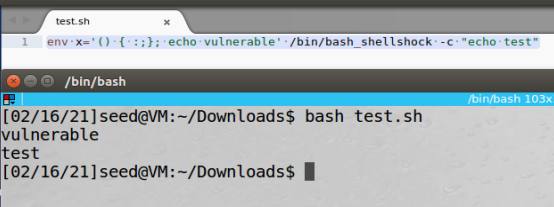
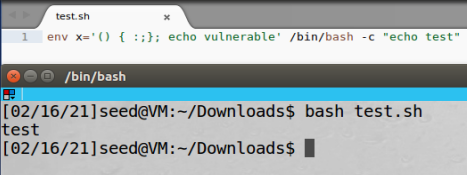
Daniel Quiroga

22 February 2021

Homework 1 Report

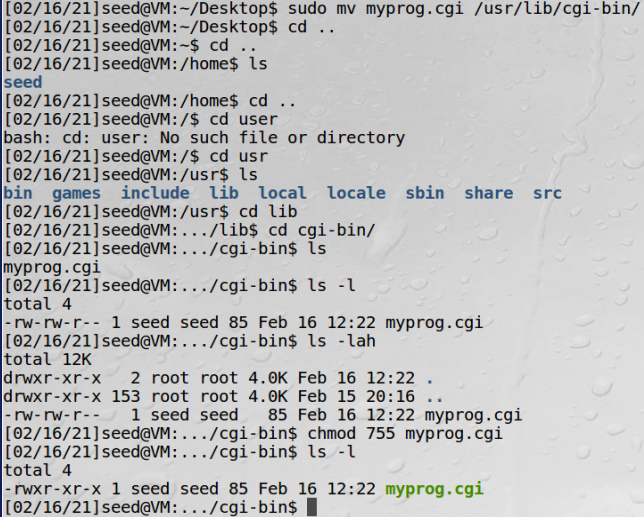
**Task1: Experimenting with Bash Function**



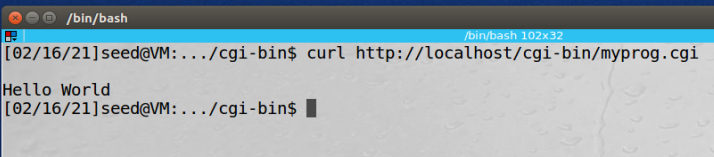


Here I have two separate files with similar functionalities but one prints out vulnerable and the other does not essentially emphasizing the vulnerability.

