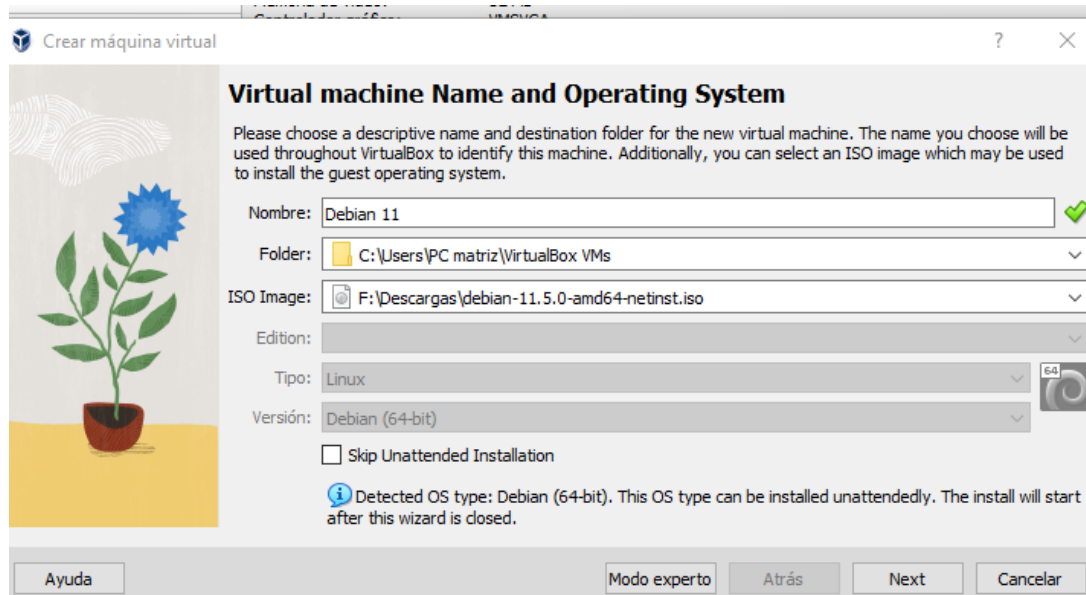


EJERCICIOS - MODSECURITY

Prerrequisitos

- Debian 11
- Windows Server 2012 Protección de Activos



Crear máquina virtual

Unattended Guest OS Install Setup

You can configure the unattended guest OS install by modifying username, password, and hostname. Additionally you can enable guest additions install. For Microsoft Windows guests it is possible to provide a product key.

Username and Password

Username: ✓

Password: ✓

Repeat Password: ✓

Opciones adicionales

Product Key:

Hostname: ✓

Domain Name:

☐ Install in Background

☒ Guest Additions

Guest Additions ISO:

