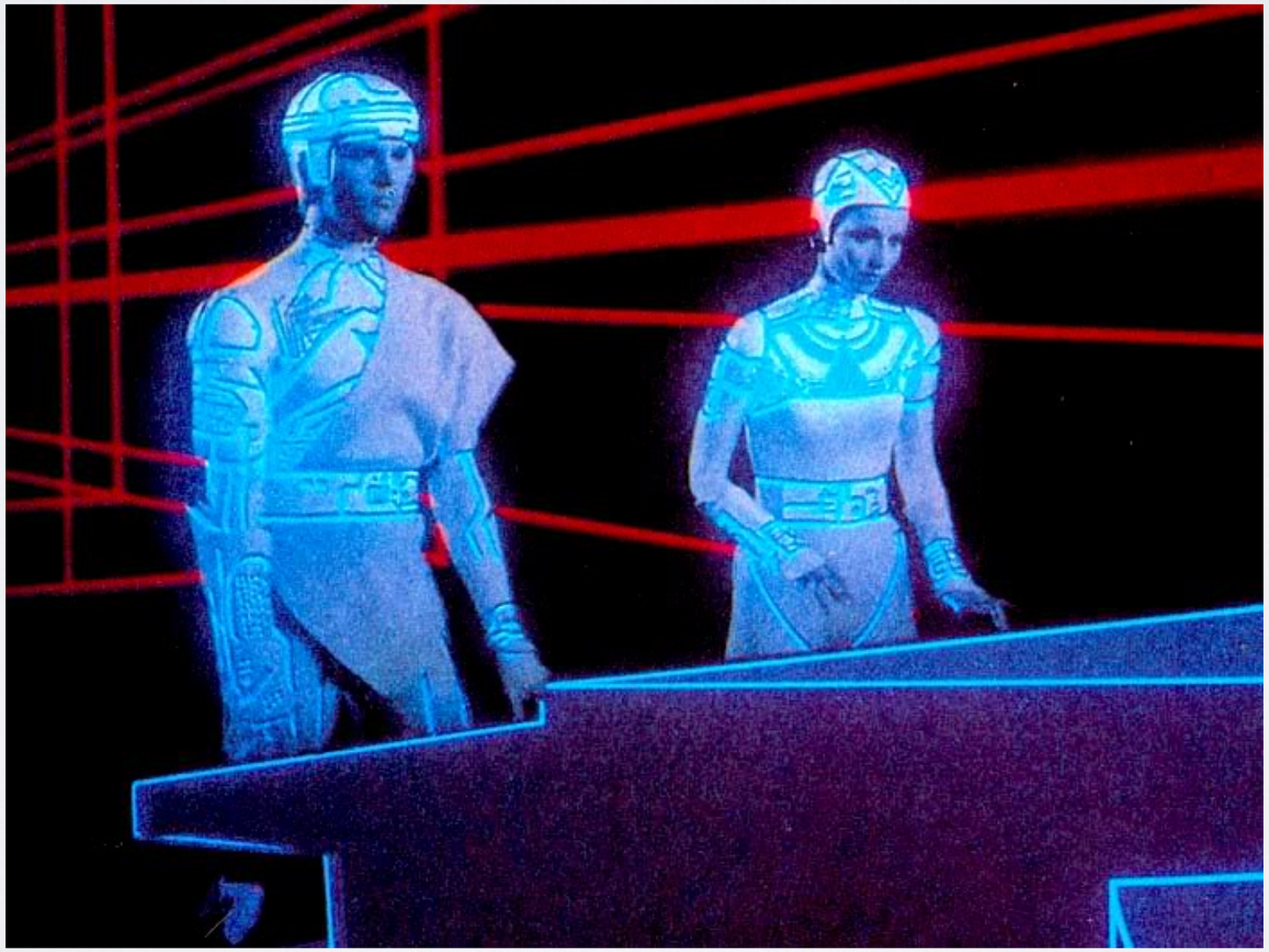
THE ACCIDENTAL SYSADMIN

Or, how I learned to stop worrying and love the terminal



A **system administrator**, or **sysadmin**, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers.

System administrator - Wikipedia, the free encyclopedia

https://en.wikipedia.org/wiki/**System_administrator** Wikipedia

WHAT IS A SYSADMIN?

I have no idea what I'm doing.

I LOVE YOU, LAMP

We're going to set up and configure
a LAMP server using Digital Ocean

WHAT IS LAMP?

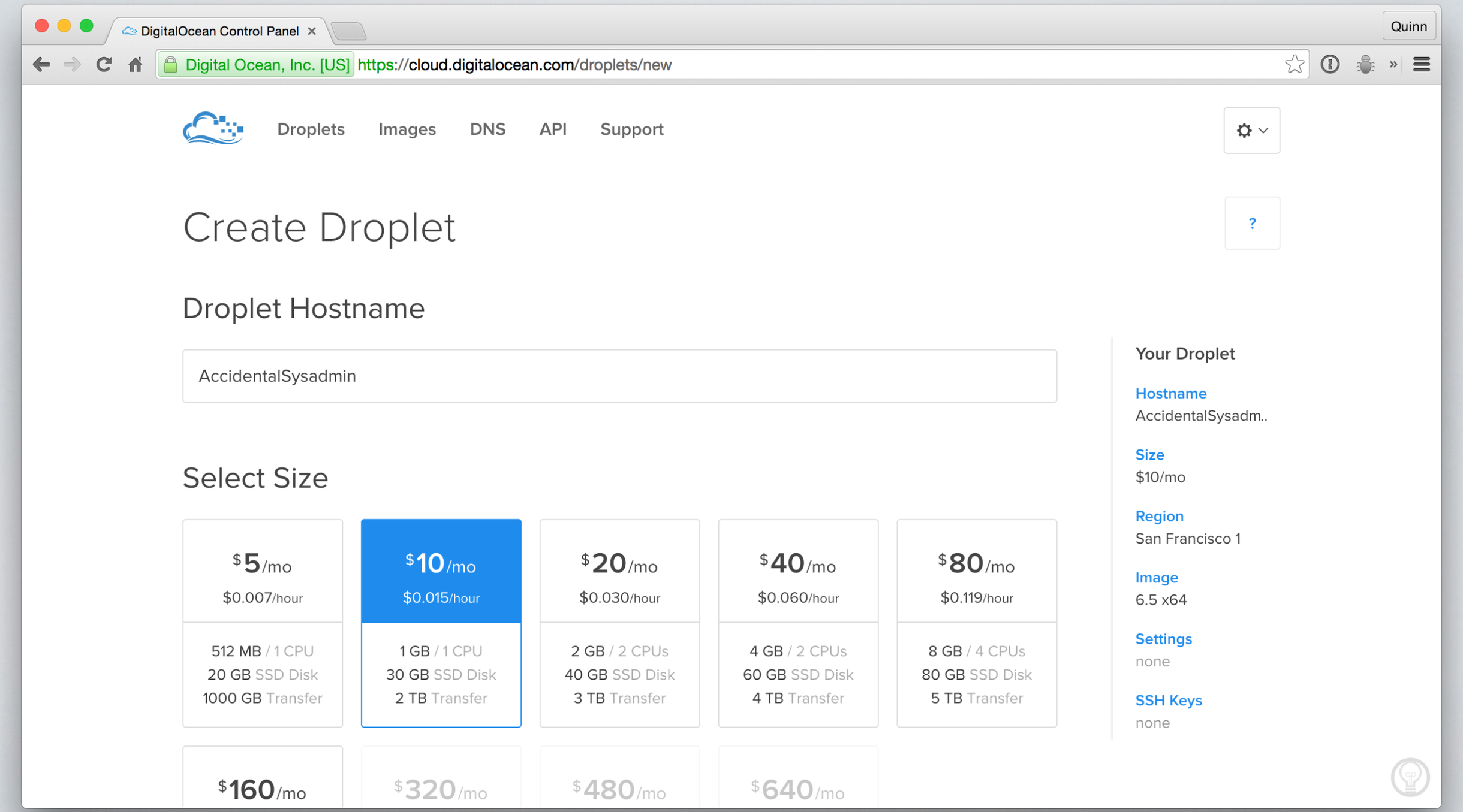
LAMP is an acronym for a "web application stack", consisting of:

- Linux
- Apache
- MySQL
- PHP

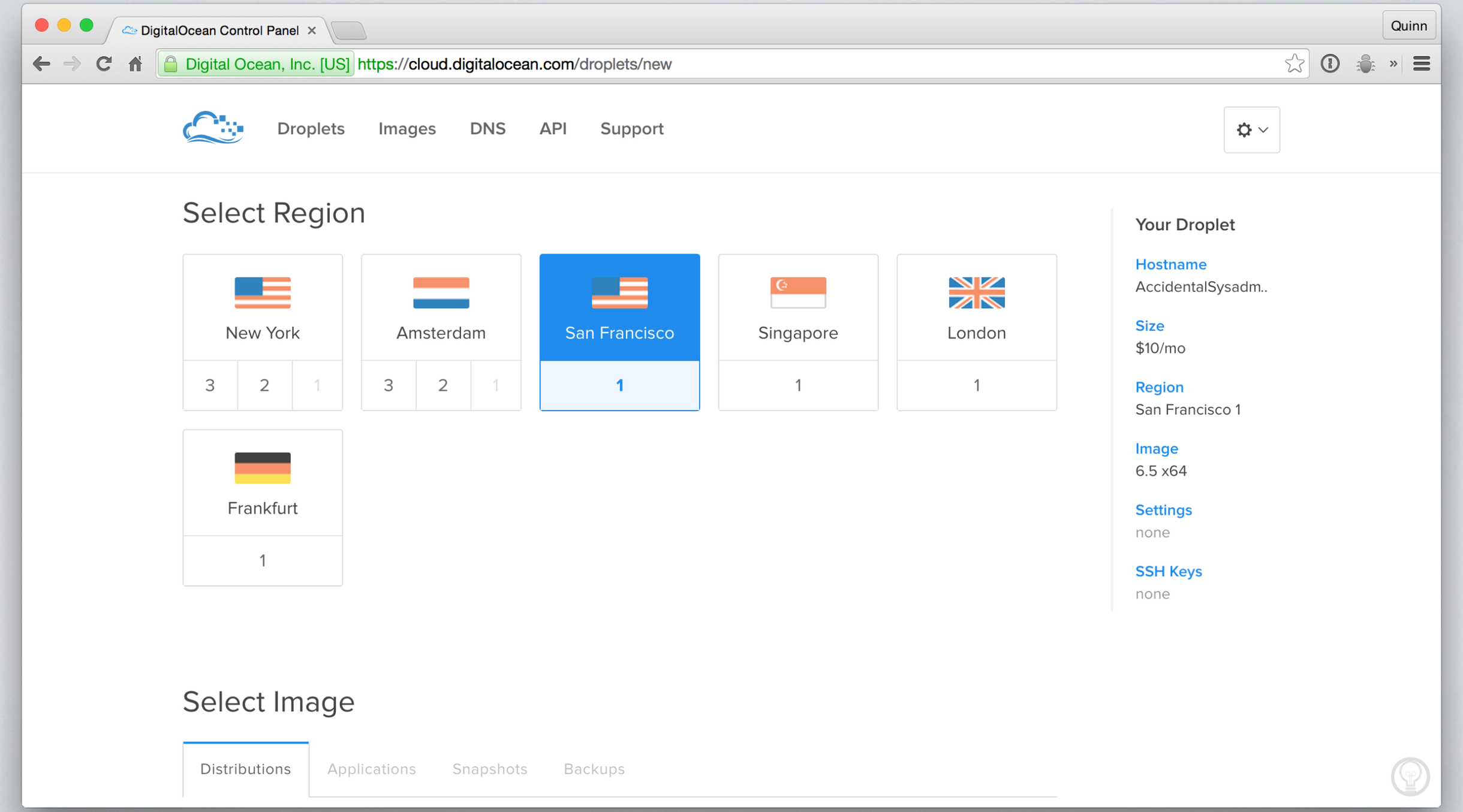
WHY DIGITAL OCEAN?

