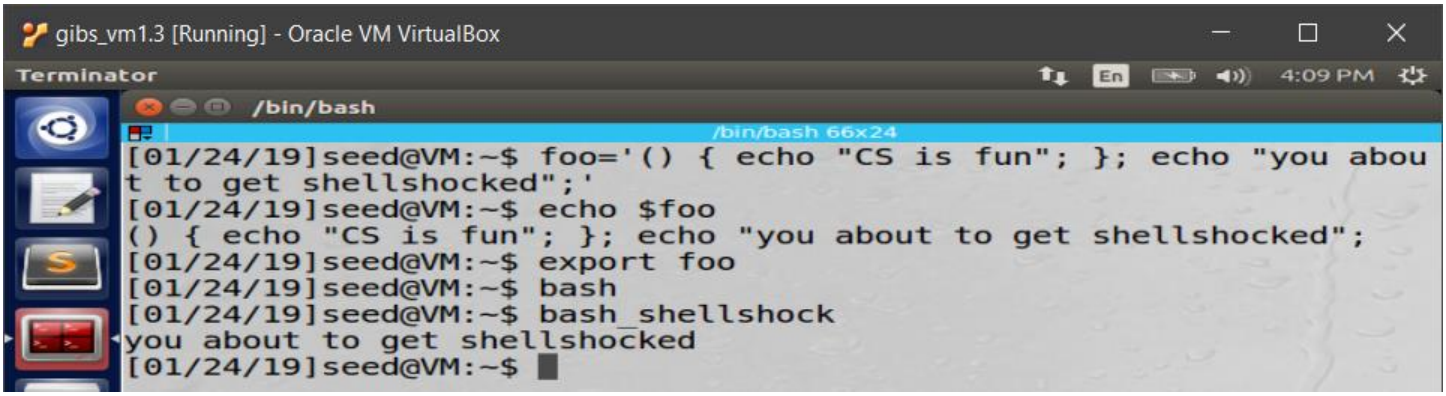
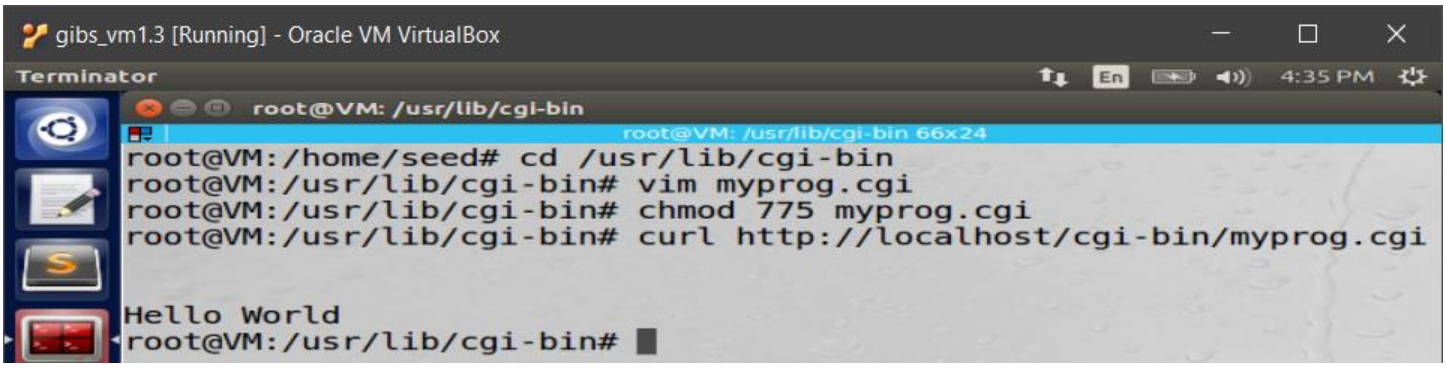
Gabriel Brehm
CS363
Lab 02

