

№2

---

21 . .  
2025

, ,



- 

- 

- 

-03-23



DVWA.

DVWA

GitHub ( . (fig:001?)).

/var/www/html.

```
udnazarmamadov@udnazarmamadov: /var/www/html

Session Actions Edit View Help

(udnazarmamadov@udnazarmamadov)-[~]
$ cd /var/www/html

(udnazarmamadov@udnazarmamadov)-[/var/www/html]
$ sudo git clone https://github.com/ethicalhack3r/DVWA
[sudo] password for udnazarmamadov:
Cloning into 'DVWA'...
remote: Enumerating objects: 5373, done.
remote: Total 5373 (delta 0), reused 0 (delta 0), pack-reused 5373 (from 1)
Receiving objects: 100% (5373/5373), 2.57 MiB | 251.00 KiB/s, done.
Resolving deltas: 100% (2673/2673), done.

(udnazarmamadov@udnazarmamadov)-[/var/www/html]
$
```

777

```
(udnazarmamadov@udnazarmamadov)-[/var/www/html]  
$ ls  
DVWA index.html index.nginx-debian.html  
  
(udnazarmamadov@udnazarmamadov)-[/var/www/html]  
$ sudo chmod -R 777 DVWA  
  
(udnazarmamadov@udnazarmamadov)-[/var/www/html]  
$
```

DVWA, /dvwa/config,

```
(udnazarmamadov@udnazarmamadov) - [/var/www/html]
$ cd DVWA/config

(udnazarmamadov@udnazarmamadov) - [/var/www/html/DVWA/config]
$ ls
config.inc.php.dist
```

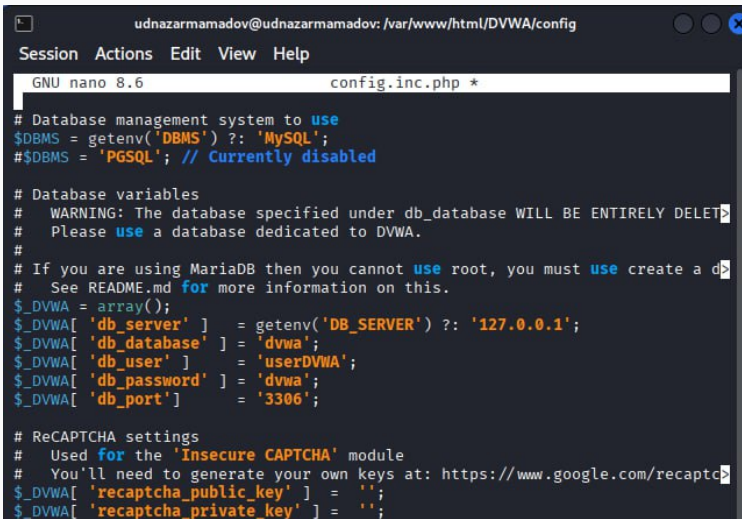


DVWA config.inc.php.dist

config.inc.php.

```
(udnazarmamadov@udnazarmamadov)-[/var/www/html/DVWA/config]
$ sudo cp config.inc.php.dist config.inc.php

(udnazarmamadov@udnazarmamadov)-[/var/www/html/DVWA/config]
$ ls
config.inc.php  config.inc.php.dist
```



```
udnazarmamadov@udnazarmamadov: /var/www/html/DVWA/config
Session Actions Edit View Help
GNU nano 8.6 config.inc.php *
# Database management system to use
$DBMS = getenv('DBMS') ?: 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
# WARNING: The database specified under db_database WILL BE ENTIRELY DELETED
# Please use a database dedicated to DVWA.
#
# If you are using MariaDB then you cannot use root, you must use create a database
# 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' ] = 'userDVWA';
$_DVWA[ 'db_password' ] = 'dvwa';
$_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
$_DVWA[ 'recaptcha_public_key' ] = '';
$_DVWA[ 'recaptcha_private_key' ] = '';
```

Kali Linux

mysql,

```
(udnazarmamadov@udnazarmamadov)-[/var/www/html/DVWA/config]
$ sudo systemctl start mysql

(udnazarmamadov@udnazarmamadov)-[/var/www/html/DVWA/config]
$ systemctl status mysql
● mariadb.service - MariaDB 11.8.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; pres>
   Active: active (running) since Sun 2025-09-21 16:26:33 EDT; 15s ago
 Invocation: a63e5b51f926413582cfdb63b7e50b8b
    Docs: man:mariabdb(8)
          https://mariadb.com/kb/en/library/systemd/
   Process: 229856 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d>
   Process: 229858 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery >
   Process: 229933 ExecStartPost=/bin/rm -f /run/mysqld/wsrep-start-positio>
   Process: 229943 ExecStartPost=/etc/mysql/debian-start (code=exited, stat>
  Main PID: 229910 (mariabdb)
    Status: "Taking your SQL requests now ..."
    Tasks: 14 (limit: 30005)
```

root.