- Fast to set up and deploy
- Simple, uncluttered interface
- Free to get started
- $10 credit when signing up via http://bit.ly/accidentalsysadmin

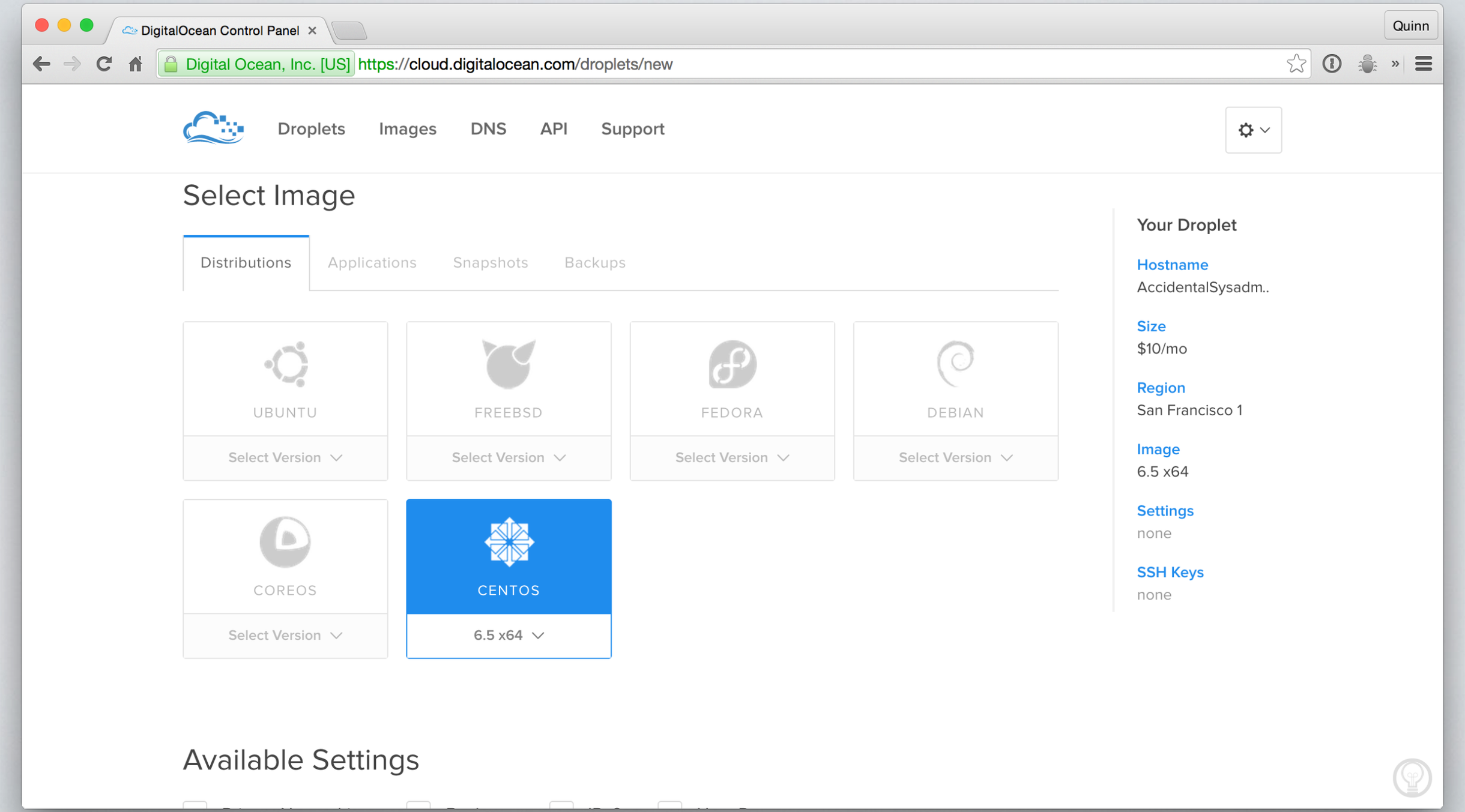
“DROPLET” IS A FUNNY WORD



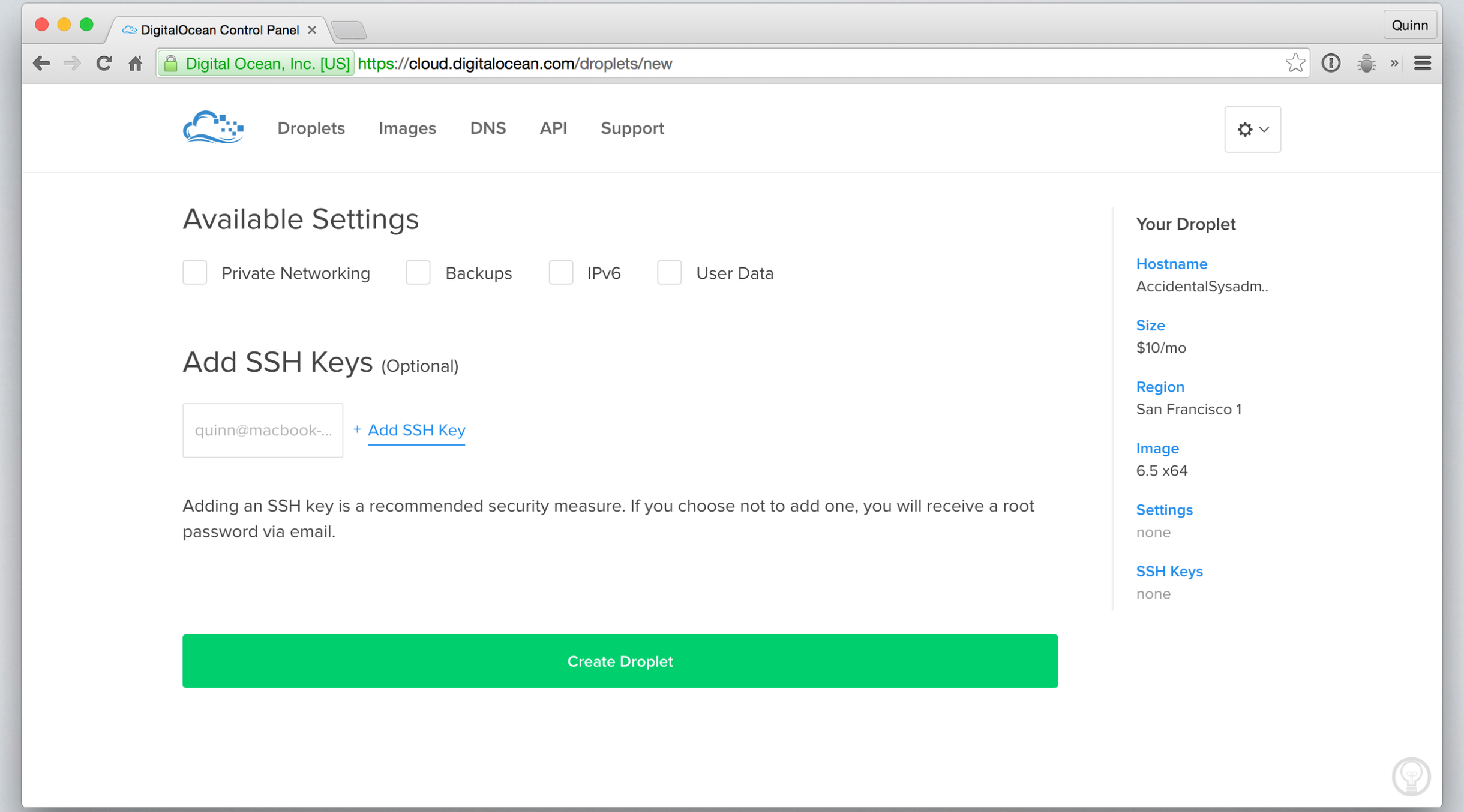
GO GIANTS!


DigitalOcean Control Panel
Quinn
Digital Ocean, Inc. [US] https://cloud.digitalocean.com/droplets/new
Droplets
Images
DNS
API
Support
Select Region
New York
3
2
1
Amsterdam
3
2
1
San Francisco
1
Singapore
1
London
1
Frankfurt
1
Your Droplet
Hostname
AccidentalSysadm..
Size
$10/mo
Region
San Francisco 1
Image
6.5 x64
Settings
none
SSH Keys
none
Select Image
Distributions
Applications
Snapshots
Backups

PICK AN OS, ANY OS



MORE OPTIONS?!



