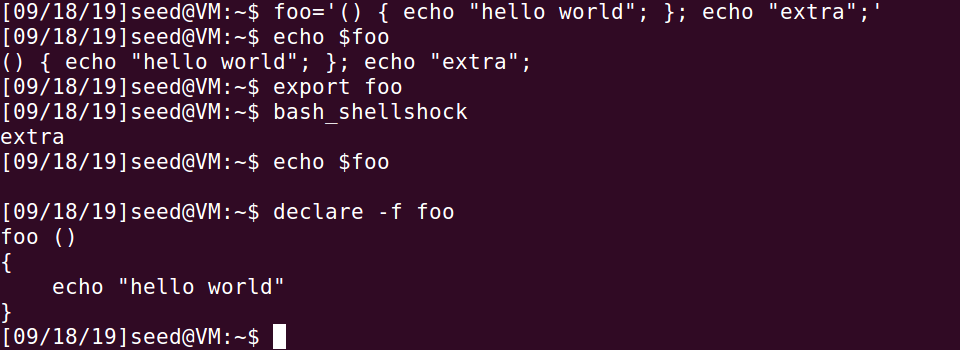
Lab2 Shellshock Attack Lab

Marco Lin

Task 1.Attack set-UID program

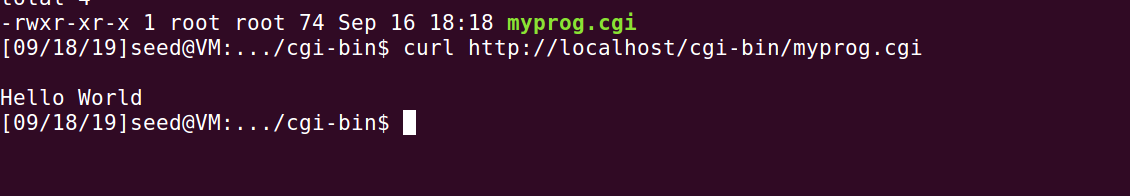




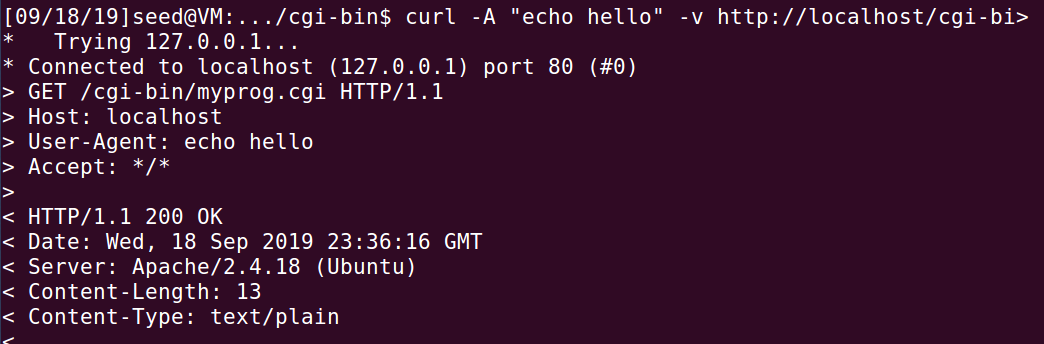
Task 2. Attack CGI programs

Step one: set up the CGI program

The script is accessible via curl:

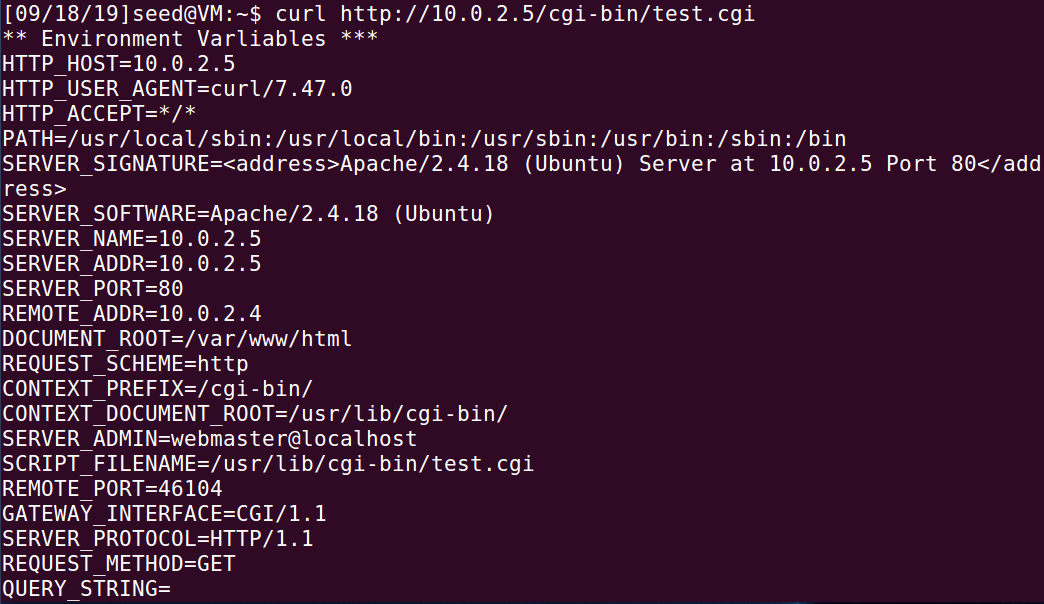
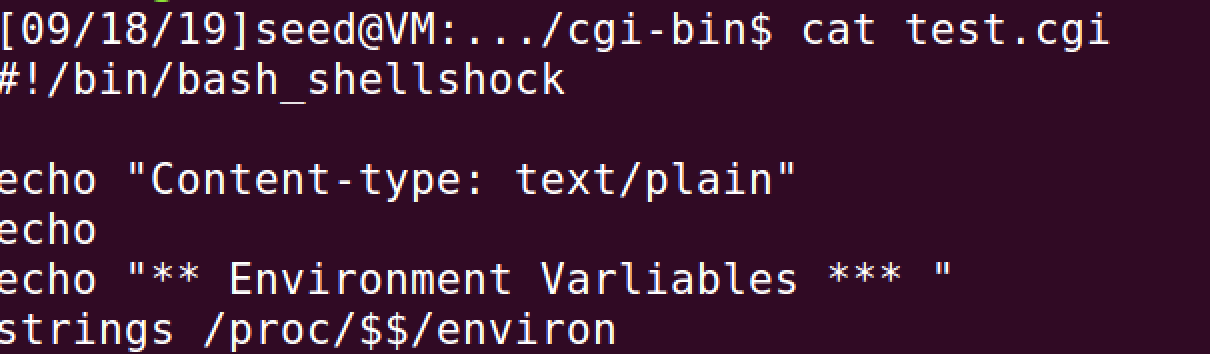


