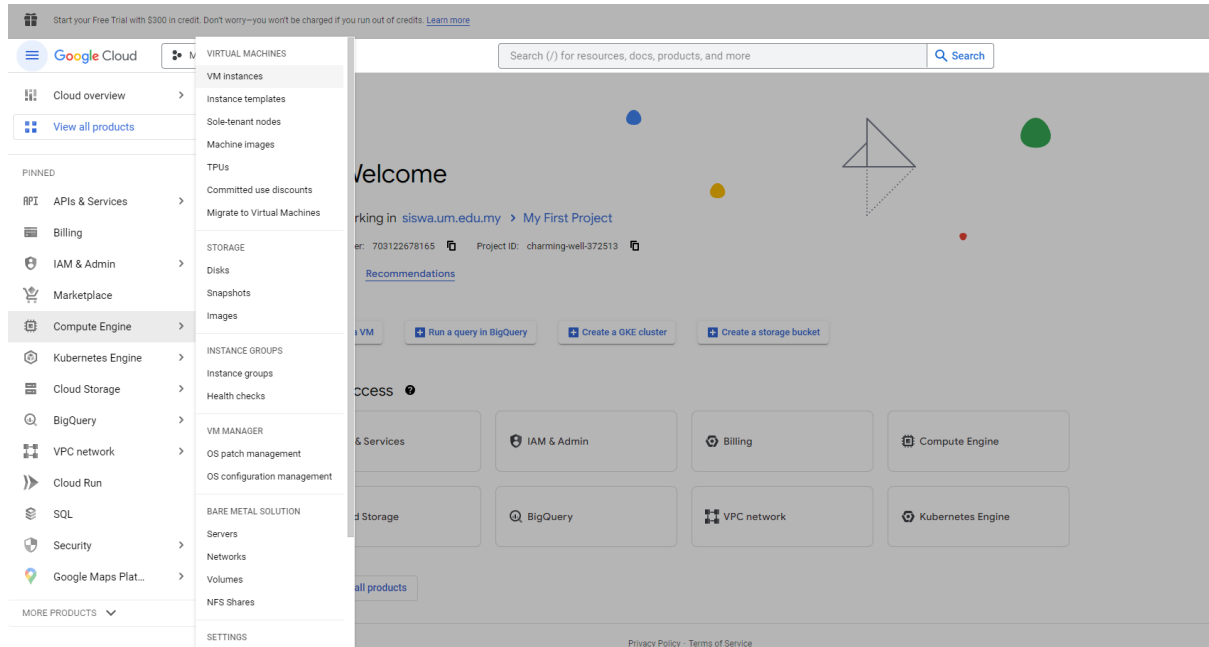


## DVWA MANUAL

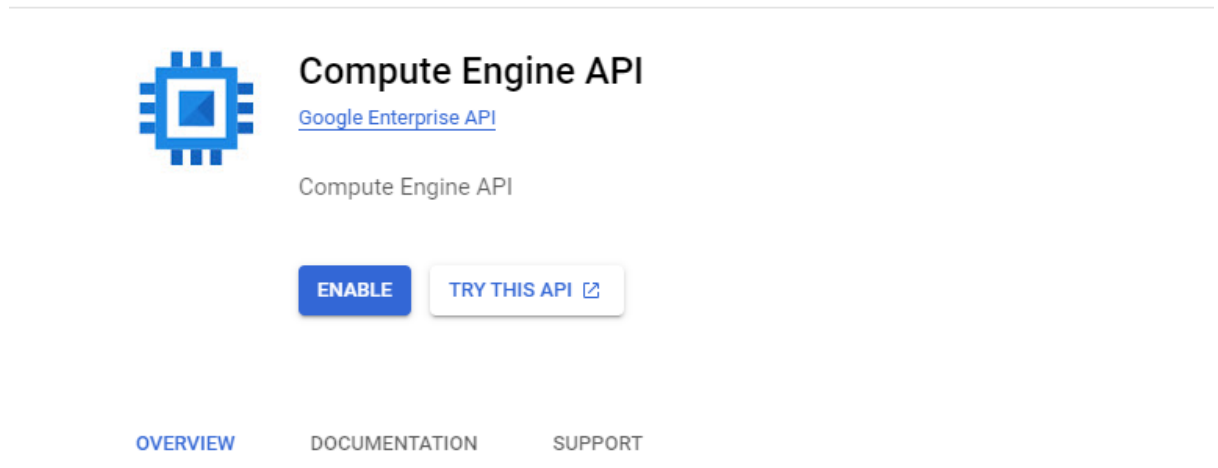
### GCP SETUP

1. Enter GCP
2. Create project
3. Go to Compute Engine > VM Instance

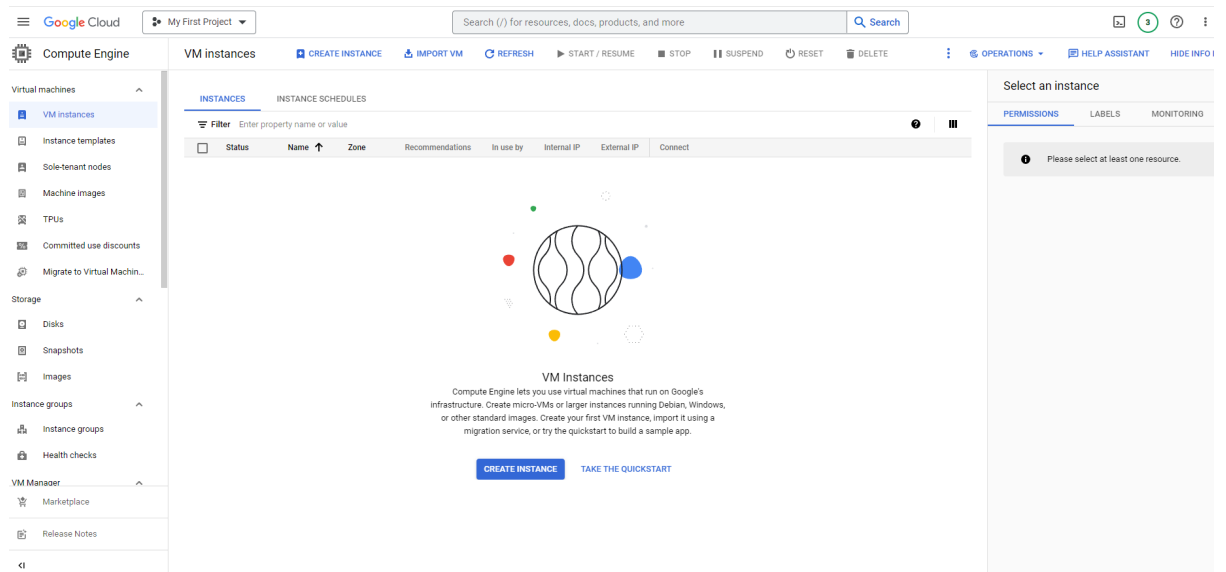


4. Enable Compute Engine API

← Product details




5. After enabling it will show this dashboard




6. Click create Instance

7. On the name field can put anything to your likings, same goes with region and zone. On machine config leave it as default

 Make sure all fields are correct to continue

Name \*  
dvwaubuntu

?

Labels 

+ ADD LABELS

Region \*  
us-central1 (Iowa)

▼

?

Region is permanent

Zone \*  
us-central1-a

▼

?

Zone is permanent

## Machine configuration

### Machine family

GENERAL-PURPOSE COMPUTE-OPTIMIZED MEMORY-OPTIMIZED GPU

Machine types for common workloads, optimized for cost and flexibility

Series

E2

▼

CPU platform selection based on availability

Machine type

e2-medium (2 vCPU, 4 GB memory)

▼



vCPU  
1-2 vCPU (1 shared core)

Memory  
4 GB

✓ CPU PLATFORM AND GPU

### Display device

Enable to use screen capturing and recording tools.

—

8. Go to boot disk and change operating system as shown:

### Boot disk

Select an image or snapshot to create a boot disk; or attach an existing disk. Can't find what you're looking for? Explore hundreds of VM solutions in [Marketplace](#)

PUBLIC IMAGES

CUSTOM IMAGES

SNAPSHOTS

ARCHIVE SNAPSHOTS

EXISTING DISKS

Operating system

Ubuntu

Version \*

Ubuntu 22.04 LTS

x86/64, amd64 jammy image built on 2022-12-06, supports Shielded VM features

