

# **WEB SECURITY:** **VULNERABLE WEB APPLICATION** **(DVWA)**

RRC Polytech  
Full Stack Web Development  
Winnipeg, MB Canada

# Motivation

---

- **Hackers are (or could be) actually good, pleasant and extremely intelligent people who could keep computer criminals on the run (run away, escaping).**

**Ankit Fadia**

# All Installed Software for DVWA

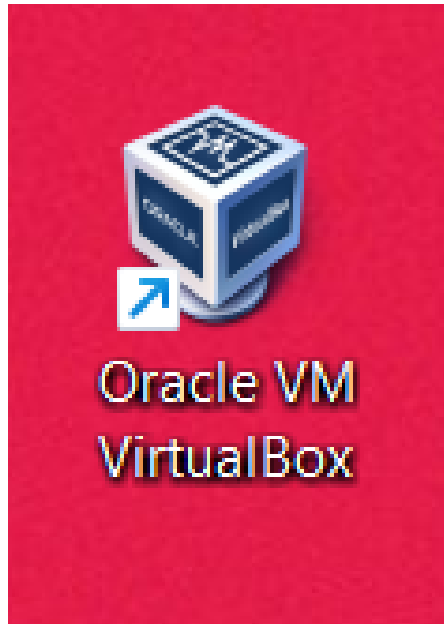
---

- VirtualBox
- Debian
- SQLManager for MySQL
- PuTTY
- WinSCP

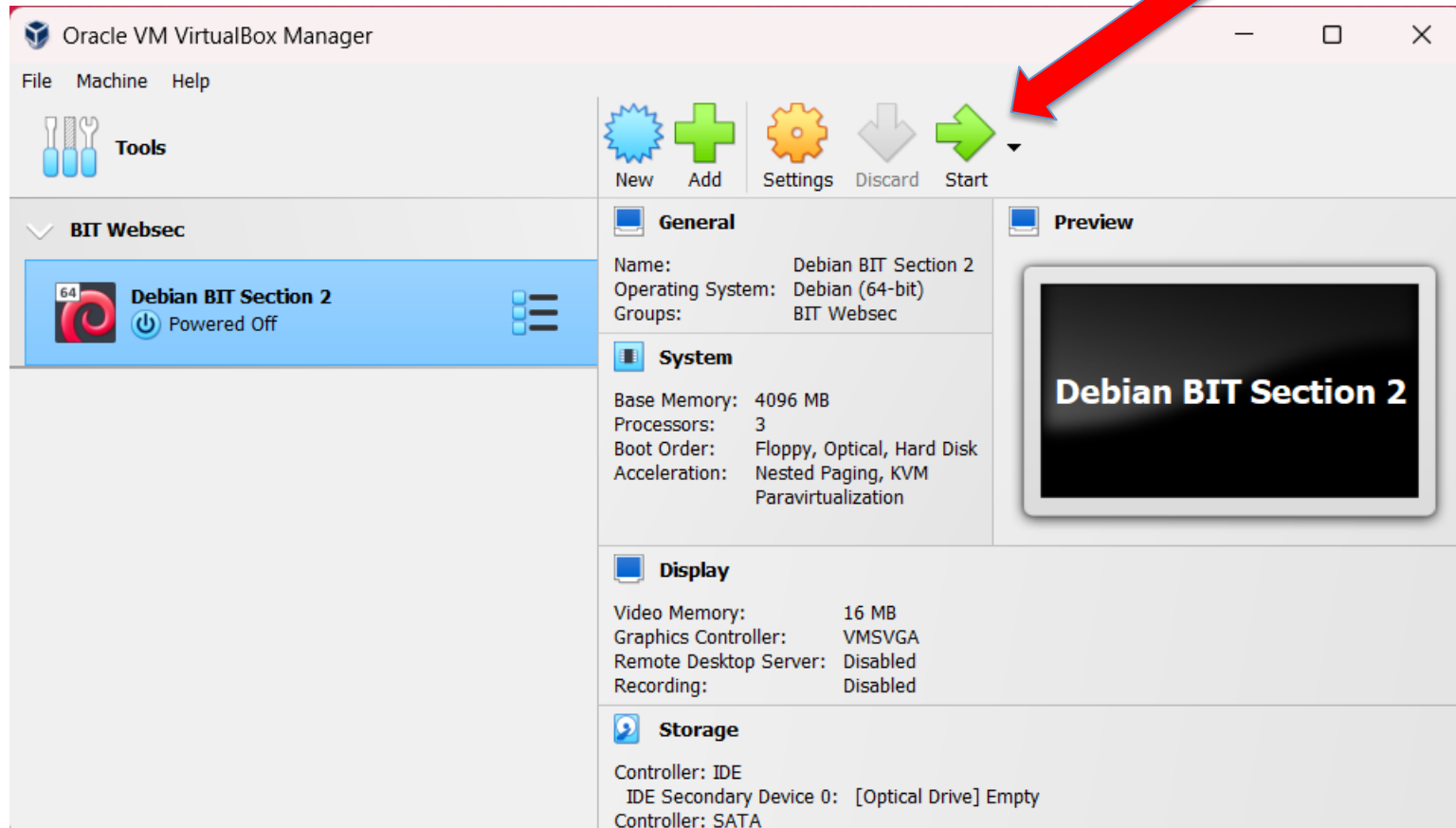
# Oracle VM VirtualBox

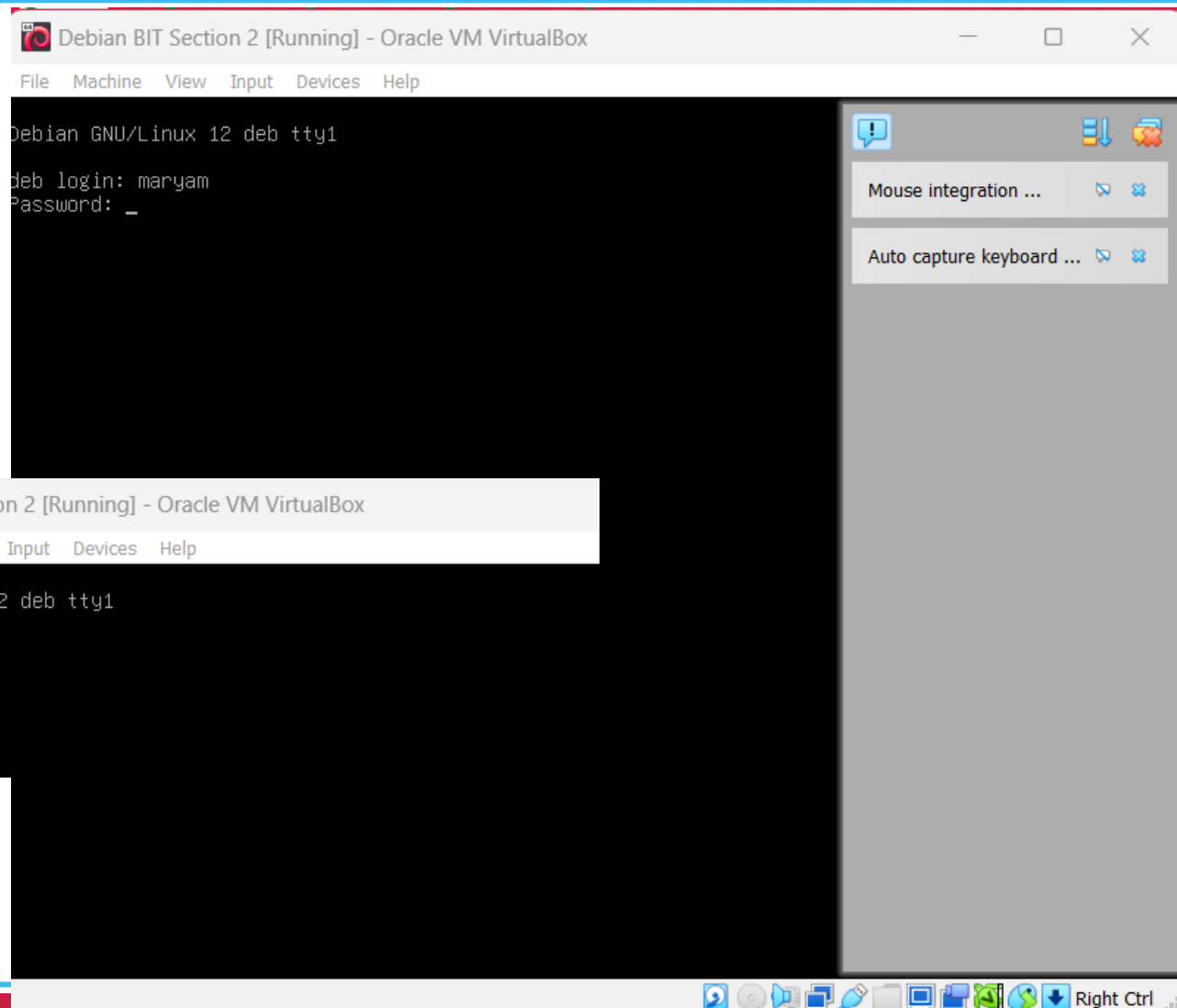
---

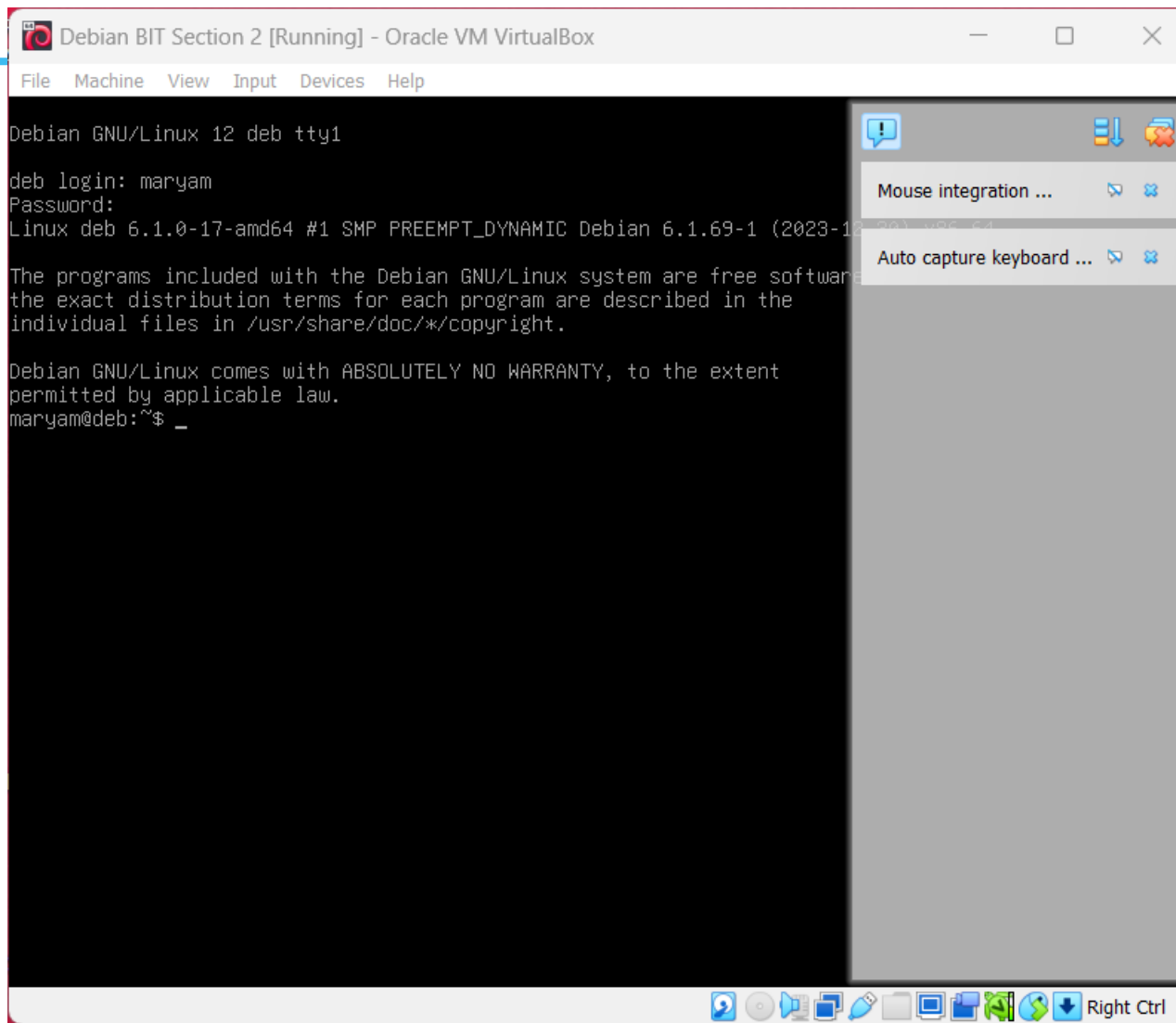
- Click the “Oracle VM VirtualBox” on your desktop

