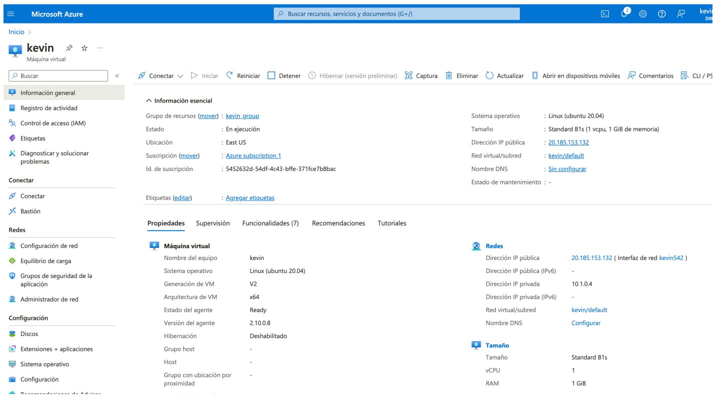
Procedure for Creating the Virtual Machine and WAF. An example attacks.

Name: Kevin Huertas

---------Procedure-------

Starting VM on Azure::



kevin
Máquina virtual

Información esencial

Grupo de recursos (mover) : kevin_group
Estado : En ejecución
Ubicación : East US
Suscripción (mover) : Azure subscription 1
Id. de suscripción : 5452632d-54df-4c43-bffe-371fce7b8bac

Etiquetas (editar) : Agregar etiquetas

Sistema operativo : Linux (ubuntu 20.04)
Tamaño : Standard B1s (1 vcpu, 1 GiB de memoria)
Dirección IP pública : 20.185.153.132
Red virtual/subred : kevin/default
Nombre DNS : Sin configurar
Estado de mantenimiento : -

Máquina virtual

Nombre del equipo kevin
Sistema operativo Linux (ubuntu 20.04)
Generación de VM V2
Arquitectura de VM x64
Estado del agente Ready
Versión del agente 2.10.0.8
Hibernación Deshabilitado
Grupo host -
Host -
Grupo con ubicación por proximidad -

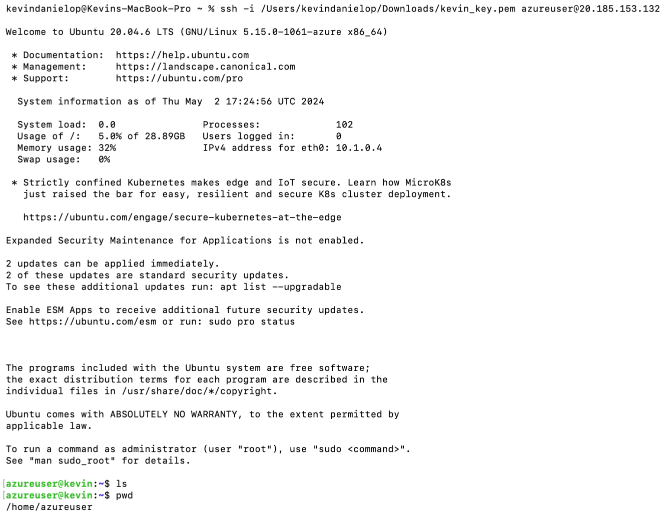
Redes

Dirección IP pública 20.185.153.132 (Interfaz de red kevin542)
Dirección IP pública (IPv6) -
Dirección IP privada 10.1.0.4
Dirección IP privada (IPv6) -
Red virtual/subred kevin/default
Nombre DNS Configurar

Tamaño

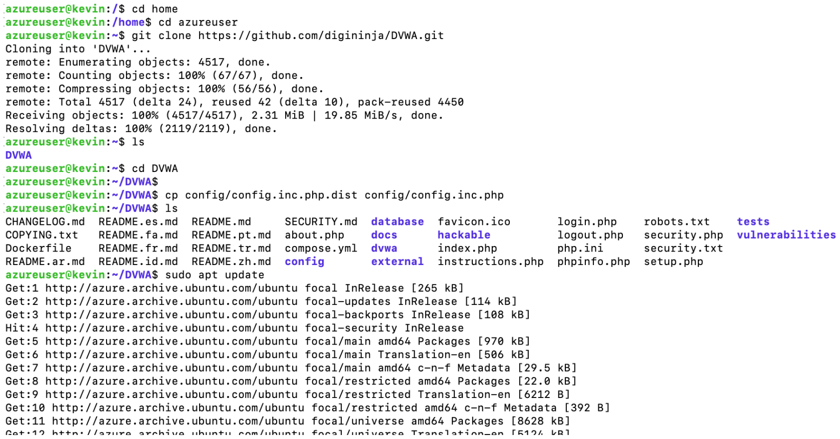
Tamaño Standard B1s
vCPU 1
RAM 1 GiB

Once the virtual machine is created, I connect to it through my terminal using the SSH key.

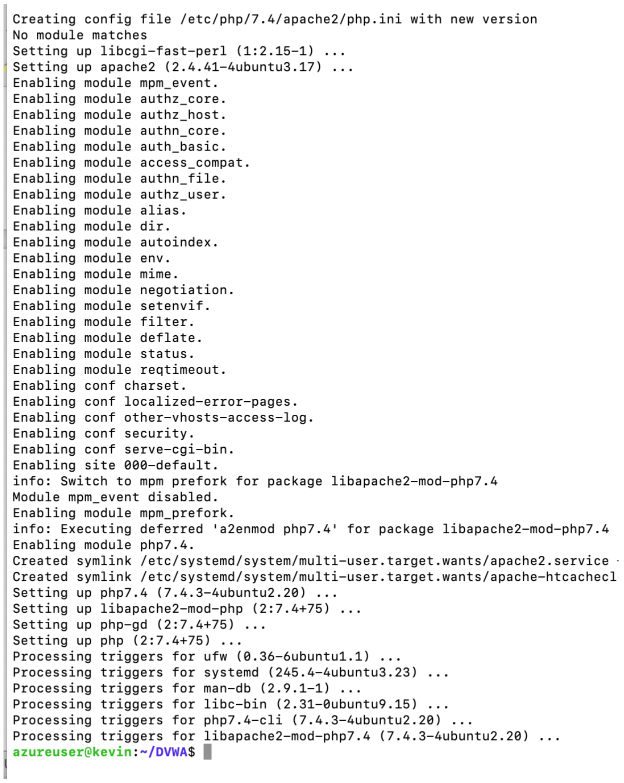


```
kevindanielop@Kevins-MacBook-Pro ~ % ssh -i /Users/kevindanielop/Downloads/kevin_key.pem azureuser@20.185.153.132

Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1061-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

  System information as of Thu May  2 17:24:56 UTC 2024

  System load:  0.0               Processes:             102
  Usage of /:   5.0% of 28.89GB   Users logged in:       0
  Memory usage: 32%               IPv4 address for eth0: 10.1.0.4
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

2 updates can be applied immediately.
2 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

azureuser@kevin:~$ ls
azureuser@kevin:~$ pwd
/home/azureuser
```

Once connected, I proceed to clone the DVWA project and follow the steps outlined in the GitHub Readme.

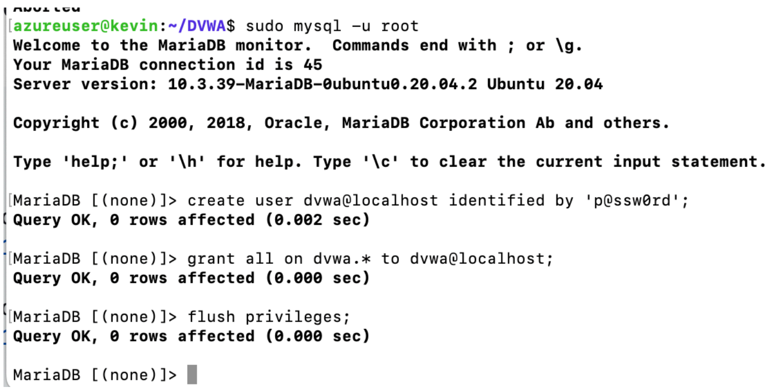


```
azureuser@kevin:/$ cd home
azureuser@kevin:/home$ cd azureuser
azureuser@kevin:~$ git clone https://github.com/digininja/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 4517, done.
remote: Counting objects: 100% (67/67), done.
remote: Compressing objects: 100% (56/56), done.
remote: Total 4517 (delta 24), reused 42 (delta 10), pack-reused 4450
Receiving objects: 100% (4517/4517), 2.31 MiB | 19.85 MiB/s, done.
Resolving deltas: 100% (2119/2119), done.
azureuser@kevin:~$ ls
DVWA
azureuser@kevin:~$ cd DVWA
azureuser@kevin:~/DVWA$
azureuser@kevin:~/DVWA$ cp config/config.inc.php.dist config/config.inc.php
azureuser@kevin:~/DVWA$ ls
CHANGELOG.md  README.es.md  README.md     SECURITY.md  database  favicon.ico       login.php    robots.txt    tests
COPYING.txt   README.fa.md  README.pt.md  about.php    docs      hackable          logout.php   security.php  vulnerabilities
Dockerfile    README.fr.md  README.tr.md  compose.yml  dvwa      index.php         php.ini      security.txt
README.ar.md  README.id.md  README.zh.md  config       external  instructions.php  phpinfo.php  setup.php
azureuser@kevin:~/DVWA$ sudo apt update
Get:1 http://azure.archive.ubuntu.com/ubuntu focal InRelease [265 kB]
Get:2 http://azure.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Hit:4 http://azure.archive.ubuntu.com/ubuntu focal-security InRelease
Get:5 http://azure.archive.ubuntu.com/ubuntu focal/main amd64 Packages [970 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu focal/main Translation-en [506 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu focal/main amd64 c-n-f Metadata [29.5 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu focal/restricted amd64 Packages [22.0 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu focal/restricted Translation-en [6212 B]
Get:10 http://azure.archive.ubuntu.com/ubuntu focal/restricted amd64 c-n-f Metadata [392 B]
Get:11 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB]
Get:12 http://azure.archive.ubuntu.com/ubuntu focal/universe Translation-en [5124 kB]
```

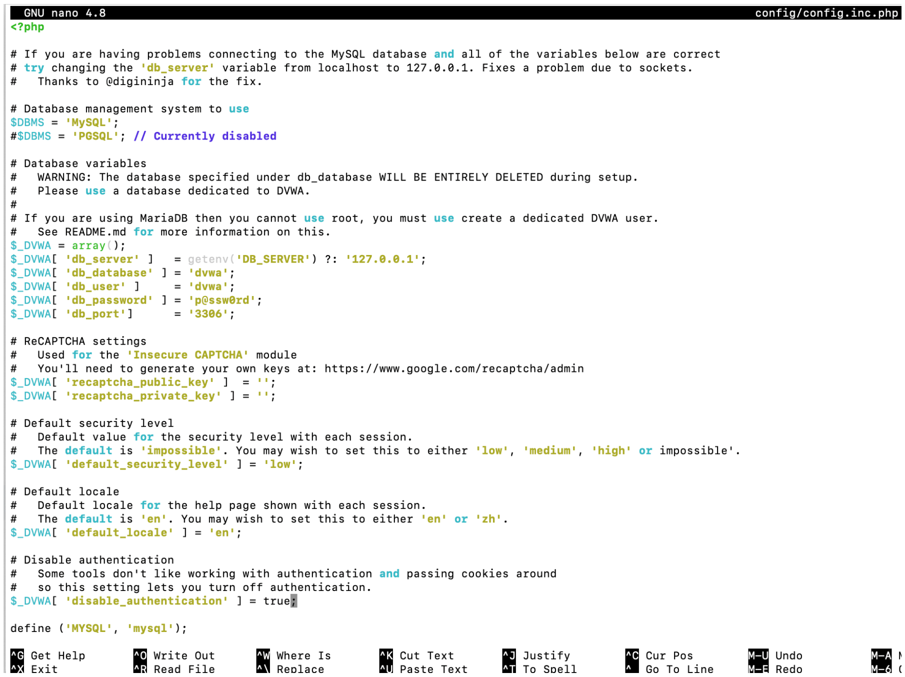


```
Creating config file /etc/php/7.4/apache2/php.ini with new version
No module matches
Setting up libcgi-fast-perl (1:2.15-1) ...
Setting up apache2 (2.4.41-4ubuntu3.17) ...
Enabling module mpm_event.
Enabling module authz_core.
Enabling module authz_host.
Enabling module authn_core.
Enabling module auth_basic.
Enabling module access_compat.
Enabling module authn_file.
Enabling module authz_user.
Enabling module alias.
Enabling module dir.
Enabling module autoindex.
Enabling module env.
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
info: Switch to mpm prefork for package libapache2-mod-php7.4
Module mpm_event disabled.
Enabling module mpm_prefork.
info: Executing deferred 'a2enmod php7.4' for package libapache2-mod-php7.4
Enabling module php7.4.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcachecl
Setting up php7.4 (7.4.3-4ubuntu2.20) ...
Setting up libapache2-mod-php (2:7.4+75) ...
Setting up php-gd (2:7.4+75) ...
Setting up php (2:7.4+75) ...
Processing triggers for ufw (0.36-6ubuntu1.1) ...
Processing triggers for systemd (245.4-4ubuntu3.23) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.15) ...
Processing triggers for php7.4-cli (7.4.3-4ubuntu2.20) ...
Processing triggers for libapache2-mod-php7.4 (7.4.3-4ubuntu2.20) ...
azureuser@kevin:~/DVWA$
```

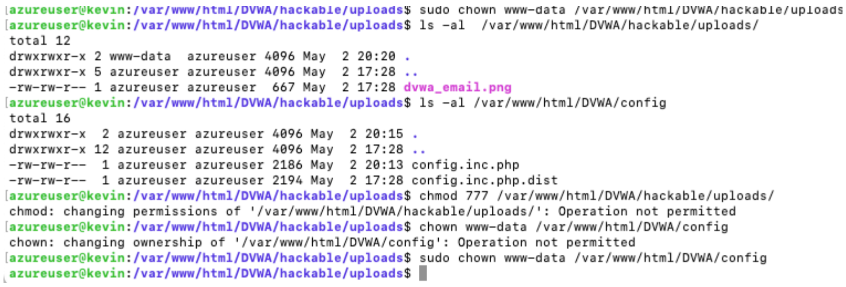
I start the database with the configuration provided in the Readme.q



```
Aborted
azureuser@kevin:~/DVWA$ sudo mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 45
Server version: 10.3.39-MariaDB-0ubuntu0.20.04.2 Ubuntu 20.04

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 user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]>
```

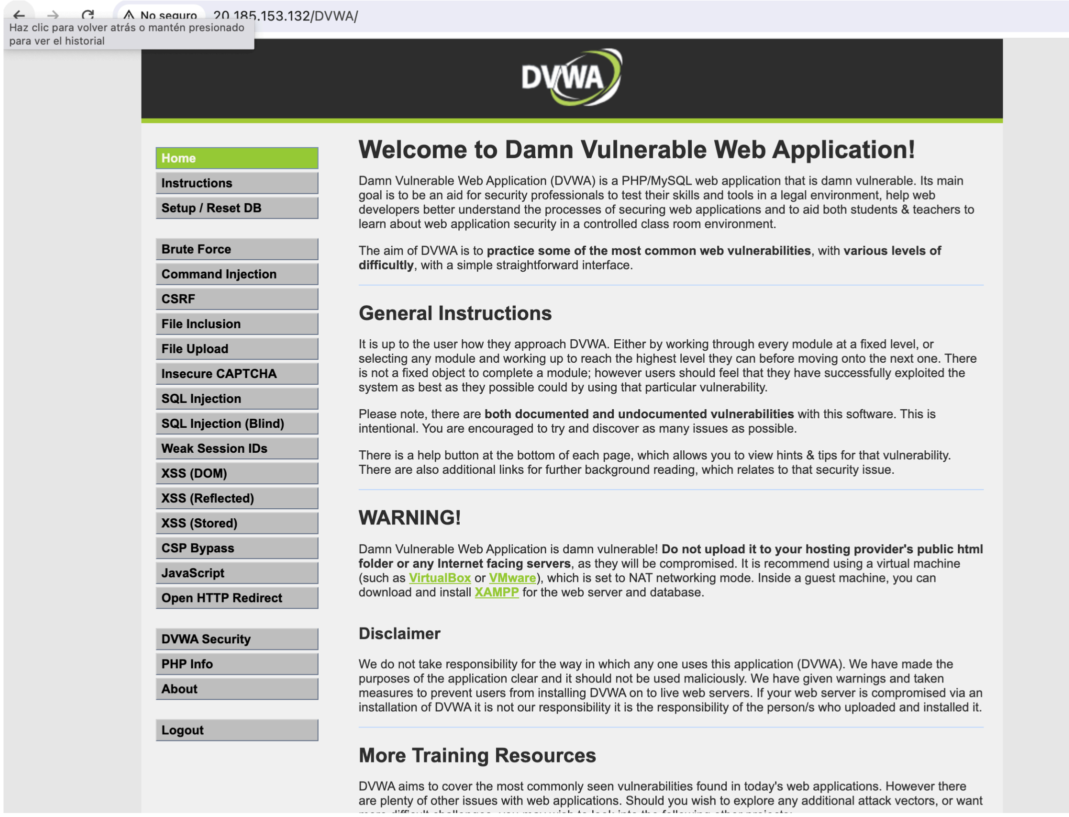


```
  GNU nano 4.8                                                                                        config/config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a dedicated DVWA user.
#   See README.md for more information on this.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'dvwa';
$_DVWA[ 'db_password' ] = 'p@ssw0rd';
$_DVWA[ 'db_port']      = '3306';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin
$_DVWA[ 'recaptcha_public_key' ]  = '';
$_DVWA[ 'recaptcha_private_key' ] = '';

# Default security level
#   Default value for the security level with each session.
#   The default is 'impossible'. You may wish to set this to either 'low', 'medium', 'high' or impossible'.
$_DVWA[ 'default_security_level' ] = 'low';

# Default locale
#   Default locale for the help page shown with each session.
#   The default is 'en'. You may wish to set this to either 'en' or 'zh'.
$_DVWA[ 'default_locale' ] = 'en';

# Disable authentication
#   Some tools don't like working with authentication and passing cookies around
#   so this setting lets you turn off authentication.
$_DVWA[ 'disable_authentication' ] = true;

define ('MYSQL', 'mysql');

^G Get Help      ^O Write Out     ^W Where Is      ^K Cut Text      ^J Justify       ^C Cur Pos       M-U Undo         M-A
^X Exit          ^R Read File     ^\ Replace       ^U Paste Text    ^T To Spell      ^_ Go To Line    M-E Redo         M-6
```



```
azureuser@kevin:/var/www/html/DVWA/hackable/uploads$ sudo chown www-data /var/www/html/DVWA/hackable/uploads
azureuser@kevin:/var/www/html/DVWA/hackable/uploads$ ls -al  /var/www/html/DVWA/hackable/uploads/
total 12
drwxrwxr-x 2 www-data  azureuser 4096 May  2 20:20 .
drwxrwxr-x 5 azureuser azureuser 4096 May  2 17:28 ..
-rw-rw-r-- 1 azureuser azureuser  667 May  2 17:28 dvwa_email.png
azureuser@kevin:/var/www/html/DVWA/hackable/uploads$ ls -al /var/www/html/DVWA/config
total 16
drwxrwxr-x  2 azureuser azureuser 4096 May  2 20:15 .
drwxrwxr-x 12 azureuser azureuser 4096 May  2 17:28 ..
-rw-rw-r--  1 azureuser azureuser 2186 May  2 20:13 config.inc.php
-rw-rw-r--  1 azureuser azureuser 2194 May  2 17:28 config.inc.php.dist
azureuser@kevin:/var/www/html/DVWA/hackable/uploads$ chmod 777 /var/www/html/DVWA/hackable/uploads/
chmod: changing permissions of '/var/www/html/DVWA/hackable/uploads/': Operation not permitted
azureuser@kevin:/var/www/html/DVWA/hackable/uploads$ chown www-data /var/www/html/DVWA/config
chown: changing ownership of '/var/www/html/DVWA/config': Operation not permitted
azureuser@kevin:/var/www/html/DVWA/hackable/uploads$ sudo chown www-data /var/www/html/DVWA/config
azureuser@kevin:/var/www/html/DVWA/hackable/uploads$
```

Once configured, we have our web app up and running. We set everything to carry out the attacks.



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

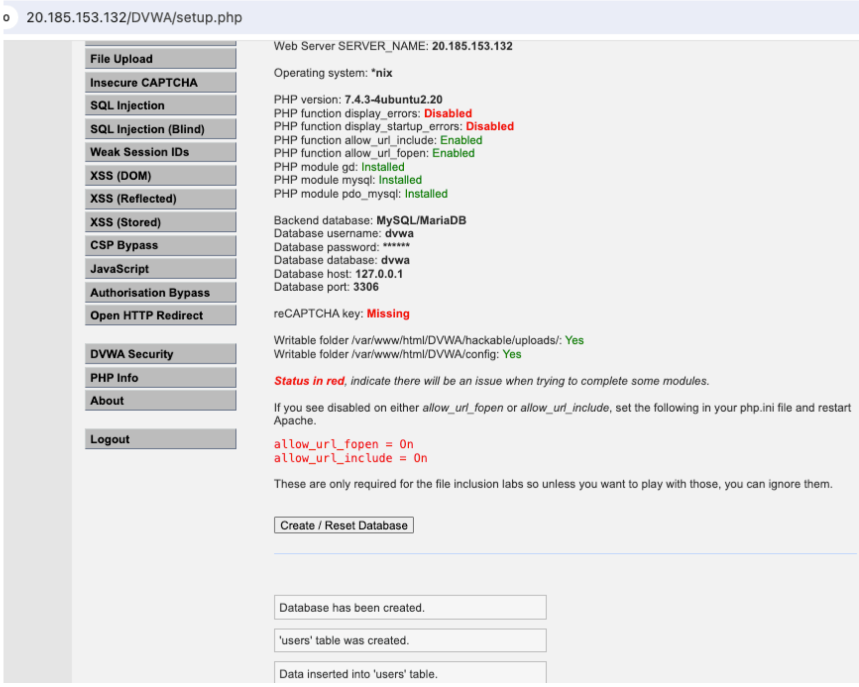
Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want



Web Server SERVER_NAME: **20.185.153.132**

Operating system: ***nix**

PHP version: **7.4.3-4ubuntu2.20**
PHP function display_errors: **Disabled**
PHP function display_startup_errors: **Disabled**
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

Backend database: **MySQL/MariaDB**
Database username: **dvwa**
Database password: **********
Database database: **dvwa**
Database host: **127.0.0.1**
Database port: **3306**

reCAPTCHA key: **Missing**

Writable folder /var/www/html/DVWA/hackable/uploads/: Yes
Writable folder /var/www/html/DVWA/config: Yes

***Status in red**, indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

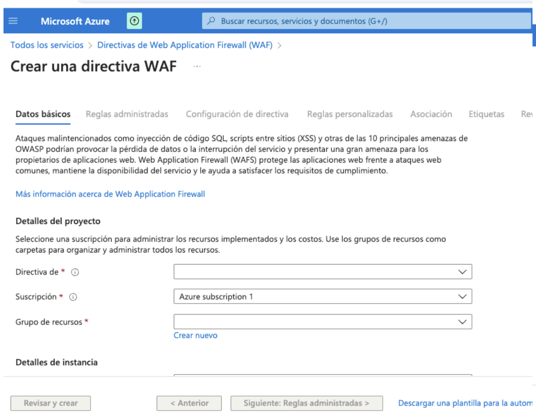
These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Database has been created.

'users' table was created.

Data inserted into 'users' table.

Ahora creamos el recurso WAF en Azure:


Microsoft Azure
Buscar recursos, servicios y documentos (G+/)
Todos los servicios > Directivas de Web Application Firewall (WAF) >
Datos básicos
Reglas administradas
Configuración de directiva
Reglas personalizadas
Asociación
Etiquetas
Revisar y crear
< Anterior
Siguiente: Reglas administradas >
Descargar una plantilla para la autom

Crear una directiva WAF

Ataques malintencionados como inyección de código SQL, scripts entre sitios (XSS) y otras de las 10 principales amenazas de OWASP podrían provocar la pérdida de datos o la interrupción del servicio y presentar una gran amenaza para los propietarios de aplicaciones web. Web Application Firewall (WAFS) protege las aplicaciones web frente a ataques web comunes, mantiene la disponibilidad del servicio y le ayuda a satisfacer los requisitos de cumplimiento.

Más información acerca de Web Application Firewall

Detalles del proyecto

Seleccione una suscripción para administrar los recursos implementados y los costos. Use los grupos de recursos como carpetas para organizar y administrar todos los recursos.