Ayuda Atrás Next Cancelar

```
vboxuser@Debian11: ~  
root@Debian11:~# apt install build-essential dkms linux-headers-$(uname -r)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
build-essential is already the newest version (12.9).  
The following additional packages will be installed:  
  dctrl-tools linux-headers-5.10.0-21-common linux-headers-amd64  
Suggested packages:  
  debtags menu  
The following NEW packages will be installed:  
  dctrl-tools dkms linux-headers-5.10.0-21-amd64  
  linux-headers-5.10.0-21-common linux-headers-amd64  
0 upgraded, 5 newly installed, 0 to remove and 0 not upgraded.  
Need to get 10.3 MB of archives.  
After this operation, 59.7 MB of additional disk space will be used.  
Do you want to continue? [Y/n] Y  
Get:1 http://security.debian.org/debian-security bullseye-security/main amd64 li  
nux-headers-5.10.0-21-common all 5.10.162-1 [9,060 kB]  
Get:2 http://deb.debian.org/debian bullseye/main amd64 dctrl-tools amd64 2.24-3+  
b1 [104 kB]  
Get:3 http://deb.debian.org/debian bullseye/main amd64 dkms all 2.8.4-3 [78.2 kB  
]  
Get:4 http://security.debian.org/debian-security bullseye-security/main amd64 li  
nux-headers-5.10.0-21-amd64 amd64 5.10.162-1 [1,066 kB]
```

```
vboxuser@Debian11: ~
dkms: running auto installation service for kernel 5.10.0-21-amd64:.
Setting up linux-headers-amd64 (5.10.162-1) ...
Processing triggers for man-db (2.9.4-2) ...
root@Debian11:~# apt-get install build-essential module-assistant
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
build-essential is already the newest version (12.9).
The following NEW packages will be installed:
  module-assistant
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 101 kB of archives.
After this operation, 400 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://deb.debian.org/debian bullseye/main amd64 module-assistant all 0.11.10 [101 kB]
Fetched 101 kB in 0s (514 kB/s)
Selecting previously unselected package module-assistant.
(Reading database ... 184080 files and directories currently installed.)
Preparing to unpack .../module-assistant_0.11.10_all.deb ...
Unpacking module-assistant (0.11.10) ...
Setting up module-assistant (0.11.10) ...
Processing triggers for man-db (2.9.4-2) ...
root@Debian11:~#
```

```
Processing triggers for man-db (2.9.4-2) ...
root@Debian11:~# m-a prepare
Getting source for kernel version: 5.10.0-21-amd64
Kernel headers available in /lib/modules/5.10.0-21-amd64/build
Creating symlink...
apt-get install build-essential
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
build-essential is already the newest version (12.9).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Done!
root@Debian11:~#
```

```
vboxuser@Debian11: ~  
root@Debian11:/tmp# ./VBoxLinuxAdditions.run  
Verifying archive integrity... 100% MD5 checksums are OK. All good.  
Uncompressing VirtualBox 7.0.6 Guest Additions for Linux 100%  
VirtualBox Guest Additions installer  
This system appears to have a version of the VirtualBox Guest Additions  
already installed. If it is part of the operating system and kept up-to-date,  
there is most likely no need to replace it. If it is not up-to-date, you  
should get a notification when you start the system. If you wish to replace  
it with this version, please do not continue with this installation now, but  
instead remove the current version first, following the instructions for the  
operating system.  
  
If your system simply has the remains of a version of the Additions you could  
not remove you should probably continue now, and these will be removed during  
installation.  
  
Do you wish to continue? [yes or no]  
yes  
update-initramfs: Generating /boot/initrd.img-5.10.0-21-amd64  
VirtualBox Guest Additions: Starting.  
VirtualBox Guest Additions: Setting up modules  
VirtualBox Guest Additions: Building the VirtualBox Guest Additions kernel  
modules. This may take a while.  
VirtualBox Guest Additions: To build modules for other installed kernels. run
```

```
vboxuser@Debian11: ~  
root@Debian11:~# apt install libmodsecurity-dev libmodsecurity3 modsecurity-crs  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  geoip-database libapache2-mod-security2 libfuzzy2 libgeoip1 liblua5.1-0  
Suggested packages:  
  geoip-bin lua geoip-database-contrib ruby python  
The following NEW packages will be installed:  
  geoip-database libapache2-mod-security2 libfuzzy2 libgeoip1 liblua5.1-0  
  libmodsecurity-dev libmodsecurity3 modsecurity-crs  
0 upgraded, 8 newly installed, 0 to remove and 0 not upgraded.  
Need to get 4,841 kB of archives.  
After this operation, 21.5 MB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://deb.debian.org/debian bullseye/main amd64 geoip-database all 201912  
24-3 [3,032 kB]  
Get:2 http://deb.debian.org/debian bullseye/main amd64 liblua5.1-0 amd64 5.1.5-8  
.1+b3 [109 kB]  
Get:3 http://deb.debian.org/debian bullseye/main amd64 libapache2-mod-security2  
amd64 2.9.3-3+deb11u1 [259 kB]  
Get:4 http://deb.debian.org/debian bullseye/main amd64 libfuzzy2 amd64 2.14.1+gi  
t20180629.57fcfff-2 [19.5 kB]  
Get:5 http://deb.debian.org/debian bullseye/main amd64 libgeoip1 amd64 1.6.12-7
```

```
root@Debian11:~# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-data apache2-utils
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
The following NEW packages will be installed:
  apache2 apache2-data apache2-utils
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 695 kB of archives.
After this operation, 2,004 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 apache2-data all 2.4.54-1~deb11u1 [160 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 apache2-utils amd64 2.4.54-1~deb11u1 [260 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 apache2 amd64 2.4.54-1~deb11u1 [275 kB]
Fetched 695 kB in 0s (1,800 kB/s)
Selecting previously unselected package apache2-data.
```

```
vboxuser@Debian11: ~
root@Debian11:~# apt install apt-file
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libapt-pkg-perl libexporter-tiny-perl liblist-moreutils-perl
  liblist-moreutils-xs-perl libregexp-assemble-perl
The following NEW packages will be installed:
  apt-file libapt-pkg-perl libexporter-tiny-perl liblist-moreutils-perl
  liblist-moreutils-xs-perl libregexp-assemble-perl
0 upgraded, 6 newly installed, 0 to remove and 0 not upgraded.
Need to get 322 kB of archives.
After this operation, 901 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://deb.debian.org/debian bullseye/main amd64 libapt-pkg-perl amd64 0.1.39 [72.1 kB]
Get:2 http://deb.debian.org/debian bullseye/main amd64 libexporter-tiny-perl all 1.002002-1 [37.8 kB]
Get:3 http://deb.debian.org/debian bullseye/main amd64 liblist-moreutils-xs-perl amd64 0.430-2 [40.9 kB]
Get:4 http://deb.debian.org/debian bullseye/main amd64 liblist-moreutils-perl all 0.430-2 [46.9 kB]
Get:5 http://deb.debian.org/debian bullseye/main amd64 libregexp-assemble-perl all 0.36-1.1 [85.5 kB]
```

Ejercicio 1

Instalar y configurar ModSecurity en Debian 11

```
vboxuser@Debian11: ~  
root@Debian11:~# apt-file update  
Get:1 http://security.debian.org/debian-security bullseye-security InRelease [48  
.4 kB]  
Hit:2 http://deb.debian.org/debian bullseye InRelease  
Hit:3 http://deb.debian.org/debian bullseye-updates InRelease  
Get:4 http://deb.debian.org/debian bullseye/main all Contents (deb) [31.1 MB]  
Get:5 http://deb.debian.org/debian bullseye/main amd64 Contents (deb) [10.3 MB]  
Get:6 http://deb.debian.org/debian bullseye-updates/main amd64 Contents (deb) [6  
8.7 kB]  
Get:7 http://deb.debian.org/debian bullseye-updates/main all Contents (deb) [25.  
0 kB]  
Fetched 41.5 MB in 7s (5,646 kB/s)  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
All packages are up to date.  
root@Debian11:~# █
```

```
root@Debian11:/usr/bin# apt install libapache2-mod-security2 --reinstall  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
0 upgraded, 0 newly installed, 1 reinstalled, 0 to remove and 0 not upgraded.  
Need to get 259 kB of archives.  
After this operation, 0 B of additional disk space will be used.  
Get:1 http://deb.debian.org/debian bullseye/main amd64 libapache2-mod-security2  
amd64 2.9.3-3+deb11u1 [259 kB]  
Fetched 259 kB in 0s (1,268 kB/s)  
(Reading database ... 185001 files and directories currently installed.)  
Preparing to unpack ../libapache2-mod-security2_2.9.3-3+deb11u1_amd64.deb ...  
Unpacking libapache2-mod-security2 (2.9.3-3+deb11u1) over (2.9.3-3+deb11u1) ...  
Setting up libapache2-mod-security2 (2.9.3-3+deb11u1) ...  
apache2_invoke: Enable module security2  
root@Debian11:/usr/bin# █
```

```
vboxuser@Debian11: ~  
version_module (static)  
unixd_module (static)  
access_compat_module (shared)  
alias_module (shared)  
auth_basic_module (shared)  
authn_core_module (shared)  
authn_file_module (shared)  
authz_core_module (shared)  
authz_host_module (shared)  
authz_user_module (shared)  
autoindex_module (shared)  
deflate_module (shared)  
dir_module (shared)  
env_module (shared)  
filter_module (shared)  
mime_module (shared)  
mpm_event_module (shared)  
negotiation_module (shared)  
reqtimeout_module (shared)  
security2_module (shared)  
setenvif_module (shared)  
status_module (shared)  
unique_id_module (shared)  
root@Debian11:/usr/bin#
```

```
vboxuser@Debian11: ~  
root@Debian11:/etc/modsecurity# ls  
crs modsecurity.conf-recommended unicode.mapping  
root@Debian11:/etc/modsecurity# cp modsecurity.conf-recommended modsecurity.conf  
root@Debian11:/etc/modsecurity# ls  
crs modsecurity.conf modsecurity.conf-recommended unicode.mapping  
root@Debian11:/etc/modsecurity#
```

```
vboxuser@Debian11: ~  
GNU nano 5.4 modsecurity.conf *  
# -- Rule engine initialization -----  
  
# Enable ModSecurity, attaching it to every transaction. Use detection  
# only to start with, because that minimises the chances of post-installation  
# disruption.  
#  
SecRuleEngine DetectionOnly  
#SecRuleEngine On  
  
# -- Request body handling -----  
  
# Allow ModSecurity to access request bodies. If you don't, ModSecurity  
# won't be able to see any POST parameters, which opens a large security  
# hole for attackers to exploit.  
#  
SecRequestBodyAccess On  
  
# Enable XML request body parser.  
# Initiate XML Processor in case of xml content-type  
  
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