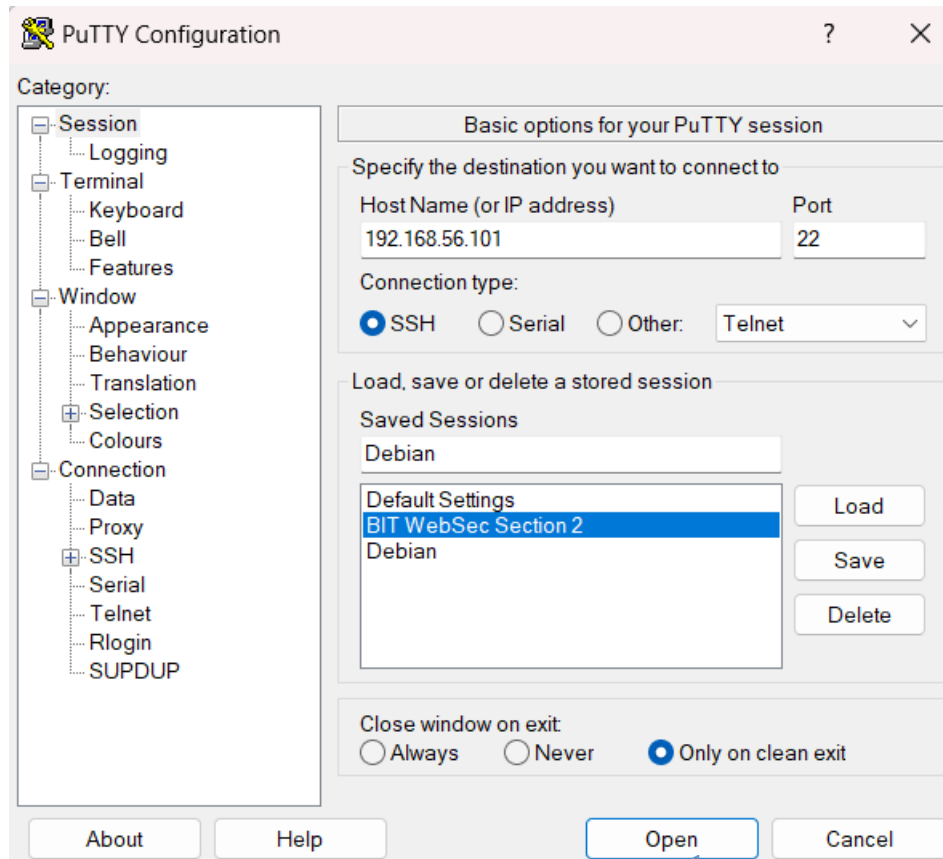


# Debian











# In PuTTY Login and Become Root

maryam@deb: ~

login as: maryam

maryam@192.168.56.101's password:

Linux deb 6.1.0-17-amd64 #1 SMP PREEMPT\_DYNAMIC Debian 6.1.69-1 (2023-12-30)  
\_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.

Last login: Tue Jan 23 15:14:22 2024

maryam@deb:~\$ su -

Password:

# Check that You are Root

---

- You should become as root

```
root@deb:~# whoami  
root  
root@deb:~#
```

# You Should be Connected to “enp0s3” (Adapter 1:NAT) to have Internet Access on Debian

```
root@deb:~# apt update
```


```
root@deb:~# apt update
Get:1 http://deb.debian.org/debian bookworm InRelease [151 kB]
Get:2 http://security.debian.org/debian-security bookworm-security InRelease [48
.0 kB]
Get:3 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Get:4 http://security.debian.org/debian-security bookworm-security/main Sources
[96.2 kB]
Get:5 http://security.debian.org/debian-security bookworm-security/main amd64 Pa
ckages [156 kB]
Get:6 http://security.debian.org/debian-security bookworm-security/main Translat
ion-en [92.9 kB]
Get:7 http://deb.debian.org/debian bookworm/main Sources [9,489 kB]
Get:8 http://deb.debian.org/debian bookworm-updates/main Sources.diff/Index [10.
6 kB]
Get:9 http://deb.debian.org/debian bookworm-updates/main amd64 Packages.diff/Ind
ex [10.6 kB]
Get:10 http://deb.debian.org/debian bookworm-updates/main Translation-en.diff/In
dex [10.6 kB]
Get:11 http://deb.debian.org/debian bookworm-updates/main Sources T-2024-04-23-2
036.10-F-2024-04-23-2036.10.pdiff [831 B]
Get:11 http://deb.debian.org/debian bookworm-updates/main Sources T-2024-04-23-2
036.10-F-2024-04-23-2036.10.pdiff [831 B]
Get:12 http://deb.debian.org/debian bookworm-updates/main amd64 Packages T-2024-
04-23-2036.10-F-2024-04-23-2036.10.pdiff [1,595 B]
Get:12 http://deb.debian.org/debian bookworm-updates/main amd64 Packages T-2024-
04-23-2036.10-F-2024-04-23-2036.10.pdiff [1,595 B]
Get:13 http://deb.debian.org/debian bookworm-updates/main Translation-en T-2024-
04-23-2036.10-F-2024-04-23-2036.10.pdiff [2,563 B]
Get:13 http://deb.debian.org/debian bookworm-updates/main Translation-en T-2024-
04-23-2036.10-F-2024-04-23-2036.10.pdiff [2,563 B]
Get:14 http://deb.debian.org/debian bookworm/main amd64 Packages [8,786 kB]
Get:15 http://deb.debian.org/debian bookworm/main Translation-en [6,109 kB]
Get:16 http://deb.debian.org/debian bookworm-updates/non-free-firmware Sources [
2,076 B]
Get:17 http://deb.debian.org/debian bookworm-updates/non-free-firmware amd64 Pac
kages [616 B]
Get:18 http://deb.debian.org/debian bookworm-updates/non-free-firmware Translati
on-en [384 B]
Fetched 25.0 MB in 4s (6,410 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
63 packages can be upgraded. Run 'apt list --upgradable' to see them.
N: Repository 'http://deb.debian.org/debian bookworm InRelease' changed its 'Ver
sion' value from '12.4' to '12.5'
root@deb:~#
```

# PuTTY (Debian) update and upgrade

---

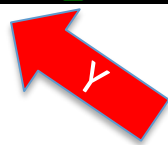
➤ apt update

➤ apt upgrade



```
root@deb:~# apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@deb:~#
```

```
root@deb:~# apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following NEW packages will be installed:
  linux-image-6.1.0-21-amd64
The following packages will be upgraded:
  apache2 apache2-bin apache2-data apache2-utils base-files bind9-dnsutils bind9-host bind9-libs
  bsdxtrautils bsduutils eject fdisk less libapache2-mod-php8.2 libblkid1 libc-bin libc-l10n libc6
  libcryptsetup12 libfdisk1 libglib2.0-0 libglib2.0-data libgnutls30 libmariadb3 libmount1
  libnss-systemd libpam-systemd libsmartcols1 libsystemd-shared libsystemd0 libudev1 libuuid1 libuv1
  linux-image-amd64 locales mariadb-client mariadb-client-core mariadb-common
  mariadb-plugin-provider-bzip2 mariadb-plugin-provider-lz4 mariadb-plugin-provider-lzma
  mariadb-plugin-provider-lzo mariadb-plugin-provider-snappy mariadb-server mariadb-server-core
  mount php8.2 php8.2-cli php8.2-common php8.2-mysql php8.2-opcache php8.2-readline systemd
  systemd-sysv systemd-timesyncd tar tzdata udev usbutils usr-is-merged util-linux util-linux-extra
  util-linux-locales
63 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 117 MB of archives.
After this operation, 408 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```



#### Modified configuration file

php.ini: A new version (/usr/lib/php/8.2/php.ini-production) of configuration file /etc/php/8.2/apache2/php.ini is available, but the version installed currently has been locally modified.

What do you want to do about modified configuration file php.ini?

install the package maintainer's version

keep the local version currently installed

show the differences between the versions

show a side-by-side difference between the versions

start a new shell to examine the situation

<Ok>

•  
•  
•

```
Processing triggers for man-db (2.11.2-2) ...  
Processing triggers for dbus (1.14.10-1~deb12u1) ...  
Processing triggers for mailcap (3.70+nmu1) ...  
Processing triggers for initramfs-tools (0.142) ...  
update-initramfs: Generating /boot/initrd.img-6.1.0-21-amd64  
Processing triggers for libc-bin (2.36-9+deb12u7) ...  
Processing triggers for php8.2-cli (8.2.18-1~deb12u1) ...  
Processing triggers for libapache2-mod-php8.2 (8.2.18-1~deb12u1) ...  
root@deb:~# █
```



---

```
root@deb:~# apt install apache2
```

---

```
root@deb:~# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.59-1~deb12u1).
The following package was automatically installed and is no longer required:
  linux-image-6.1.0-15-amd64
Use 'apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@deb:~#
```

---

```
root@deb:~# apt install php
```

---

```
root@deb:~# apt install php
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
php is already the newest version (2:8.2+93).
The following package was automatically installed and is no longer required:
  linux-image-6.1.0-15-amd64
Use 'apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@deb:~# █
```

---