KILL YOUR PASSWORD

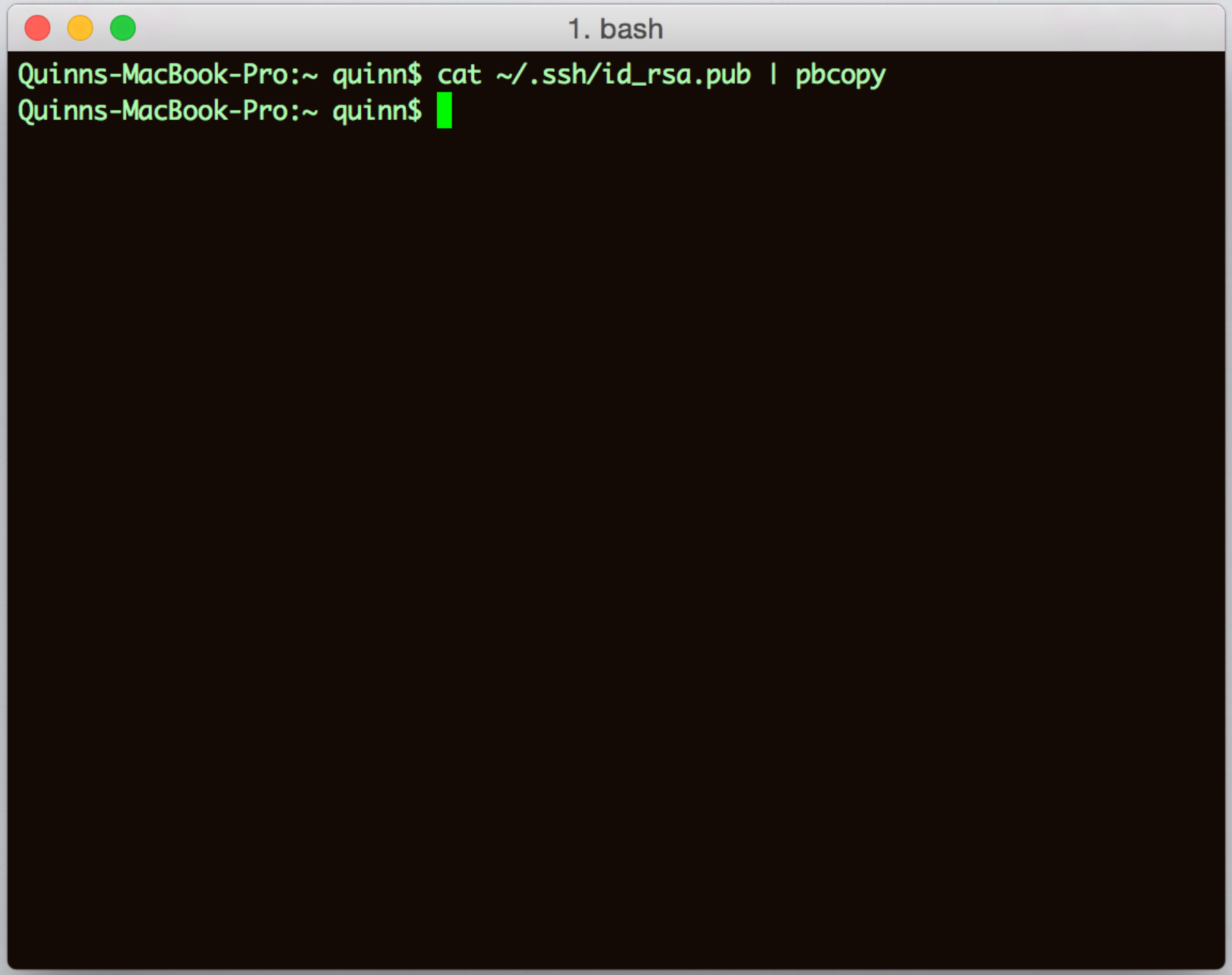
`ssh-keygen`

1. bash

```
Quinns-MacBook-Pro:~ quinn$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/quinn/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/quinn/.ssh/id_rsa.
Your public key has been saved in /Users/quinn/.ssh/id_rsa.pub.
The key fingerprint is:
6c:e1:34:38:ea:fe:59:1c:2b:de:0c:93:d0:7e:2a:87 quinn@Quinns-MacBook-Pro.local
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|        .        |
|       o +       |
|      o = o      |
|     o . S       |
|    . o + o      |
|     ..* =       |
|    .E..@        |
|     .+= o       |
+-----------------+
Quinns-MacBook-Pro:~ quinn$
```

COPY TO CLIPBOARD

```
cat ~/.ssh/id_rsa.pub | pbcopy
```



VI IS THE TEXT EDITOR FROM HELL

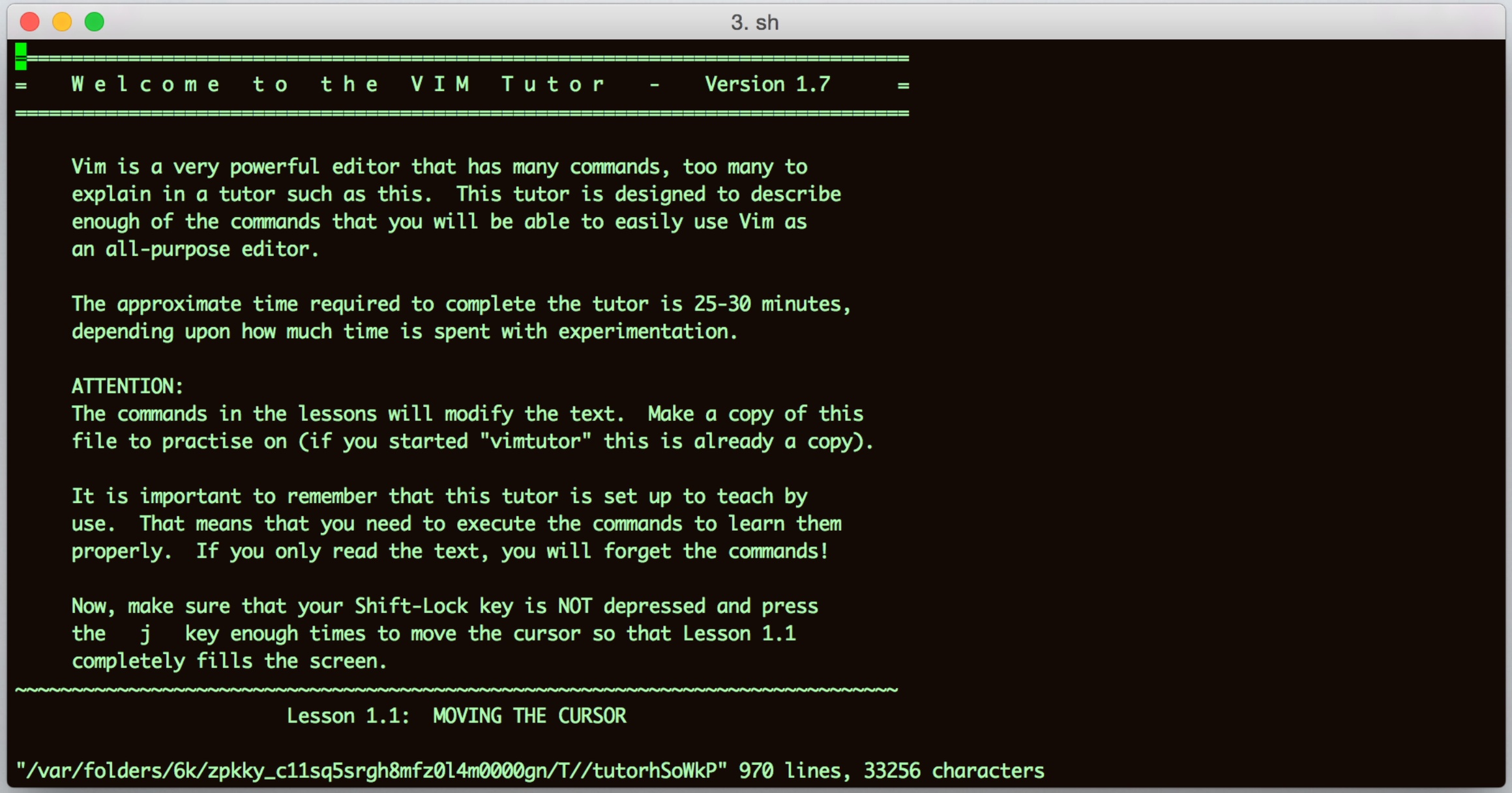
Honestly, getting your head around Vi is the hardest part of any of this.

*"Some people say **vye**, some say **vee-eye** (the vi manual suggests this) and some Roman numerologists say **six**."*

http://ss64.com/bash/syntax-pronounce.html

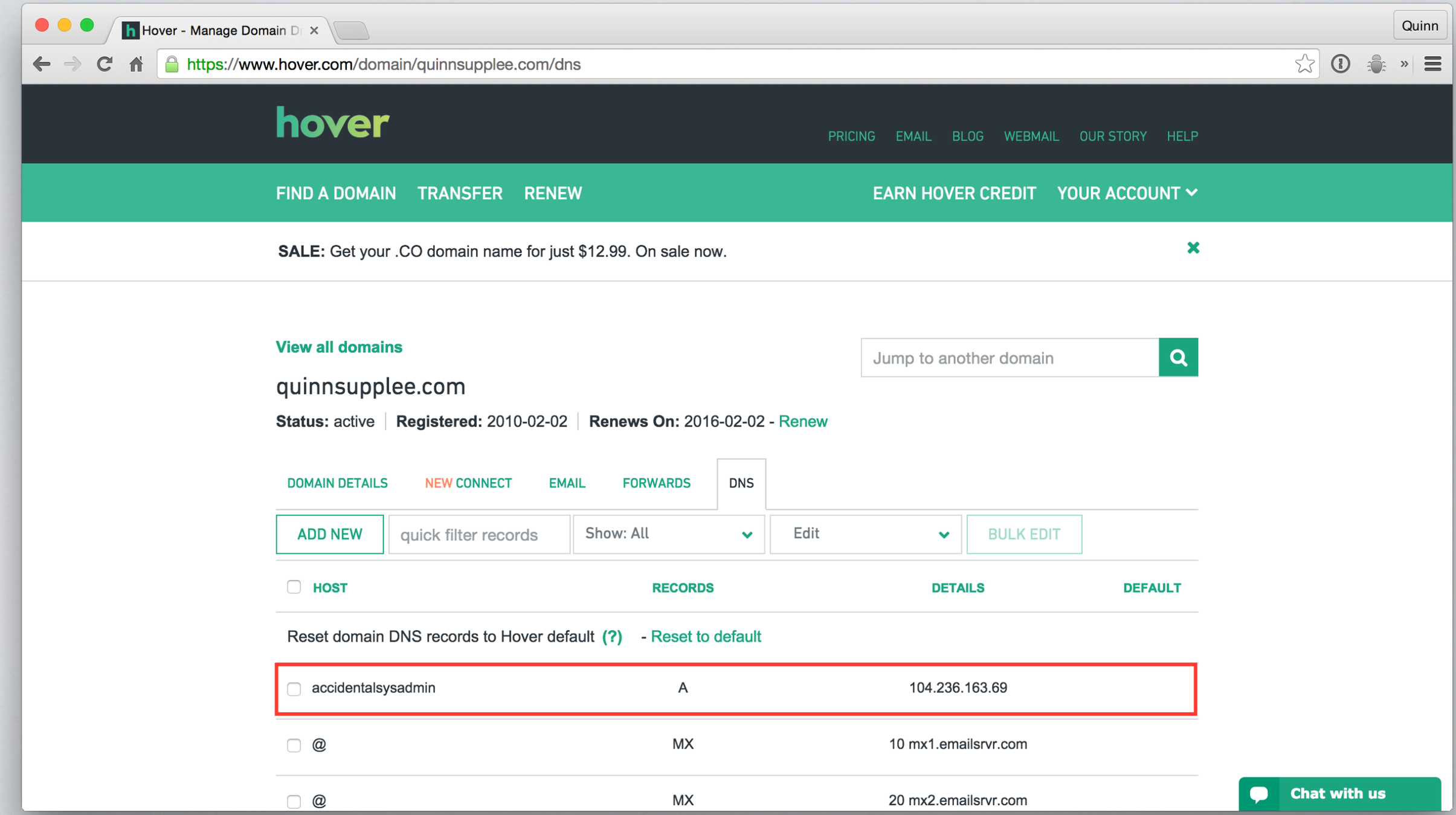
BUT, VI/VIM WILL TEACH YOU HOW TO USE IT

```
vimtutor
```



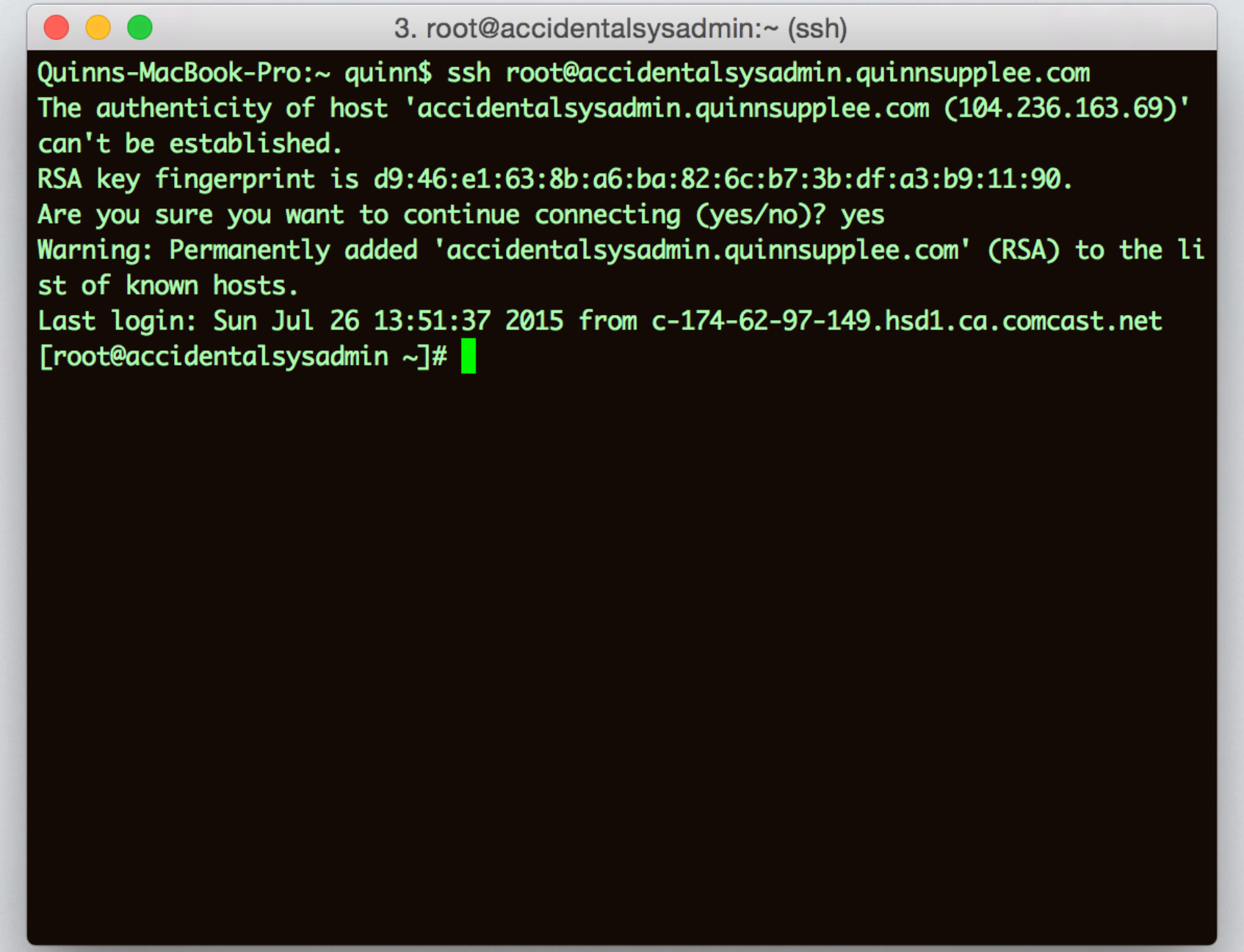
SET UP YOUR DOMAIN

Or, sub-domain



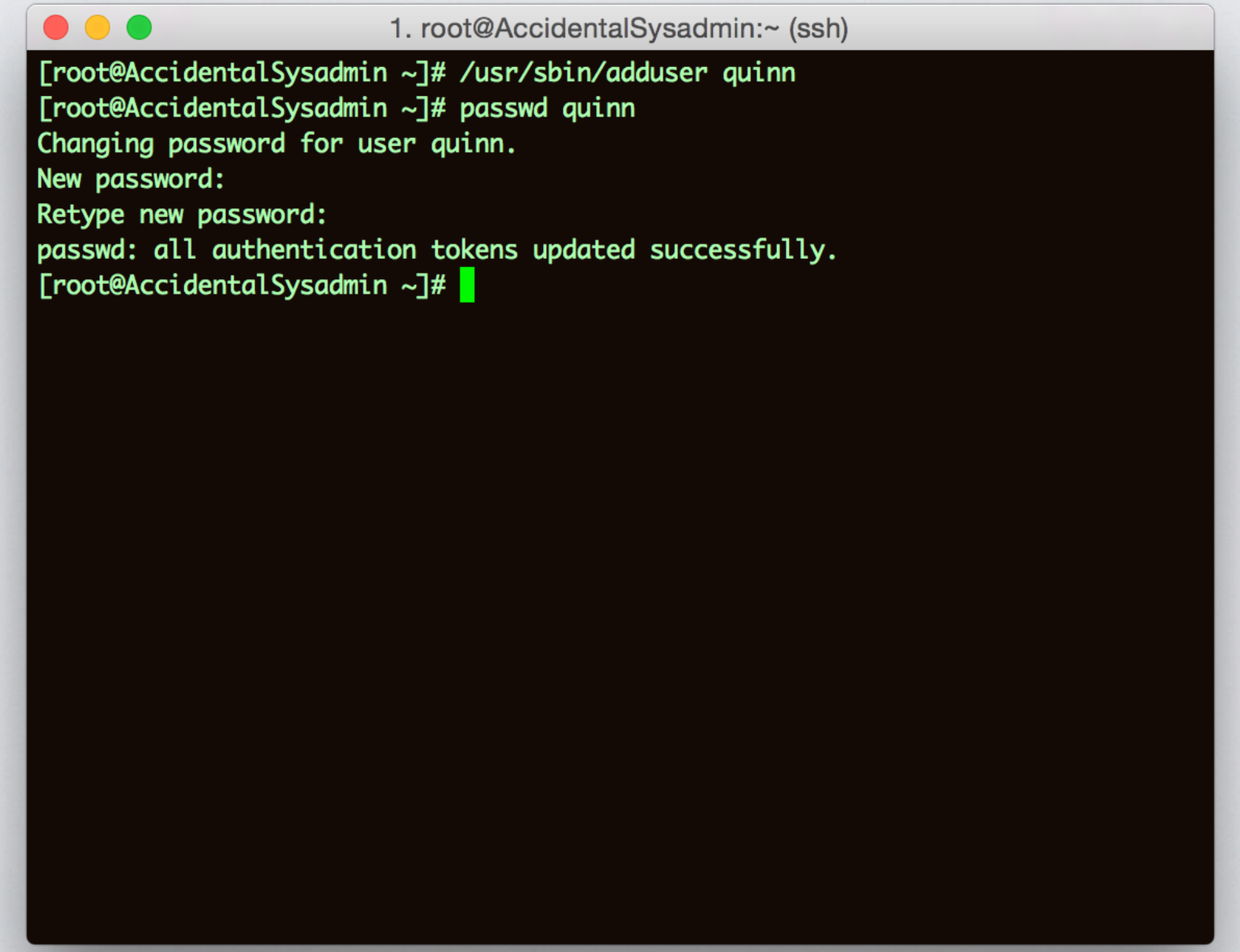
NOW LET'S START HACKIN'

```
ssh root@accidentalsysadmin.quinnsupplee.com
```



CREATE A NEW USER

```
/usr/sbin/adduser quinn
passwd quinn
```



CHANGE DEFAULT SSH PORT

Change the line that says "Port 22"

```
Port 22022
```

3. root@accidentalsysadmin:~ (ssh)

```
#       $OpenBSD: sshd_config,v 1.80 2008/07/02 02:24:18 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options change a
# default value.

#Port 22
Port 22022
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# Disable legacy (protocol version 1) support in the server for new
# installations. In future the default will change to require explicit
# activation of protocol 1
Protocol 2

# HostKey for protocol version 1
"/etc/ssh/sshd_config" 141L, 3910C
```

DISABLE ROOT LOGIN

```
PermitRootLogin no
```

3. root@accidentalsysadmin:~ (ssh)

```
#ServerKeyBits 1024

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PermitRootLogin no

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authorized_keys
#AuthorizedKeysCommand none
#AuthorizedKeysCommandRunAs nobody
```

GIVE YOURSELF SUPERPOWERS

Edit your **sudo** configuration to grant root power to your new user

```
/usr/sbin/visudo
```