Boot disk type \*

Balanced persistent disk

COMPARE DISK TYPES

Size (GB) \*

10

SHOW ADVANCED CONFIGURATION

SELECT

CANCEL

9. On firewall section disallow http and https traffic

### Firewall ?

Add tags and firewall rules to allow specific network traffic from the Internet

- ☐ Allow HTTP traffic
- ☐ Allow HTTPS traffic

### Advanced options

Networking, disks, security, management, sole-tenancy

You will be billed for this instance. [Compute Engine pricing](#)

CREATE

CANCEL

EQUIVALENT COMMAND LINE

10. Create the instance

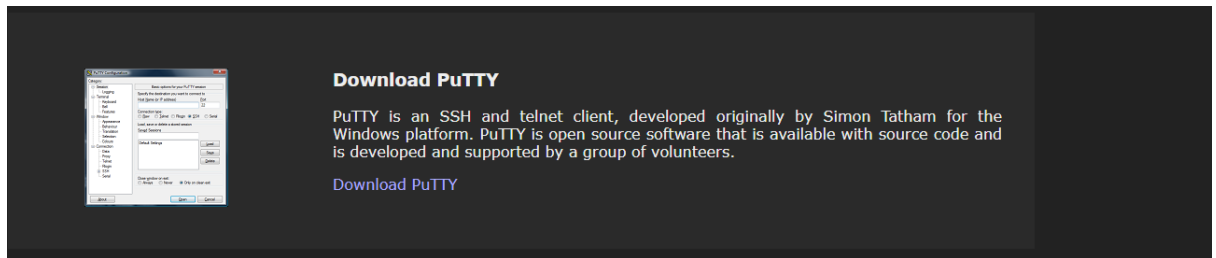
11. It will show this if its successful

VM instances are highly configurable virtual machines for running workloads on Google infrastructure. [Learn more](#)

Filter	Enter property name or value								
<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect	
<input type="checkbox"/>	✓	<a href="#">dvwaubuntu</a>	us-central1-a			10.128.0.2 ( <a href="#">nic0</a> )	34.170.58.56 ( <a href="#">nic0</a> )	SSH ▾	⋮

## PuTTY SETUP

1. Go to [putty.org](#)



2. Download the correct installer for your computer

**Package files**

You probably want one of these. They include versions of all the PuTTY utilities (except the new and slightly experimental Windows pterm).

(Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

We also publish the latest PuTTY installers for all Windows architectures as a free-of-charge download at the [Microsoft Store](#); they usually take a few days to appear there after we release them.