```
root@deb:~# apt install mariadb-server
```

---

```
root@deb:~# apt install mariadb-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
mariadb-server is already the newest version (1:10.11.6-0+deb12u1).
The following package was automatically installed and is no longer required:
  linux-image-6.1.0-15-amd64
Use 'apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@deb:~# █
```

---

```
root@deb:~# apt install php-mysqli
```

```
root@deb:~# apt install php-mysqli
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'php8.2-mysql' instead of 'php-mysqli'
php8.2-mysql is already the newest version (8.2.18-1~deb12u1).
The following package was automatically installed and is no longer required:
  linux-image-6.1.0-15-amd64
Use 'apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@deb:~# █
```



---

```
root@deb:~# apt install vsftpd
```

---

```
root@deb:~# apt install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
vsftpd is already the newest version (3.0.3-13+b2).
The following package was automatically installed and is no longer required:
  linux-image-6.1.0-15-amd64
Use 'apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@deb:~# █
```

---

```
root@deb:~# nano /etc/mysql/mariadb.conf.d/50-server.cnf
```

```
# * Basic Settings
#

#user                = mysql
pid-file             = /run/mysqld/mysqld.pid
socket               = /run/mysqld/mysqld.sock
#port                = 3306
basedir              = /usr
#datadir              = /var/lib/mysql
#tmpdir               = /tmp

# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address          = 0.0.0.0

#
# * Fine Tuning
#
```



---

➤ ^O - - - > Save

```
File Name to Write: /etc/mysql/mariadb.conf.d/50-server.cnf
^G Help      M-D DOS Format  M-A Append    M-B Backup File
^C Cancel    M-M Mac Format  M-P Prepend   ^T Browse
```

➤ Hit Enter

➤ ^X - - - > Exit

# Edit vsftpd Configuration

---

```
root@deb:~# nano /etc/vsftpd.conf
```

# Edit vsftpd Configuration

---

```
#  
# Uncomment this to enable any form of FTP write command.  
#write_enable=YES  
#
```

```
#  
# Uncomment this to enable any form of FTP write command.  
write_enable=YES  
#
```

# Create

---

➤ ^O - - - > Save

```
File Name to Write: /etc/vsftpd.conf|
^G Help          M-D DOS Format    M-A Append       M-B Backup File
^C Cancel        M-M Mac Format    M-P Prepend      ^T Browse
```

➤ Hit Enter

➤ ^X - - - > Exit



# Restart ...

---

```
root@deb:~# systemctl restart mysql.service
```

```
root@deb:~# systemctl restart mariadb.service
```

```
root@deb:~# systemctl restart vsftpd
```

```
root@deb:~# systemctl restart apache2
```

# Error

---

➤ Students who have problem at this step, their configuration is not set up properly. Please check for

`nano /etc/mysql/mariadb.conf.d/50-server.cnf`

➤ to check:

- pid-file
- socket
- bind-address

# Error

---

systemctl restart mysql.service

- error: Job for mariadb.service failed because the control process exited with error code
- [https://www.google.com/search?q=systemctl+restart+mysql.service%0Aerror%3A+Job+for+mariadb.service+failed+because+the+control+process+exited+with+error+code&sca\\_esv=21d142fe9e0fef6b&udm=50&source=hp&fbs=AlljpHxU7SXXniUZfeShr2fp4giZud1z6kQpMfoEdCJxnpm\\_3YIUqOpj4OTU\\_HmqxOd8LCZRmCXZfilaEd7O0OWEblyuXRFklyLCRXrxWNyn5IQQps0XaIWR4lysgApcAokXMyLMc5paSdoFuY48P0VW2G1X-BT8Glvpc\\_psfCYpzb7exd0la77U7j3c-QnkKIhEzoGULNxHJaIDRCf4gfWU\\_FmoEtjfA&aep=1&ntc=1&sa=X&ved=2ahUKEwjMkfQ277yPAxX1ADQIHdpaDkkQ2J8OegQIERAD&biw=1485&bih=731&dpr=1.25&mstk=AUtExfD81RU\\_RWjzdz\\_qtrE3xK0w3jZOm2eGpp8\\_Zm8v2m18f4H7YUahifMu798vX78RNpN9mNEpysmbb7BNQpwACri8X6QKudxpJlQXmlcwUP0g1jNWePCoPtVO6km9AjJ1YNZ0zg8uYMKGXIDA0ujjkX\\_uCebi\\_MRxf-M&csuir=1](https://www.google.com/search?q=systemctl+restart+mysql.service%0Aerror%3A+Job+for+mariadb.service+failed+because+the+control+process+exited+with+error+code&sca_esv=21d142fe9e0fef6b&udm=50&source=hp&fbs=AlljpHxU7SXXniUZfeShr2fp4giZud1z6kQpMfoEdCJxnpm_3YIUqOpj4OTU_HmqxOd8LCZRmCXZfilaEd7O0OWEblyuXRFklyLCRXrxWNyn5IQQps0XaIWR4lysgApcAokXMyLMc5paSdoFuY48P0VW2G1X-BT8Glvpc_psfCYpzb7exd0la77U7j3c-QnkKIhEzoGULNxHJaIDRCf4gfWU_FmoEtjfA&aep=1&ntc=1&sa=X&ved=2ahUKEwjMkfQ277yPAxX1ADQIHdpaDkkQ2J8OegQIERAD&biw=1485&bih=731&dpr=1.25&mstk=AUtExfD81RU_RWjzdz_qtrE3xK0w3jZOm2eGpp8_Zm8v2m18f4H7YUahifMu798vX78RNpN9mNEpysmbb7BNQpwACri8X6QKudxpJlQXmlcwUP0g1jNWePCoPtVO6km9AjJ1YNZ0zg8uYMKGXIDA0ujjkX_uCebi_MRxf-M&csuir=1)

# mysql

---

```
root@deb:~# mysql -u root
```

```
MariaDB [(none)]> create database dvwa;  
ERROR 1007 (HY000): Can't create database 'dvwa'; database exists
```

# Create 2 users: dvwadmin / dvwa and grant them access

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'dvwadmin'@'%' identified by 'password' with grant option;  
Query OK, 0 rows affected (0.007 sec)
```

```
MariaDB [(none)]> grant all privileges on dvwa.* to 'dvwa'@'localhost' identified by 'password' with grant option;  
Query OK, 0 rows affected (0.009 sec)
```

# Find the Word Document File from Learn

⋮ Tips and Fixes 12

⋮ Module 1 - Ethical Hacking 12

⋮ Module 2 - VM Setup 37

⋮ DVWA - Vulnerable Web Application 12

⋮ Passwords 25

⋮ Module 3 - SQL/XSS Injection 23

⋮ Module 4 - Privacy & Secure Storage 36

Download and unarchive DVWA zip file to a folder you can then use to move/copy over to Debian using WinSCP.

New ▾

Add Existing Activities ▾

⋮ Download of Database Frontend Software ▾

🔗 Link



⋮ Installing Debian, setting up SQL, uploading DVWA ▾

📄 Word Document



⋮ DVWA-master ▾

📁 Zip Compressed File



⋮ Attacking DVWA ▾

📄 Word Document



# “Installing Debian, setting up SQL, uploading DVWA” File

learn WEBD-3013 (259269) Web Security



Maryam Ghanbari



Course Content ▾ Assessments ▾ Communication ▾ Resources ▾ Edit Course

Table of Contents ▸ Module 2 - VM Setup ▸ DVWA - Vulnerable Web Application ▸ Installing Debian, setting up SQL, uploading DVWA

## Installing Debian, setting up SQL, uploading DVWA ▾



1 of 31 Automatic Zoom ▾ View as Text Download

Download the following files:

- ▾ Setting up Debian for a Secure Web Server and a Database
  - Database Access
  - Test Deployment

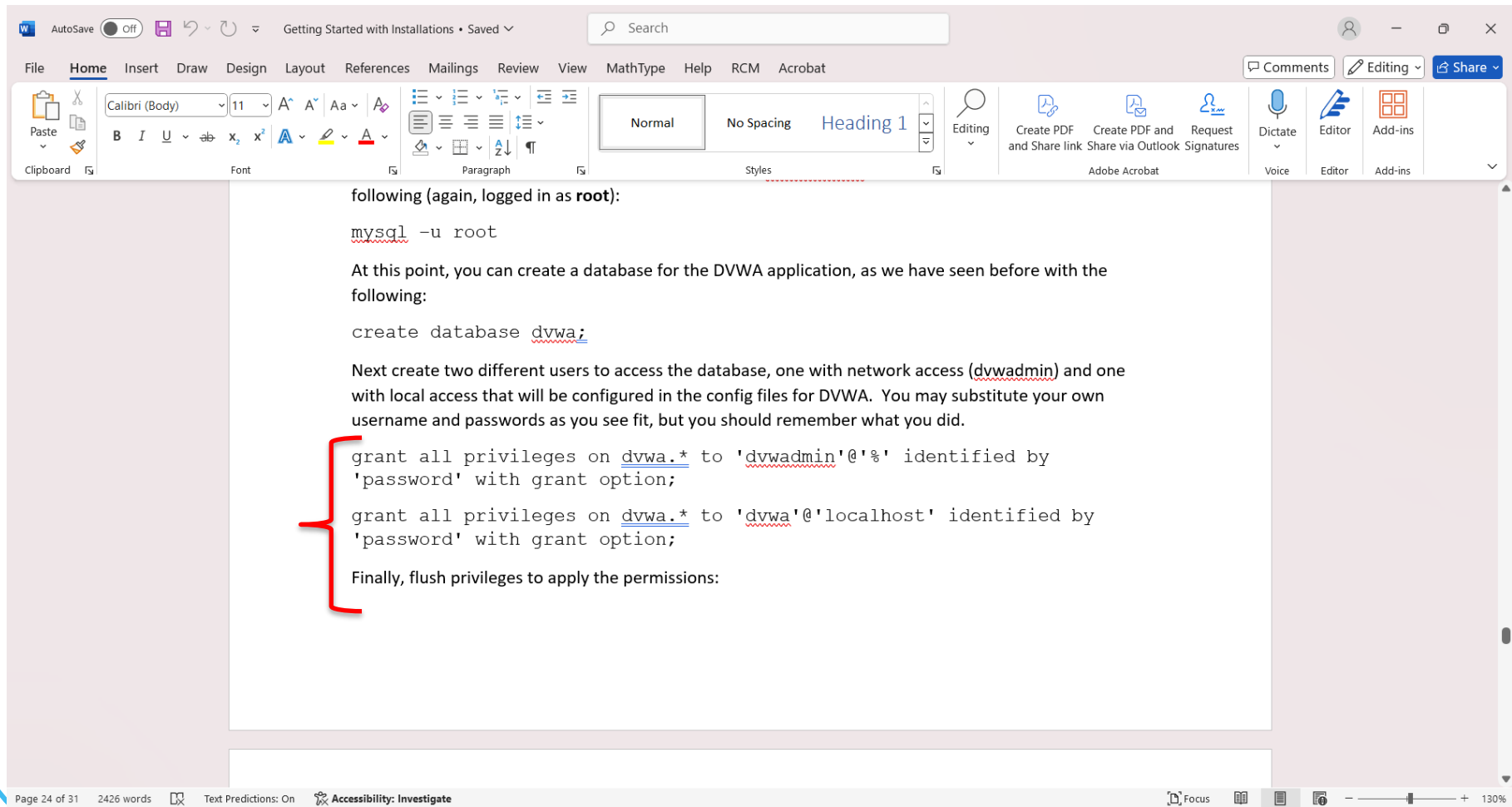
### Download the following files:

**SQL Manager:**  
<https://www.sqlmanager.net/tools/free>  
-> For MySQL (<https://www.sqlmanager.net/products/mysql/manager/download/128>)

**VirtualBox VM Client:**  
<https://www.virtualbox.org/wiki/Downloads>  
-> Windows hosts (<https://download.virtualbox.org/virtualbox/6.1.30/VirtualBox-6.1.30-148432-Win.exe>)

**Linux OS - Debian Distribution:**

# You can copy from Word document (Page 24) and paste to PUTTY



The screenshot shows a Microsoft Word document with the following content:

following (again, logged in as **root**):

```
mysql -u root
```

At this point, you can create a database for the DVWA application, as we have seen before with the following:

```
create database dvwa;
```

Next create two different users to access the database, one with network access (**dvwadmin**) and one with local access that will be configured in the config files for DVWA. You may substitute your own username and passwords as you see fit, but you should remember what you did.

```
grant all privileges on dvwa.* to 'dvwadmin'@'%' identified by 'password' with grant option;
```

```
grant all privileges on dvwa.* to 'dvwa'@'localhost' identified by 'password' with grant option;
```

Finally, flush privileges to apply the permissions:

The document is titled "Getting Started with Installations" and is on page 24 of 31. The status bar shows 2426 words, Text Predictions are on, and Accessibility is being investigated. The zoom level is 130%.



# Grant

---

➤ `grant all privileges on dvwa.* to 'dvwadmin'@'%' identified by 'password' with grant option;`

➤ `grant all privileges on dvwa.* to 'dvwa'@'localhost' identified by 'password' with grant option;`

---

```
MariaDB [(none)]> flush privileges;  
Query OK, 0 rows affected (0.002 sec)
```

```
MariaDB [(none)]> exit;  
Bye  
root@deb:~#
```

# Create

```
root@deb:~# ip addr
```

```
root@deb:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:04:70:a0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 80780sec preferred_lft 80780sec
    inet6 fe80::a00:27ff:fe04:70a0/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:72:c4:58 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic enp0s8
        valid_lft 517sec preferred_lft 517sec
    inet6 fe80::a00:27ff:fe72:c458/64 scope link
        valid_lft forever preferred_lft forever
```



debian

# Apache2 Debian Default Page

## It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

## Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   |-- ports.conf  
|-- mods-enabled  
|   |-- *.load  
|   |-- *.conf  
|-- conf-enabled  
|   |-- *.conf  
|-- sites-enabled  
|   |-- *.conf
```

# Make sure you are Root


---

```
root@deb:~# whoami  
root
```


# www directory

---

```
root@deb:~# cd /var/www  
root@deb:/var/www#
```



```
root@deb:/var/www# pwd  
/var/www  
root@deb:/var/www#
```



# Set the permissions for that directory

---

- **Step 1:** Set the permissions for that directory to 775
- We allow a group to change the content of that directory (the html directory)

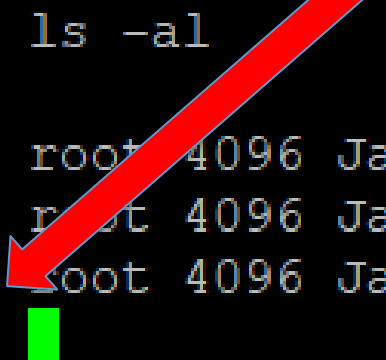
```
root@deb:/var/www# chmod 775 html/  
root@deb:/var/www#
```

- Anybody who is part of the group ownership, can modify that directory

# ls

---

```
root@deb:/var/www# ls -al
total 12
drwxr-xr-x  3 root root 4096 Jan 23 16:18 .
drwxr-xr-x 12 root root 4096 Jan 23 16:18 ..
drwxr-xr-x  2 root root 4096 Jan 23 16:18 html
root@deb:/var/www#
```





# Set the permissions for that directory

---

- **Step 2:** we need to change what group owns that.
- Currently, the “root user” owns it.
- We want to change that ownership - - - > to the “www-data” group
- The www-data user and group are the def (default) user and group that created when you deploy apache to your environment


- 
- We change the ownership, not of the owner of the group owner to www-data and that is the html item as well.
  - Change the owner of the html directory to be the group: www-data

```
root@deb:/var/www# chown root:www-data html/
```

- 
- when I do an `ls -al` `www` group has access to write to that directory.

```
root@deb:/var/www# ls -al
total 12
drwxr-xr-x  3 root root    4096 Jan 23 16:18 .
drwxr-xr-x 12 root root    4096 Jan 23 16:18 ..
drwxrwxr-x  2 root root    4096 Jan 23 16:18 html
root@deb:/var/www#
```

➤ **Step 3:** the third command is user mode



```
root@deb:/var/www# adduser maryam www-data
Adding user `maryam' to group `www-data' ...
Done.
root@deb:/var/www# _
```

```
root@deb:/var/www# adduser maryam www-data
adduser: The user `maryam' is already a member of `www-data'.
```

```
root@deb:/var/www# ls
html
root@deb:/var/www# ls -al
total 12
drwxr-xr-x  3 root root    4096 Jan 23 16:18 .
drwxr-xr-x 12 root root    4096 Jan 23 16:18 ..
drwxrwxr-x  6 root www-data 4096 May 15 20:47 html
root@deb:/var/www#
```

---

