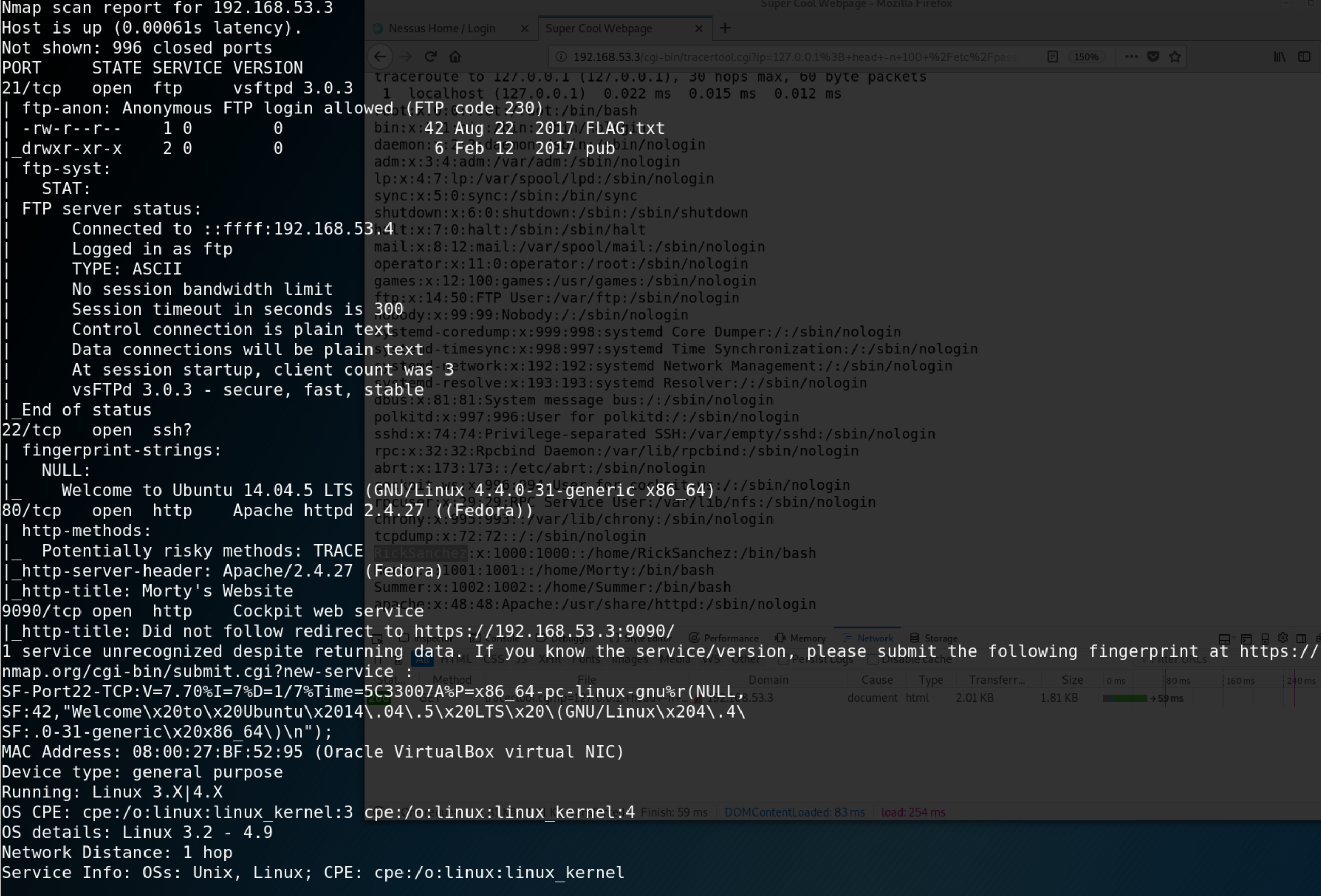
**Rickdiculosly Easy PWNED**

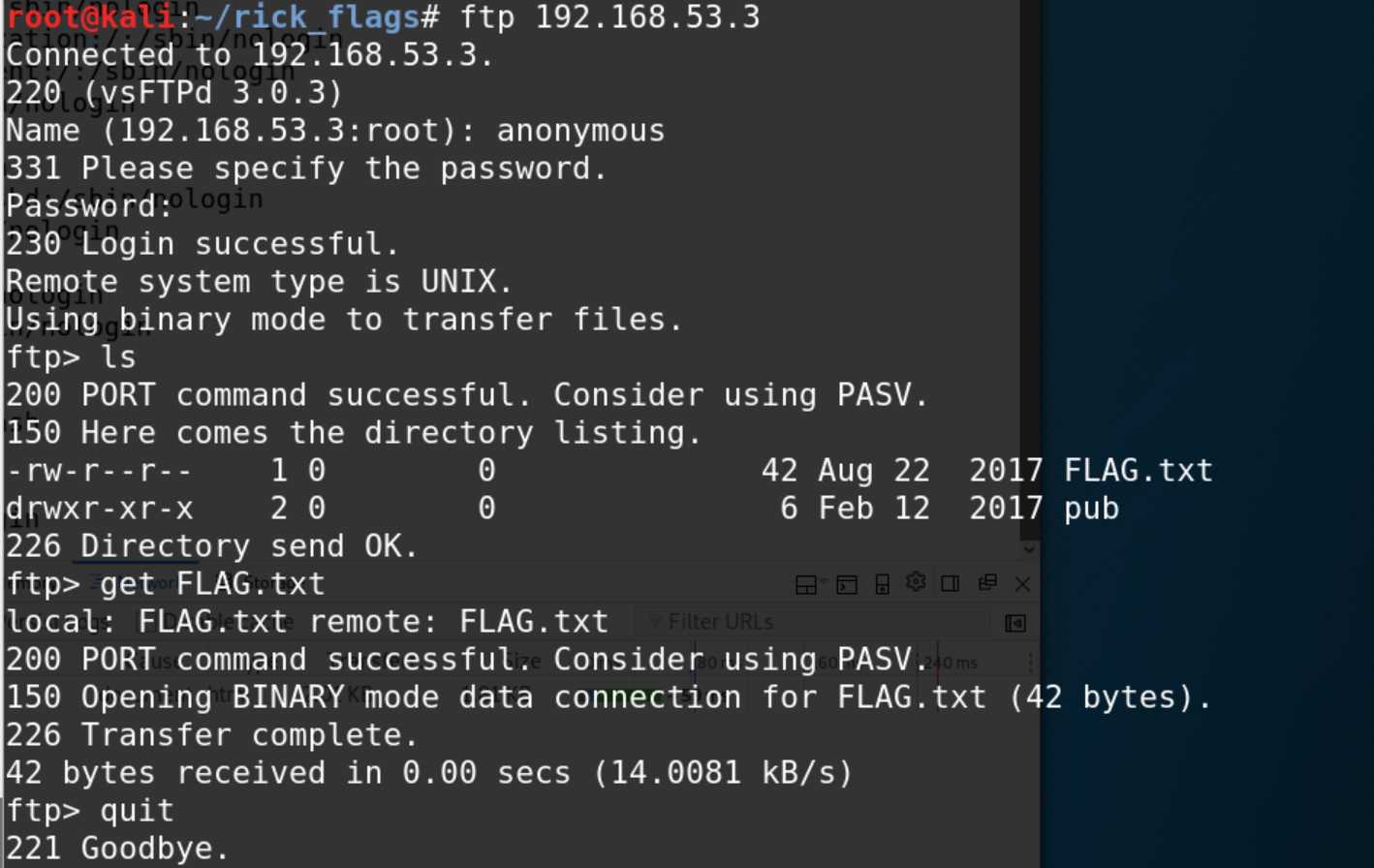
The Rick and Morty themed Fedora Linux machine from Vulnhub was a fun machine to attack. Keeping track of the information gathered from port scans, captured flags, and other files on the victim machine is really helpful and will save anyone a great deal of time.