```
vboxuser@Debian11: ~  
root@Debian11:/etc/modsecurity# ls  
crs modsecurity.conf-recommended unicode.mapping  
root@Debian11:/etc/modsecurity# cp modsecurity.conf-recommended modsecurity.conf  
root@Debian11:/etc/modsecurity# ls  
crs modsecurity.conf modsecurity.conf-recommended unicode.mapping  
root@Debian11:/etc/modsecurity# nano modsecurity.conf  
root@Debian11:/etc/modsecurity# cd /var/log/apache2/  
root@Debian11:/var/log/apache2# service apache2 reload  
root@Debian11:/var/log/apache2# ls -l  
total 8  
-rw-r----- 1 root adm  501 Feb 18 20:06 access.log  
-rw-r----- 1 root adm 2069 Feb 18 20:06 error.log  
-rw-r----- 1 root root   0 Feb 18 20:06 modsec_audit.log  
-rw-r----- 1 root adm   0 Feb 18 19:52 other_vhosts_access.log  
root@Debian11:/var/log/apache2#
```



```

root@Debian11:/var/www/html# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese
   Active: active (running) since Sat 2023-02-18 19:58:38 -03; 10min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 3793 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU
   Process: 4259 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=
 Main PID: 3797 (apache2)
    Tasks: 55 (limit: 4659)
   Memory: 35.3M
      CPU: 286ms
   CGroup: /system.slice/apache2.service
           └─3797 /usr/sbin/apache2 -k start
             └─4263 /usr/sbin/apache2 -k start
               └─4264 /usr/sbin/apache2 -k start

Feb 18 19:58:38 Debian11 systemd[1]: Starting The Apache HTTP Server...
Feb 18 19:58:38 Debian11 systemd[1]: Started The Apache HTTP Server.
Feb 18 20:06:47 Debian11 systemd[1]: Reloading The Apache HTTP Server.
Feb 18 20:06:47 Debian11 systemd[1]: Reloaded The Apache HTTP Server.
lines 1-19/19 (END)

```

```

vboxuser@Debian11: ~
GNU nano 5.4 login.php *
<html>
<body>
<?php
    if(isset($_POST['login']))
    {
        $username = $_POST['username'];
        $password = $_POST['password'];
        $con = mysqli_connect('localhost','root','password','sample');
        $result = mysqli_query($con, "SELECT * FROM `users` WHERE username='$us
        if(mysqli_num_rows($result) == 0)
            echo 'Invalid username or password';
        else
            echo '<h1>Logged in</h1><p>A Secret for you....</p>';
    }
    else
    {
        <form action="" method="post">
            Username: <input type="text" name="username"/><br />
            Password: <input type="password" name="password"/><br />

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace  ^U Paste     ^J Justify   ^_ Go To Line

```

```
vboxuser@Debian11: ~  
root@Debian11:/var/www/html# ls  
index.html  
root@Debian11:/var/www/html# nano login.php  
root@Debian11:/var/www/html# ls  
index.html  login.php  
root@Debian11:/var/www/html# apt install php  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  libapache2-mod-php7.4 php-common php7.4 php7.4-cli php7.4-common php7.4-json  
  php7.4-opcache php7.4-readline  
Suggested packages:  
  php-pear  
The following NEW packages will be installed:  
  libapache2-mod-php7.4 php php-common php7.4 php7.4-cli php7.4-common  
  php7.4-json php7.4-opcache php7.4-readline  
0 upgraded, 9 newly installed, 0 to remove and 0 not upgraded.  
Need to get 4,128 kB of archives.  
After this operation, 18.0 MB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://deb.debian.org/debian bullseye/main amd64 php-common all 2:76 [15.6  
kB]  
Get:2 http://deb.debian.org/debian bullseye/main amd64 php7.4-common amd64 7.4.3
```

localhost/login.php × + ×

← → ↻ 🔒 📄 localhost/login.php ☆ 📁 ☰

Username:

Password:

Login

```
vboxuser@Debian11: ~  
root@Debian11:/var/www/html# apt install mariadb-server  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  galera-4 gawk libaio1 libcgi-fast-perl libcgi-pm-perl  
  libconfig-inifiles-perl libdbd-mariadb-perl libdbi-perl libfcgi-bin  
  libfcgi-perl libfcgi0ldbl libhtml-template-perl libmariadb3 libsigsegv2  
  libterm-readkey-perl mariadb-client-10.5 mariadb-client-core-10.5  
  mariadb-common mariadb-server-10.5 mariadb-server-core-10.5 mysql-common  
  rsync socat  
Suggested packages:  
  gawk-doc libmldbm-perl libnet-daemon-perl libsql-statement-perl  
  libipc-sharedcache-perl mailx mariadb-test netcat-openbsd openssh-server  
The following NEW packages will be installed:  
  galera-4 gawk libaio1 libcgi-fast-perl libcgi-pm-perl  
  libconfig-inifiles-perl libdbd-mariadb-perl libdbi-perl libfcgi-bin  
  libfcgi-perl libfcgi0ldbl libhtml-template-perl libmariadb3 libsigsegv2  
  libterm-readkey-perl mariadb-client-10.5 mariadb-client-core-10.5  
  mariadb-common mariadb-server mariadb-server-10.5 mariadb-server-core-10.5  
  mysql-common rsync socat  
0 upgraded, 24 newly installed, 0 to remove and 0 not upgraded.  
Need to get 17.2 MB of archives.  
After this operation, 158 MB of additional disk space will be used.
```

```
vboxuser@Debian11: ~  
root@Debian11:/var/www/html# apt install php-mysql  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  php7.4-mysql  
The following NEW packages will be installed:  
  php-mysql php7.4-mysql  
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.  
Need to get 128 kB of archives.  
After this operation, 483 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://deb.debian.org/debian bullseye/main amd64 php7.4-mysql amd64 7.4.33-1+deb11u1 [121 kB]  
Get:2 http://deb.debian.org/debian bullseye/main amd64 php-mysql all 2:7.4+76 [6360 B]  
Fetched 128 kB in 0s (518 kB/s)  
Selecting previously unselected package php7.4-mysql.  
(Reading database ... 186051 files and directories currently installed.)  
Preparing to unpack .../php7.4-mysql_7.4.33-1+deb11u1_amd64.deb ...  
Unpacking php7.4-mysql (7.4.33-1+deb11u1) ...  
Selecting previously unselected package php-mysql.  
Preparing to unpack .../php-mysql_2%3a7.4+76_all.deb ...  
Unpacking php-mysql (2:7.4+76) ...
```

```
vboxuser@Debian11: ~
GNU nano 5.4 login.php *
:html>
:body>
<?php
    if(isset($_POST['login']))
    {
        $username = $_POST['username'];
        $password = $_POST['password'];
        $con = mysqli_connect('localhost','root','toor','sample');
        $result = mysqli_query($con, "SELECT * FROM `users` WHERE username='$us
        if(mysqli_num_rows($result) == 0)
            echo 'Invalid username or password';
        else
            echo '<h1>Logged in</h1><p>A Secret for you....</p>';
    }
    else
    {
        <form action="" method="post">
            Username: <input type="text" name="username"/><br />
            Password: <input type="password" name="password"/><br />
        </form>
    }
}
'>

^G Help      ^O Write Out ^W Where Is  ^K Cut      ^T Execute  ^C Location
^X Exit      ^R Read File ^\ Replace  ^U Paste    ^J Justify  ^_ Go To Line
```

```
vboxuser@Debian11: ~
Unpacking php-mysql (2:7.4+76) ...
Setting up php7.4-mysql (7.4.33-1+deb11u1) ...

Creating config file /etc/php/7.4/mods-available/mysqlnd.ini with new version

Creating config file /etc/php/7.4/mods-available/mysqli.ini with new version

Creating config file /etc/php/7.4/mods-available/pdo_mysql.ini with new version
Setting up php-mysql (2:7.4+76) ...
Processing triggers for libapache2-mod-php7.4 (7.4.33-1+deb11u1) ...
Processing triggers for php7.4-cli (7.4.33-1+deb11u1) ...
root@Debian11:/var/www/html# nano login.php
root@Debian11:/var/www/html# mysqladmin --user=root password toor
root@Debian11:/var/www/html# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.5.18-MariaDB-0+deb11u1 Debian 11

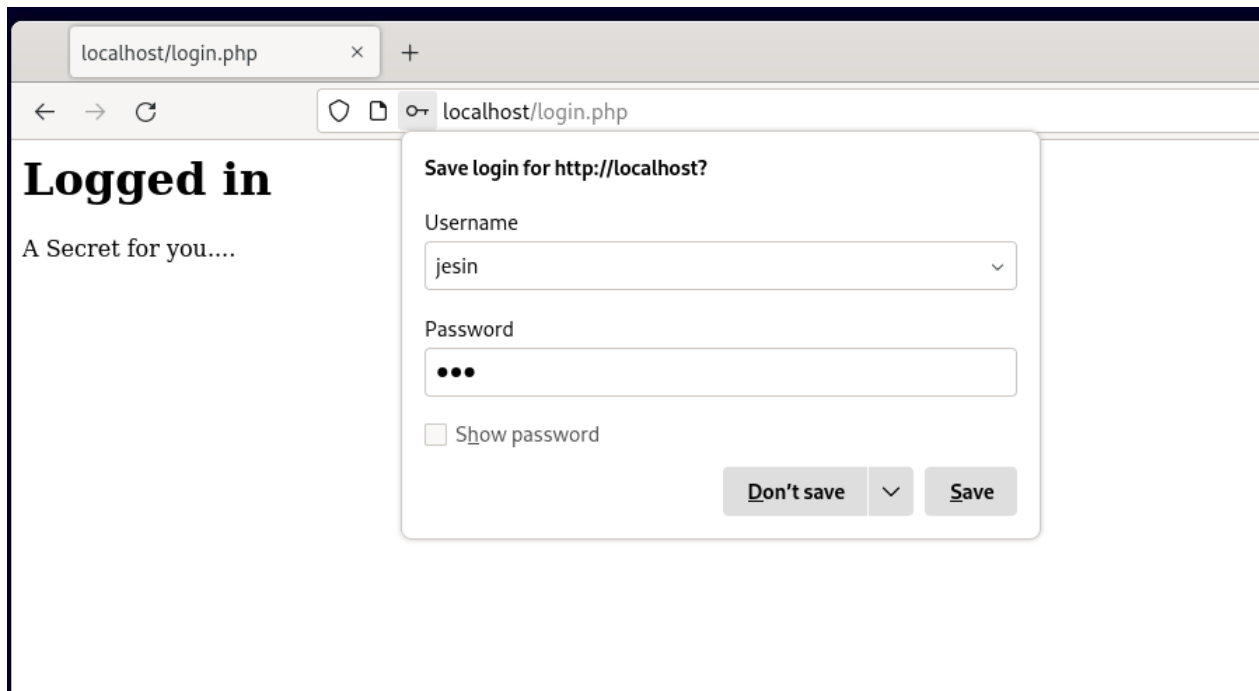
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

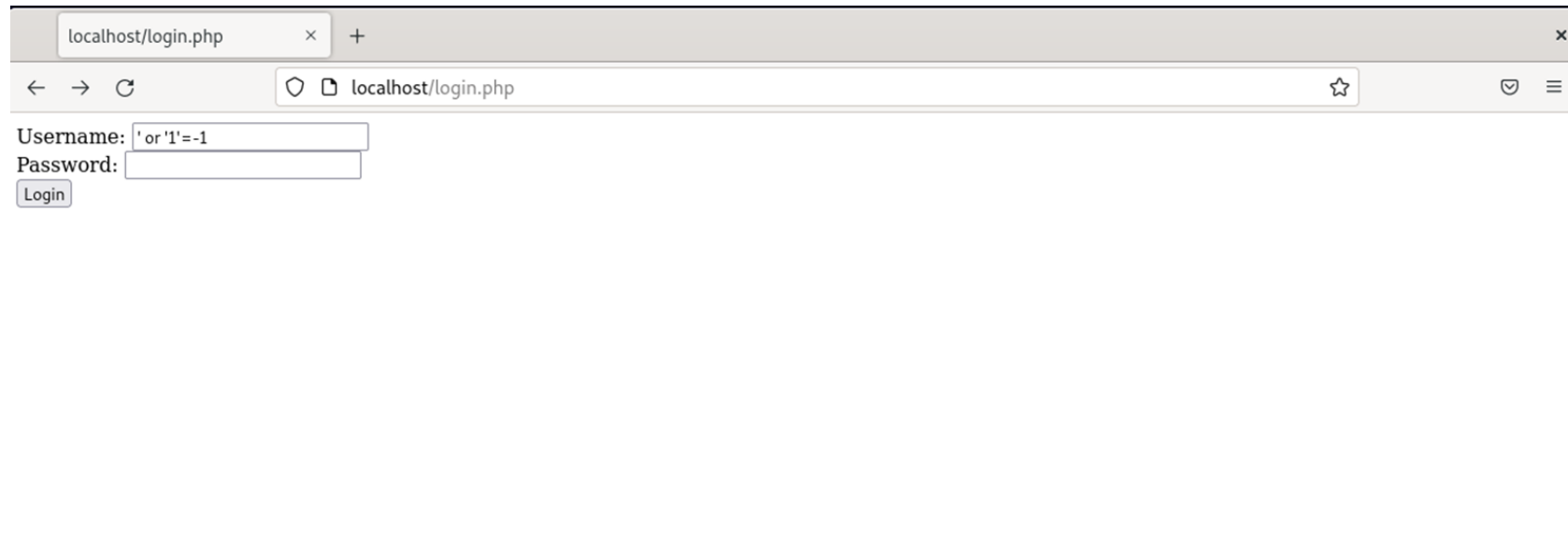
MariaDB [(none)]>
```

```
vboxuser@Debian11: ~  
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.  
  
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.  
  
MariaDB [(none)]> create database sample;  
Query OK, 1 row affected (0.001 sec)  
  
MariaDB [(none)]> connect sample;  
Connection id: 32  
Current database: sample  
  
MariaDB [sample]> create table users(username VARCHAR(100),password VARCHAR(100)  
);  
Query OK, 0 rows affected (0.010 sec)  
  
MariaDB [sample]> insert into users values('jesin','pwd');  
Query OK, 1 row affected (0.006 sec)  
  
MariaDB [sample]> insert into users values('alice','secret');  
Query OK, 1 row affected (0.002 sec)  
  
MariaDB [sample]> quit;  
Bye  
root@Debian11:/var/www/html#
```

```
vboxuser@Debian11: ~  
MariaDB [(none)]> create database sample;  
Query OK, 1 row affected (0.001 sec)  
  
MariaDB [(none)]> connect sample;  
Connection id: 32  
Current database: sample  
  
MariaDB [sample]> create table users(username VARCHAR(100),password VARCHAR(100  
);  
Query OK, 0 rows affected (0.010 sec)  
  
MariaDB [sample]> insert into users values('jesin','pwd');  
Query OK, 1 row affected (0.006 sec)  
  
MariaDB [sample]> insert into users values('alice','secret');  
Query OK, 1 row affected (0.002 sec)  
  
MariaDB [sample]> quit;  
Bye  
root@Debian11:/var/www/html# systemctl restart mysql  
root@Debian11:/var/www/html# systemctl restart apache2  
root@Debian11:/var/www/html#  
root@Debian11:/var/www/html#
```

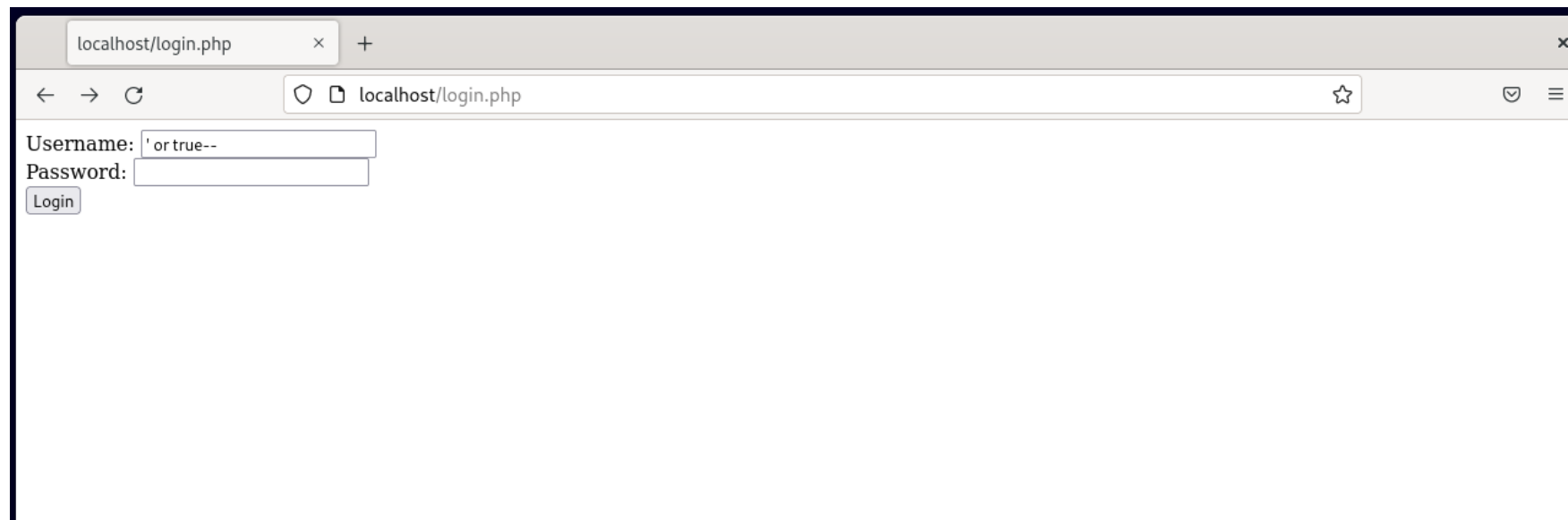


Replica el ataque SQL realizado en clase



A screenshot of a web browser window with the address bar showing 'localhost/login.php'. The page contains a login form with the following fields and elements:

- Username:** A text input field containing the payload `'or '1'=-1`.
- Password:** An empty password input field.
- Login:** A button labeled 'Login'.



A second screenshot of the same web browser window, showing the login page with a different SQL injection payload in the username field:

- Username:** A text input field containing the payload `'or true--`.
- Password:** An empty password input field.
- Login:** A button labeled 'Login'.

Demuestra que ModSecurity funciona en modo detección y en modo bloqueo

```
vboxuser@Debian11: ~  
g "platform-multi"] [tag "attack-generic"]  
Message: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "91"] [id "980130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 5 - SQLI=5,XSS=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 5, 0, 0, 0"] [ver "OWASP_CRS/3.3.0"] [tag "event-correlation"]  
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 127.0.0.1] ModSecurity: Warning. detected SQLi using libinjection with fingerprint 's&sol' [file "/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [line "65"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [data "Matched Data: s&sol found within ARGS:username: ' or '1'=-1"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWASP_CRS"] [tag "capec/1000/152/248/66"] [tag "PCI/6.5.2"] [hostname "localhost"] [uri "/login.php"] [unique_id "Y_GdRm8tyDI6Iu216SLewQAAAAE"]  
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 127.0.0.1] ModSecurity: Warning. Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 5)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "localhost"] [uri "/login.php"] [unique_id "Y_GdRm8tyDI6Iu216SLewQAAAAE"]  
Apache-Error: [file "./sapi/apache2handler/sapi_apache2.c"] [line 349] [level 4] PHP Warning: mysqli_num_rows() expects parameter 1 to be mysqli_result, bool g
```


Logged in

A Secret for you....

```
vboxuser@Debian11: ~
--dlcaf617-H--
Message: Warning. detected SQLi using libinjection with fingerprint 's&lc' [file
"/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [l
ine "65"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [
data "Matched Data: s&lc found within ARGS:username: ' or true-- "] [severity "C
RITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi
"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWA
SP_CRS"] [tag "capec/1000/152/248/66"] [tag "PCI/6.5.2"]
Message: Warning. Operator GE matched 5 at TX:anomaly_score. [file "/usr/share/m
odsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "93"] [id "949
110"] [msg "Inbound Anomaly Score Exceeded (Total Score: 5)"] [severity "CRITICA
L"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi"] [ta
g "platform-multi"] [tag "attack-generic"]
Message: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr
/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "91"] [id "98
0130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 5 - SQLI=5,XSS
=0,RFI=0,LFI=0,RCE=0,PHPI=0,HTTP=0,SESS=0): individual paranoia level scores: 5,
0, 0, 0"] [ver "OWASP_CRS/3.3.0"] [tag "event-correlation"]
Apache-Error: [file "apache2_util.c"] [line 271] [level 3] [client 127.0.0.1] Mo
dSecurity: Warning. detected SQLi using libinjection with fingerprint 's&lc' [fi
le "/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"]
[line "65"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"]
[data "Matched Data: s&lc found within ARGS:username: ' or true-- "] [severity
"CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-mul
```

```
vboxuser@Debian11: ~
GNU nano 5.4 modsecurity.conf *
# -- Rule engine initialization -----

# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
#SecRuleEngine DetectionOnly
SecRuleEngine On

# -- Request body handling -----

# Allow ModSecurity to access request bodies. If you don't, ModSecurity
# won't be able to see any POST parameters, which opens a large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On

# Enable XML request body parser.
# Initiate XML Processor in case of xml content-type
[ Read 226 lines ]
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^ Go To Line
```

localhost/login.php × +

← → ↻

localhost/login.php

☆

🔒 ☰

Username:

' or true--

Password:

Login

403 Forbidden

localhost/login.php

Forbidden

You don't have permission to access this resource.

Apache/2.4.54 (Debian) Server at localhost Port 80

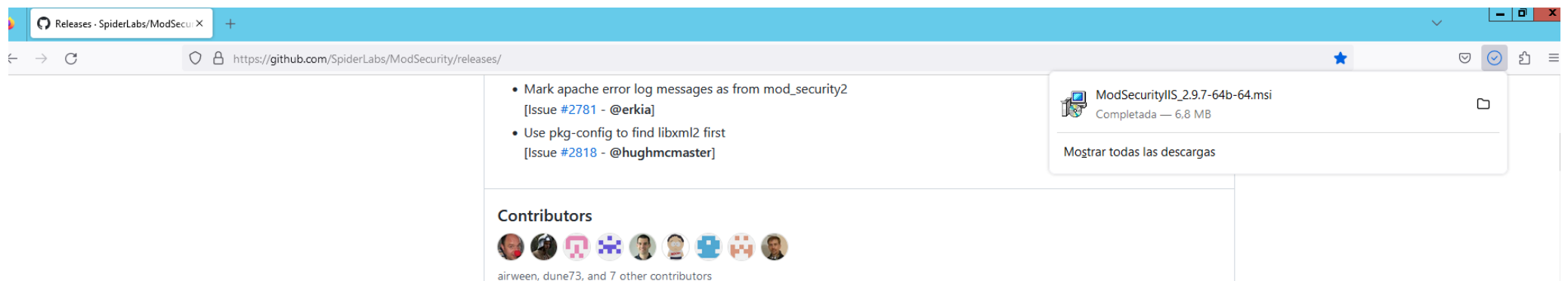
vboxuser@Debian11: ~

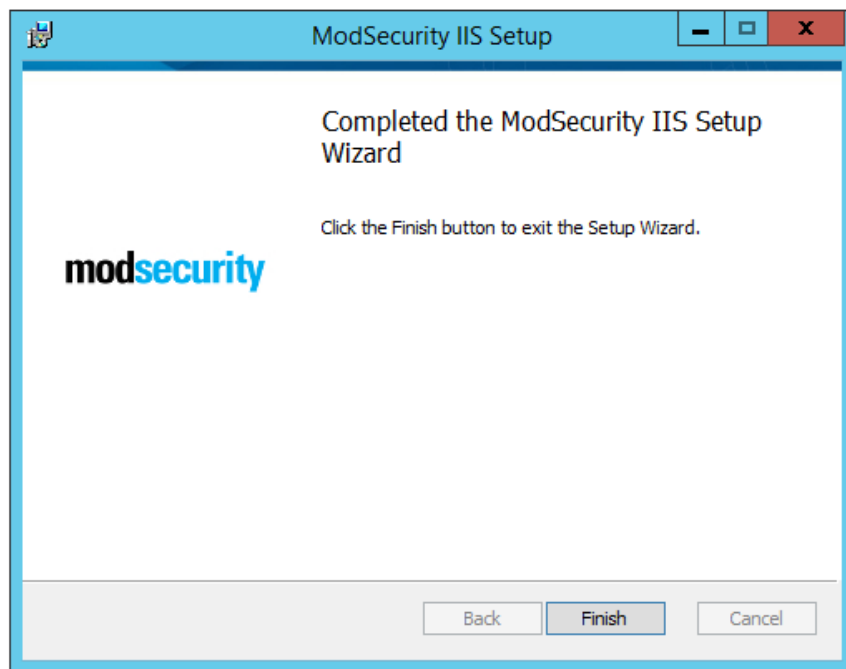
```
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.54 (Debian) Server at localhost Port 80</address>
</body></html>

--d9810a54-H--
Message: Warning. detected SQLi using libinjection with fingerprint 's&lc' [file
"/usr/share/modsecurity-crs/rules/REQUEST-942-APPLICATION-ATTACK-SQLI.conf"] [l
ine "65"] [id "942100"] [msg "SQL Injection Attack Detected via libinjection"] [
data "Matched Data: s&lc found within ARGS:username: 'or true--'"] [severity "C
RITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-multi"] [tag "language-multi
"] [tag "platform-multi"] [tag "attack-sqli"] [tag "paranoia-level/1"] [tag "OWA
SP_CRS"] [tag "capec/1000/152/248/66"] [tag "PCI/6.5.2"]
Message: Access denied with code 403 (phase 2). Operator GE matched 5 at TX:anom
aly_score. [file "/usr/share/modsecurity-crs/rules/REQUEST-949-BLOCKING-EVALUATI
ON.conf"] [line "93"] [id "949110"] [msg "Inbound Anomaly Score Exceeded (Total
Score: 5)"] [severity "CRITICAL"] [ver "OWASP_CRS/3.3.0"] [tag "application-mult
i"] [tag "language-multi"] [tag "platform-multi"] [tag "attack-generic"]
Message: Warning. Operator GE matched 5 at TX:inbound_anomaly_score. [file "/usr
/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.conf"] [line "91"] [id "98
0130"] [msg "Inbound Anomaly Score Exceeded (Total Inbound Score: 5 - SQLI=5,XSS
```

Instalar ModSecurity en Windows Server 2012:

<https://techexpert.tips/es/iis-es/iis-instalacion-de-modsecurity/>





Microsoft Windows [Versión 6.3.9600]

(c) 2013 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>cd ..

C:\Users>cd ..

C:\>cd /"Program Files"

C:\Program Files>dir

El volumen de la unidad C no tiene etiqueta.

El número de serie del volumen es: 2E22-7144

Directorio de C:\Program Files

19/02/2023	21:35	<DIR>	.
19/02/2023	21:35	<DIR>	..
22/08/2013	16:39	<DIR>	Common Files
18/03/2014	10:55	<DIR>	Internet Explorer
19/02/2023	21:35	<DIR>	ModSecurity IIS
19/02/2023	21:32	<DIR>	Mozilla Firefox
02/03/2021	21:55	<DIR>	Oracle
22/08/2013	16:39	<DIR>	Windows Mail
22/08/2013	16:39	<DIR>	Windows NT
22/08/2013	16:39	<DIR>	WindowsPowerShell
		0 archivos	0 bytes
		10 dirs	10.942.070.784 bytes libres

C:\Program Files>cd "ModSecurity IIS"

C:\Program Files\ModSecurity IIS>dir

El volumen de la unidad C no tiene etiqueta.

El número de serie del volumen es: 2E22-7144

Directorio de C:\Program Files\ModSecurity IIS

19/02/2023	21:35	<DIR>	.
19/02/2023	21:35	<DIR>	..
04/01/2023	17:49		9.829 EULA.rtf
04/01/2023	17:49		2.042 list_dependencies.bat
04/01/2023	17:49		8.620 modsecurity.conf
04/01/2023	17:48		366 ModSecurity.xml
04/01/2023	17:49		25 modsecurity_iis.conf
04/01/2023	17:49		659 README.TXT
04/01/2023	17:49		53.146 unicode.mapping
		7 archivos	74.687 bytes
		2 dirs	10.942.070.784 bytes libres



Pegar



Copiar

Courier New 11

A A



N K S

abc

X₂ X₂

A



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo



Párrafo

```
# based on modsecurity.conf-recommended
# -- Rule engine
initialization -----

# Enable ModSecurity, attaching it to every transaction. Use
detection
# only to start with, because that minimises the chances of
post-installation
# disruption.
#
SecRuleEngine DetectionOnly

# -- Request body
handling -----

# Allow ModSecurity to access request bodies. If you don't,
ModSecurity
# won't be able to see any POST parameters, which opens a
large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On

# SecStreamInBodyInspection is required by IIS for proper body
inspection
# See issue #1299 for more information
```


Archivo Inicio Ver



Pegar



Cortar

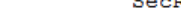
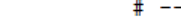
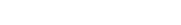
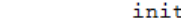
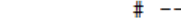
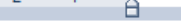
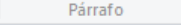
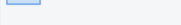


Copiar

Portapapeles

Courier New 11 A⁺ A⁻N K S abe x₂ x²

Fuente



Párrafo



Imagen



Pintar



Fecha



y hora



Insertar



objeto



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Insertar



Buscar

Reemplazar

Seleccionar todo

Edición

```
# based on modsecurity.conf-recommended
# -- Rule engine
initialization -----

# Enable ModSecurity, attaching it to every transaction. Use
detection
# only to start with, because that minimises the chances of
post-installation
# disruption.
#
SecRuleEngine On

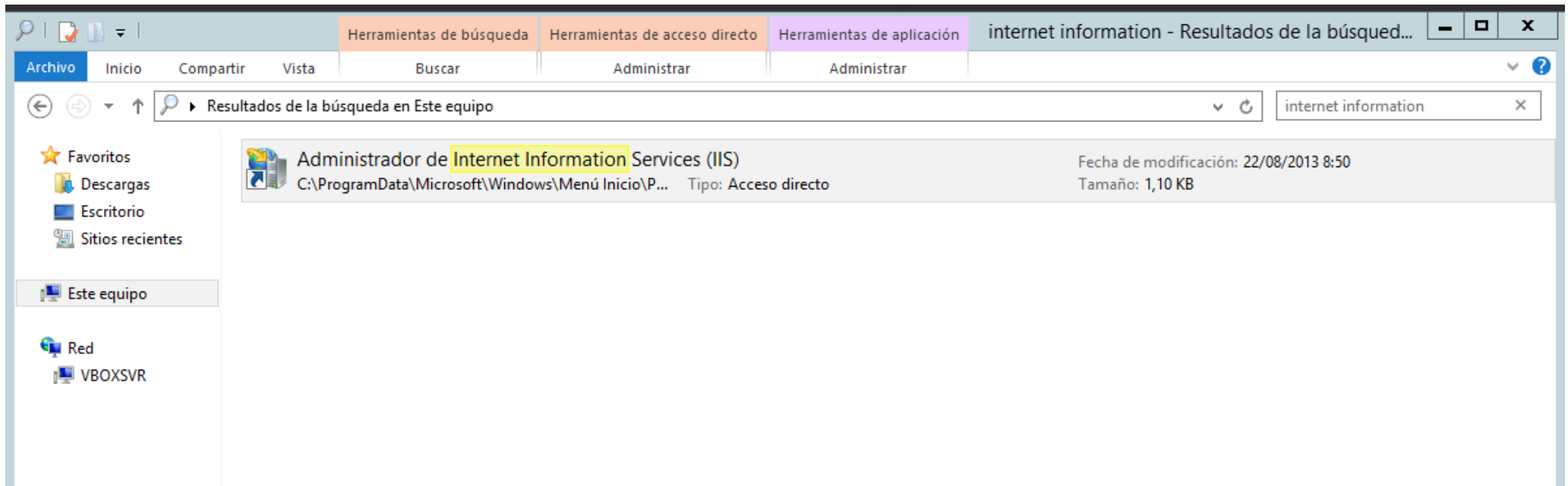
# -- Request body
handling -----

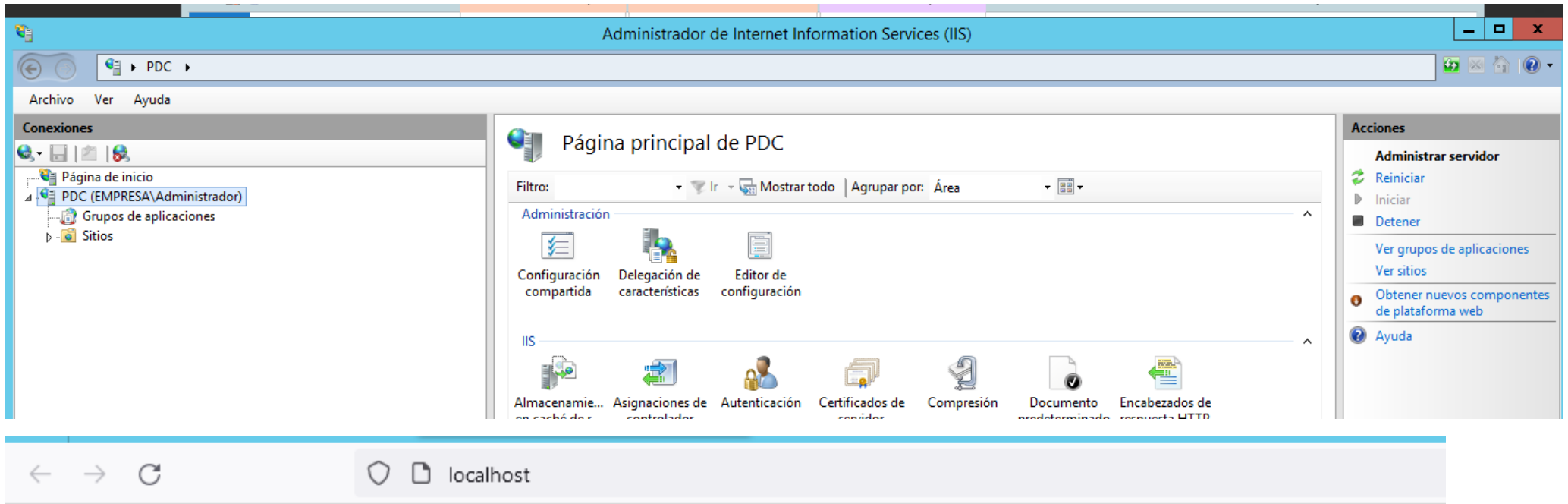
# Allow ModSecurity to access request bodies. If you don't,
ModSecurity
# won't be able to see any POST parameters, which opens a
large security
# hole for attackers to exploit.
#
SecRequestBodyAccess On

# SecStreamInBodyInspection is required by IIS for proper body
inspection
# See issue #1299 for more information
```

```
C:\Program Files\ModSecurity IIS>caccls C:\inetpub\temp /e /p IIS_IUSRS:f
directorio procesado: C:\inetpub\temp

C:\Program Files\ModSecurity IIS>
```





Service Unavailable

HTTP Error 503. The service is unavailable.