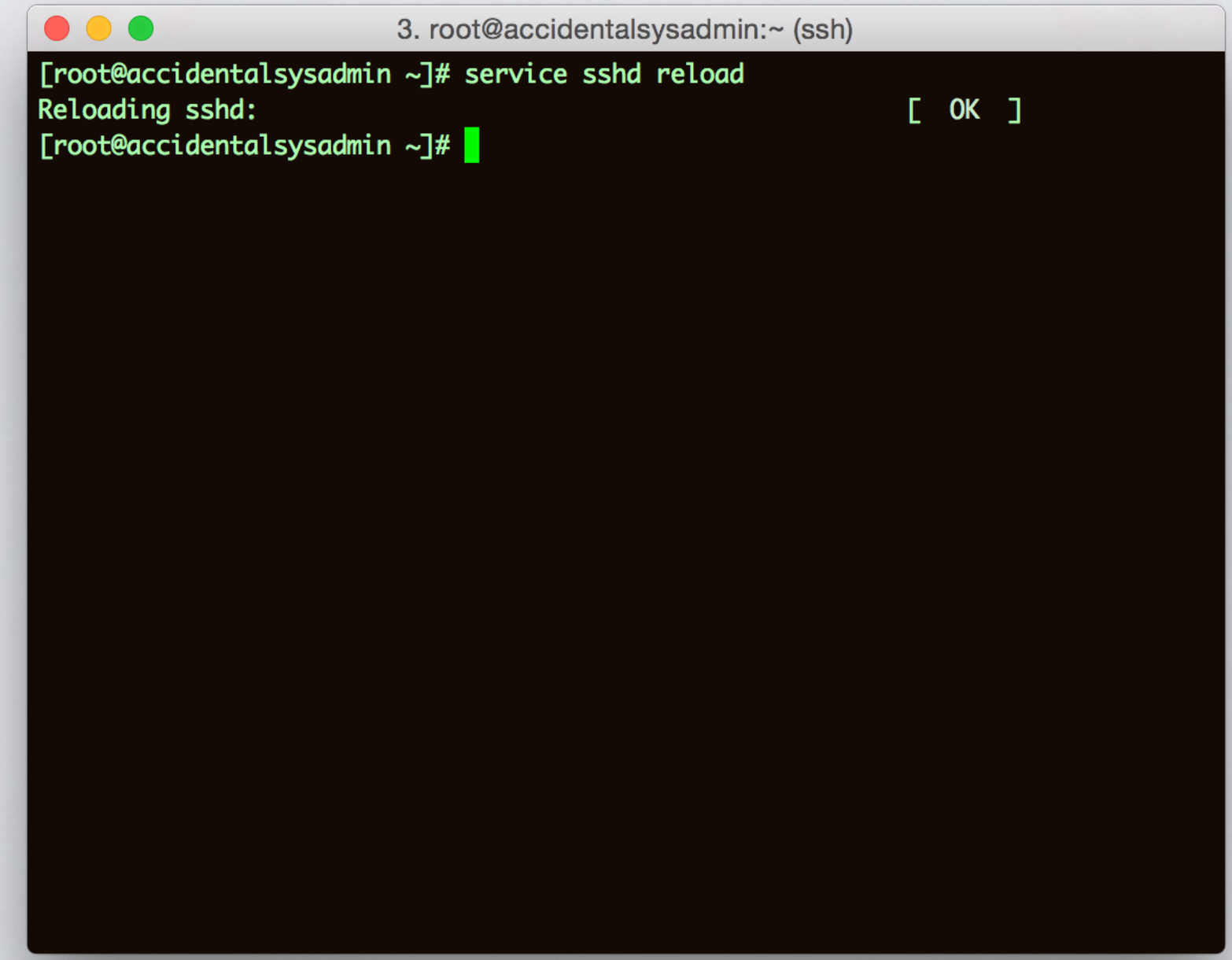
Find the line "`root  ALL=(ALL)  ALL`",
and add, below it:

```
"quinn     ALL=(ALL)          ALL"
```

Save and exit Vi *(Hahahahahaha!)*

RELOAD SSH SERVICE

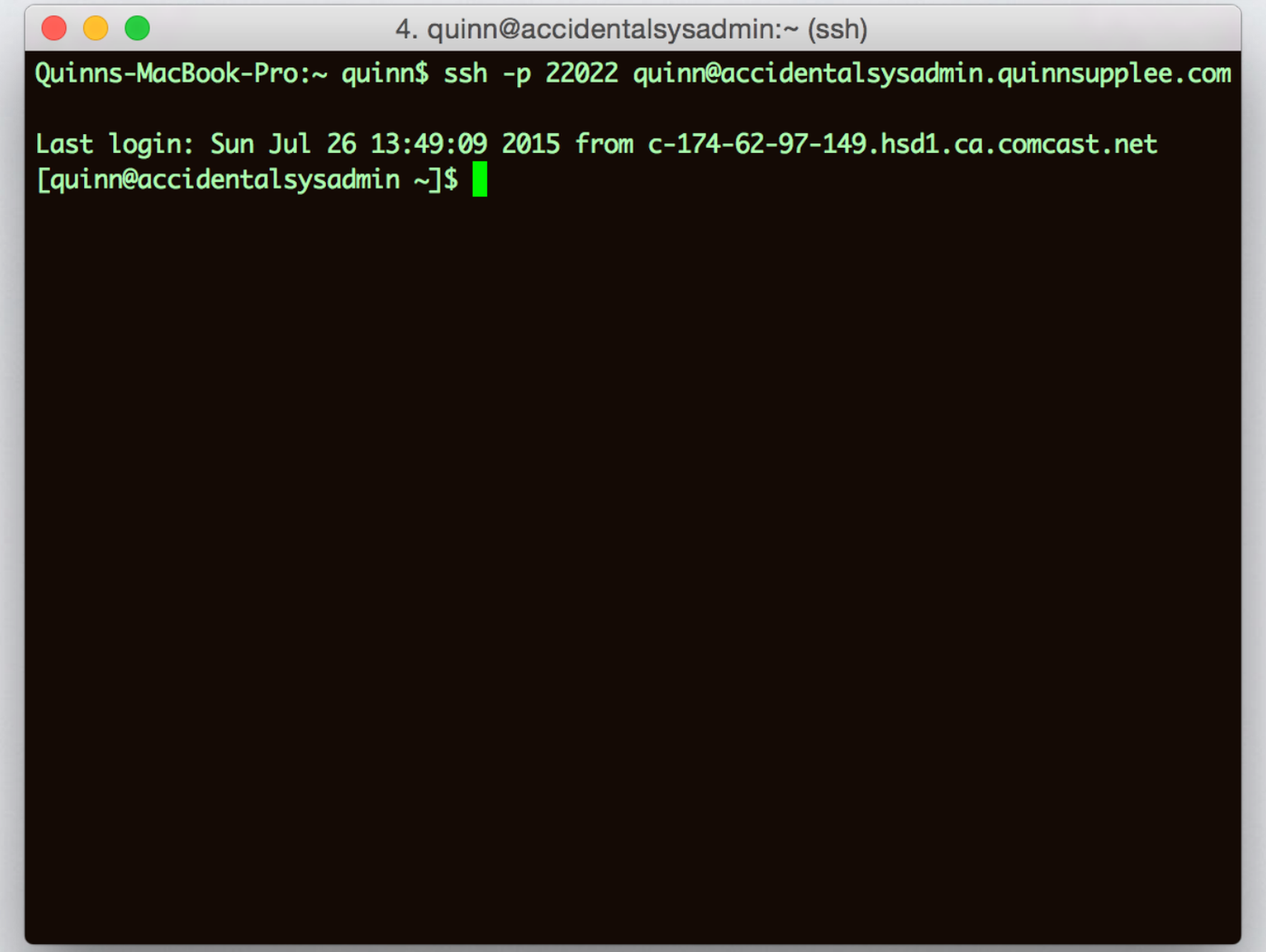
```
service sshd reload
```



LOG IN AS YOUR NEW USER

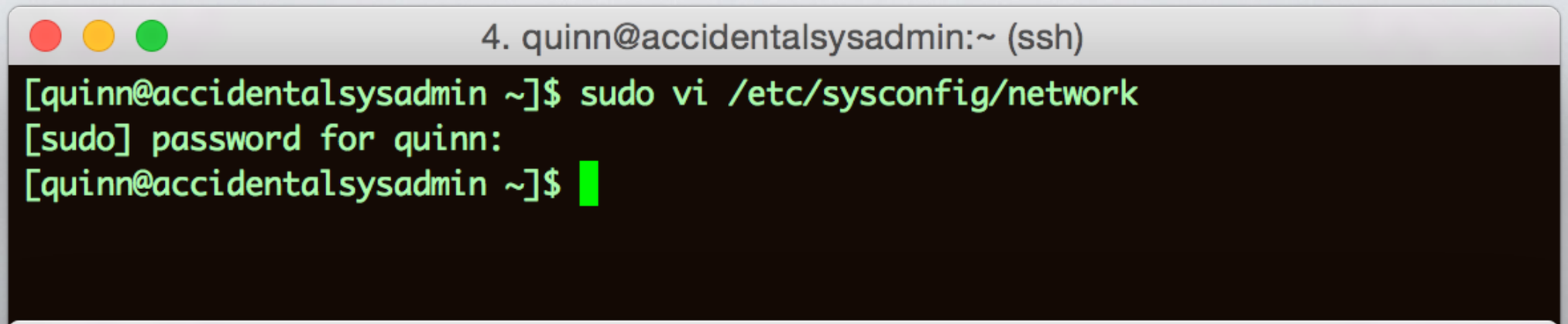
Keep "root" session running for now, so in a new terminal window:

```
ssh -p 22022 quinn@accidentalsysadmin.quinnsupplee.com
```



SET UP THE HOSTNAME

```
sudo /etc/sysconfig/network
```



Yum is a package manager for Linux. To download and install many components of Linux, you just need to type:

```
sudo yum install <program>
```

The **Yellowdog Updater, Modified** (**yum**) is an open-source command-line package-management utility for **Linux** operating systems using the RPM Package Manager. Though **yum** has a command-line interface, several other tools provide graphical user interfaces to **yum** functionality.