**Gathering Information**

As mentioned above, the information gathering phase is crucial. Running a basic NMAP scan against the target machine (192.168.53.3) yielded the following results:



The first thing to note is that the target machine allows anonymous FTP access, which can allow anyone to login to the FTP server. Furthermore, the NMAP scan results reveal a FLAG in the ftp server’s anonymous login directory. The first flag will be easy to capture. Running the command ftp 192.168.53.3 allows access to the ftp server (NOTE: if FTP is not installed on the attacking machine, run the command apt-get install ftp before continuing).

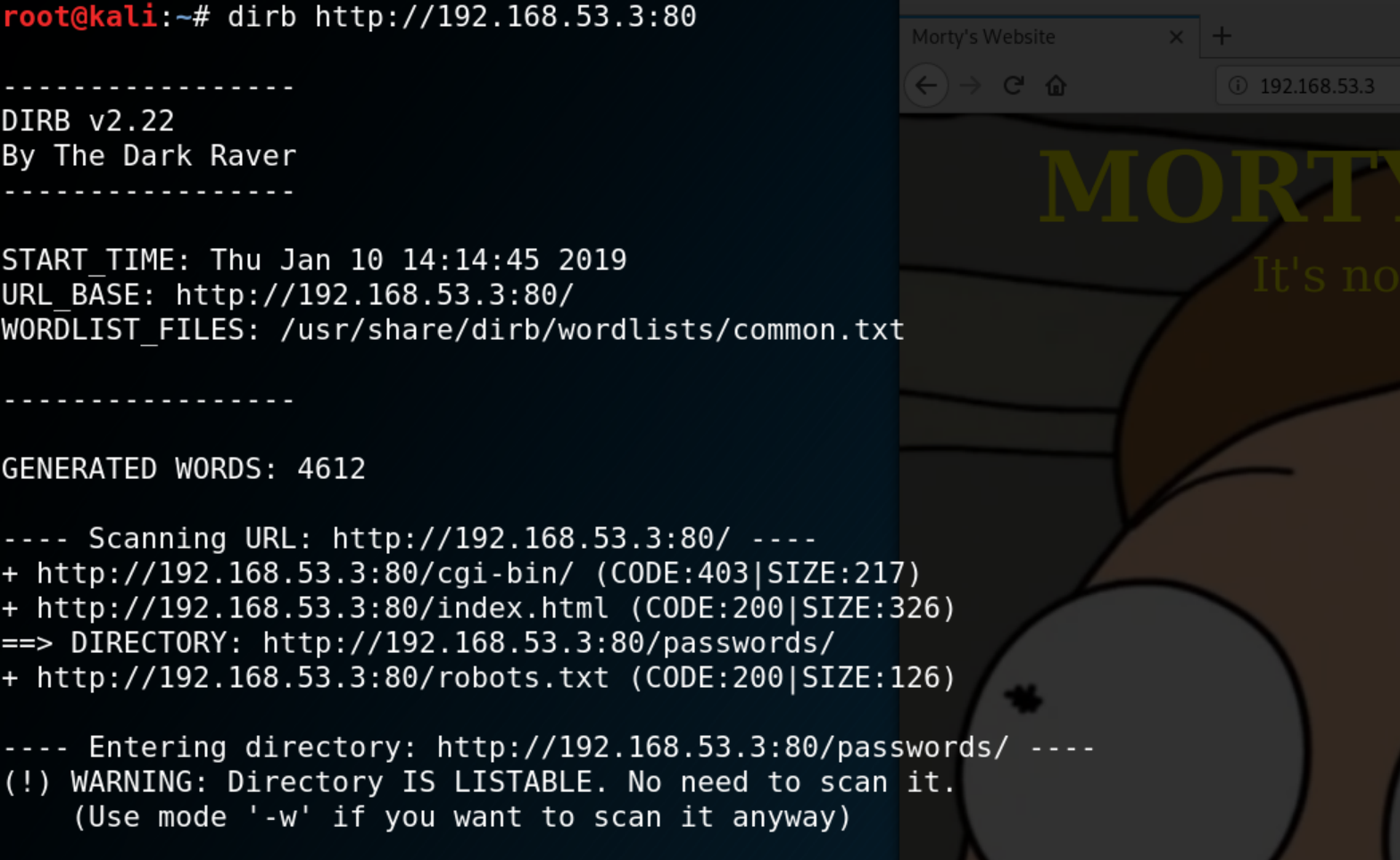


Once the flag has been obtained it can be viewed via the cat command (cat FLAG.txt). *Important note: make sure to keep the captured flags, and any information gathered about the target in a separate directory. Being organized will save time and is vital for successful exploitation of this machine.*

The target machine is also running an apache server on port 80. Navigating to the webpage using Firefox yields an unfinished webpage.