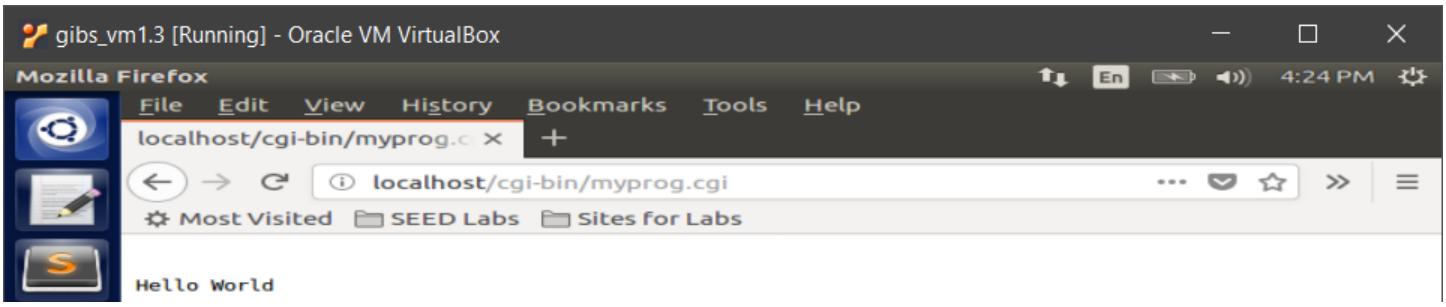
2 Lab Tasks

Task 1: As one can see, after the foo function is exported, and bash is run, nothing happens, but when bash_shellshock is run, the additional echo is executed. I do know that the patched version is not vulnerable to the shellshock attack, but the bash_shellshock version is.