**Task2**: **Setting up CGI programs**

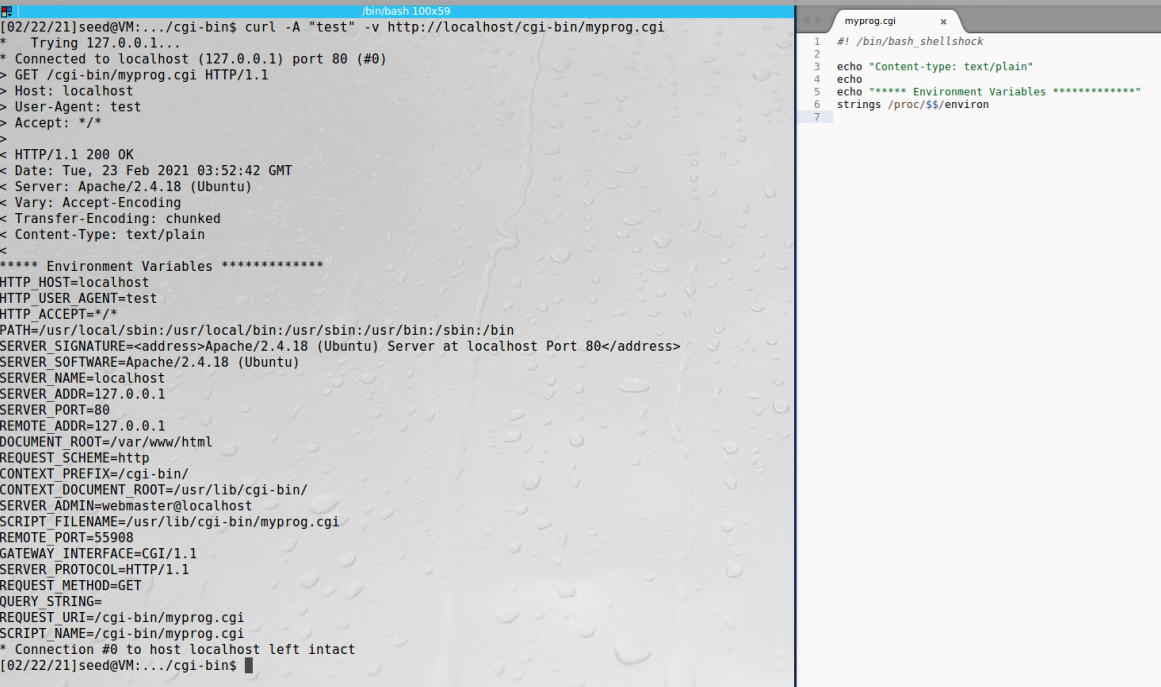


Here I create my file with the information and move it to the proper location. After I change the permissions on the file so that it becomes an executable.



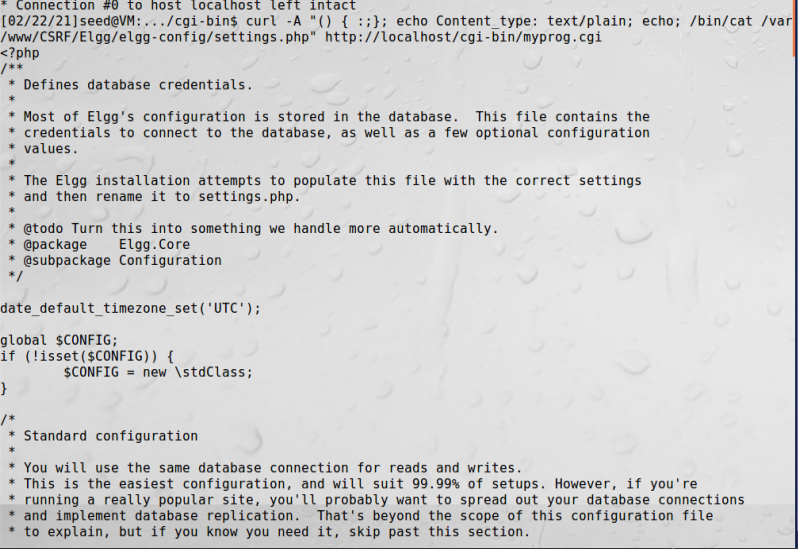
This is my output when I run the curl command

**Task 3: Passing Data to Bash via Environment Variable**



Here I can change the User-Agent and HTTP\_USER\_AGENT variables in the server by the curl -A tag making it possible to pass information to the bash.

**Task 4: Launching the Shellshock Attack**



Byrunningcurl -A " () { :; }; echo Content\_type : text/plain ; echo ; /bin/cat /var/www/CSRF/Elgg/elgg-config/settings . php " http : //localhost/cgi-bin/myprog . cgi I was able to have all the sensitive information from the database print out into one of the environment variables. We can very easily zip all this information and steal the sensitive information from the server.

It did not seem like I was able to steal the contents in shadow since I as a normal user do not have read access to the file to begin with since only root and shadow have read access and others do not have any access in terms of file. I would need to find a way to get in as a superuser or pass in information as a superuser here to have a chance to see the contents of shadow.

**Task 6: Using the Patched Bash**

When I ran the exact same command with the patched version of bash I got no relevant information and was not able to get any information as I was able to in the shellshock attack I did in task 4. Here is the output from the patched version:

