File Inclusion Walkthrough on DVWA

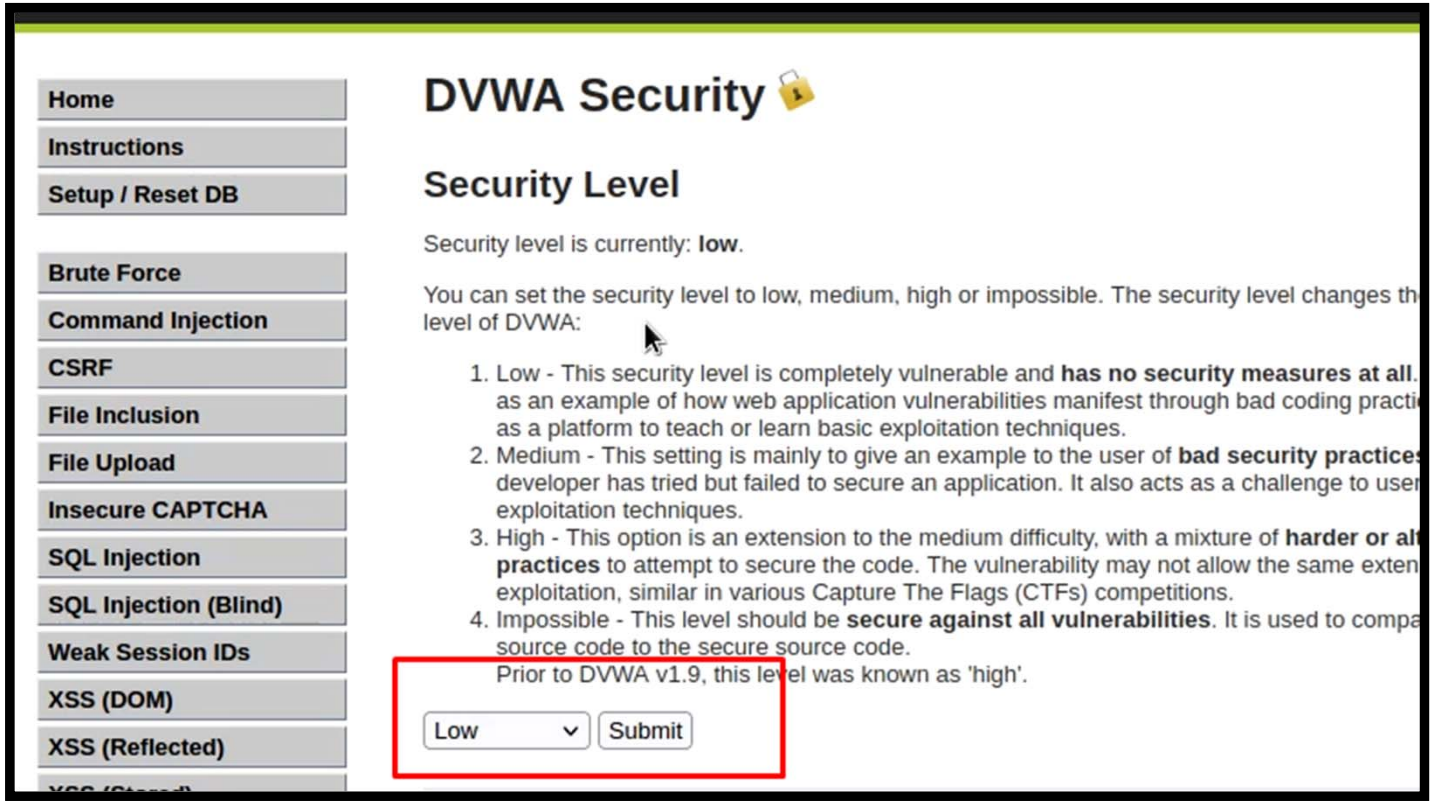
File inclusion vulnerability is a type of vulnerability that allows an attacker to include a file, usually, through a script on a web server, that is not properly checked for validity. This can allow an attacker to execute arbitrary code, including PHP code, on the server, potentially leading to server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



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 passed file as under and open the passwd file on the system that contains the user details

DEMO

THANKS