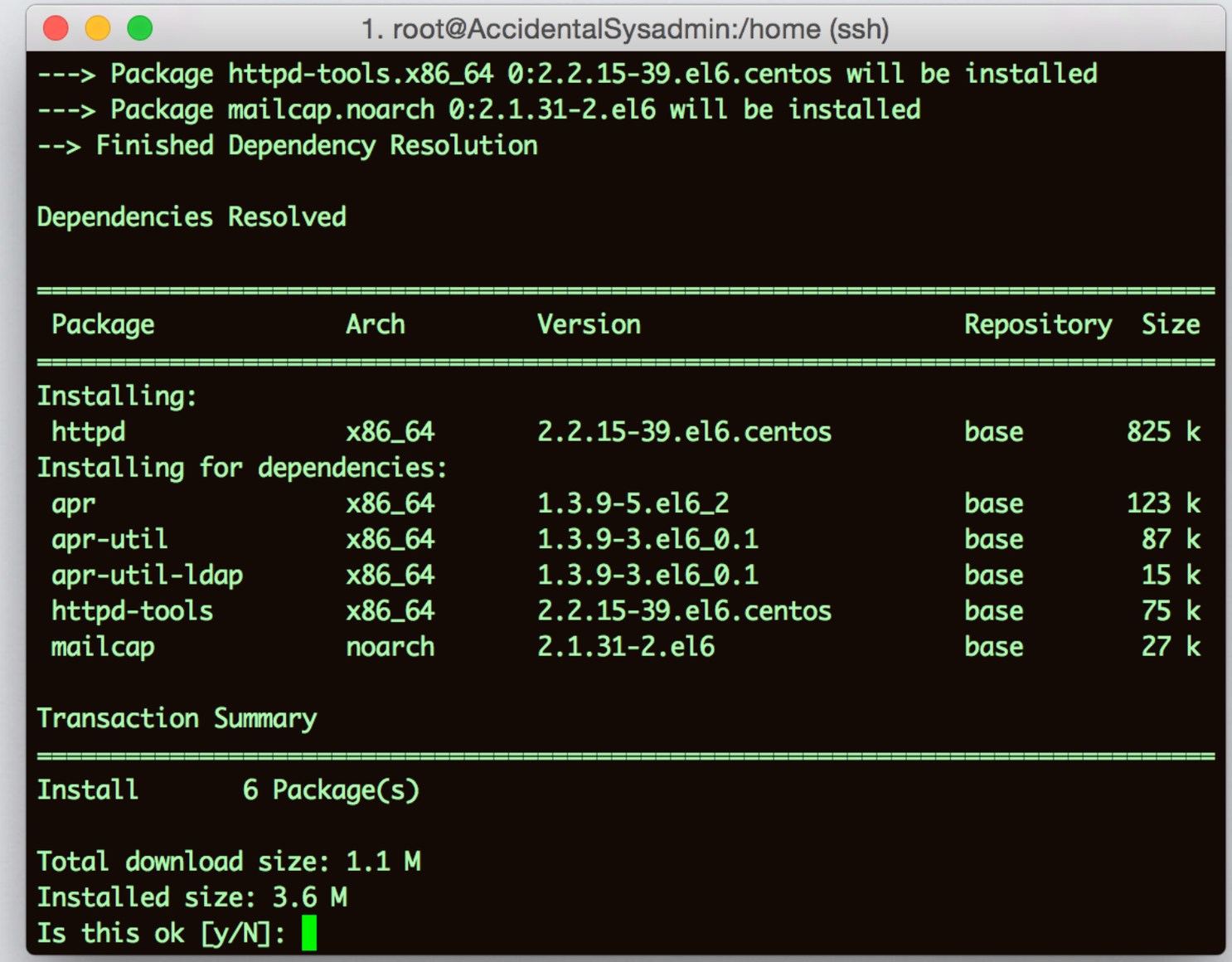
Yum - Wikipedia

https://en.wikipedia.org/wiki/Yellowdog_Updater,_Modified Wikipedia

OK, LET'S GET LAMP'D

GIVE ME AN "A" (APACHE)

```
sudo yum install httpd
```



Hey! We just installed a web server!

START APACHE

Once HTTPD is installed, let's tell it what the server name is

```
vi /etc/httpd/conf/httpd.conf
```

Find "ServerName" and add:

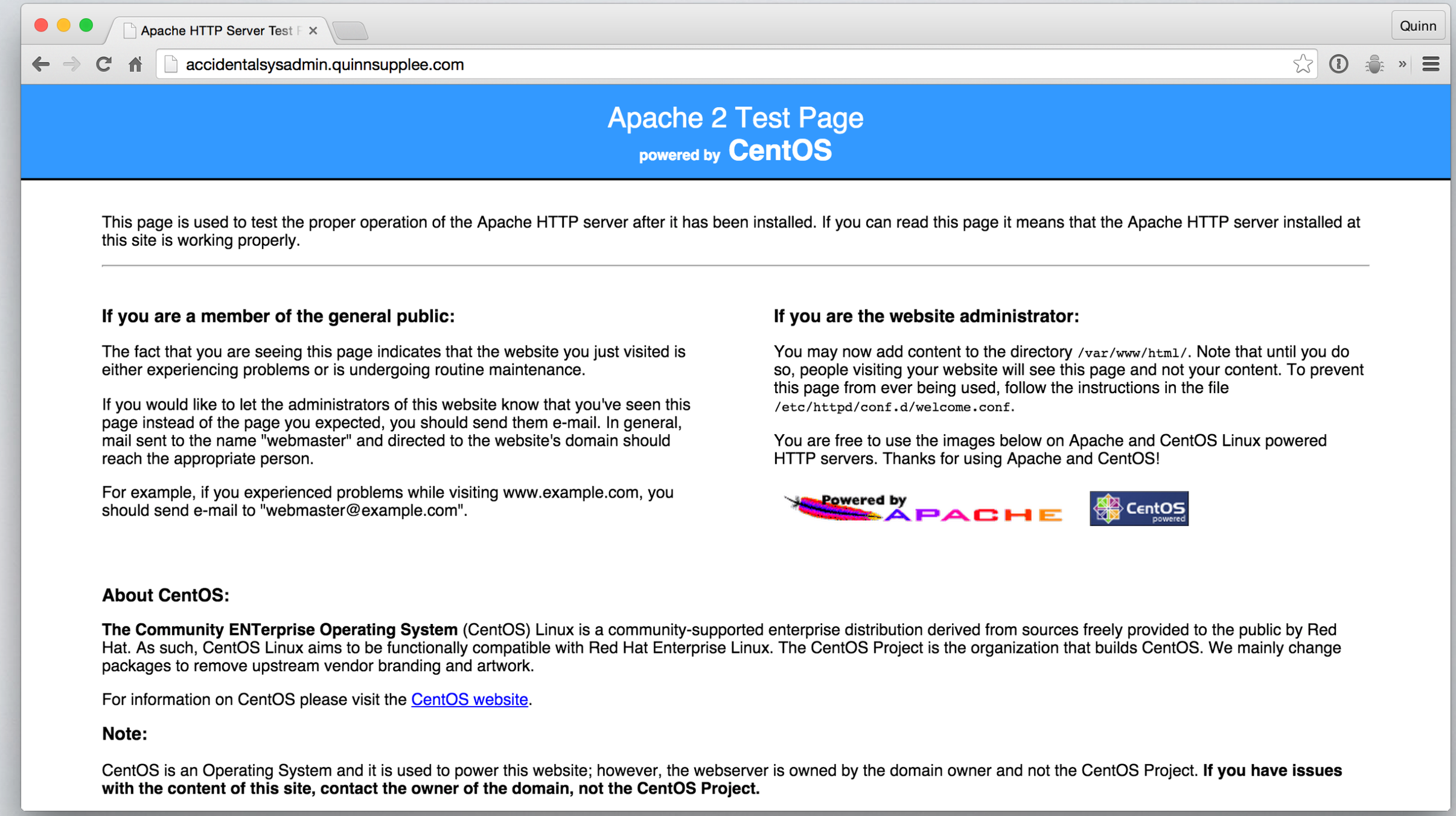
```
ServerName accidentalsysadmin.quinnsupplee.com
```

Save and exit

```
service httpd start
```

Now go see your site! http://accidentalsysadmin.quinnsupplee.com

IT'S JUST LIKE A NEW BABY



GIVE ME AN "M" (MYSQL)

```
sudo yum install mysql-server
sudo service mysqld start
```

Now, MySQL should be running. Let's secure it!

```
sudo /usr/bin/mysql_secure_installation
```

Press ENTER to all prompts.
Be sure to provide a strong password and store it somewhere safe.

GIVE ME A "P" (PHP)

Now we're going to install PHP with MySQL support

```
yum install php php-mysql
```

And we can check our PHP configuration by adding a quick info file:

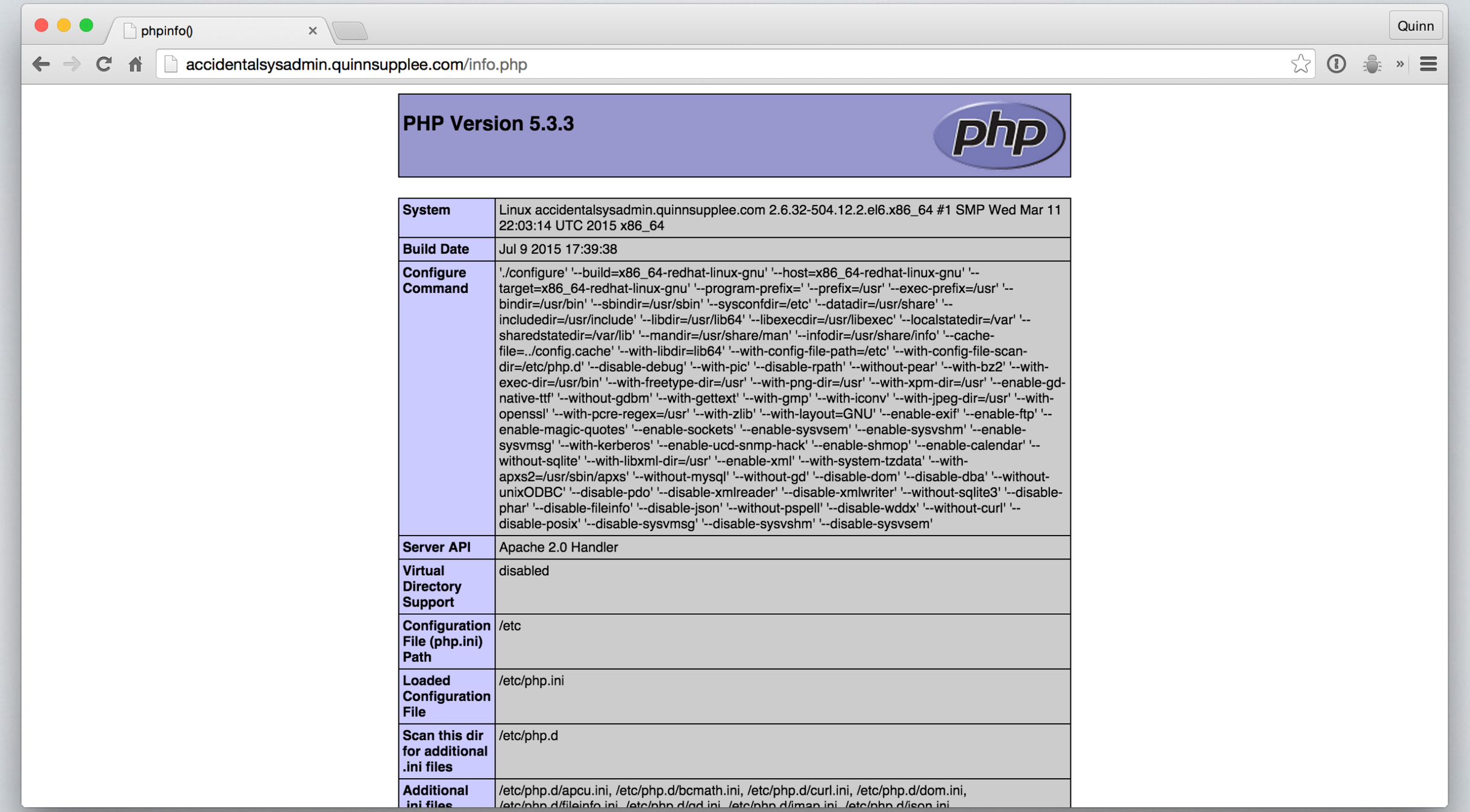
```
vi info.php

<?php phpinfo(); ?>
```

Save and exit

Then check it out at:
http://accidentalsysadmin.quinnsupplee.com/info.php

CHECK THE PHP SWEETNESS



THAT WAS EASY!