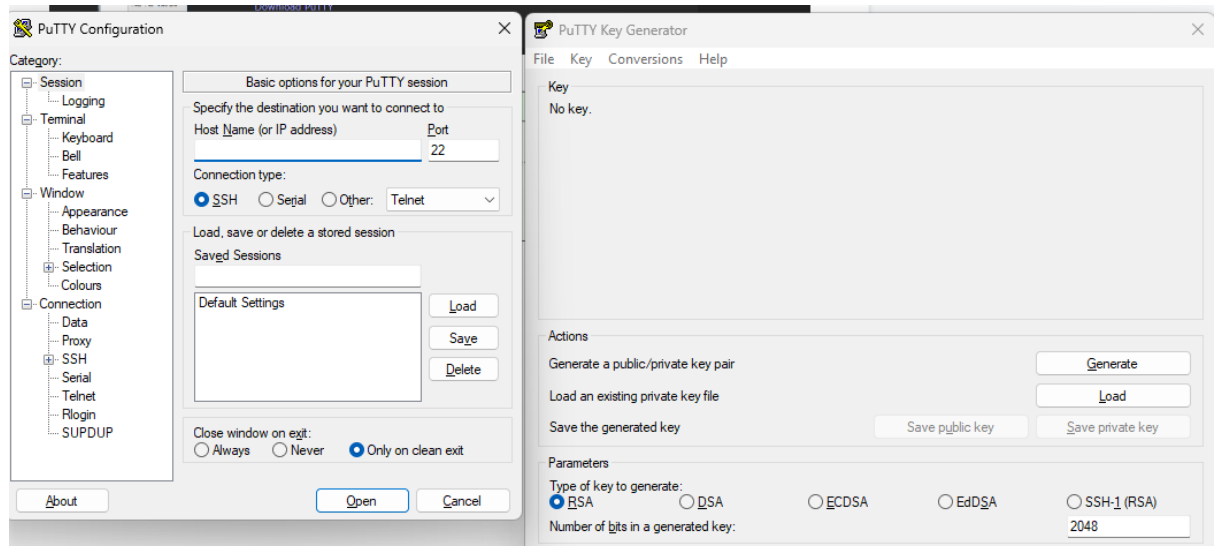
**MSI (Windows Installer)**

64-bit x86:	<a href="#">putty-64bit-0.78-installer.msi</a>	( <a href="#">signature</a> )
64-bit Arm:	<a href="#">putty-arm64-0.78-installer.msi</a>	( <a href="#">signature</a> )
32-bit x86:	<a href="#">putty-0.78-installer.msi</a>	( <a href="#">signature</a> )

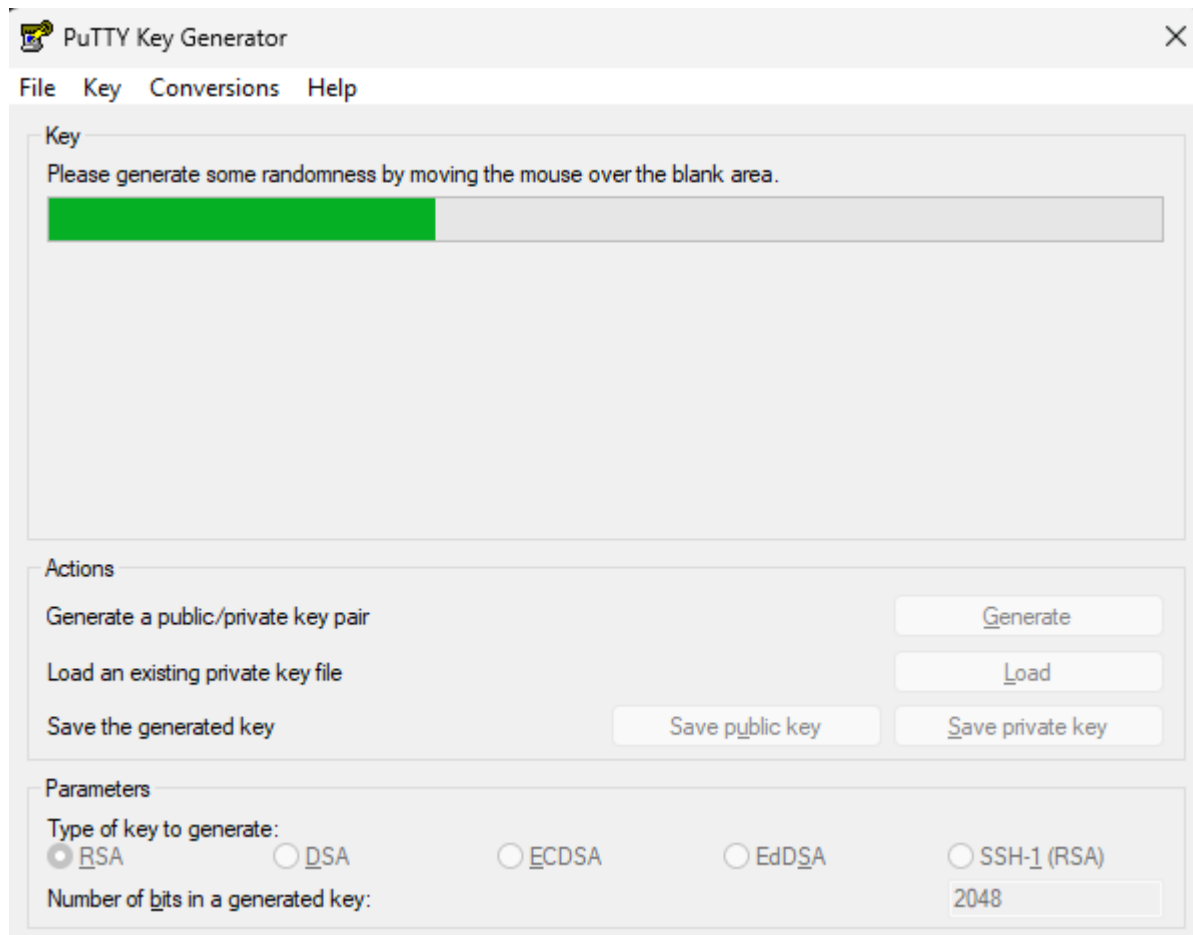
**Unix source archive**

.tar.gz:	<a href="#">putty-0.78.tar.gz</a>	( <a href="#">signature</a> )
----------	-----------------------------------	-------------------------------

3. Run the installer and install PuTTY



4. You will have these 2, PuTTY and PuTTYGen
5. Create SSH Key using PuTTYGen
6. Press generate public/private key pair (While generating, you must move your cursor!)



