Vulnerability Name:	File Inclusion
Affected Vendor:	DVWA
Affected Product name:	http://dvwa/vulnerabilities/fi/?page=include.php
Product Official Website URL:	http://dvwa/login.php
Affected Component:	Affected URL

Description: - File Inclusion Vulnerabilities arise when a web application allows users to include files or resources dynamically, without proper validation or access controls, leading to unauthorized access, remote code execution, or data leakage.

Root Cause: - Insecure file path handling, lack of input validation or sanitization, improper file permissions or access controls.

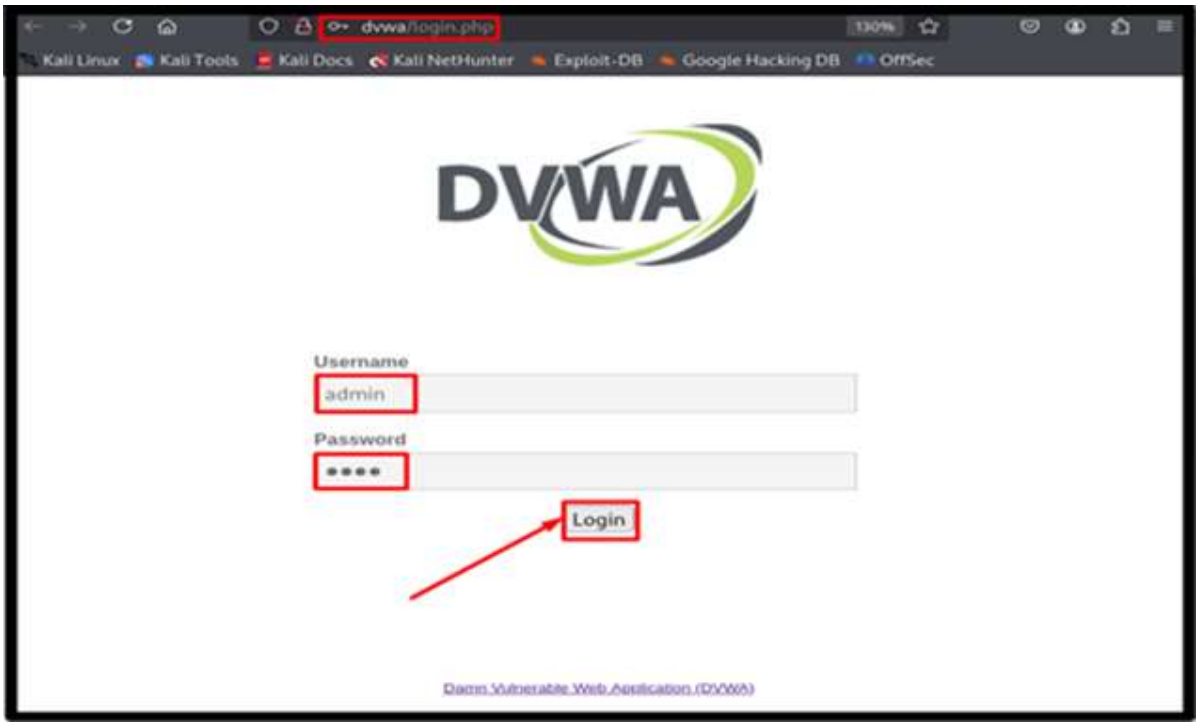
Impact: - Unauthorized access to sensitive files or resources, remote code execution, data disclosure or leakage, compromise of server integrity.

Mitigation: - Implement strict file path validation, restrict file inclusion to trusted directories, enforce proper file permissions and access controls, utilize whitelist-based validation, avoid user-controlled input in file inclusion functions, implement secure coding practices.

Remediation: - To remediate File Inclusion vulnerabilities:
1. Validate user input to prevent directory traversal.
2. Use a whitelist of allowed files and directories.
3. Avoid using user-inputted data in file inclusion statements.
4. Use a secure file inclusion mechanism, such as a PHP framework's built-in functions.
5. Limit file permissions and access controls.
6. Regularly update and patch software and frameworks.
7. Implement a Web Application Firewall (WAF) to detect and prevent file inclusion attacks.