Step two: Launch the Attack

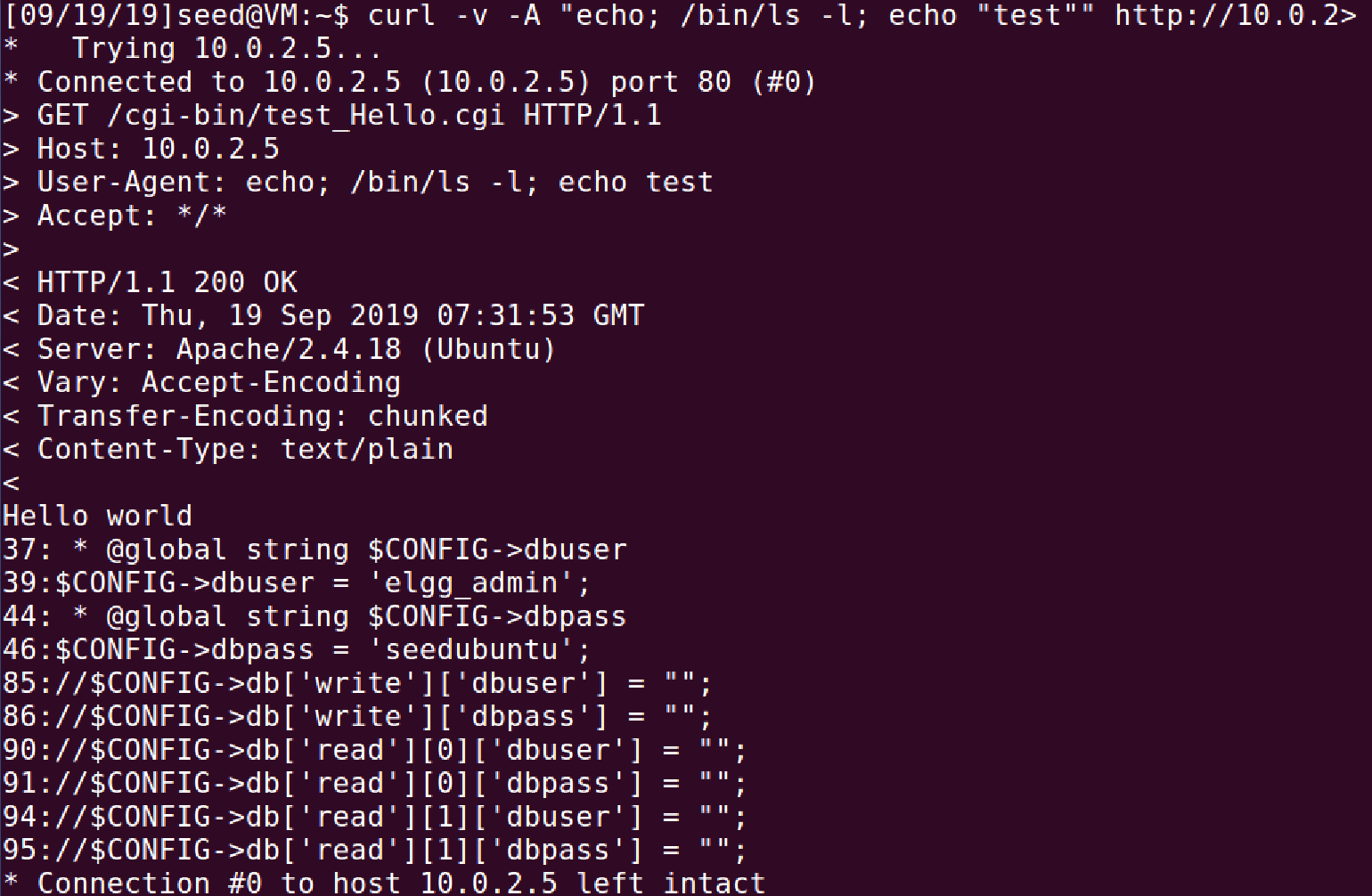
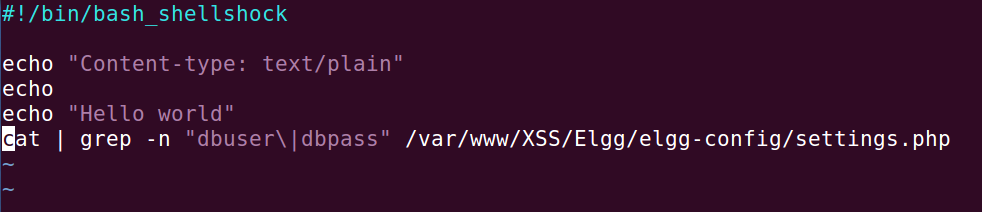
A Shellshock attack is able to be executed on the web server from a remote agent by adding a function to the agent variable:

Task 3. Remote attack

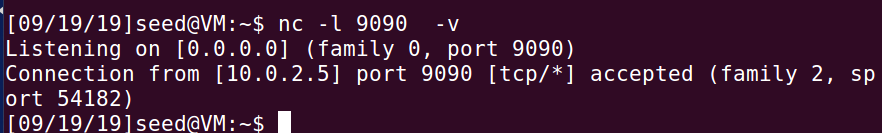
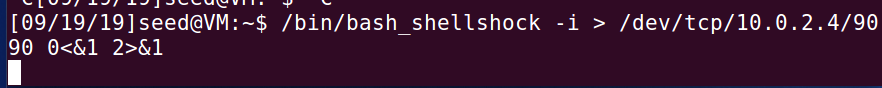
3A. Change the localhost to server address, and after execute the program, we got the environmental variables.



3B using the cat command to get the dbuser and dbpass information which are elgg\_admin and seedubuntu.



3C. We can remotely control the shell



Task 4. Questions

1.No, the vulnerability exists only when the variable value starts with '() {'.

2. The target process should run bash. And, the process must obtain some environment variable from outside.

3.upgrade system.