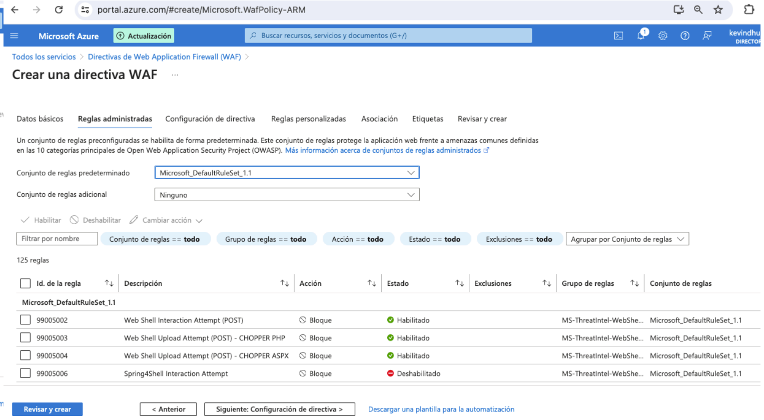
Directiva de *:

Suscripción *: Azure subscription 1

Grupo de recursos *:

Crear nuevo

Detalles de instancia


portal.azure.com/#create/Microsoft.WafPolicy-ARM
Microsoft Azure
Actualización
Buscar recursos, servicios y documentos (G+/)
kevindhu
DIRECTOR
Todos los servicios > Directivas de Web Application Firewall (WAF) >
Datos básicos
Reglas administradas
Configuración de directiva
Reglas personalizadas
Asociación
Etiquetas
Revisar y crear
Habilitar
Deshabilitar
Cambiar acción
Revisar y crear
< Anterior
Siguiente: Configuración de directiva >
Descargar una plantilla para la automatización

Crear una directiva WAF

Un conjunto de reglas preconfiguradas se habilita de forma predeterminada. Este conjunto de reglas protege la aplicación web frente a amenazas comunes definidas en las 10 categorías principales de Open Web Application Security Project (OWASP). Más información acerca de conjuntos de reglas administrados

Conjunto de reglas predeterminado: Microsoft_DefaultRuleSet_1.1

Conjunto de reglas adicional: Ninguno

Filtrar por nombre | Conjunto de reglas == **todo** | Grupo de reglas == **todo** | Acción == **todo** | Estado == **todo** | Exclusiones == **todo** | Agrupar por Conjunto de reglas

125 reglas

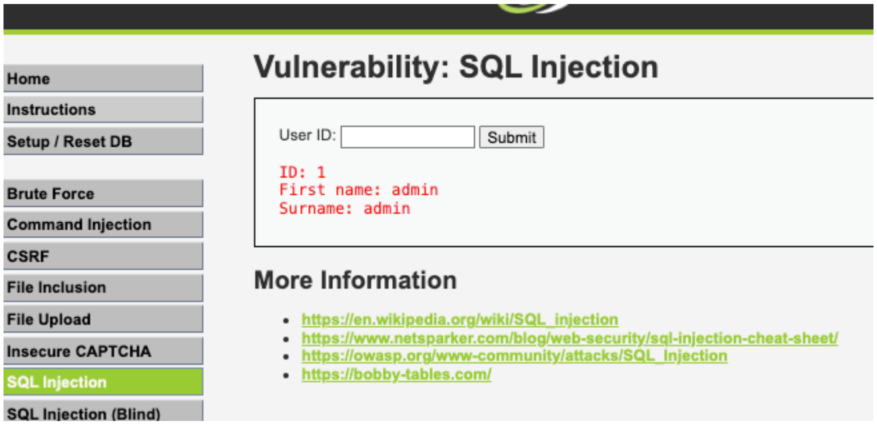
Id. de la regla	Descripción	Acción	Estado	Exclusiones	Grupo de reglas	Conjunto de reglas
Microsoft_DefaultRuleSet_1.1						
□ 99005002	Web Shell Interaction Attempt (POST)	Bloque	Habilitado		MS-ThreatIntel-WebShe...	Microsoft_DefaultRuleSet_1.1
□ 99005003	Web Shell Upload Attempt (POST) - CHOPPER PHP	Bloque	Habilitado		MS-ThreatIntel-WebShe...	Microsoft_DefaultRuleSet_1.1
□ 99005004	Web Shell Upload Attempt (POST) - CHOPPER ASPX	Bloque	Habilitado		MS-ThreatIntel-WebShe...	Microsoft_DefaultRuleSet_1.1
□ 99005006	Spring4Shell Interaction Attempt	Bloque	Deshabilitado		MS-ThreatIntel-WebShe...	Microsoft_DefaultRuleSet_1.1