Proof of Concept

Step: -1 First navigate to http://dvwa/login.php and login with username and Password.



Local File Inclusion :- LFI (Local File Inclusion) vulnerability enables attackers to read—and in some cases, execute—files on the target system. This poses a significant security risk, as misconfigured web servers running with elevated privileges may expose **sensitive information**. Additionally, if an attacker can upload malicious code through another method, they could potentially execute **arbitrary commands**, leading to complete system compromise.

Security Level :- Low

As we Know, we will first view the source code.

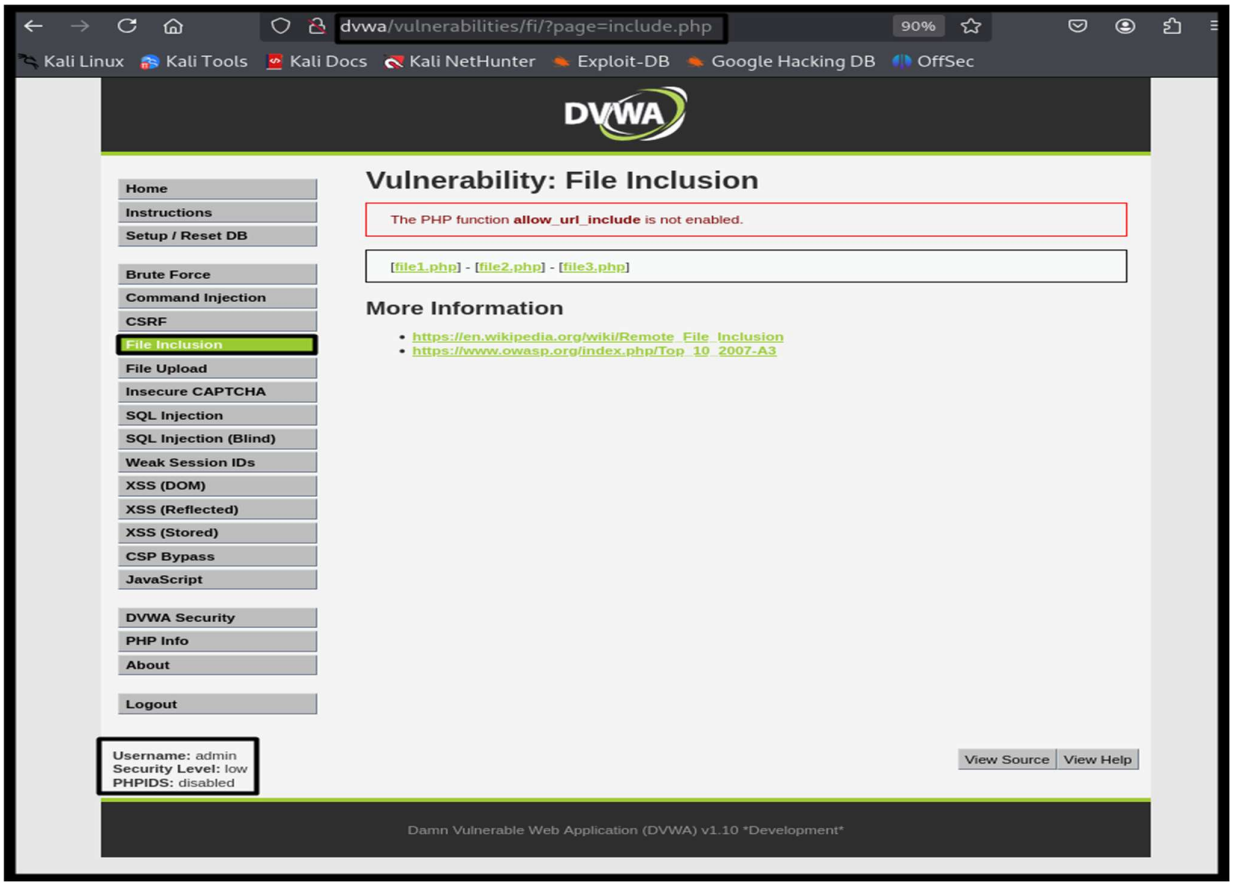
The source code seems simple as the code is using a GET page parameter.