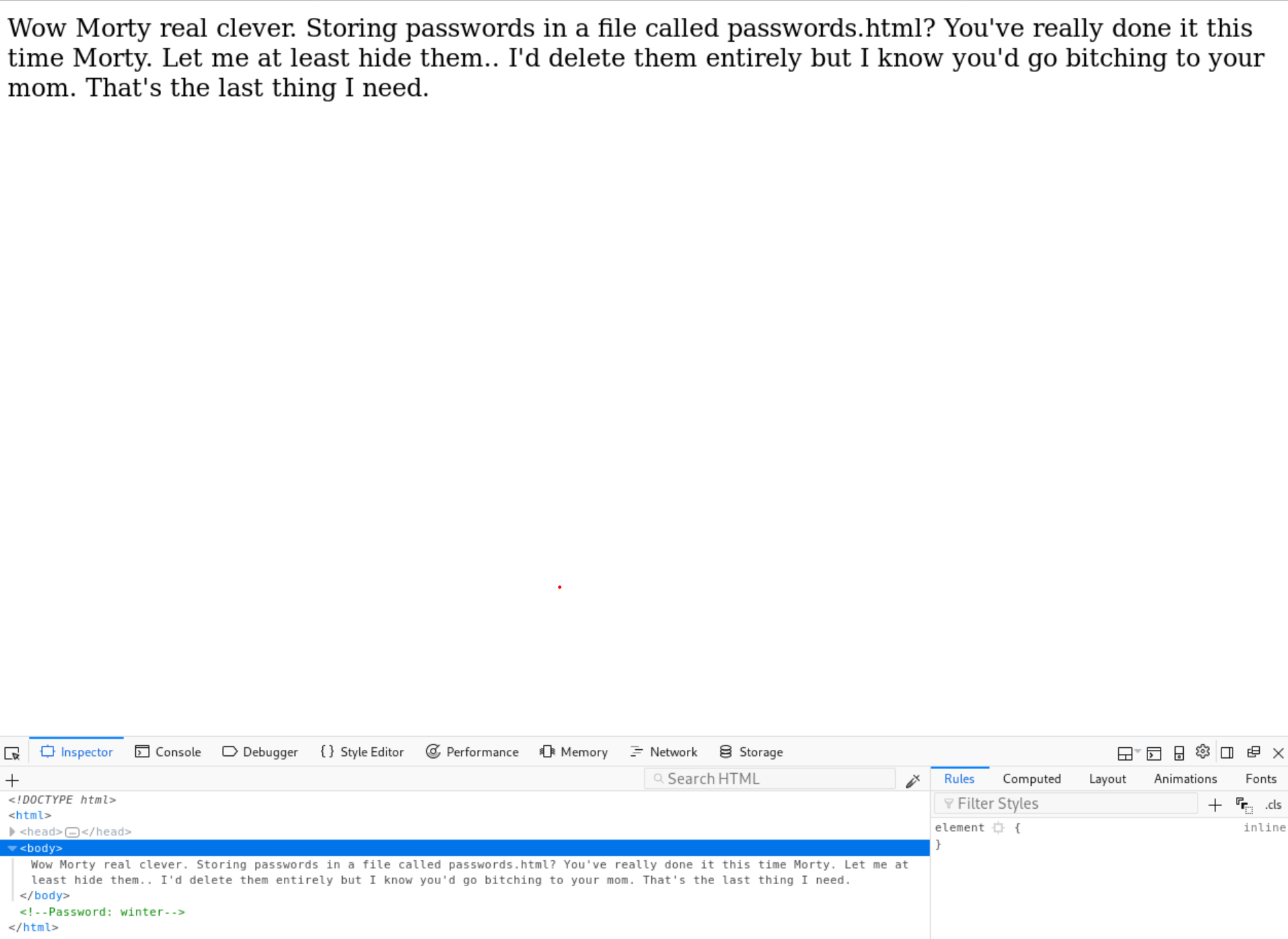


At first glance there appears to be nothing of interest here; however, further inspection (using dirbuster) reveals some hidden directories housed within the webserver.

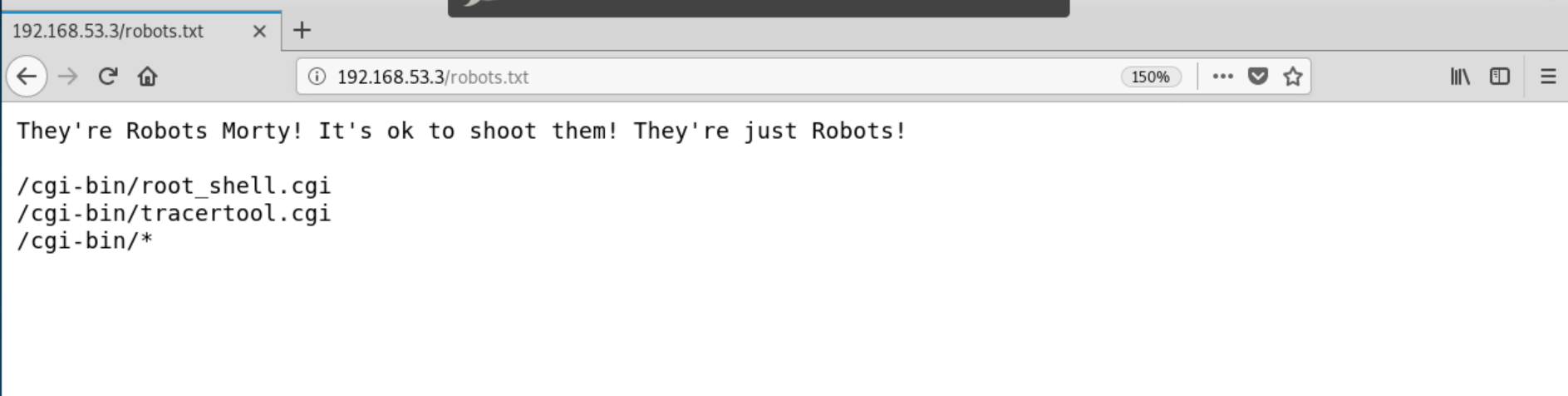


As can be seen in the scan above the target contains a directory called passwords, as well as, a directory titled robots.txt. The passwords directory contains a FLAG and a file called passwords.html. Here are the contents of the FLAG file. 

The passwords.html file contains a not to Morty chastising him for storing his password in a file called passwords.html (real clever Morty). The note also mentions that the password was hidden. Inspecting the webpage reveals a comment that contains a password.



Put the password somewhere safe. Checking the robots.txt file should be interesting.



The robots.txt file seems to contain paths to applications. The root\_shell.cgi file looks promising.