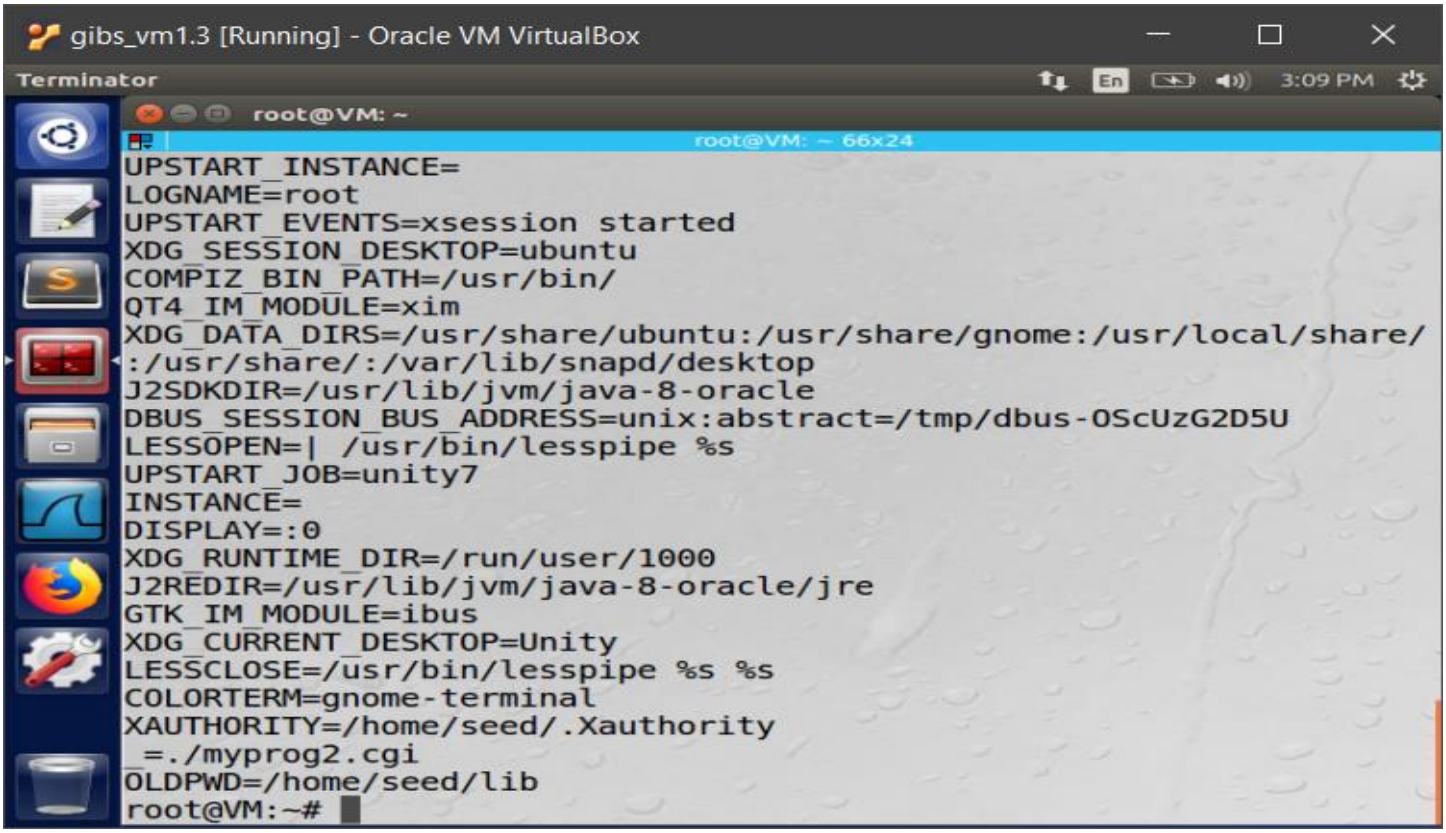


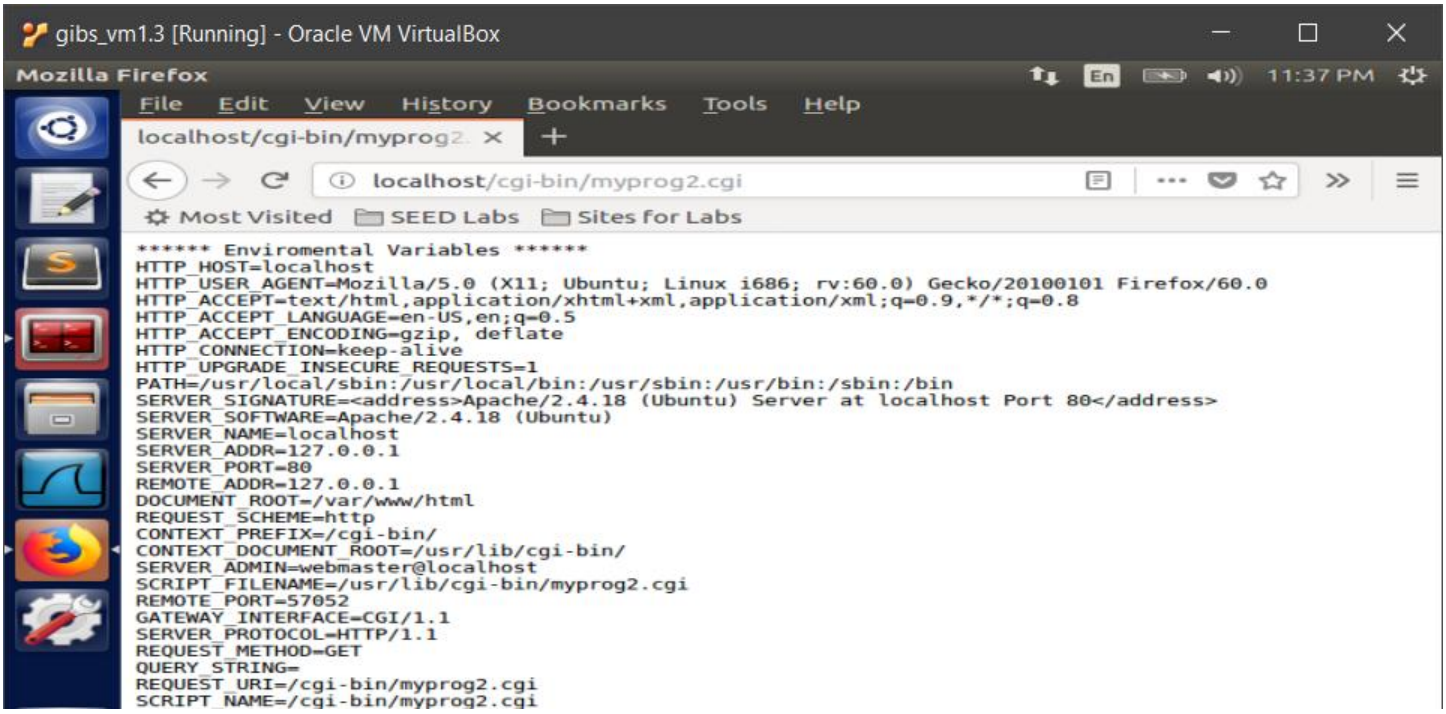
Task 2:



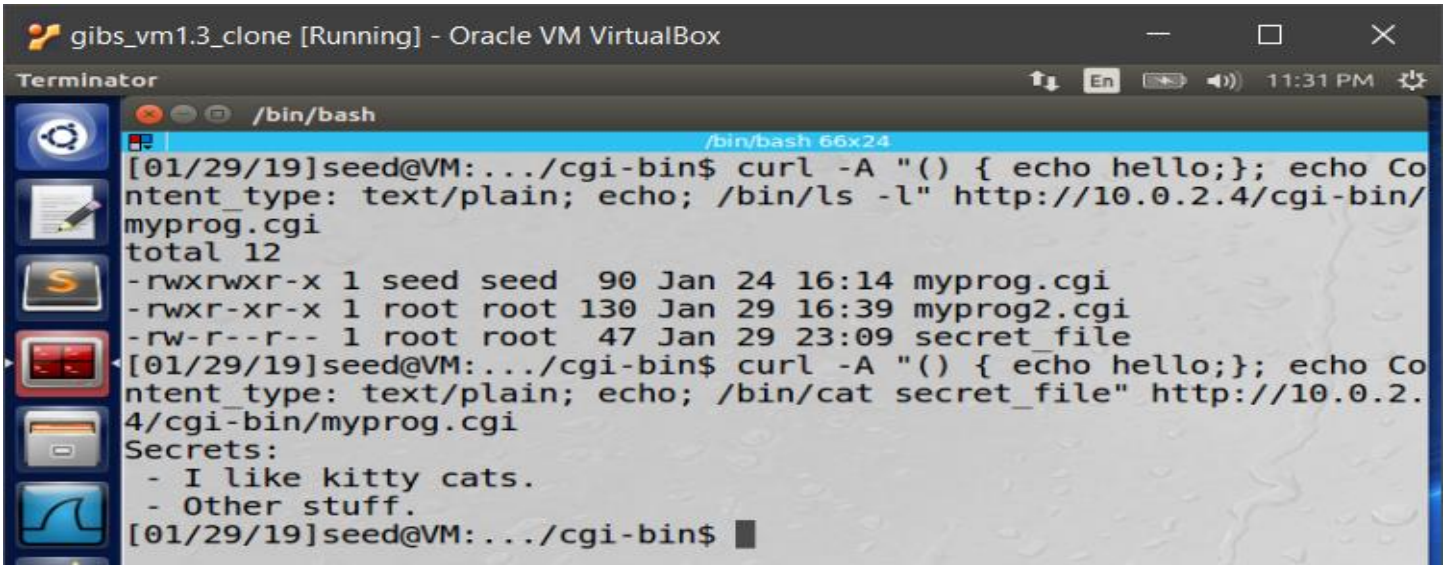


Task 3: We can make use of a CGI program to add any string we want to the print out of the environmental variables.