```
root@deb:/var/www# adduser maryam www-data
```

```
root@deb:/var/www# adduser maryam www-data  
adduser: The user `maryam' is already a member of `www-data'.
```

# Open WinSCP -> Create a Folder

html – maryam@192.168.56.101 – WinSCP

Synchronize Queue Transfer Settings Default

Local Mark Files Commands Tabs Options Remote Help

maryam@192.168.56.101 × New Tab

C:\Windows

Upload Edit Properties New

C:\Users\mghanbari\Downloads\

Name	Size	Type	Changed
..		Parent directory	5/14/2024 9:37:13 PM
desktop.ini	1 KB	Configuration setti...	8/30/2023 2:38:02 PM

html

Download Edit Properties New Find Files

/var/www/html/

Name	Size	Changed	Rights	Owner
..		1/23/2024 4:18:24 PM	rw-r--r--	root
dwwa_backup		1/28/2024 7:58:25 PM	rw-r--r--	maryam
dwwa		5/15/2024 8:47:21 PM	rw-r--r--	maryam
blog_backup		4/4/2024 10:34:01 PM	rw-r--r--	maryam
blog		4/19/2024 2:18:40 AM	rw-r--r--	maryam
test.php	1 KB	3/10/2024 5:30:15 PM	rw-r--r--	maryam
index.html	11 KB	1/23/2024 4:18:26 PM	rw-r--r--	root

Go To

Refresh Ctrl+R

Add Path to Bookmarks Ctrl+B

Filter... Ctrl+Alt+F

Copy Path to Clipboard Ctrl+]

New

Paste from Clipboard Ctrl+V

Static Custom Commands

File... Shift+F4

Directory... F7

Link...

# Create

Create folder ? X

New folder name:

Test

Attributes

☐ Set permissions

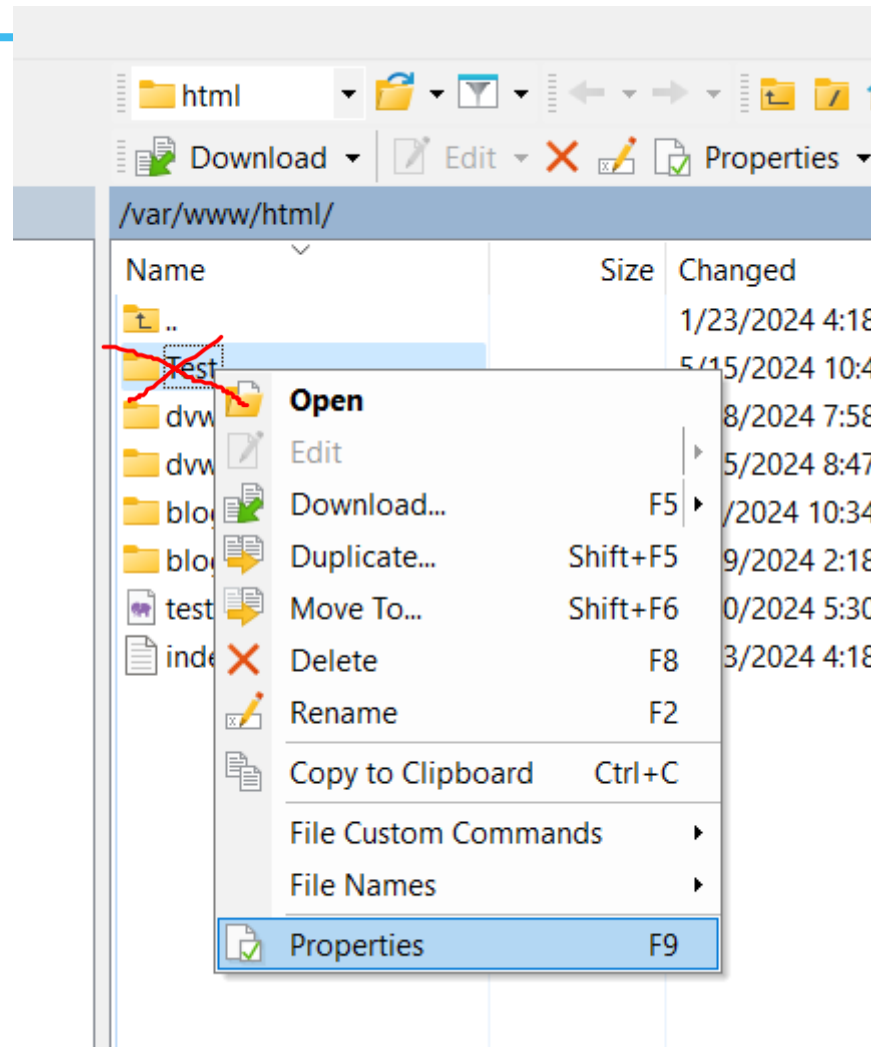
Owner	<input checked="" type="checkbox"/> R	<input checked="" type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input type="checkbox"/> Set UID
Group	<input checked="" type="checkbox"/> R	<input type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input type="checkbox"/> Set GID
Others	<input checked="" type="checkbox"/> R	<input type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input type="checkbox"/> Sticky bit

Octal: 0755

☐ Use same settings next time

OK Cancel Help






# Set owner, group and permissions recursively

Test Properties

Common Checksum

 Test

Location: /var/www/html

Size: Unknown Calculate

Owner: maryam [1000]

Group: maryam [1000]

Permissions:

Owner	<input checked="" type="checkbox"/> R	<input checked="" type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input type="checkbox"/> Set UID
Group	<input checked="" type="checkbox"/> R	<input type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input type="checkbox"/> Set GID
Others	<input checked="" type="checkbox"/> R	<input type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input type="checkbox"/> Sticky bit

Octal: 0755

☐ Add X to directories

☒ Set owner, group and permissions recursively

OK Cancel Help

---

# **dvwa:** **Down Vulnerable Web Application**

# Find DVWA-master zip file from Learn

⋮ Tips and Fixes 12

⋮ Module 1 - Ethical Hacking 12

⋮ Module 2 - VM Setup 39

⋮ DVWA - Vulnerable Web Application 14

⋮ Passwords 25

⋮ Module 3 - SQL/XSS Injection 23

⋮ Module 4 - Privacy & Secure Storage 36

⋮ Module 5 - Risks 75

⋮ Module 6 - 55

Download and unarchive DVWA zip file to a folder you can then use to move/copy over to Debian using WinSCP.

New ▾

Add Existing Activities ▾

⋮ Download of Database Frontend Software ▾

🔗 Link



⋮ Installing Debian, setting up SQL, uploading DVWA ▾

📄 Word Document



⋮ DVWA-master ▾

📁 Zip Compressed File



⋮ Attacking DVWA ▾

📄 Word Document

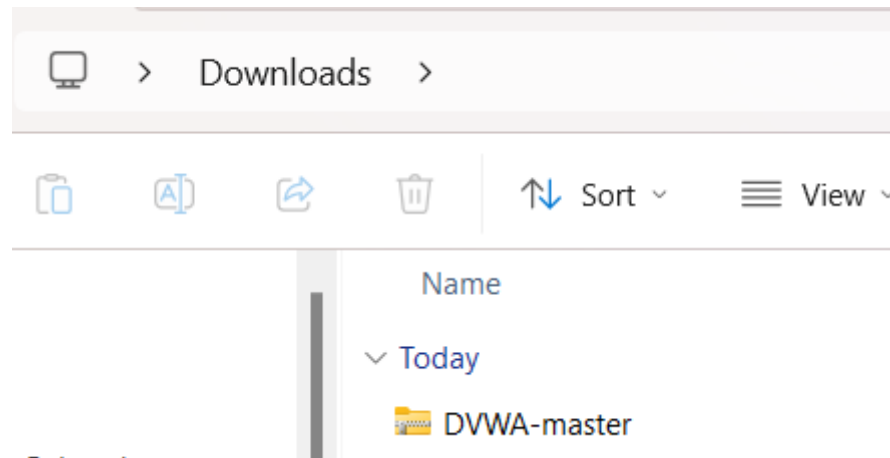


⋮ Configuring Debian for a Web Application ▾

📄 Word Document



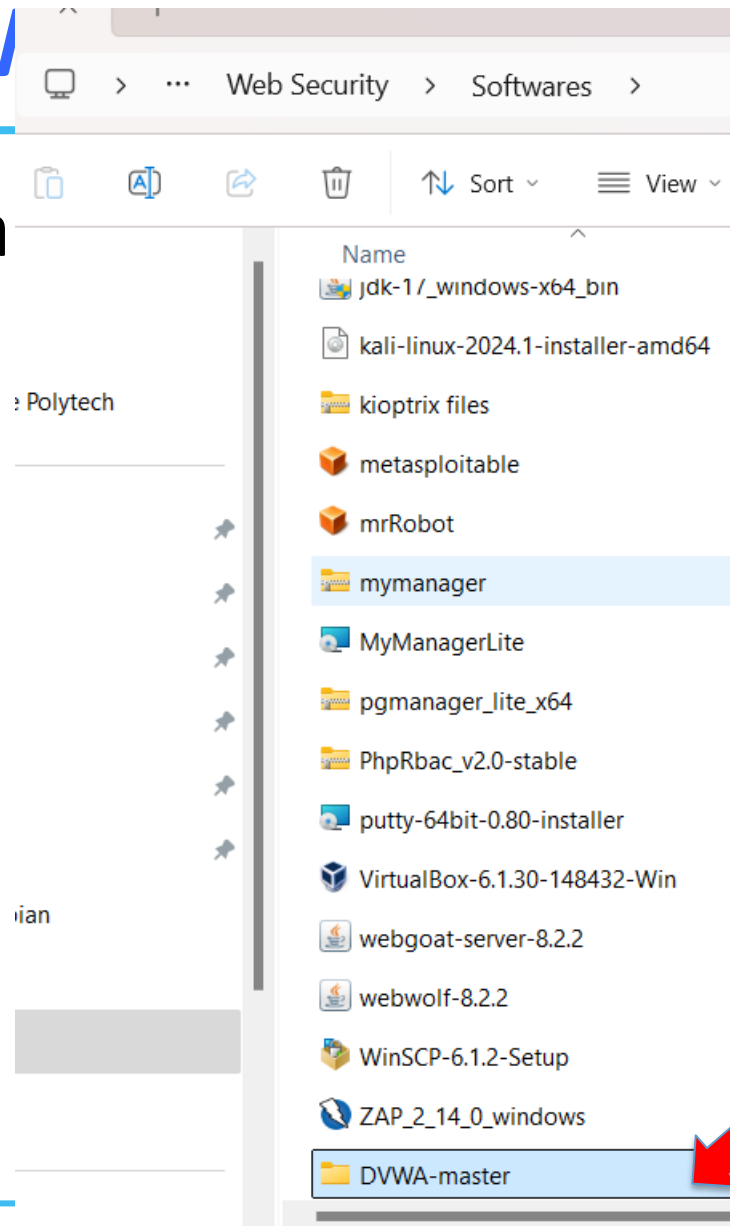
# Download DVWA-master from Learn and put it in Software Folder



# Deploy DVWA

➤ What we wa

oy DVWA



# Rename DVWA-master to dvwa

---

➤ Rename DVWA-master to dvwa



dvwa

Maryam Ghanbari > RRC Courses > Winter 2024 > Web Security > Softwares > dvwa >

New ▾

Sort ▾ View ▾

Home

Gallery

Maryam - Red Rive

Desktop

Downloads

Documents

Pictures

Music

Videos

Screenshots

Assignment 2

Fourth Navigation

Lecture 13

Creative Cloud Files

This PC

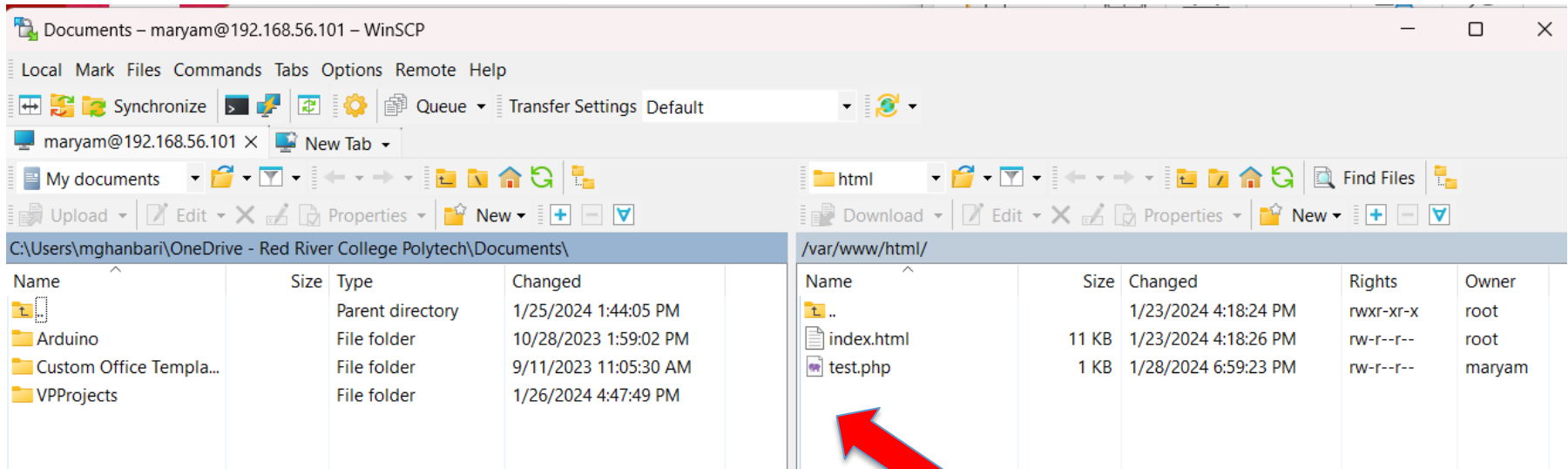
Windows (C:)

Network

Name	Date modified	Type	Size
config	1/28/2024 7:36 PM	File folder	
docs	1/28/2024 7:36 PM	File folder	
dvwa	1/28/2024 7:36 PM	File folder	
external	1/28/2024 7:36 PM	File folder	
hackable	1/28/2024 7:36 PM	File folder	
vulnerabilities	1/28/2024 7:36 PM	File folder	
.gitignore	12/5/2018 12:45 AM	Git Ignore Source ...	1 KB
.htaccess	12/5/2018 12:45 AM	HTACCESS File	1 KB
about	12/5/2018 12:45 AM	PHP Source File	4 KB
CHANGELOG	12/5/2018 12:45 AM	Markdown Source ...	8 KB
COPYING	12/5/2018 12:45 AM	Text Document	33 KB
favicon	12/5/2018 12:45 AM	ICO File	2 KB
ids_log	12/5/2018 12:45 AM	PHP Source File	1 KB
index	12/5/2018 12:45 AM	PHP Source File	5 KB
instructions	12/5/2018 12:45 AM	PHP Source File	2 KB
login	12/5/2018 12:45 AM	PHP Source File	5 KB
logout	12/5/2018 12:45 AM	PHP Source File	1 KB
php	12/5/2018 12:45 AM	Configuration setti...	1 KB
phpinfo	12/5/2018 12:45 AM	PHP Source File	1 KB



# Copy and paste dvwa in WinSCP (or drag it)

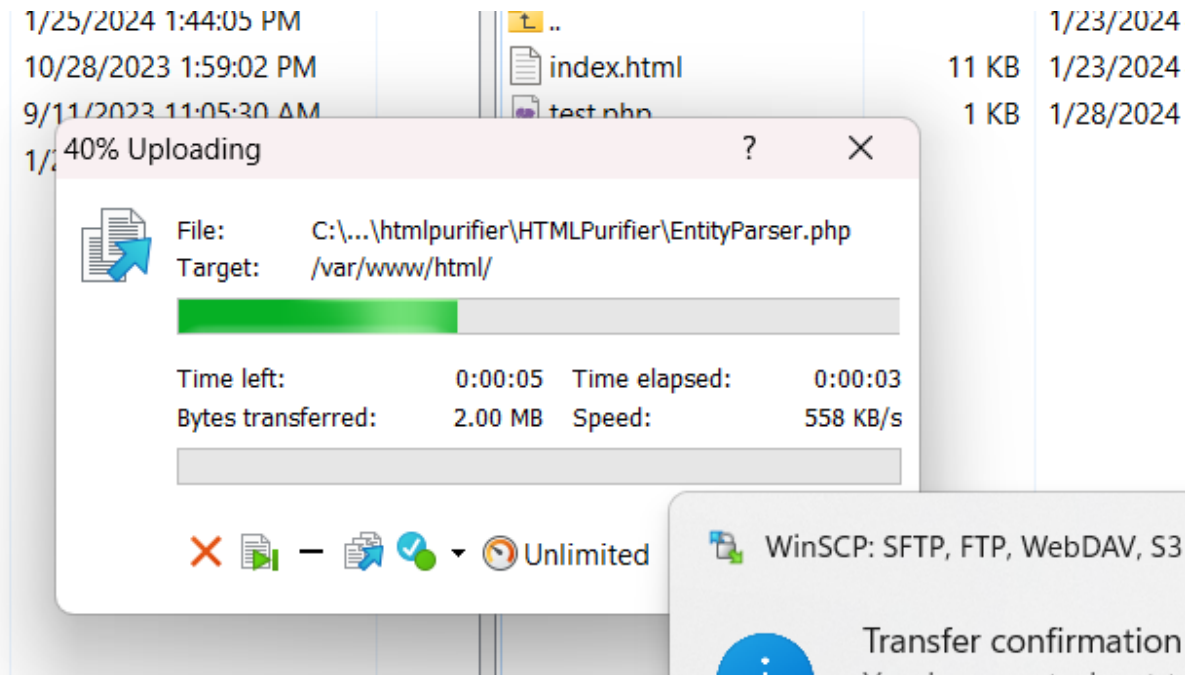


# Put the content of downloaded dvwa file in WinSCP

---

- Copy and paste the content of the downloaded dvwa file in WinSCP
  - Or
- Drag the downloaded dvwa file in WinSCP

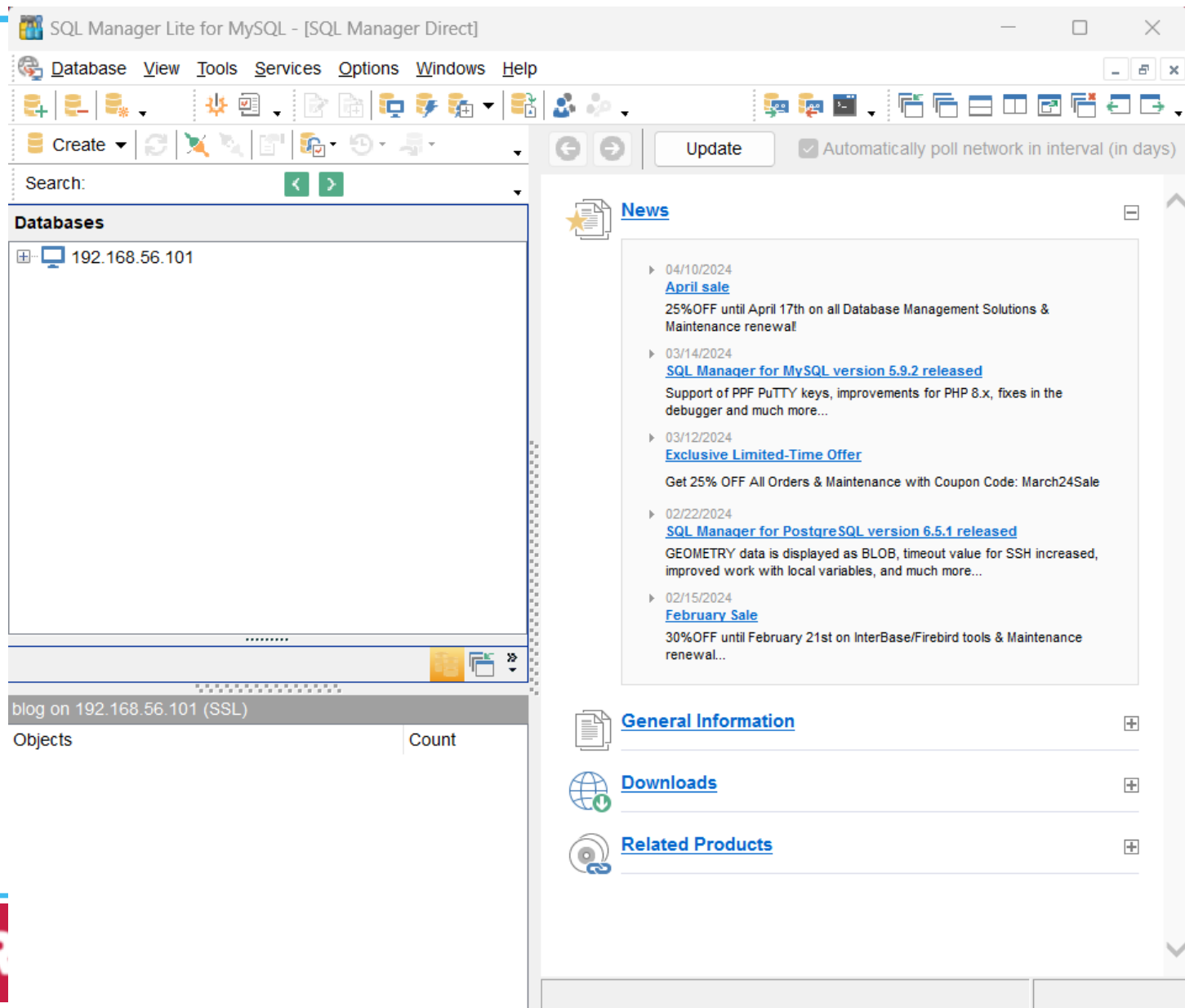
# drag the downloaded dvwa file in WinSCP



---

