Man Tik Li

CS 377 - 001

October 19, 2020

**Lab 2**

1. Nothing happened when run “/bin/bash\_shellshock” in the patched version of bash. (bin/bash).But when running the bash\_shellshock (not patched), it displayed the message I parse from shell variable foo. During the parsing, due to the bug, shell will execute the command after the curl bracket and this is the reason why when bash starts in the child process, a message “extra” is printed out. Text

   Description automatically generated
2. Text, chat or text message

   Description automatically generated
3. I used command “curl -A “test” -v <http://localhost/cgi-bin/test.cgi>” to sends data to bash as the attacker. The screenshot below showing the User-Agent and HTTP\_USER\_AGENT was appeared as test.

Text

Description automatically generated

1. Yes, I’m able to steal the password from the server. The file is saved as myprog.cgi.1.

Text

Description automatically generated

I can also be able to steal the content of the shadow file. The file is saved as myprog.cgi.2. Because the owner of the shadow file is usually the user root, if user run the command as the root, user can able to take the file but not normal user.

Text

Description automatically generated

1. N/A
2. After replaced the header with /bin/bash. I’m not getting the results I got when I used the bash\_shellshock.