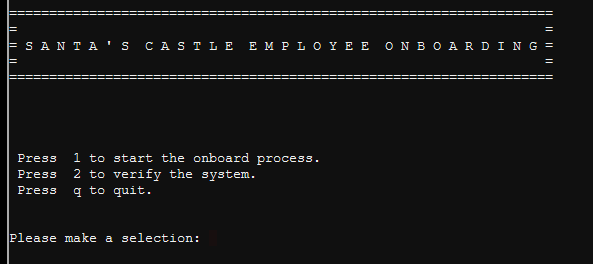
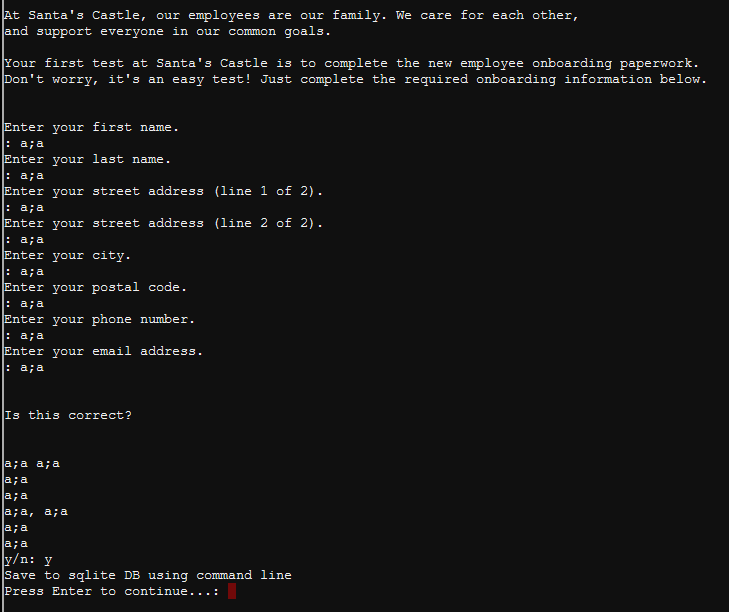
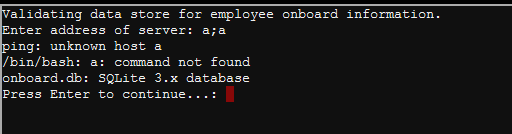
Terminal Challenge--The Name Game (part 2)

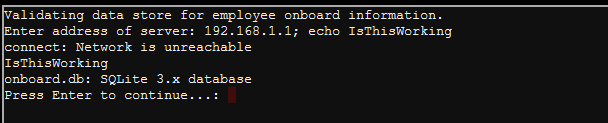
# Command Injection

In the last section you were tasked with finding a field that was vulnerable to command injection. We can start by selecting the first option and entering a;a everywhere.  


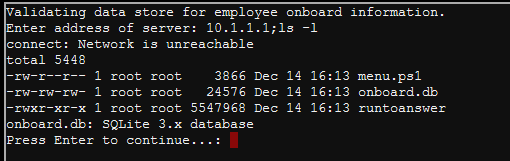
Press 1 and we go here:  


When we press Enter, we go back to the main screen. No obvious injection there.

Try the same thing for the second option.  


Now that is interesting! It looks like the site tried to ping a, and then tried to execute a. If that is correct, then something like 192.168.1.1; echo IsThisWorking may work.  


That’s it! It appears they are running PowerShell (at least that is what the hints say) on top of Linux (/bin/bash error message). It also appears the information we need is in a SQLite 3.x database. That is nice of them to tell us! Note: when you are writing applications, error messages may help you, but they also help attackers. Remove helpful error messages before your application is put in production!

  
Yep! They are running on top of Linux (or maybe they installed the BASH shell in Windows 10.)

# Exploitation

Read the article at <https://www.digitalocean.com/community/questions/how-do-i-dump-an-sqlite-database>. It will show you how to dump the database so you can find the answer to the challenge.

# Hand In

1. Show the commands you used to dump the database.
2. What is the first name of the new employee with the last name Chan?