File Inclusion Source

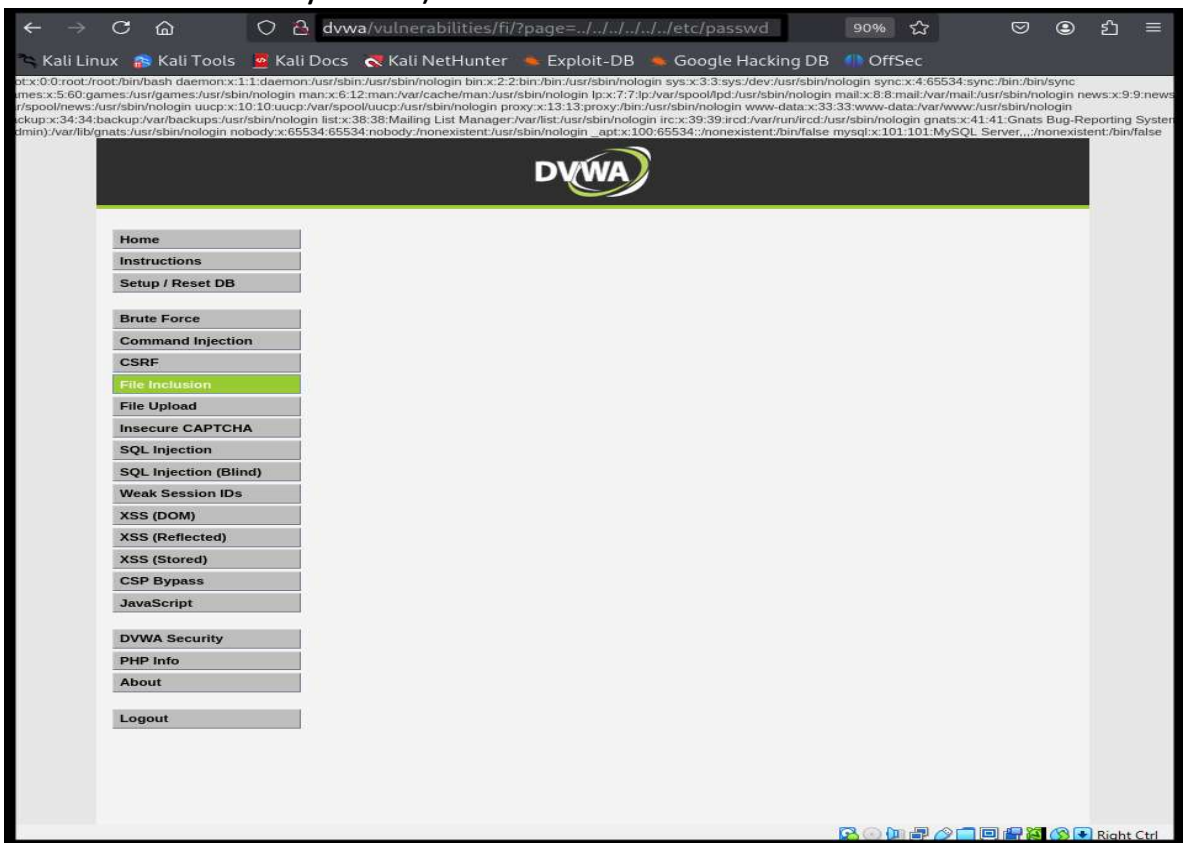
vulnerabilities/fi/source/low.php

```
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

?>
```

Step:-2 log in the home page of DVWA then click to the File Inclusion Section.



Step:-3 A list that uses several techniques to find the file /etc/password (to check if the vulnerability exists) can be found here.