# Database

# Open “Sql Lite Manager”



The screenshot displays the SQL Manager Lite for MySQL application window. The title bar reads "SQL Manager Lite for MySQL - [SQL Manager Direct]". The menu bar includes Database, View, Tools, Services, Options, Windows, and Help. The toolbar contains various icons for database operations. Below the toolbar is a "Create" dropdown menu and a "Search:" field with navigation buttons. The main left pane is titled "Databases" and shows a single entry: "192.168.56.101". Below this, a status bar indicates "blog on 192.168.56.101 (SSL)". The bottom left pane shows a table with two columns: "Objects" and "Count". The right pane is titled "News" and contains a list of updates with dates and links. Below the news section are links for "General Information", "Downloads", and "Related Products".

SQL Manager Lite for MySQL - [SQL Manager Direct]

Database View Tools Services Options Windows Help

Create Search: Update Automatically poll network in interval (in days)

**Databases**

- 192.168.56.101

blog on 192.168.56.101 (SSL)

Objects	Count
---------	-------

**News**

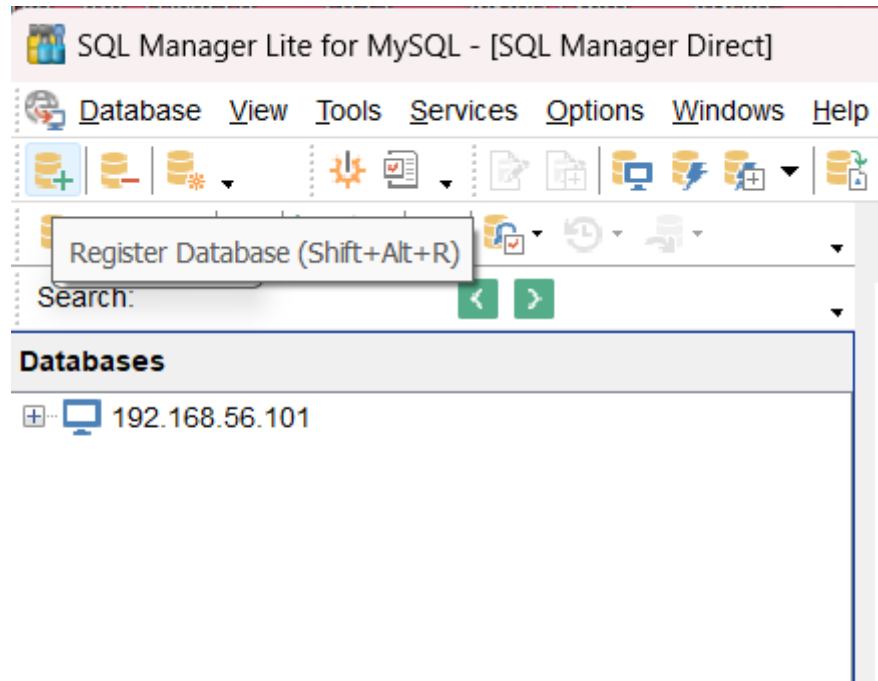
- 04/10/2024  
[April sale](#)  
25%OFF until April 17th on all Database Management Solutions & Maintenance renewal
- 03/14/2024  
[SQL Manager for MySQL version 5.9.2 released](#)  
Support of PPF PuTTY keys, improvements for PHP 8.x, fixes in the debugger and much more...
- 03/12/2024  
[Exclusive Limited-Time Offer](#)  
Get 25% OFF All Orders & Maintenance with Coupon Code: March24Sale
- 02/22/2024  
[SQL Manager for PostgreSQL version 6.5.1 released](#)  
GEOMETRY data is displayed as BLOB, timeout value for SSH increased, improved work with local variables, and much more...
- 02/15/2024  
[February Sale](#)  
30%OFF until February 21st on InterBase/Firebird tools & Maintenance renewal...

**General Information**

**Downloads**

**Related Products**

# Register Database



# Create

## Register Database Wizard



### Register Database

Specify the connection parameters



**SQL  
Manager  
for  
MySQL**

Welcome to the Register Database Wizard!

This wizard allows you to set the connection parameters for the selected databases only once, giving you the possibility to connect them quickly afterwards.

This wizard will guide you through the process of setting the connection parameters, selecting databases, and customizing their specific options.

Host name

192.168.56.101



Port

3306



User name

dwadmin

Password

••••••••

Named pipe

Method

Direct



Help

< Back


Next >

Cancel

Register Database Wizard

**Register Database**

Set some specific options for registered database(s) and click the Finish button



**SQL  
Manager  
for  
MySQL**

Database name: dwwa

Database alias: dwwa on 192.168.56.101

☒ Refresh objects on connection

☐ Login prompt before connection

☐ Use compression protocol

☐ Interactive mode

☒ Quote identifiers

☐ Autoconnect at startup

Help

< Back Finish Cancel



# Crea

SQL Manager Lite for MySQL - [SQL Manager Direct]

Database View Tools Services Options Windows Help

Create

Search:

**Databases**

- 192.168.56.101
  - Databases (2)
    - blog on 192.168.56.101 (SSL)
    - dvwa on 192.168.56.101 (SSL)**
  - Server Objects

dvwa on 192.168.56.101 (SSL)

Objects	Count
---------	-------

**News**

- 04/10/2024  
[April sale](#)  
25%OFF until April 17th or Maintenance renewal!
- 03/14/2024  
[SQL Manager for MySQL](#)  
Support of PPF PuTTY key debugger and much more.
- 03/12/2024  
[Exclusive Limited-Time](#)  
Get 25% OFF All Orders 8
- 02/22/2024  
[SQL Manager for PostgreSQL](#)  
GEOMETRY data is displayed; improved work with local
- 02/15/2024  
[February Sale](#)  
30%OFF until February 21 renewal...

**General Information**

**Downloads**

**Related Products**

# In WinSCP

Default

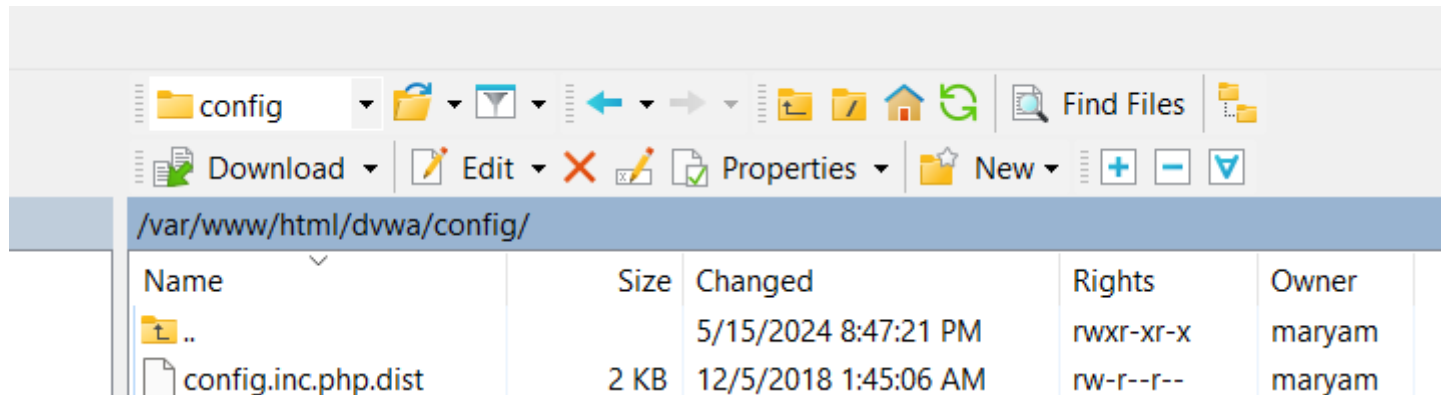
html

Download Edit Properties New

/var/www/html/

	Name	Size	Changed	Rights	Owner
3 PM	..		1/23/2024 4:18:24 PM	rw-r--r--	root
2 PM	Test		5/15/2024 10:41:36 PM	rw-r--r--	maryam
	dvwa_backup		1/28/2024 7:58:25 PM	rw-r--r--	maryam
	dvwa		5/15/2024 8:47:21 PM	rw-r--r--	maryam
	blog_backup		4/4/2024 10:34:01 PM	rw-r--r--	maryam
	blog		4/19/2024 2:18:40 AM	rw-r--r--	maryam
	test.php	1 KB	3/10/2024 5:30:15 PM	rw-r--r--	maryam
	index.html	11 KB	1/23/2024 4:18:26 PM	rw-r--r--	root

# Select the “ config.inc.php.dist ” file

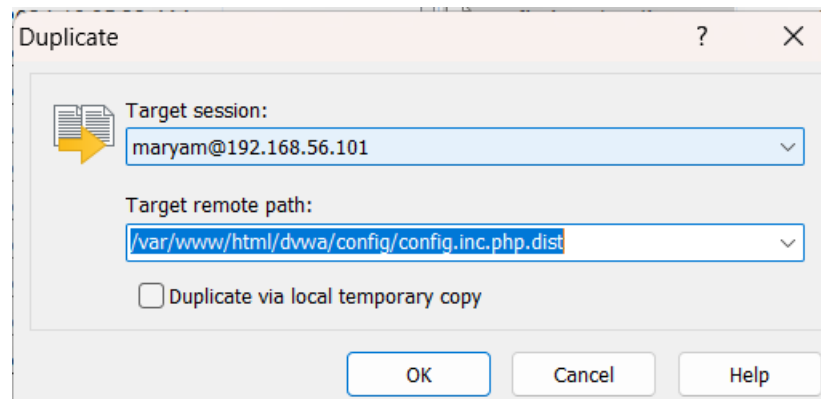


The screenshot shows a file manager window with the address bar displaying `/var/www/html/dvwa/config/`. The file list contains two entries: a parent directory `..` and a file `config.inc.php.dist` of size 2 KB, last modified on 12/5/2018 at 1:45:06 AM. The file permissions are `rw-r--r--` and the owner is `maryam`.

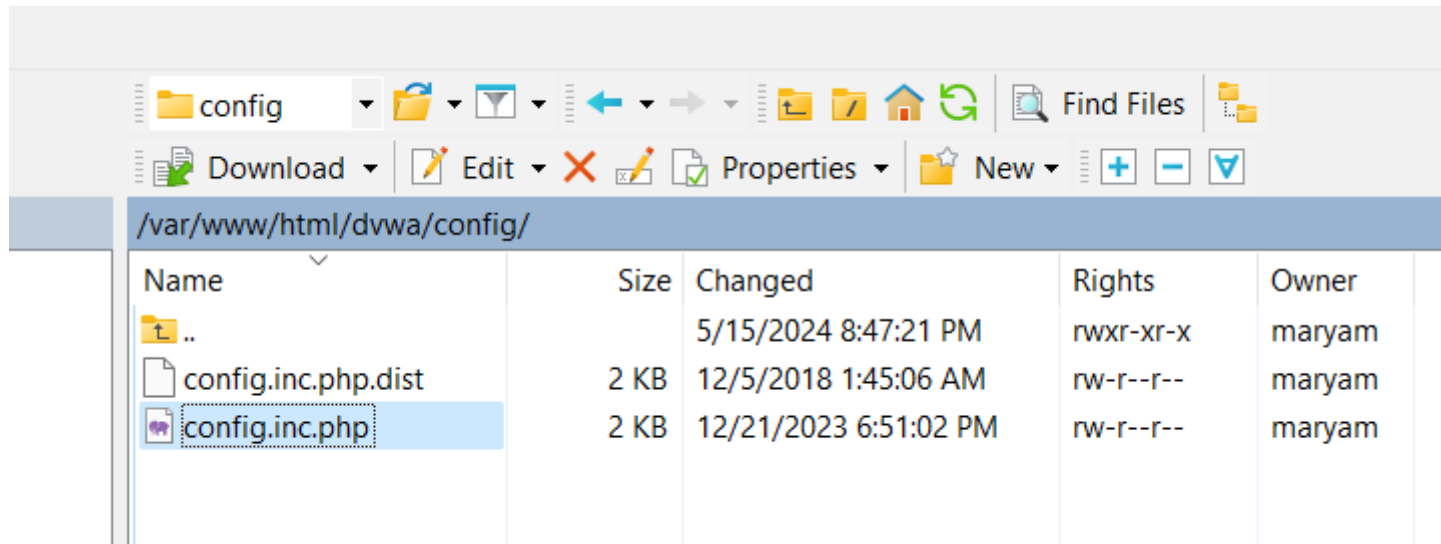
Name	Size	Changed	Rights	Owner
..		5/15/2024 8:47:21 PM	<code>rw-r--r--</code>	maryam
config.inc.php.dist	2 KB	12/5/2018 1:45:06 AM	<code>rw-r--r--</code>	maryam

# Select the “ config.inc.php.dist ” file

---



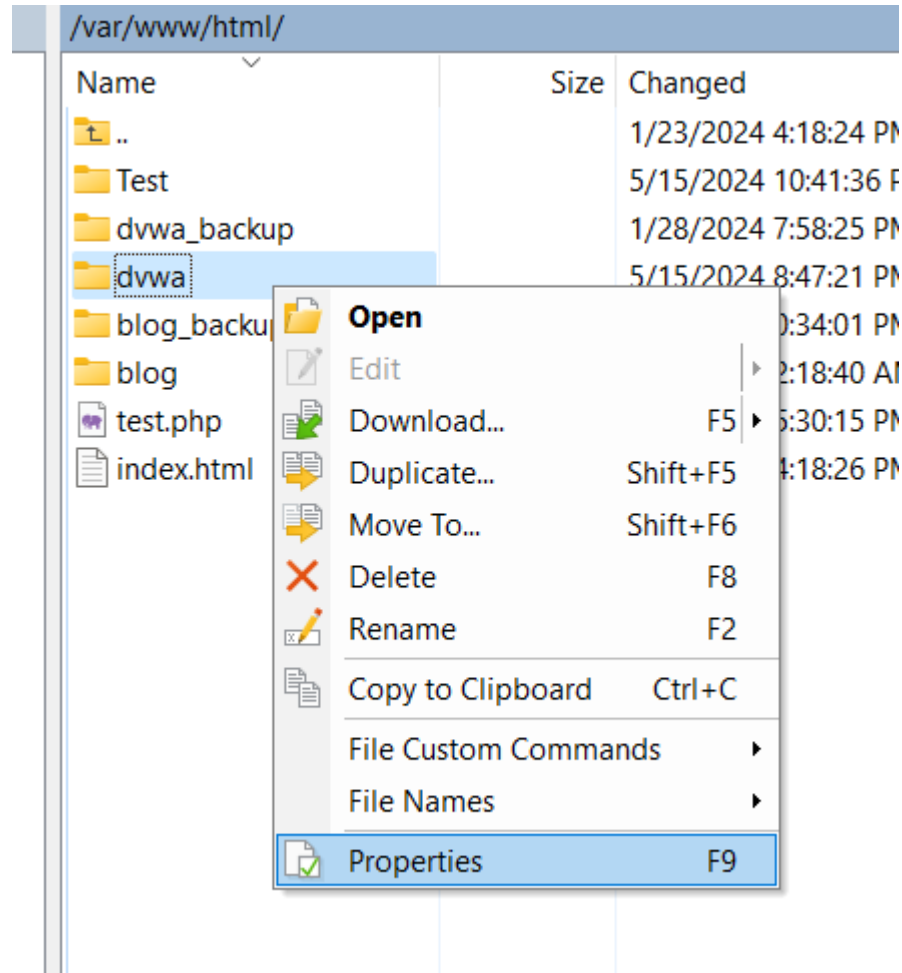
# Open DVWA



Name	Size	Changed	Rights	Owner
..		5/15/2024 8:47:21 PM	rw-r--r--	maryam
config.inc.php.dist	2 KB	12/5/2018 1:45:06 AM	rw-r--r--	maryam
config.inc.php	2 KB	12/21/2023 6:51:02 PM	rw-r--r--	maryam