Esta es una forma de hacerlo, pero luego despues de investigar me di cuenta que se puede hacer con un gateway, siendo una manera mas facil de conectar el WAF con la red de nuestra app.

---------Attacks-------

Probe con SQL Injection.

Without WAF, with ip: http://20.185.153.132/DVWA/vulnerabilities/sqli/



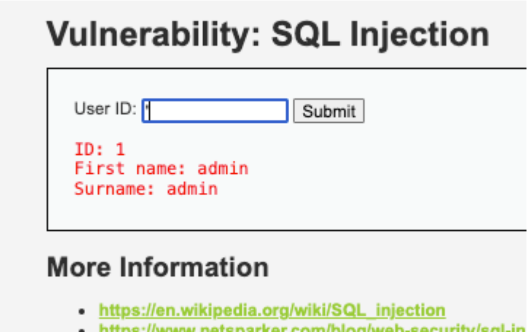
Vulnerability: SQL Injection

User ID:

```
ID: 1
First name: admin
Surname: admin
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/



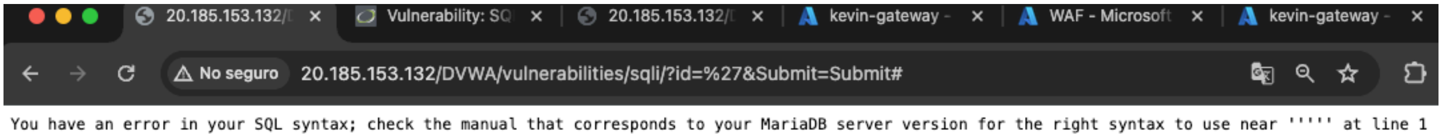
Vulnerability: SQL Injection

User ID: '

```
ID: 1
First name: admin
Surname: admin
```

More Information

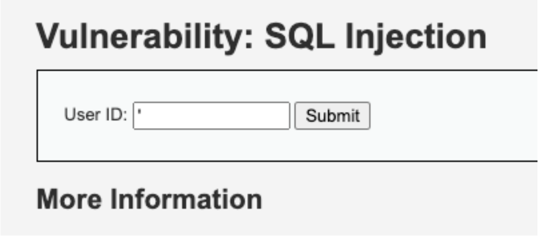
- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-in



20.185.153.132/DVWA/vulnerabilities/sqli/?id=%27&Submit=Submit#

```
You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''''' at line 1
```

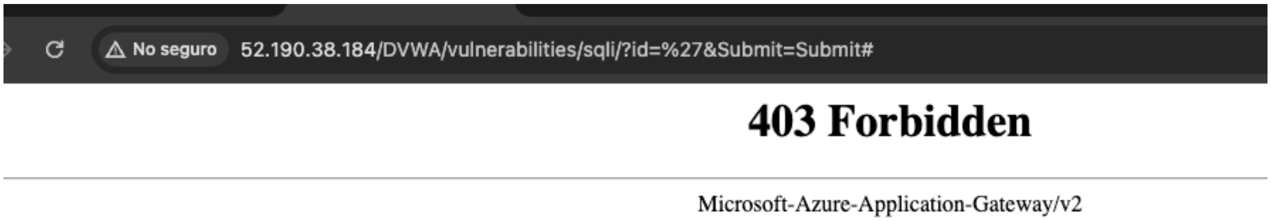
Now with WAF, with ip: http://52.190.38.184/DVWA/vulnerabilities/sqli/



Vulnerability: SQL Injection

User ID: '

More Information



52.190.38.184/DVWA/vulnerabilities/sqli/?id=%27&Submit=Submit#

403 Forbidden

Microsoft-Azure-Application-Gateway/v2

We can verify that the WAF is working by conducting an attack.