

Installing DVWA on Kali Linux

@mmar



DVWA, or Damn Vulnerable Web Application, is a web application intentionally designed to be vulnerable to various security vulnerabilities. It is often used as a training and learning tool to learn about web application security and for testing the effectiveness of web application security tools. DVWA contains several types of vulnerabilities, including:

- ✓ **SQL injection**
- ✓ **File Inclusion**
- ✓ **Cross-Site Request Forgery (CSRF)**
- ✓ **Insecure Direct Object Reference**

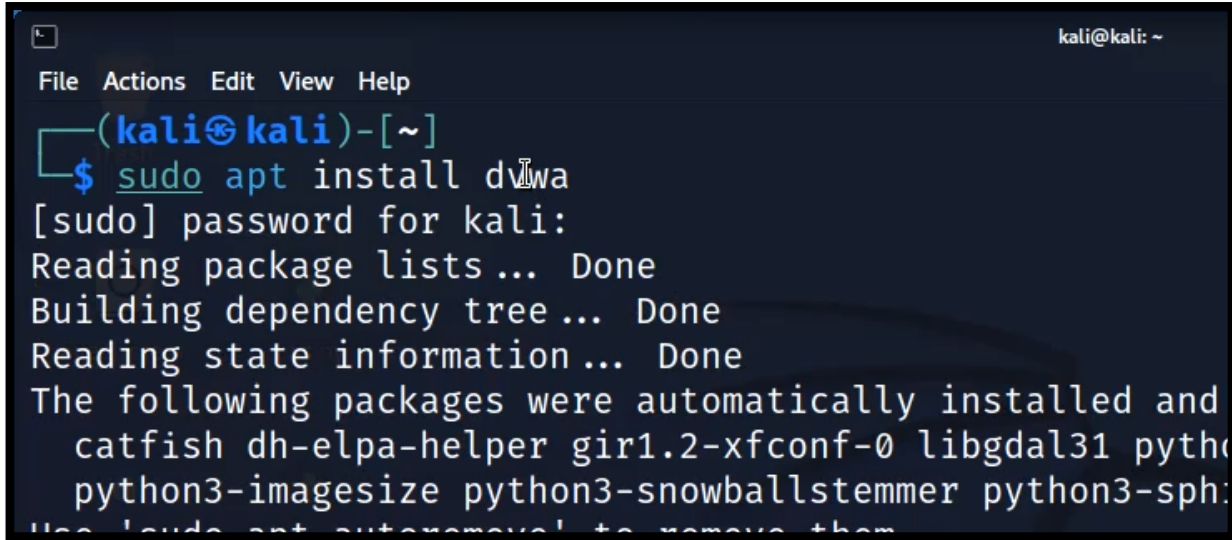


You should be on Kali Linux or Parrot OS in VMWARE, Virtual Box or running natively on your PC

Step- 1

- ❖ we can simply install DVWA in automated manner with kali repositories. Just use the following command

```
>sudo apt install DVWA
```

A terminal window screenshot with a dark background. The title bar shows 'kali@kali: ~'. The menu bar includes 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~]'. The command '\$ sudo apt install dvwa' is entered. The output shows the password prompt, progress bars for reading package lists, building dependency tree, and reading state information, all marked as 'Done'. It then lists several packages that were automatically installed along with 'dvwa'.

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ sudo apt install dvwa  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and  
  catfish dh-elpa-helper gir1.2-xfconf-0 libgdal31 python3-  
  python3-imagesize python3-snowballstemmer python3-sph  
Use 'sudo apt autoremove' to remove them
```

Step- 2

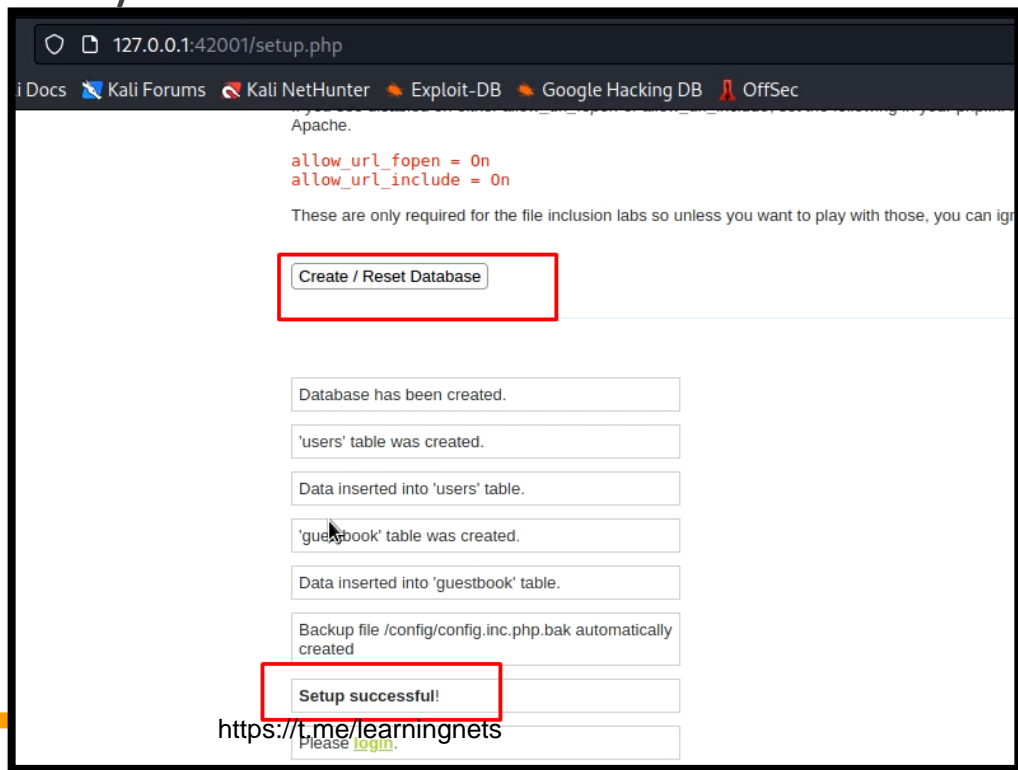
- ❖ Once DVWA is installed, you can use the following command to start it

```
>dvwa-start
```

```
(kali@kali)-[~]  
└─$ dvwa-start
```

Step- 3

- ❖ Use the default credentials (admin/password) to log in to the DVWA web interface. A setup page will open. Scroll down and click on create/ reset the database



The screenshot shows a web browser window with the address bar displaying `127.0.0.1:42001/setup.php`. The browser's tab bar includes links to 'Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. The main content area of the browser shows the DVWA setup page. At the top, it says 'Apache.' followed by two lines of code: `allow_url_fopen = On` and `allow_url_include = On`. Below this, a note states: 'These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.' A red rectangular box highlights the 'Create / Reset Database' button. Below the button, a series of status messages are displayed in separate boxes: 'Database has been created.', ''users' table was created.', 'Data inserted into 'users' table.', ''guestbook' table was created.', and 'Data inserted into 'guestbook' table.'. A final message states: 'Backup file /config/config.inc.php.bak automatically created'. At the bottom of the page, a red rectangular box highlights the text 'Setup successful!'. Below this, there is a 'Please Login.' prompt and a 'Login' button. A URL `https://t.me/learningnets` is visible at the bottom left of the image.

Step- 4

- ❖ Now, you can access DVWA and start your web pentesting. Once done, you can stop dvwa with the following command

```
>dvwa-stop
```

```
(kali@kali)-[~]  
└─$ dvwa-stop
```

DEMO



THANKS