```
config.inc.php x
1 |k?php
2
3 # If you are having problems connecting to the MySQL
  database and all of the variables below are correct
4 # try changing the 'db_server' variable from local
  127.0.0.1. Fixes a problem due to sockets.
5 # Thanks to @digininja for the fix.
6
7 # Database management system to use
8 $DBMS = 'MySQL';
9 #$DBMS = 'PGSQL'; // Currently disabled
10
11 # Database variables
12 # WARNING: The database specified under db_database
  WILL BE ENTIRELY DELETED during setup.
13 # Please use a database dedicated to DVWA.
14 #
15 # If you are using MariaDB then you cannot use root
  must use create a dedicated DVWA user.
16 # See README.md for more information on this.
17 $_DVWA = array();
18 $_DVWA[ 'db_server' ] = '127.0.0.1';
19 $_DVWA[ 'db_database' ] = 'dvwa';
20 $_DVWA[ 'db_user' ] = 'dvwa';
21 $_DVWA[ 'db_password' ] = 'password';
22
23 # Only used with PostgreSQL/PGSQL database selecti
24 $_DVWA[ 'db_port ' ] = '5432';
25
```


# Create



# Create

dwva Properties

Common Checksum

 dwva

Location: /var/www/html

Size: Unknown Calculate

Owner: maryam [1000]

Group: maryam [1000]

Permissions:

Owner	<input checked="" type="checkbox"/> R	<input checked="" type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input type="checkbox"/> Set UID
Group	<input checked="" type="checkbox"/> R	<input type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input type="checkbox"/> Set GID
Others	<input checked="" type="checkbox"/> R	<input type="checkbox"/> W	<input checked="" type="checkbox"/> X	<input type="checkbox"/> Sticky bit

Octal: 0755

☐ Add X to directories

☒ Set owner, group and permissions recursively

OK Cancel Help



# Debian (or PuTTY): look at current network setting

## ➤ ip addr