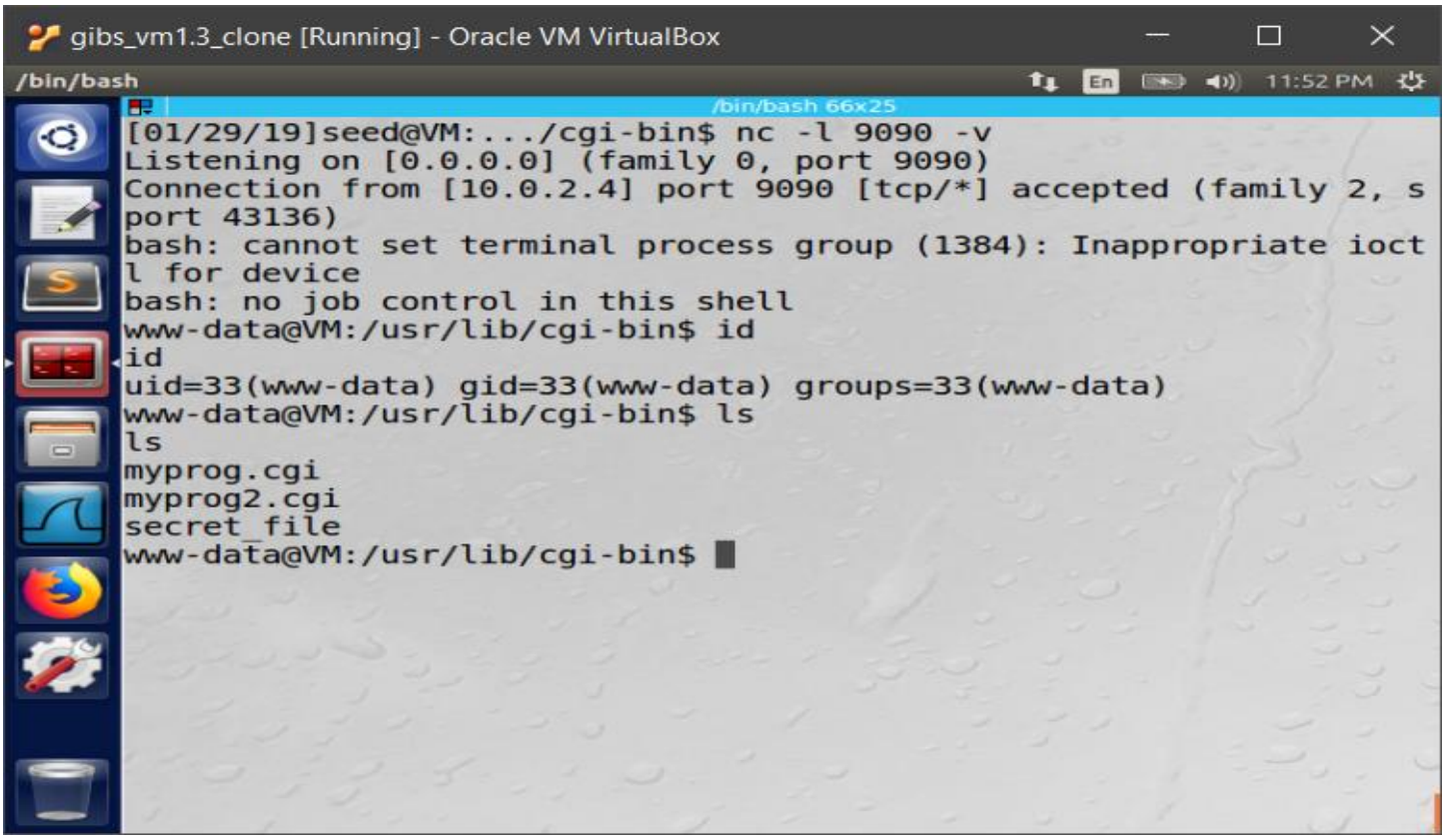




Task 4: We can steal the content of the secret file in the directory, but we cannot steal the content of the shadow file, and I believe that is because when we remote we only have a standard user access, and you must be root in order to access the shadow file.



Task 5: The attacker listens on a port, and the victim connects to that port. This gives the attacker remote access to the victims shell.



Task 6: When the patched version of bash is used, no strings are printed out with the environmental variables, and the reverse shell cannot be obtained.