“MariaDB”,

config.inc.php

```
(udnazarmamadov@udnazarmamadov)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
[sudo] password for udnazarmamadov:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.8.3-MariaDB-1+b1 from Debian -- Please help get to 10k stars at https://github.com/MariaDB/Server

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)]> █
```

```
(udnazarmamadov@udnazarmamadov)-[/var/www/html/DVWA/config]
$ sudo mysql -u root -p
[sudo] password for udnazarmamadov:
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 11.8.3-MariaDB-1+b1 from Debian -- Please help get to 10k s
rs at https://github.com/MariaDB/Server

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

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

MariaDB [(none)]> grant all privileges on dvwa.* to 'userDVWA'@'127.0.0.1'
Query OK, 0 rows affected (0.005 sec)

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

apache2,

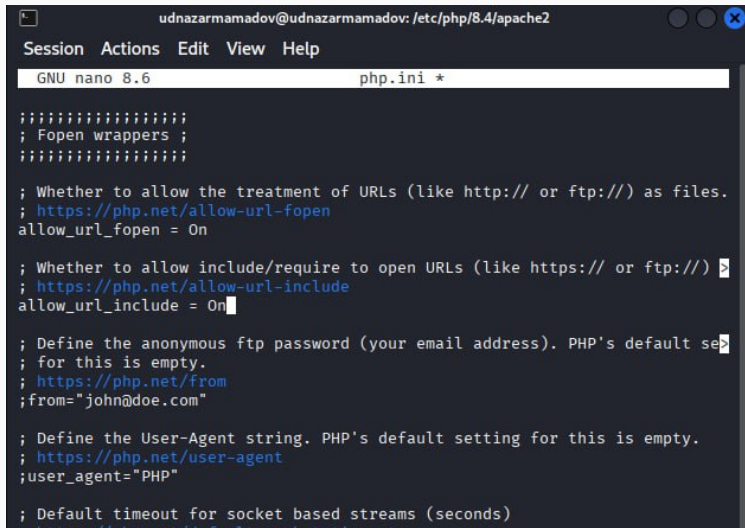
```
(udnazarmamadov@udnazarmamadov) - [/var/www/html/DVWA/config]
$ cd /etc/php/8.4/apache2

(udnazarmamadov@udnazarmamadov) - [/etc/php/8.4/apache2]
$
```

## 3.1

php.ini

,



```
udnazarmamadov@udnazarmamadov: /etc/php/8.4/apache2
Session Actions Edit View Help
GNU nano 8.6 php.ini *

;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; https://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require to open URLs (like https:// or ftp://) >
; https://php.net/allow-url-include
allow_url_include = On

; Define the anonymous ftp password (your email address). PHP's default se>
; for this is empty.
; https://php.net/from
;from="john@doe.com"

; Define the User-Agent string. PHP's default setting for this is empty.
; https://php.net/user-agent
user_agent="PHP"

; Default timeout for socket based streams (seconds)
```

allow\_url\_fopen allow\_url\_include

On

```
(udnazarmamadov@udnazarmamadov)-[/etc/php/8.4/apache2]
$ sudo systemctl start apache2

(udnazarmamadov@udnazarmamadov)-[/etc/php/8.4/apache2]
$ systemctl status start apache2
Unit start.service could not be found.
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; pr>
   Active: active (running) since Sun 2025-09-21 16:39:02 EDT; 29s ago
 Invocation: b1ed58ac61174625a5d07d50ca5a86e0
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 236217 ExecStart=/usr/sbin/apachectl start (code=exited, stat>
   Main PID: 236263 (apache2)
     Tasks: 6 (limit: 4546)
    Memory: 20.8M (peak: 21.2M)
       CPU: 73ms
    CGroup: /system.slice/apache2.service
            └─236263 /usr/sbin/apache2 -k start
              └─236266 /usr/sbin/apache2 -k start
                └─236267 /usr/sbin/apache2 -k start
                  └─236268 /usr/sbin/apache2 -k start
```



- apache ,

← → ↻ 🏠 127.0.0.1/DVWA/setup.php 📄 ☆ 📧 📁 ☰

Kali Linux 🌐 Kali Tools 📄 Kali Docs 🌐 Kali Forums 📄 Kali NetHunter 🔥 Exploit-DB 🔥 Google Hacking DB 🌐 OffSec

# DVWA

## 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

Web Server SERVER\_NAME: **127.0.0.1**

Operating system: **\*nix**

PHP version: **8.2.12**  
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: **Missing - Only an issue if you want to play with captchas**  
PHP module mysql: **Installed**  
PHP module pdo\_mysql: **Installed**

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

DVWA, Apache  
127.0.0.1/DVWA

**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  
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

Create / Reset Database

create/reset database



Username

admin

Password

••••••••|

Login

127.0.0.1/DVWA/index.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# DVWA

## 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.

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 recommended 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 persons who uploaded and installed it.

### More Training Resources

- 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
- Authorisation Bypass
- Open HTTP Redirect
- DVWA Security
- PHP Info
- About
- Logout

127.0.0.1/DVWA/index.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# DVWA

## 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.

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 recommended 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 persons who uploaded and installed it.

### More Training Resources

- 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
- Authorisation Bypass
- Open HTTP Redirect
- DVWA Security
- PHP Info
- About
- Logout



- DVWA.