Parrot ... x echo "hi $NAME.zip" - Parrot T... x
0!0 000000000000~ulcZQH?6-$
                                U0
00 /.0000000X0T0>0-0&0~ 0}d0|A0{70zp0y0x00w00v00u0t0s0r0q0p0
?0blv000000000000
          *4=GQ[eoy000000000000XND0&000000000000 U"
                                0"
0" 0" 0" X" T" >
" -" &!0 !0 d!0 A!0 7!0 p!0 !0 0
c!4!0 0!0 0!0 0!0 0!0 0!0 0!0 0!0 0!0 0!0 0!
0000_00000|TB0/'=invoice_itemsIFK_InvoiceLineInvoiceId2240 6-'9invoice_itemsIFK
#media_types5&ackId2240 2
          7invoicesIFK_InvoiceCustomerId412 7
                                genres25%
7employeesIFK_EmployeeReportsTo8 2 playlists18=customersIFK_CustomerSupport
RepId59 20rtists275 /albumsIFK_AlbumArtistId347 2=)0!playlist_tracksqliite_autoin
dex_playlist_track_18715 623 10)=playlist_trackIFK PlaylistTrackTrackId8715 3!-r
acksIFK_TrackAlbumId3503 11"-tracksIFK_TrackGenreId3503 141&5tracksIFK_TrackMedi
aTypeId3503 701%
[hacktheboxVM]-[08:10-24/10]-[/home/nqlp/HTB/Eternal Loop]
nqlp$
```

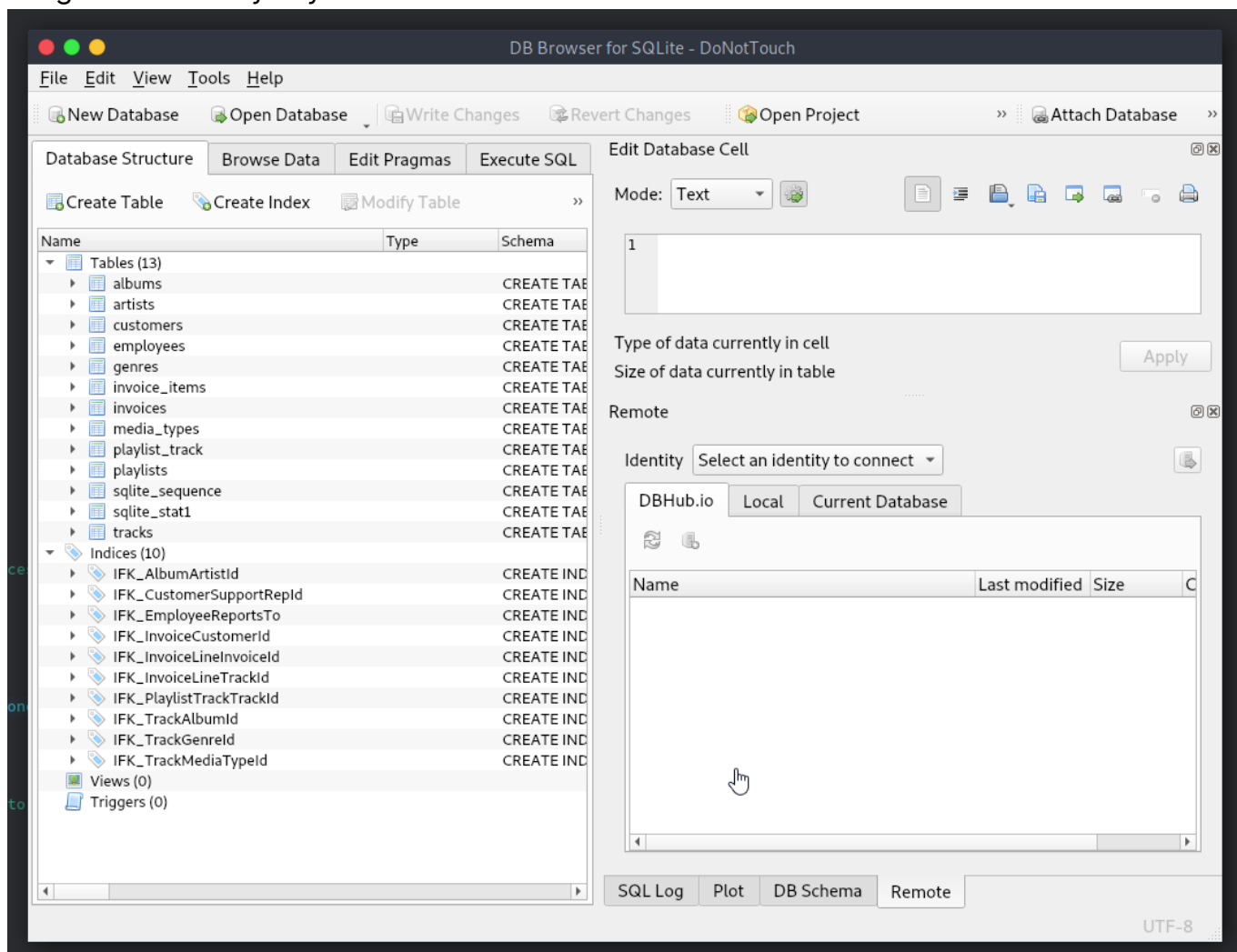
Alright, a sqlite database.

```
[hacktheboxVM]~[08:10-24/10]~[/home/nq1p/HTB/Eternal Loop]
nq1p$ file DoNotTouch
DoNotTouch: SQLite 3.x database, last written using SQLite version 3021000
[hacktheboxVM]~[08:11-24/10]~[/home/nq1p/HTB/Eternal Loop]
```

Little bit cheaty it feels like because I didn't actually need to open up the database but uh.

```
[hacktheboxVM]~[08:11-24/10]~[/home/nq1p/HTB/Eternal Loop]
nq1p$ strings DoNotTouch | grep HTB
1969-01-01 00:00:002069-01-01 00:00:00Chillin with SatanHellHTB{z1p_and_unz1p_ma
_bruddahs}
[hacktheboxVM]~[08:11-24/10]~[/home/nq1p/HTB/Eternal Loop]
```

I'm gonna do it anyways.



Andddd nvm, you were clearly meant to search through the database somehow anyways for sure because it's not exactly small.


3500	3500	String Quartet No. 12 in C
3501	3501	L'orfeo, Act 3, Sinfonia (O
3502	3502	Quintet for Horn, Violin, 2
3503	3503	Koyaanisqatsi

3484 - 3502 of 3503


And there we go, I found the flag without using the slightly cheaty feeling "| grep HTB" lol.

EmployeeId	LastName	FirstName	Title	ReportsTo	BirthDate	HireDate	Address	City	State	Country	PostalCode	Phone	HomePhone	Extension	Email
1	YoMomma	YoPapa	Your Lord	1	1969-01-01 00:00:00	2069-01-01 00:00:00	Chillin with Satan	Hell							HTB{z1p_and_unz1p_ma_bruddahs}

:D



Eternal Loop has been Pwned!

Congratulations  **nq1p**, best of luck in capturing flags ahead!

#9574	24 Oct 2021	20
CHALLENGE RANK	PWN DATE	POINTS EARNED

OK
SHARE