Let's install some additional PHP modules!

```
sudo yum install php-cli php-fpm php-cgi php-
mysql php-xmlrpc php-curl php-gd php-apc php-
pear php-imap php-mcrypt php-pspell
```

There are lots more you may be interested in. To get a list of available PHP modules, type:

```
yum search php-
```

A FEW MORE THINGS

Now let's make sure PHP and MySQL start on every server reboot:

```
sudo chkconfig httpd on
sudo chkconfig mysqld on
```

Let's install some other stuff we'll surely need:

```
sudo yum install zip unzip gzip rsync wget
```

I CAN HAZ PHPMYADMIN?

Let's install and setup phpMyAdmin

```
sudo yum install wget

cd ~

wget http://download.fedoraproject.org/pub/
epel/6/x86_64/epel-release-6-8.noarch.rpm

sudo yum install phpmyadmin
```

CONFIGURE PHPMYADMIN

Let's configure and secure phpMyAdmin

```
sudo vi /etc/httpd/conf.d/phpMyAdmin.conf
```

You want to replace all instances of **127.0.0.1**
with your own **local IP address**

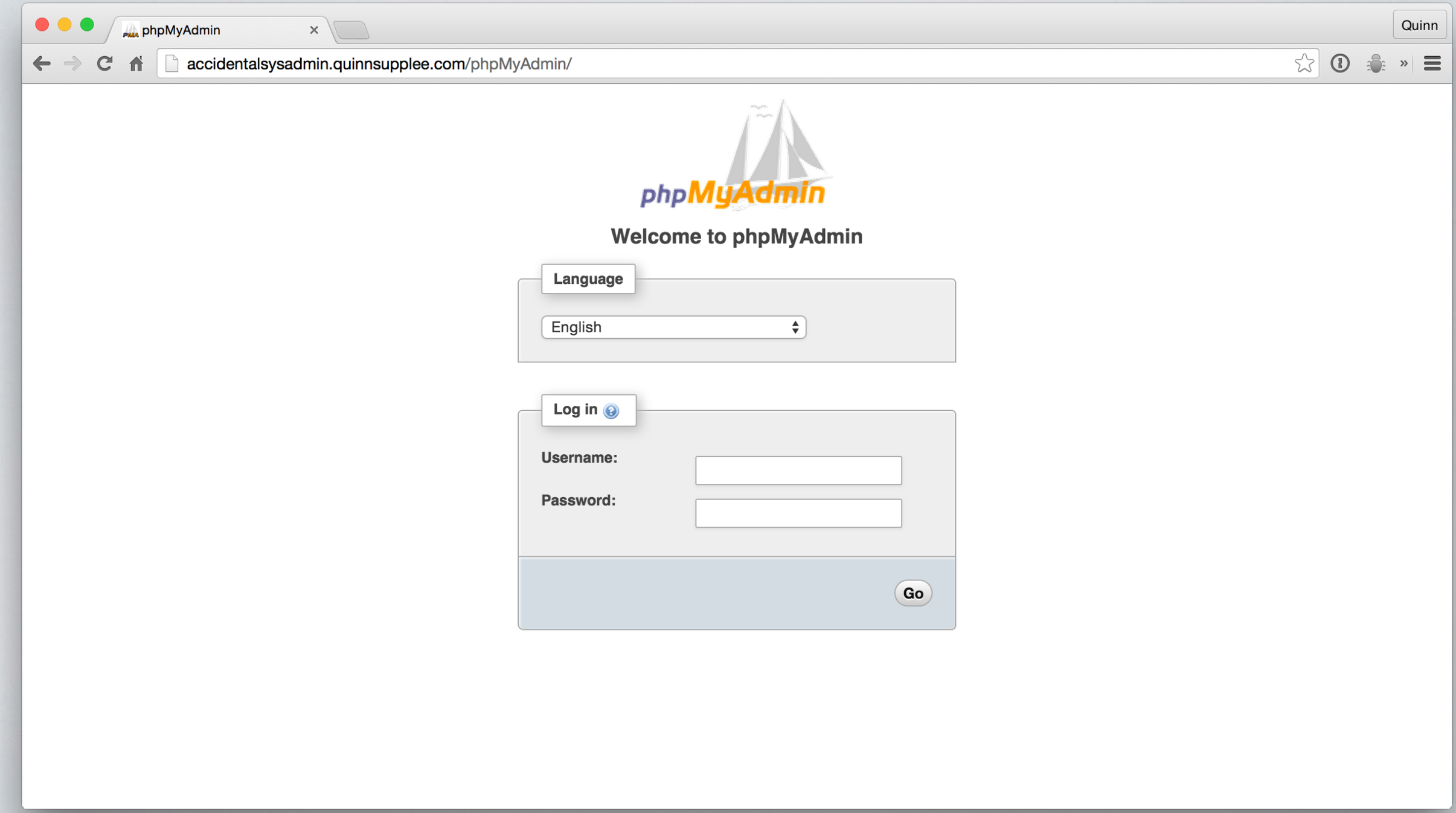
Do it manually or with a find-replace:

```
:%s/127.0.0.1/255.255.255.255/g
```

Now restart apache:

```
sudo service httpd restart
```

VISIT YOUR NEW PHPMYADMIN



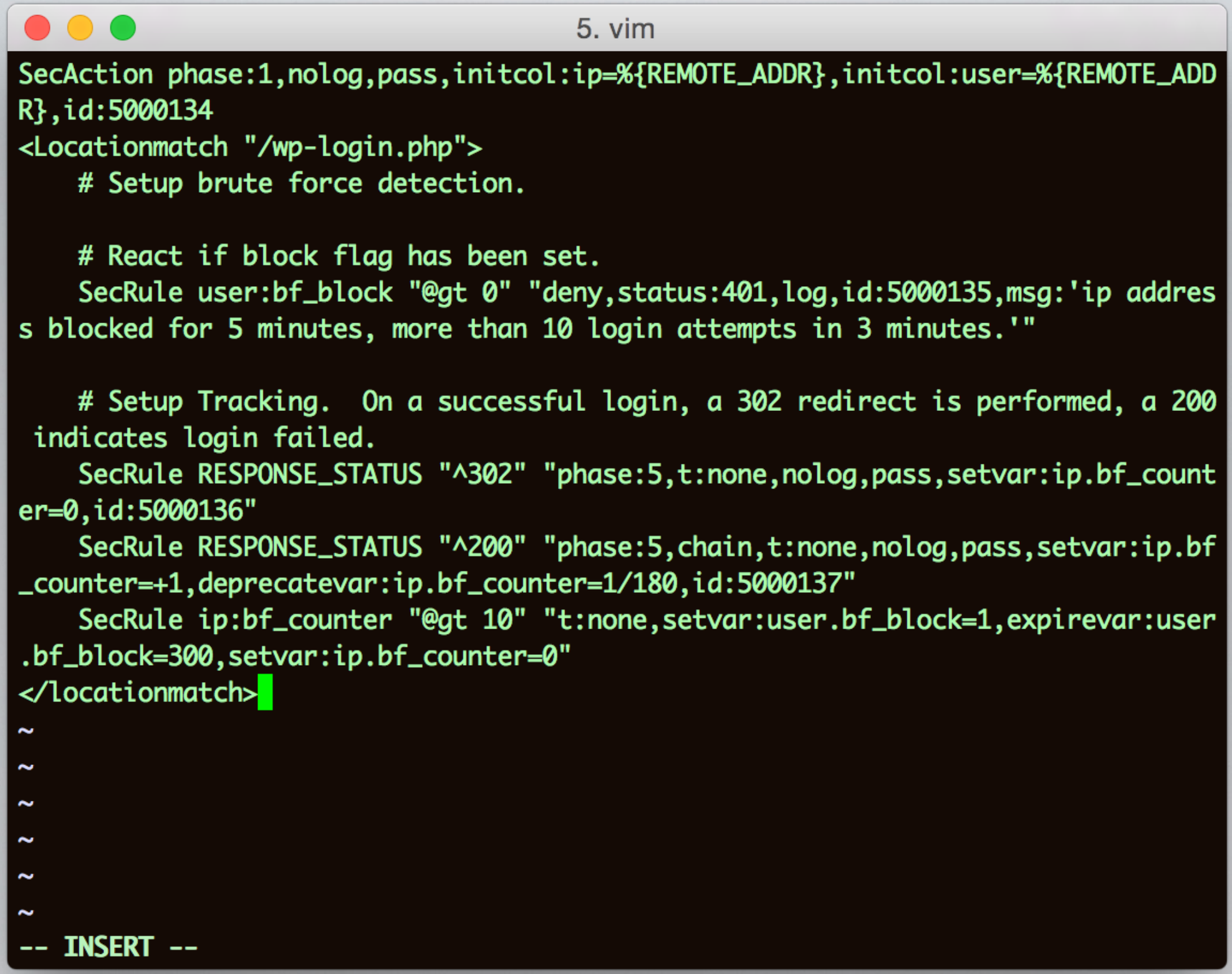
LET'S INSTALL MOD_SECURITY

```
sudo yum install pcre* libxml2* libcurl* lua*
libtool openssl mod_security
```

Now let's add some custom WP-focused brute-force protection to it:

```
sudo vi /etc/httpd/conf.d/mod_security.conf
```

Add to end of file, right BEFORE closing **</IfModule>**…



https://halfelf.org/2013/wp-login-protection-modsec/

WORDPRESS, THE NINJA METHOD

LET'S INSTALL WP-CLI

WP-CLI is a Swiss Army Knife for WordPress management

```
cd ~

curl -O https://raw.githubusercontent.com/wp-cli/builds/gh-pages/phar/wp-cli.phar

sudo chmod +x wp-cli.phar

sudo mv wp-cli.phar /usr/local/bin/wp
```

http://wp-cli.org/

SET UP DB AND ROCK WP

Using phpMyAdmin, create a new user, a database,
and grant all permissions:

username: accidentalsys
password: w0rdpr3ssSVCKS

Back in Terminal:

```
cd /var/www/
sudo chown -R quinn.quinn html
cd html
wp core download
```

RUN THE "5-MINUTE WP INSTALLER"

Below you should enter your database connection details. If you're not sure about these, contact your host.

Database Name	accidentalsys	The name of the database you want to run WP in.
User Name	accidentalsys	Your MySQL username
Password	w0rdpr3ssSVCKS	...and your MySQL password.
Database Host	localhost	You should be able to get this info from your web host, if `localhost` does not work.
Table Prefix	wp_	If you want to run multiple WordPress installations in a single database, change this.

Submit

LET'S SECURE OUR WP INSTALLATION

Make sure you aren't using "admin" as your admin username
Make sure you have a wicked-strong password

Install some super useful security plugins

```
wp plugin install sucuri-scanner
wp plugin install login-lockdown
```

Create and secure our WP Uploads directory

```
mkdir wp-content/uploads
sudo chown apache.apache wp-content/uploads
```

Enable and configure Sucuri Scanner and Login Lockdown plugins

WP HARDENING, CONTINUED

Disable file editing from within WordPress. Add to **wp-config.php**:

```
define('DISALLOW_FILE_EDIT',true);
```

Disable PHP execution from within **wp-content** and **uploads** directories.

