

# **File Inclusion Walkthrough on DVWA**

**File inclusion vulnerability** is a type of vulnerability that allows an attacker to include a file, usually, through a script on a web server, that is not properly checked for validity. This can allow an attacker to execute arbitrary code, including PHP code, on the server, potentially leading to server compromise. There are two main types of file inclusion vulnerabilities:

- ✓ **Local file inclusion (LFI)** allows an attacker to include files that are stored locally on the server
- ✓ **Remote file inclusion (RFI)** allows an attacker to include files from a remote server, such as through a URL

“

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

# Step-1

- ❖ Go to DVWA security settings and set the difficulty to low



The screenshot shows the DVWA Security settings page. On the left is a navigation menu with buttons for 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), and XSS (Stored). The main content area is titled "DVWA Security" with a lock icon. Below the title is the "Security Level" section, which states "Security level is currently: low." and provides instructions on how to change the level. A list of four levels is provided: 1. Low (completely vulnerable), 2. Medium (bad security practices), 3. High (harder or all practices), and 4. Impossible (secure against all vulnerabilities). A red box highlights the "Low" dropdown menu and the "Submit" button.

## DVWA Security

### Security Level

Security level is currently: **low**.

You can set the security level to low, medium, high or impossible. The security level changes the level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**, as an example of how web application vulnerabilities manifest through bad coding practices as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices** a developer has tried but failed to secure an application. It also acts as a challenge to user exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or all practices** to attempt to secure the code. The vulnerability may not allow the same extent of exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare source code to the secure source code.  
Prior to DVWA v1.9, this level was known as 'high'.

## Step- 2

- ❖ Click on the first file. We can see that file name is included in the URL. Now we can provide any file name that is on the system to open it. For example, we can check the passwd file as under and open the passwd file on the system that contains the user details



```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/g
an:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/
roxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailng List Manager:/var/list:/usr/sbin/nologin irc
apt:x:42:65534:./nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin systemd-timesync:x:997:9
usr/sbin/nologin messagebus:x:100:107:./nonexistent:/usr/sbin/nologin tss:x:101:109:TPM software stack,./var/lib/tpm:/bin/false strongswan:x:102:65534:./var/lib/strongswan:/usr/sbin/nologin tcpdump:x:103:110:./
sbmux:x:104:46:usbmux daemon,./var/lib/usbmux:/usr/sbin/nologin sshd:x:105:65534:./run/ssh:/usr/sbin/nologin dnsmasq:x:106:65534:dnsmasq,./var/lib/misc:/usr/sbin/nologin avahi:x:107:113:Avahi mDNS da
nologin speech-dispatcher:x:108:29:Speech Dispatcher,./run/speech-dispatcher:/bin/false pulse:x:109:114:PulseAudio daemon,./run/pulse:/usr/sbin/nologin saned:x:110:117:./var/lib/saned:/usr/sbin/nologin lightd
b/lightdm:/bin/false polkitd:x:996:996:polkit:/var/lib/polkit-1:/usr/sbin/nologin rtkit:x:112:119:RealtimeKit,./proc:/usr/sbin/nologin colord:x:113:120:colord colour management daemon,./var/lib/colord:/usr/sbin/nolog
penVPN,./var/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:115:123:NetworkManager OpenConnect plugin,./var/lib/NetworkManager:/usr/sbin/nologin mysql:x:116:124:MySQL Server,./nonexistent:/t
ystem account:/var/run/stunnel4:/usr/sbin/nologin _rpc:x:117:65534:./run/rpcbind:/usr/sbin/nologin geoclue:x:118:126:./var/lib/geoclue:/usr/sbin/nologin Debian-snm:x:119:127:./var/lib/snm:/bin/false ssh:x:120:12
psec:x:121:132:./nonexistent:/usr/sbin/nologin redsocks:x:122:133:./var/run/redsocks:/usr/sbin/nologin rwho:x:123:65534:./var/spool/rwho:/usr/sbin/nologin iodine:x:124:65534:./run/iodine:/usr/sbin/nologin miredo
nologin statd:x:126:65534:./var/lib/nfs:/usr/sbin/nologin redis:x:127:134:./var/lib/redis:/usr/sbin/nologin postgres:x:128:135:PostgreSQL administrator,./var/lib/postgresql/bin/bash mosquito:x:129:136:./var/lib/mosq
etsim:x:130:137:./var/lib/inetsim:/usr/sbin/nologin gvm:x:131:139:./var/lib/ovnas:/usr/sbin/nologin king-phisher:x:132:140:./var/lib/king-phisher:/usr/sbin/nologin kali:x:1000:1000:./home/kali:/usr/bin/zsh dwwa
```



**DEMO**



**THANKS**