Damn Vulnerable Web Application (DVWA)

RHEL 10 Installation & Lab Setup Guide

Purpose
This repository documents a **clean, repeatable installation of DVWA on Red Hat Enterprise Linux 10**, intended for **CTF practice, enumeration labs (dirsearch / ffuf), and web vulnerability testing** in a **controlled, non-production environment**.

⚠️ WARNING

DVWA is **intentionally vulnerable**.

- ❌ **DO NOT** expose this system to the internet
- ❌ **DO NOT** deploy on production networks
- ✅ Use **isolated lab networks only**
- ✅ Snapshots recommended before exploitation

🧱 Environment Overview

Component	Value
OS	Red Hat Enterprise Linux 10
Web Server	Apache (httpd)
PHP	PHP 8.3
Database	MariaDB 10.11
App	DVWA
SELinux	Enforcing
Firewall	firewalld enabled
Access	HTTP (port 80)

1️⃣ System Preparation

Update system

```
sudo dnf update -y
```

```
sudo reboot
```

---

2 Enable Required Repositories

Enable Base Repos

```
sudo subscription-manager repos \
--enable rhel-10-for-x86_64-baseos-rpms \
--enable rhel-10-for-x86_64-appstream-rpms
```

Enable CodeReady Builder

```
sudo subscription-manager repos \
--enable codeready-builder-for-rhel-10-x86_64-rpms
```

Enable EPEL

```
sudo dnf install -y \
https://dl.fedoraproject.org/pub/epel/epel-release-latest-10.noarch.rpm
```

Verify:

```
dnf repolist
```

---

3 Install Required Packages

```
sudo dnf install -y \
httpd \
mariadb-server mariadb \
php php-cli php-common php-mysqlnd php-gd php-json php-mbstring php-xml php-
opcache php-pdo \
git
```

---

4 Start and Enable Services

```
sudo systemctl enable --now httpd
sudo systemctl enable --now mariadb
```

Verify:

```
systemctl status httpd
systemctl status mariadb
```

---

5 Secure MariaDB

```
sudo mysql_secure_installation
```

Recommended answers:

- Set root password → **YES**
- Remove anonymous users → **YES**
- Disallow remote root login → **YES**
- Remove test database → **YES**
- Reload privilege tables → **YES**

---

6 Create DVWA Database and User

```
sudo mysql -u root -p
```

Inside MariaDB:

```
CREATE DATABASE dvwa;

CREATE USER 'dvwa'@'localhost' IDENTIFIED BY 'dvwa@123';

GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwa'@'localhost';

FLUSH PRIVILEGES;

SHOW GRANTS FOR 'dvwa'@'localhost';

EXIT;
```

📌 **Note**
`Query OK, 0 rows affected` is normal for `CREATE USER` in MariaDB.

---

7 Deploy DVWA

```
cd /var/www/html
sudo git clone https://github.com/digininja/DVWA.git dvwa
```

---

8 Configure DVWA

```
cd /var/www/html/dvwa/config
```

```
sudo cp config.inc.php.dist config.inc.php
sudo nano config.inc.php
```

Set the database section to:

```
$_DVWA = array();

$_DVWA[ 'db_server' ]   = getenv('DB_SERVER') ?: '127.0.0.1';
$_DVWA[ 'db_database' ] = getenv('DB_DATABASE') ?: 'dvwa';
$_DVWA[ 'db_user' ]     = getenv('DB_USER') ?: 'dvwa';
$_DVWA[ 'db_password' ] = getenv('DB_PASSWORD') ?: 'dvwa@123';
$_DVWA[ 'db_port' ]     = getenv('DB_PORT') ?: '3306';
```

Save and exit.

9️⃣ Fix File Ownership & Permissions

```
sudo chown -R apache:apache /var/www/html/dvwa
sudo chmod -R 755 /var/www/html/dvwa
```

🔐 1️⃣0️⃣ SELinux Configuration (CRITICAL)

Without this, DVWA will fail silently.

```
sudo setsebool -P httpd_can_network_connect_db 1
sudo chcon -R -t httpd_sys_rw_content_t /var/www/html/dvwa
```

🔥 1️⃣1️⃣ Firewall Configuration

```
sudo firewall-cmd --permanent --add-service=http
sudo firewall-cmd --reload
```

🔄 1️⃣2️⃣ Restart Apache

```
sudo systemctl restart httpd
```

🌐 1️⃣3️⃣ DVWA Setup (Web)

Open browser:

```
http://<RHEL-IP>/dvwa/setup.php
```

Click:

Create / Reset Database

You should see **all green status indicators**.

🔑 1️⃣4️⃣ Login to DVWA

```
Username: admin
Password: password
```

Set:

- **DVWA Security → Low**

✅ Final Verification

DVWA main page:

```
http://<RHEL-IP>/dvwa/index.php
```

Expected result:

- Sidebar modules visible
- No DB connection errors
- All labs accessible

🧪 Enumeration Validation (Attacker VM)

```
python3 dirsearch.py -u http://<RHEL-IP>/dvwa -e php
```

Expected discoveries:

- `/login.php`
- `/setup.php`
- `/vulnerabilities/`
- `/config/`

- `/external/`

🧠 Lab Notes / Lessons Learned

- RHEL 10 + SELinux **requires explicit DB and write permissions**
- MariaDB user creation returns `0 rows affected` by design
- DVWA must use a **dedicated DB user** (not root)
- `127.0.0.1` avoids socket issues vs `localhost`
- This setup mirrors **real enterprise hardening + misconfiguration chains**

📌 Recommended Next Steps

- Snapshot VM before exploitation
- Pair with **FFUF**, **Burp**, **sqlmap**
- Document findings per vulnerability
- Harden system → re-test
- Integrate into **CTF Cheat Dashboard**

📜 License & Attribution

- DVWA by `digininja`
- Installed for **educational and lab use only**