

# Web Application Hacking Local File Inclusion

## Objectives

- Review lecture
- Complete lab on LFI

### Lab for LFI

#### Lab Prep

Open the link to <https://hack.me>

Choose "Start a hackme"

Scroll down and select "DVWA 1.0.7"

Accept the agreement after selecting "anonymous login"

## DVWA File Inclusion

This will be a fairly short and quick guide about the File Inclusion vulnerability.

**Local File Inclusion (LFI)** is a type of vulnerability most often found on websites. It allows an attacker to include a local file, usually through a script on the web server. The vulnerability occurs due to the use of user-supplied input without proper validation. This can lead to something as minimal as outputting the contents of the file, but depending on the severity, to list a few it can lead to:

- Code execution on the web server
- Code execution on the client-side such as JavaScript which can lead to other attacks such as cross site scripting (XSS).
- Denial of Service (DoS)

- Data Theft/Manipulation

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are 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 aid teachers/students to teach/learn web application security in a quick and effective manner.

**WARNING!**

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public file folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

**Disclaimer**

We do not take responsibility for the way in which any one uses this application. 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.

**General Instructions**

The help button allows you to view hints/tips for each vulnerability and for each security level on their respective page.

Username: admin  
Security Level: high  
PHPIDS: disabled

Logout

2. Go to the DVWA Security page and change the Script Security level to low.

**DVWA Security**

**Script Security**

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

**PHPIDS** v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS](#) | [Disable PHPIDS](#)

**Logout**

Username: admin  
Security Level: low  
PHPIDS: disabled

Now we're ready to try out some file inclusion.

# The Attack:

1. Go to the File Inclusion page of DVWA and we will get started.

A screenshot of the DVWA (Damn Vulnerable Web Application) interface. The left sidebar shows various attack categories: Home, Instructions, Brute Force, Command Execution, CSRF, File Inclusion (which is highlighted in green), SQL Inject., SQL Inject. (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. Below the sidebar, the user is logged in as 'admin' with security level 'low' and PHPDS disabled. The main content area is titled 'Vulnerability: File Inclusion' with a note: 'To include a file edit the ?page=index.php in the URL to determine which file is included.' It includes a 'More info' section with links to Wikipedia and a Stack Overflow post. At the bottom right are 'View Source' and 'View Help' buttons.

2. Click the View Source button to see what the File Inclusion Source looks like, this will give us an idea of how this works and what we can do.

A screenshot of a Mozilla Firefox browser window showing the 'File Inclusion Source' page from DVWA. The title bar says 'Vulnerable Web App (DVWA) v1.0.7 :: Source - Mozilla Firefox'. The address bar shows the URL 'http://dvwa/vulnerabilities/view\_source.php?id=fi&security=low'. The main content area displays the following PHP code:

```
<?php  
$file = $_GET['page']; //The page we wish to display  
?>
```

Below the code is a 'Compare' button. The browser status bar at the bottom shows 'Done Apache/2.2... ss FoxyProxy: Disabled'.

Now we can see that there is no filtering of what we include, so lets try some things out.

3. Change the URL from **http://dvwa/vulnerabilities/fi/?page=include.php** to **http://dvwa/vulnerabilities/fi/?page=/etc/passwd** and see what happens.



As you can see, we get the contents of the passwd file and a few error messages. We now know the name of every user who can log into the local system, but what about all of the groups that exist?

4. Again change the URL to **http://dvaw/vulnerabilities/fi/?page=/etc/group** and see what happens.



Again, we get the contents of the group file and some error messages. We could view the contents of any file the web server has read access to. If this were a truly insecure website, we could also use this to view pages on other websites by changing the URL like we did before but instead pointing to a remote file or webpage.

1. Describe in your own words what Local File Inclusion is?
2. Describe why LFI is dangerous

- **Proof of Lab Instructions:**
  1. Do a <PrtScn> of lab
  2. Paste into a word document
  3. Post to teambox
-