```
root@deb:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    ✓ inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:04:70:a0 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 83238sec preferred_lft 83238sec
    ✓ inet6 fe80::a00:27ff:fe04:70a0/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:72:c4:58 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic enp0s8
        valid_lft 536sec preferred_lft 536sec
    inet6 fe80::a00:27ff:fe72:c458/64 scope link
        valid_lft forever preferred_lft forever
```

➤ You have two adapters (enp0s3, enp0s8), so your setting is good.

# Go to your browser and type your

---

- 192.168.56.101
- 192.168.56.101/dvwa/setup.php

[Setup DVWA](#)[Instructions](#)[About](#)

## Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.  
If you get an error make sure you have the correct user credentials in: `/var/www/html/dvwa/config/config.inc.php`

If the database already exists, **it will be cleared and the data will be reset.**  
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

## Setup Check

Operating system: **\*nix**  
Backend database: **MySQL**  
PHP version: **8.2.18**

Web Server SERVER\_NAME: **192.168.56.101**

PHP function display\_errors: **Enabled** (*Easy Mode!*)  
PHP function safe\_mode: **Disabled**  
PHP function allow\_url\_include: **Enabled**  
PHP function allow\_url\_fopen: **Enabled**  
PHP function magic\_quotes\_gpc: **Disabled**  
PHP module gd: **Missing**  
PHP module mysql: **Installed**  
PHP module pdo\_mysql: **Installed**

MySQL username: **dvwa**  
MySQL password: **\*\*\*\*\***  
MySQL database: **dvwa**  
MySQL host: **127.0.0.1**

reCAPTCHA key: **Missing**

---

➤ Go to:

<http://192.168.56.101/dvwa/setup.php>

PHP function display\_errors: **Enabled** (Easy Mode!)  
PHP function safe\_mode: **Disabled**  
PHP function allow\_url\_include: **Enabled**  
PHP function allow\_url\_fopen: **Enabled**  
PHP function magic\_quotes\_gpc: **Disabled**  
PHP module gd: **Missing**  
PHP module mysql: **Installed**  
PHP module pdo\_mysql: **Installed**

MySQL username: **dvwa**  
MySQL password: **\*\*\*\*\***  
MySQL database: **dvwa**  
MySQL host: **127.0.0.1**

reCAPTCHA key: **Missing**

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

[User: maryam] 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](#).

# Error

---

- Students who has error at this stage and cannot see “Setup successful!”, they did not set up the password properly as shown follows:

Setup and configuration of **DVWA on** Page 77 of this PowerPoint file

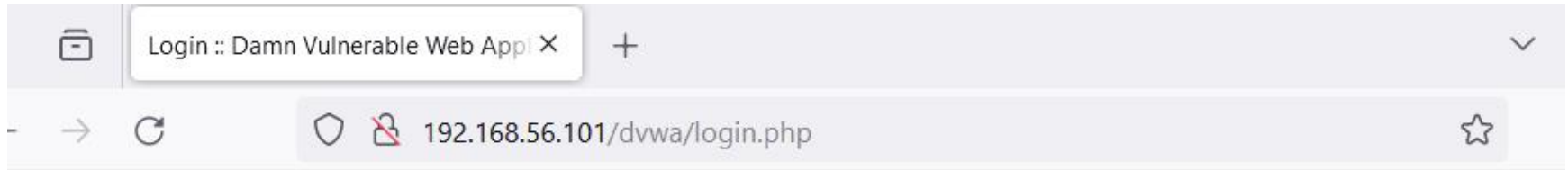
# Error

- The password, is the password that you are selected for the database. Maybe it different from my 'password'.
- Double check your setting. Otherwise, you cannot launch this website.

```
config.inc.php
1 |<?php
2
3 # If you are having problems connecting to the MySQL
  database and all of the variables below are correct
4 # try changing the 'db_server' variable from local
  127.0.0.1. Fixes a problem due to sockets.
5 # Thanks to @digininja for the fix.
6
7 # Database management system to use
8 $DBMS = 'MySQL';
9 # $DBMS = 'PGSQL'; // Currently disabled
10
11 # Database variables
12 # WARNING: The database specified under db_database
  WILL BE ENTIRELY DELETED during setup.
13 # Please use a database dedicated to DVWA.
14 #
15 # If you are using MariaDB then you cannot use root
  must use create a dedicated DVWA user.
16 # See README.md for more information on this.
17 $_DVWA = array();
18 $_DVWA[ 'db_server' ] = '127.0.0.1';
19 $_DVWA[ 'db_database' ] = 'dvwa';
20 $_DVWA[ 'db_user' ] = 'dvwa';
21 $_DVWA[ 'db_password' ] = 'password';
22
23 # Only used with PostgreSQL/PGSQL database selecti
24 $_DVWA[ 'db_port ' ] = '5432';
25
```



# Automatically you redirect to :



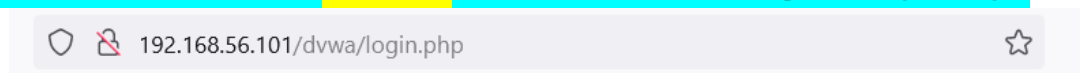
**Username**

**Password**

Login

➤ Go to the following address in the URL and hit enter

<http://192.168.56.101/dvwa/login.php>



admin

Username

password

Password

Login

Login :: Damn Vulnerable Web Appl X



192.168.56.101/dvwa/login.php



**Username**

admin

**Password**

••••••••

Login

Login failed



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

# 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

# Create

---

- Now we are free to experiment with the DVWA website. Be sure to set your **security** to the **lowest setting** in the website. It's set to impossible by default, and that's no fun for playing around!
- Also feel free to look around at the php code in the DVWA folders.
- Our next step is to do some SQL Injection.

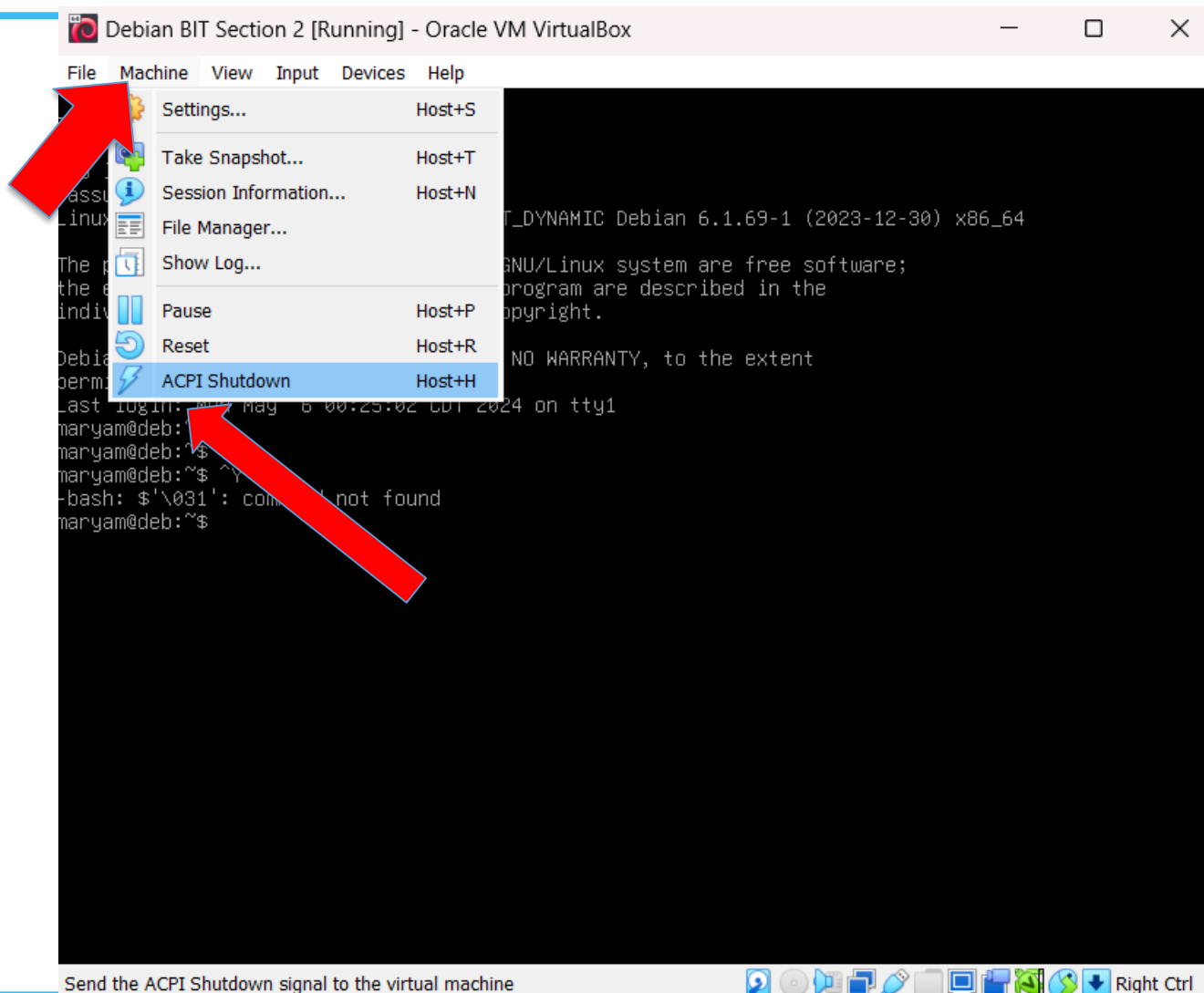
---

**You are ready to attack to  
the DVWA website**

---

# Shutdown Debian

# Debian (power off)





# Debian (power off)

---

## ➤ Second method

- Input -> Keyboard -> Insert Ctrl-Alt-Del
- Close (x) and “power of the machine” -> ok



# Oracle VM VirtualBox (Quit)

---

➤ File -> Quit