Create a **.htaccess** file in **wp-content** and **wp-content/uploads**, and add:

```
<Files *.php>
deny from all
</Files>
```

SET UP THE MAIN .HTACCESS FILE

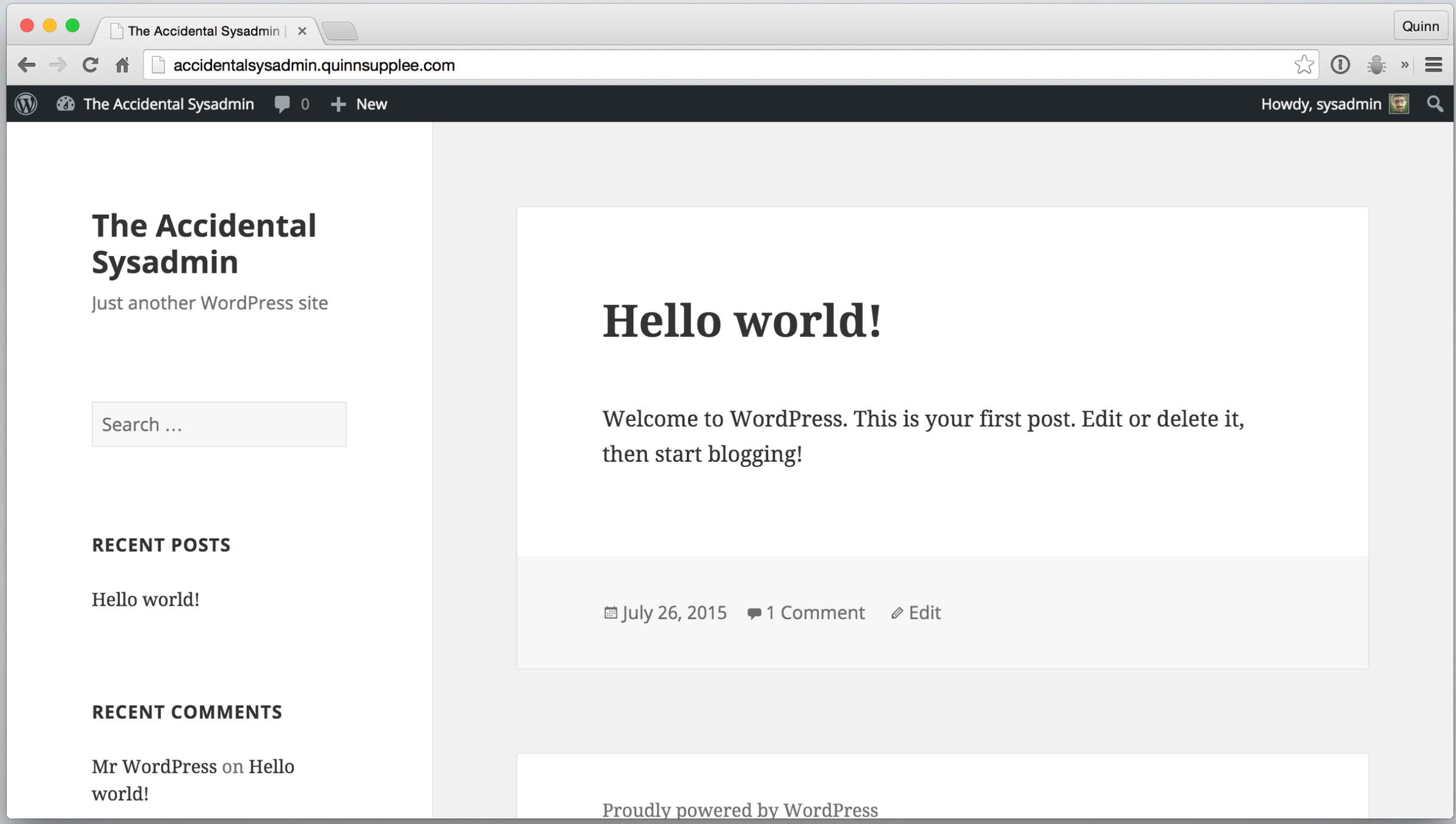
Mine looks like this. Yours might look different.

```
# Block the include-only files.
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^wp-admin/includes/ - [F,L]
RewriteRule !^wp-includes/ - [S=3]
RewriteRule ^wp-includes/[^/]+\.php$ - [F,L]
RewriteRule ^wp-includes/js/tinymce/langs/.+\.php - [F,L]
RewriteRule ^wp-includes/theme-compat/ - [F,L]
</IfModule>

# Block access to wp-config.php
<files wp-config.php>
order allow,deny
deny from all
</files>

# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
</IfModule>
# END WordPress
```

ENJOY YOUR NEW, SECURE WORDPRESS INSTALLATION



OTHER THINGS OF INTEREST

Fail2Ban
http://www.fail2ban.org/

ModPagespeed
https://developers.google.com/speed/pagespeed/module/

DenyHosts
http://denyhosts.sourceforge.net/

AWStats
http://www.awstats.org/

Apache ModInfo
https://httpd.apache.org/docs/2.2/mod/mod_info.html

Apache ModStatus
https://httpd.apache.org/docs/2.2/mod/mod_status.html

LINKS AND REFERENCES

A command line interface for WordPress
http://bit.ly/1fyBsdh

Basic vi Commands
http://bit.ly/1OvsQQ3

Red Hat / CentOS Install mod_security Apache Intrusion Detection And Prevention Engine
http://bit.ly/1gYweZl

How to Change the Hostname of a Linux System
http://bit.ly/1gf35ZK

Vi Cheat Sheet
http://bit.ly/1OvsWHz

What is my IP address?
http://bit.ly/1KsOtzT

How to harden Apache web server with mod_security and mod_evasive on CentOS
http://bit.ly/1estpxQ

Hardening WordPress
http://bit.ly/1MsblBT

WordPress Login Protection with ModSecurity
http://bit.ly/1Mvykgk

LINKS AND REFERENCES

What are PHP extensions and libraries WP needs and/or uses?
http://bit.ly/1GT1vBV

How To Get Started With mod_pagespeed with Apache on a CentOS and Fedora Cloud Server
http://do.co/1JJtFRF

How To Install DenyHosts on CentOS 6
http://do.co/113QQGb

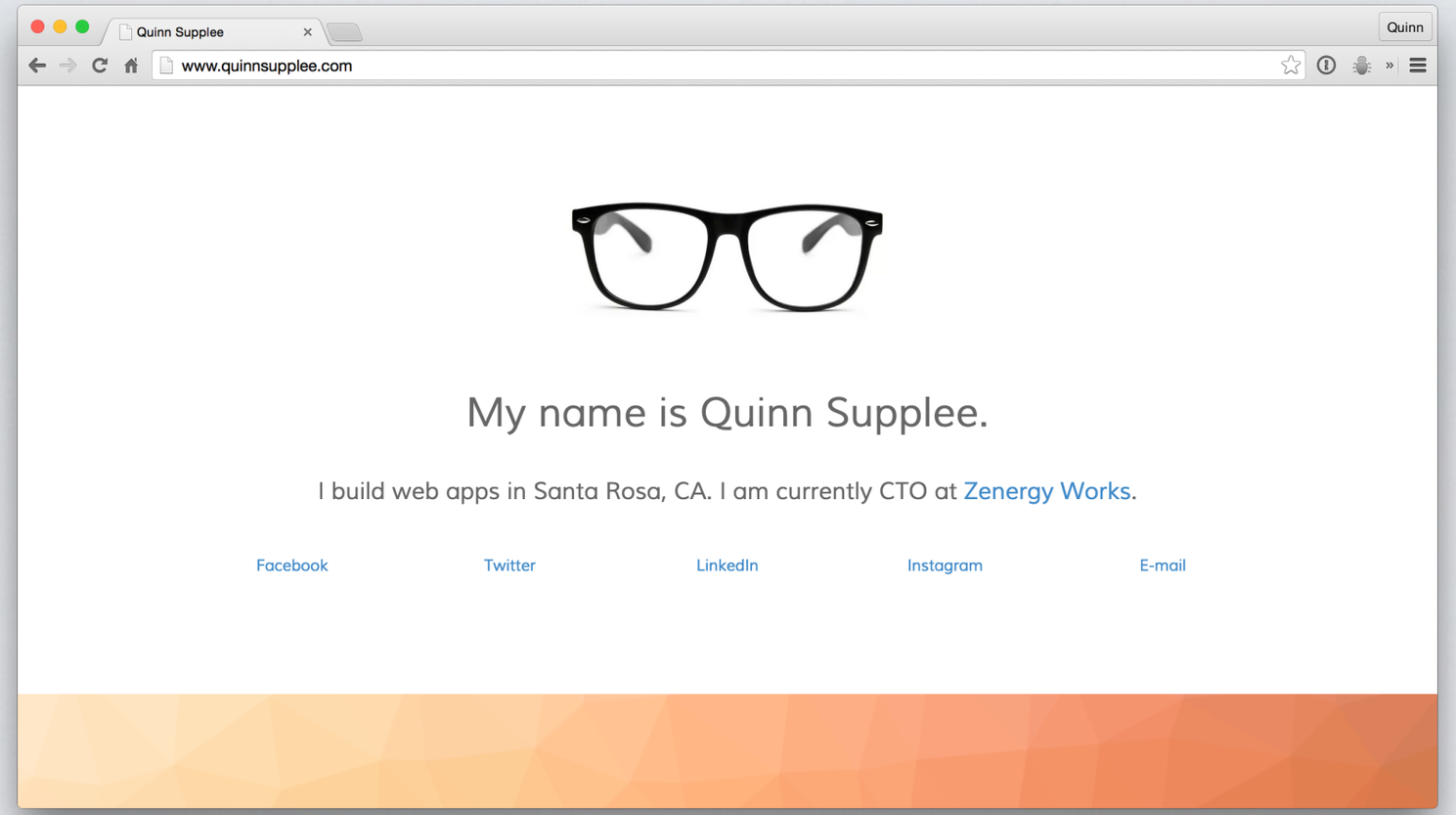
How To Install Linux, Apache, MySQL, PHP (LAMP) stack On CentOS 6
http://do.co/1gf3qvz

How To Protect SSH with fail2ban on CentOS 6
http://do.co/1ImF6h9

How To Set Up SSH Keys
http://do.co/1IA3brm

How To Use SFTP to Securely Transfer Files with a Remote Server
http://do.co/1SJg6GI

How to contact me: quinn@quinnsupplee.com



Presentation can be downloaded from:

http://www.quinnsupplee.com/accidentalsysadmin