7. Set your Key Comment (SSH User) and Key passphrase (SSH Password) to your liking

**PutTY Key Generator**

File Key Conversions Help

**Key**

Public key for pasting into OpenSSH authorized\_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDY9D
+0kEKAR6nnaVnKv5ytlKwplXqtk06GtElwFdNxbxUJiHHs34cfd5Pq4xgS/Sppa1WVzhSBF6Tz4UsxySZlhy8KWm
8oJq59rRmpahELCLScyUhiCX4Dv0fHt8zihcSDTghSeQeswcOwWEiWxfEdjpHX9iPIUJzQEixlp2LSm4GHmbvdxl
GuolMRSlfHg/kNkxckD2NFdQrB0/pAsRsvO7jnI62C0v0FPwXN0sn2NNBasuRGi636/6X/IfXlIQRVmCj7vaJu9n/
HR069Z9lv6BREy4Gf2jcbhw0l1J50gbffYUOfcQ+1FEnw4N8HUVgc2t2C53MWBAn3Y9KixbroCapang
```

Key fingerprint: ssh-rsa 2048 SHA256:izCZWdyGVQSURqiOM3n4upTQ798sb2VYjksFbD/hPG8

Key comment: broCapang

Key passphrase: •••••

Confirm passphrase: •••••

**Actions**

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

**Parameters**

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

8. Copy public key generated

File Key Conversions Help


**Key**


Public key for pasting into OpenSSH authorized\_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDY9D
+0kEKAR6nnaVnKv5ytlKwplXqtk06GtElwFdNxbxUJiHHs34cfd5Pq4xgS/Sppa1WVzhSBF6Tz4UsxySZlhy8KWm
8oJq59rRmpahELCLScyUhiCX4Dv0fHt8zihcSDTghSeQeswcOwWEiWxfEdjpHX9iPIUJzQEixlp2LSm4GHmbvdxl
GuolMRSlfHg/kNkxckD2NFdQrB0/pAsRsvO7jnI62C0v0FPwXN0sn2NNBasuRGi636/6X/IfXlIQRVmCj7vaJu9n/
HR069Z9lv6BREy4Gf2jcbhw0l1J50gbffYUOfcQ+1FEnw4N8HUVgc2t2C53MWBAn3Y9KixbroCapang
```

9. Upload public key generated into GCP (Compute Engine > Metadata > SSH Keys)

Metadata

 EDIT

 REFRESH

All instances in this project inherit these SSH keys. [Learn more](#)

METADATA

SSH KEYS

SSH key 1 \*

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDY9D+0kEKAR6nnaVnKv5y

Enter public SSH key


+ ADD ITEM

SAVE

CANCEL

METADATA

SSH KEYS

Username ↑	Key
broCapang	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDY9D+0kEKAR6nnaVnKv5ytlKwplXqtk06GtElwFdNxbxUJiIHs34cfd5Pq4xgS... 

EQUIVALENT REST

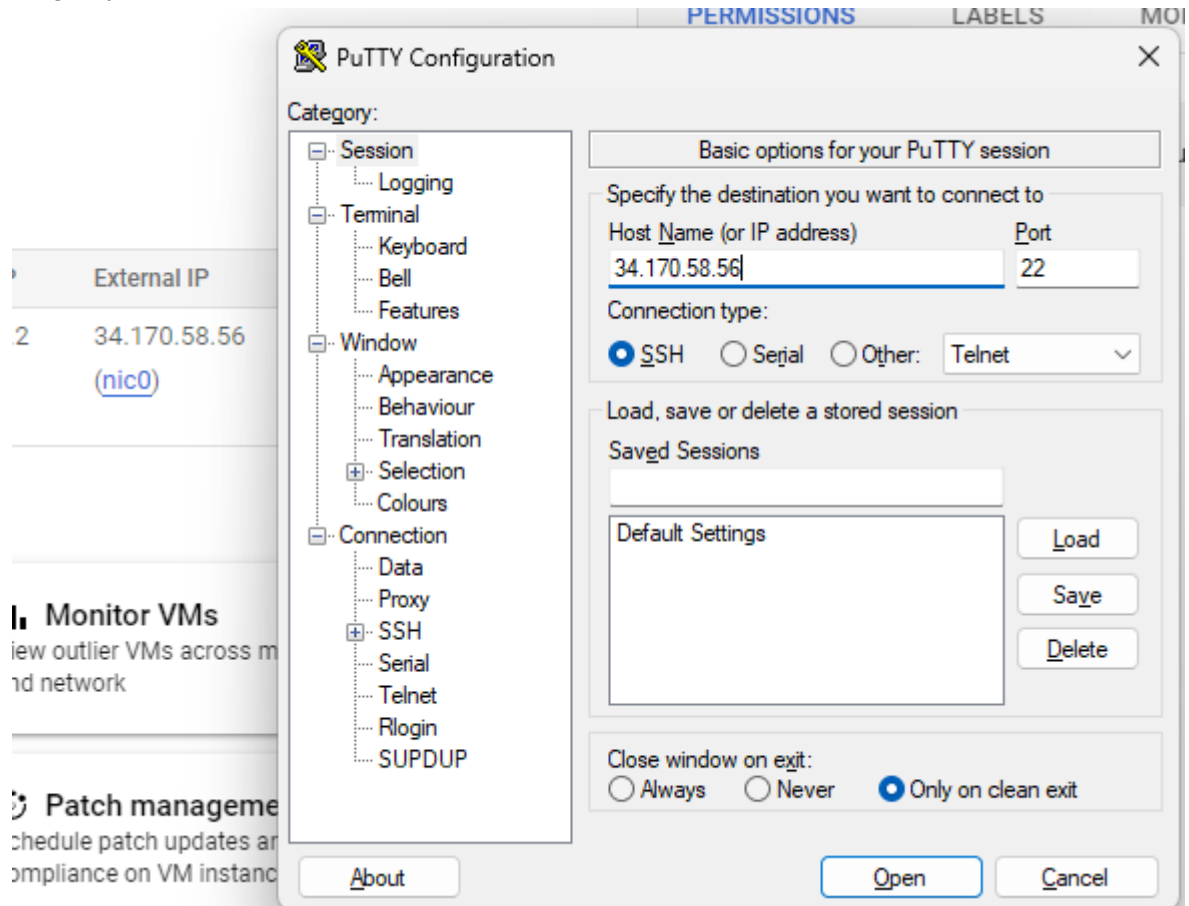
10. Save the private key that was generated.

## SSH SETUP

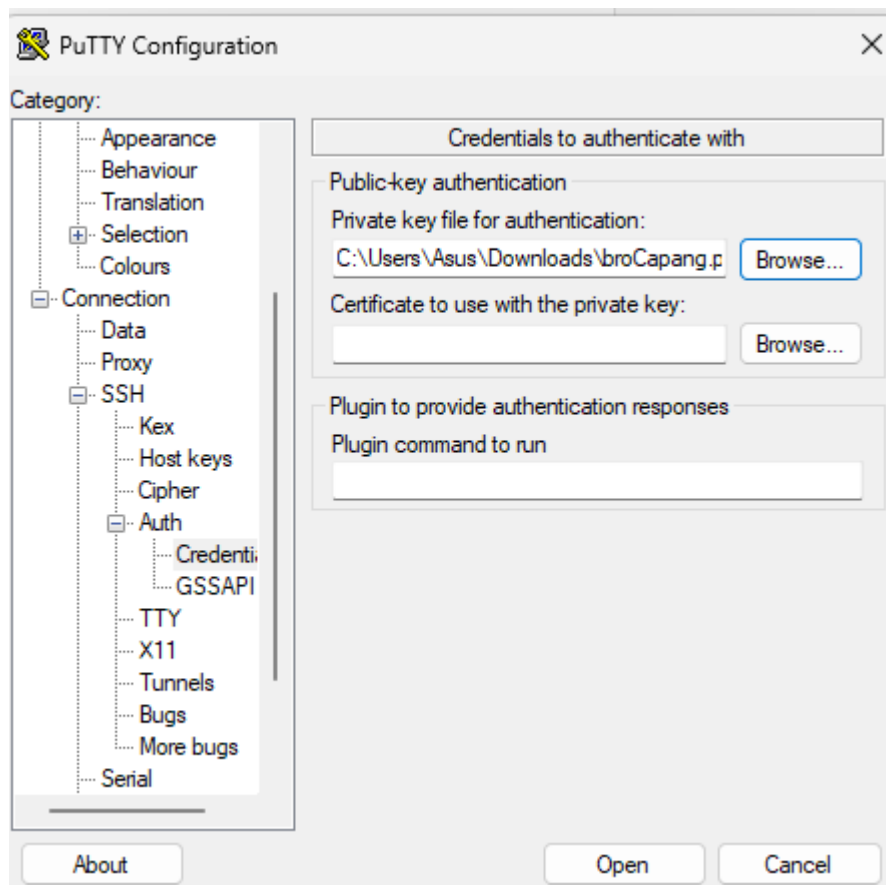
1. Open putty



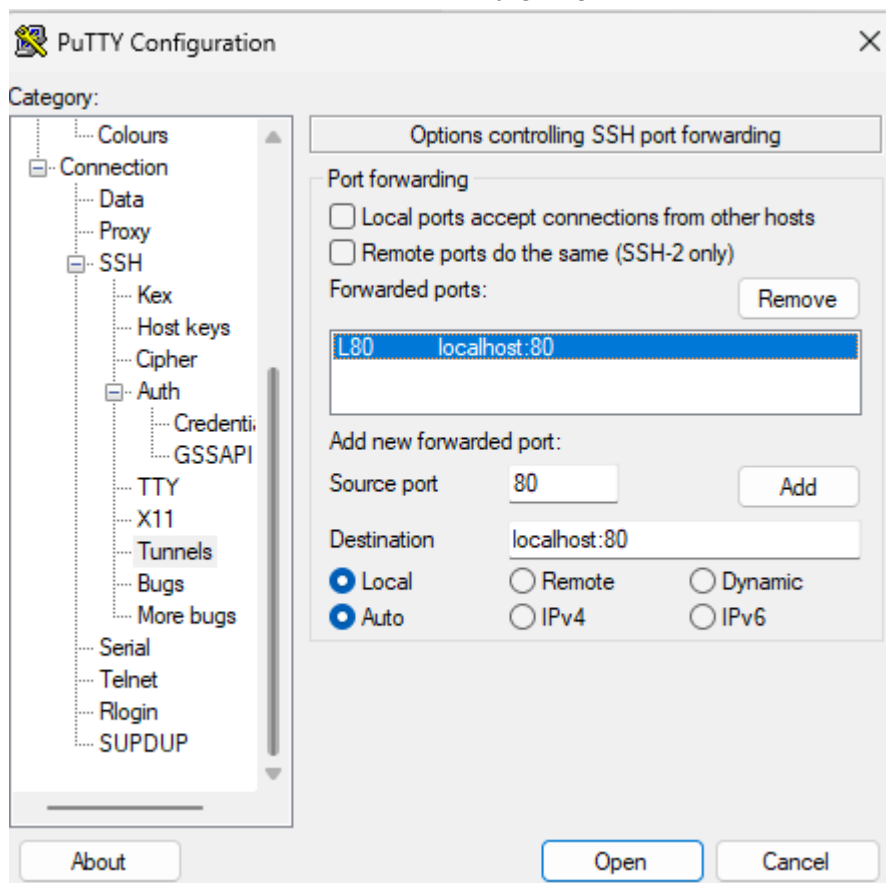
2. Plug in your instance's public ip



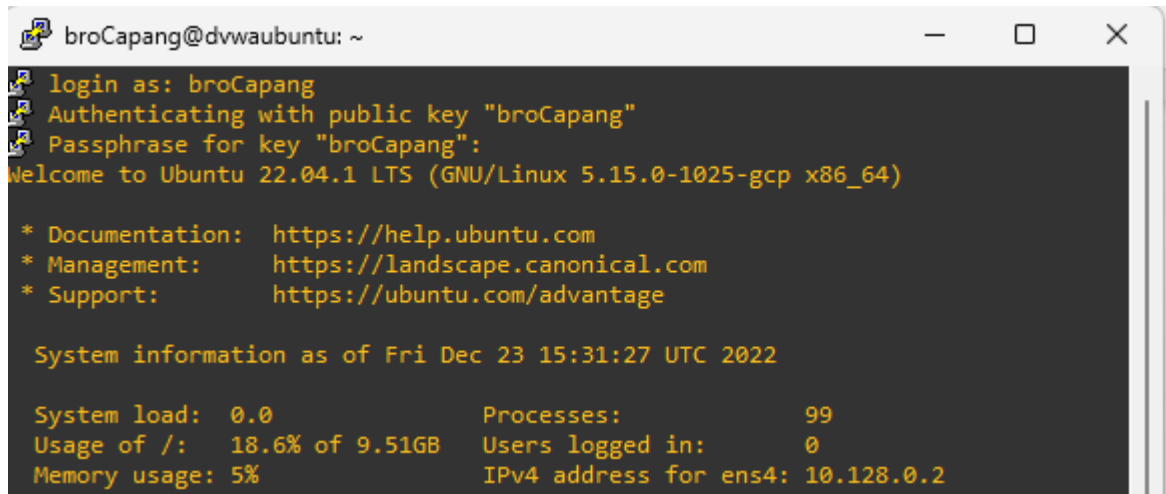
3. Go to SSH > Auth > Credentials to use private key downloaded earlier



- Port Forward port 80 to localhost:80 by going to SSH > Tunnels



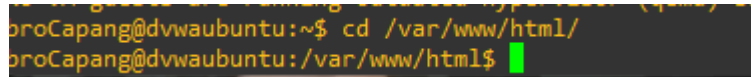
5. Click Session then connect to GCP machine using SSH
  - a. There's a popup warning just click accept
  - b. Login credentials are from PuTTY SETUP step 7



```
broCapang@dvwaubuntu: ~  
login as: broCapang  
Authenticating with public key "broCapang"  
Passphrase for key "broCapang":  
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1025-gcp x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Fri Dec 23 15:31:27 UTC 2022  
  
System load:  0.0      Processes:            99  
Usage of /:   18.6% of 9.51GB   Users logged in:     0  
Memory usage: 5%      IPv4 address for ens4: 10.128.0.2
```

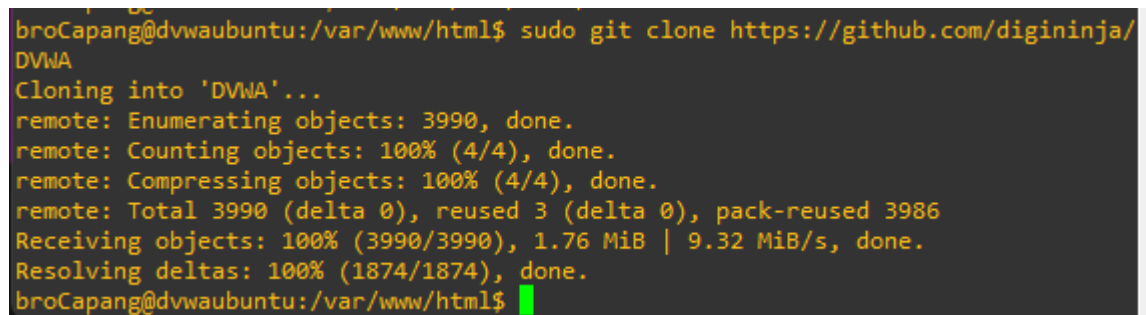
## DVWA SETUP

1. After logging in to SSH, run these commands (Click ENTER if anything needs restarting)
  - a. `sudo apt update`
  - b. `sudo apt upgrade -y`
  - c. `sudo apt install php apache2 mariadb-server php-mysql php-gd libapache2-mod-php`
2. Navigate to `/var/www/html` directory



```
broCapang@dvwaubuntu:~$ cd /var/www/html/  
broCapang@dvwaubuntu:/var/www/html$
```

3. Run `git clone https://github.com/digininja/DVWA.git`

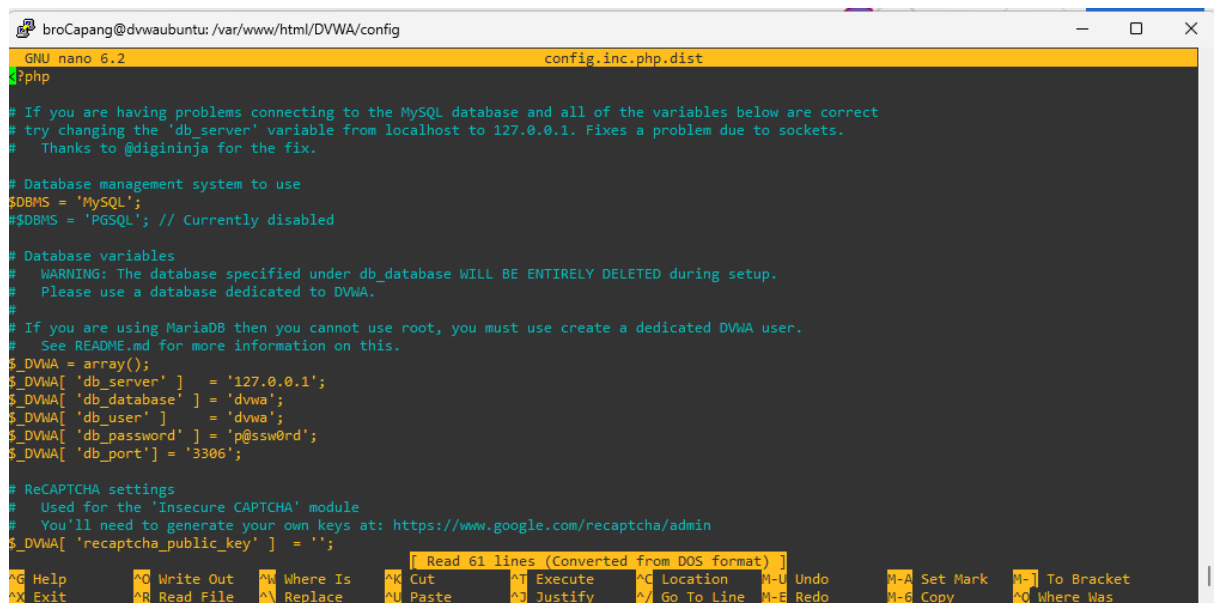


```
broCapang@dvwaubuntu:/var/www/html$ sudo git clone https://github.com/digininja/DVWA  
Cloning into 'DVWA'...  
remote: Enumerating objects: 3990, done.  
remote: Counting objects: 100% (4/4), done.  
remote: Compressing objects: 100% (4/4), done.  
remote: Total 3990 (delta 0), reused 3 (delta 0), pack-reused 3986  
Receiving objects: 100% (3990/3990), 1.76 MiB | 9.32 MiB/s, done.  
Resolving deltas: 100% (1874/1874), done.  
broCapang@dvwaubuntu:/var/www/html$
```

4. Navigate to `/DVWA/config` directory

```
broCapang@dvwaubuntu:/var/www/html$ ls
DVWA index.html
broCapang@dvwaubuntu:/var/www/html$ cd DVWA
broCapang@dvwaubuntu:/var/www/html/DVWA$ ls
CHANGELOG.md  README.zh.md  dvwa          instructions.php  security.php
COPYING.txt   SECURITY.md   external      login.php        security.txt
README.ar.md  about.php    favicon.ico   logout.php       setup.php
README.fr.md  config       hackable     php.ini          tests
README.md     database    ids_log.php  phpinfo.php     vulnerabilities
README.tr.md  docs        index.php    robots.txt
broCapang@dvwaubuntu:/var/www/html/DVWA$ cd config/
broCapang@dvwaubuntu:/var/www/html/DVWA/config$ ls
config.inc.php.dist
broCapang@dvwaubuntu:/var/www/html/DVWA/config$ sudo nano config.inc.php.dist
```

5. Run command `sudo nano config.inc.php.dist` to modify the file



```
broCapang@dvwaubuntu: /var/www/html/DVWA/config
GNU nano 6.2 config.inc.php.dist
?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

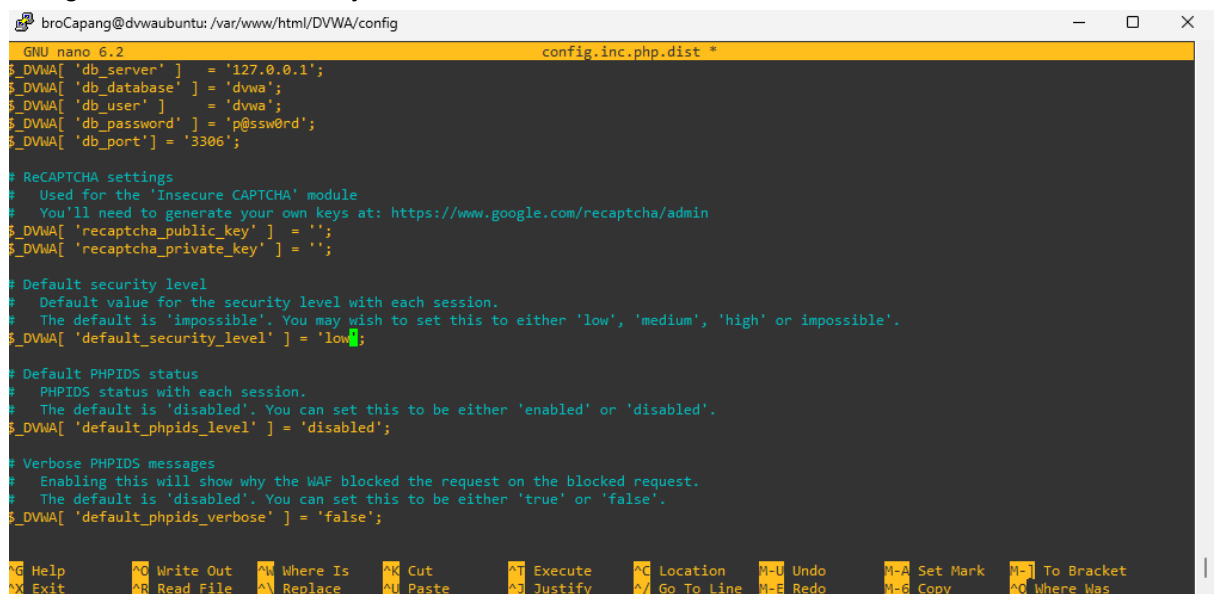
# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
# Please use a database dedicated to DVWA.

# 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' ] = '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' ] = '';

[ Read 61 lines (Converted from DOS format) ]
Help Write Out Where Is Cut Execute Location Undo M-A Set Mark M-J To Bracket
Exit Read File Replace Paste Justify Go To Line M-E Redo M-G Copy M-Q Where Was
```

6. Navigate to 'default security level' and set it to 'Low'



```
broCapang@dvwaubuntu: /var/www/html/DVWA/config
GNU nano 6.2 config.inc.php.dist *
$_DVWA[ '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 PHPIDS status
# PHPIDS status with each session.
# The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$_DVWA[ 'default_phpids_level' ] = 'disabled';

# Verbose PHPIDS messages
# Enabling this will show why the WAF blocked the request on the blocked request.
# The default is 'disabled'. You can set this to be either 'true' or 'false'.
$_DVWA[ 'default_phpids_verbose' ] = 'false';

Help Write Out Where Is Cut Execute Location M-U Undo M-A Set Mark M-J To Bracket
Exit Read File Replace Paste Justify Go To Line M-E Redo M-G Copy M-Q Where Was
```

7. CTRL+SHIFT+O to write out the file as config.inc.php

```
broCapang@dvwubuntu: /var/www/html/DVWA/config
GNU nano 6.2 config.inc.php.dist *
$DVWA['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 PHPIDS status
# PHPIDS status with each session.
# The default is 'disabled'. You can set this to be either 'enabled' or 'disabled'.
$DVWA['default_phpids_level'] = 'disabled';

# Verbose PHPIDS messages
# Enabling this will show why the WAF blocked the request on the blocked request.
# The default is 'disabled'. You can set this to be either 'true' or 'false'.
$DVWA['default_phpids_verbose'] = 'false';

File Name to Write [DOS Format]: config.inc.php
G Help M-D DOS Format M-A Append M-B Backup File
C Cancel M-M Mac Format M-E Prepend ^T Browse

broCapang@dvwubuntu: /var/www/html/DVWA/config$ sudo nano
broCapang@dvwubuntu: /var/www/html/DVWA/config$ ls
config.inc.php config.inc.php.dist
broCapang@dvwubuntu: /var/www/html/DVWA/config$
```

8. In the same directory, run `sudo mariadb`
9. Run these commands in this order
  - a. create database dvwa;
  - b. create user dvwa@localhost identified by 'p@assw0rd';
  - c. Grant all on dvwa.\* to dvwa @localhost;
  - d. flush privileges;

```
MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

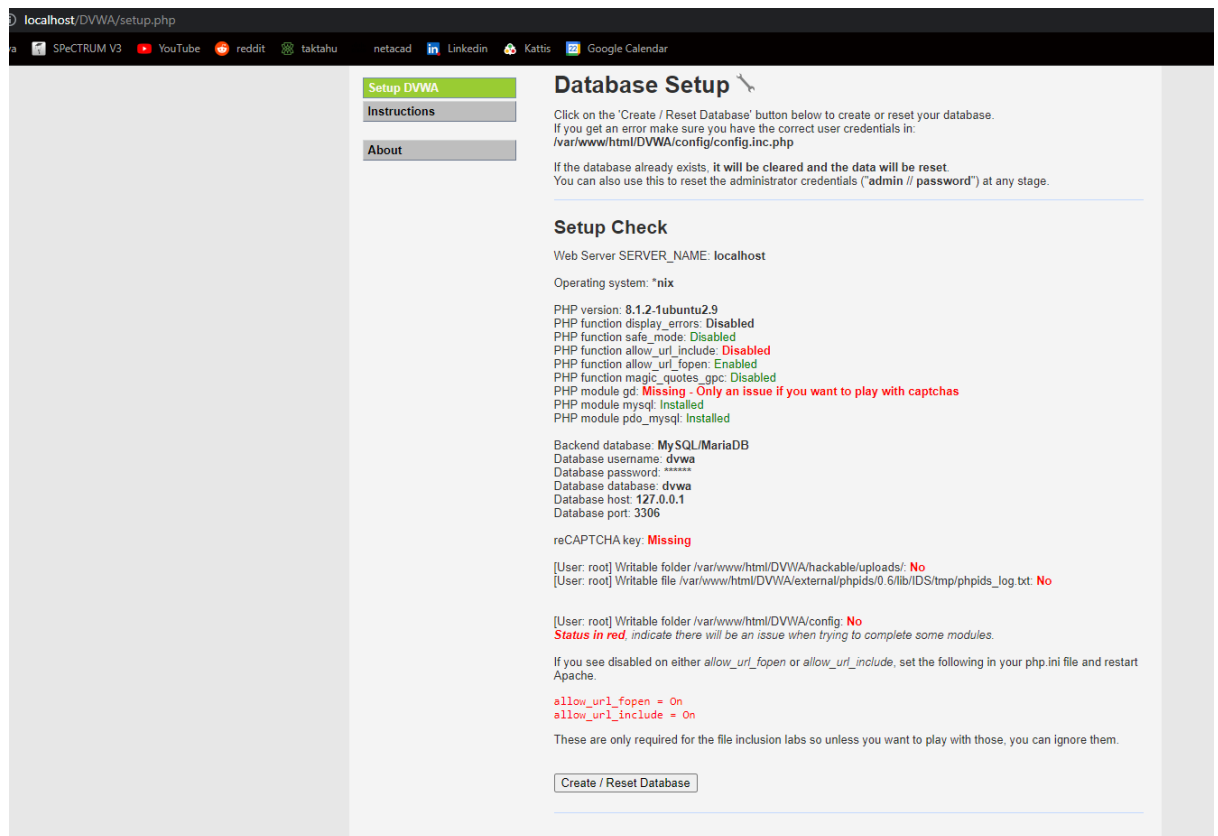
MariaDB [(none)]> create user dvwa@localhost identified by 'p@ssw0rd';
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> grant all on dvwa.* tp dvwa@localhost;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'tp dvwa@localhost' at line 1
MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost;
Query OK, 0 rows affected (0.002 sec)

MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> exit
Bye
```

10. Go to localhost/DVWA/setup.php on browser, you should be able to see the web page.



11. Press Create/Reset Database, if everything is set up properly, the output should look like this:

read: /etc/ssh/ssh-key: **missing**

[User: root] Writable folder /var/www/html/DVWA/hackable/uploads/: **No**  
[User: root] Writable file /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt: **No**

[User: root] Writable folder /var/www/html/DVWA/config: **No**  
**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.

[Create / Reset Database](#)

---

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.

Backup file /config/config.inc.php.bak automatically created

**Setup successful!**

Please [login](#).

12. After being redirected to localhost/DVWA/login.php, login using default credentials
- Username: admin
  - Password: password



Username

admin

Password

.....

Login

localhost/DVWA/index.php

SPECTRUM V3 YouTube reddit taktabu netacad LinkedIn Kattis Google Calendar

**Home**

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

## 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 difficulty, 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 vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users.)

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 more difficult challenges, you may wish to look into the following other projects.

13. Happy hacking! :D

- Shafiqps
- gnapacJabba