SECURITY LEVEL :- (Medium)

As we Know, we will first view the source code.

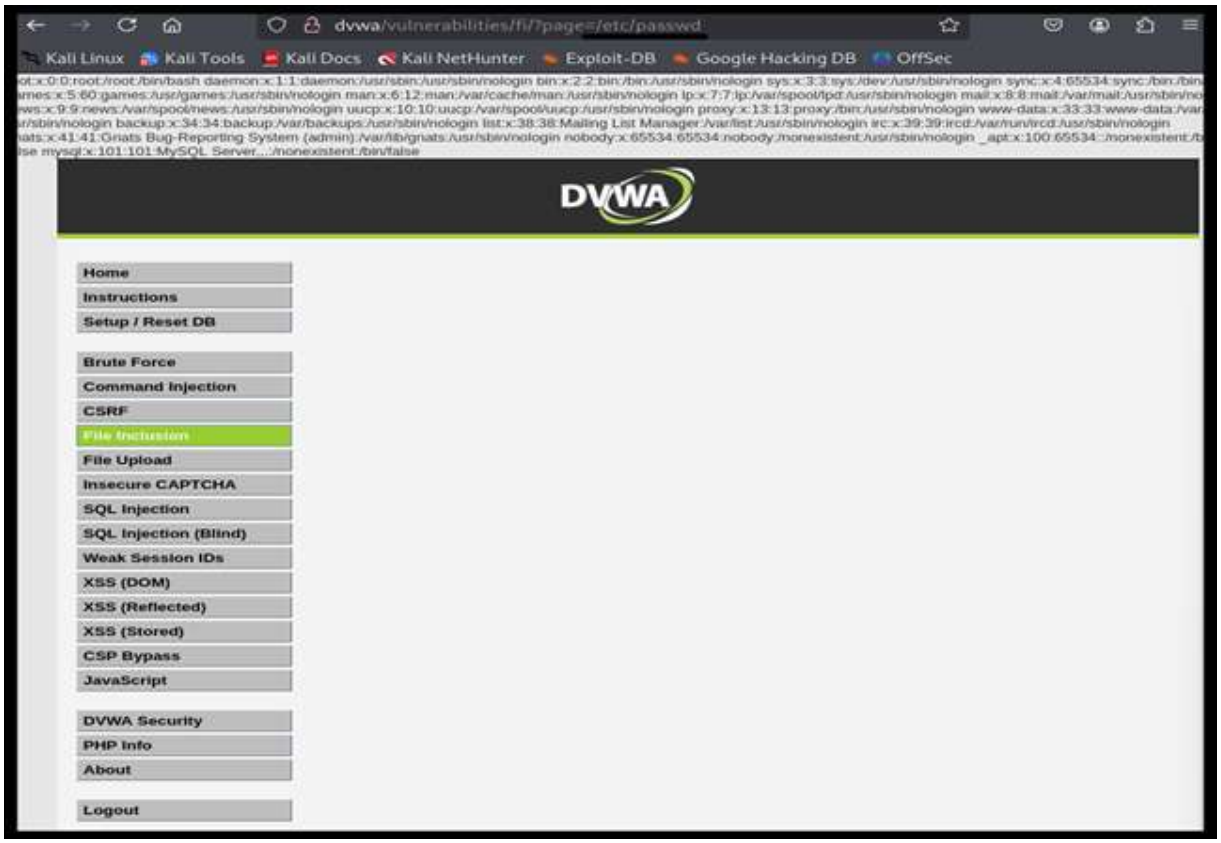
The prior attack does not work in this level. The developer appears to have used a regular expression system to validate the input given in the page argument. As shown in the source page snapshot below, the server is more secure and filters the '../' or '..'pattern.

File Inclusion Source

vulnerabilities/fi/source/medium.php

```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
$file = str_replace( array( "http://", "https://" ), "", $file );
$file = str_replace( array( "../", "..\"" ), "", $file );

?>
```

Step:-1 Let's try to access the file without '../' or '..\'.



SECURITY LEVEL:- High

As we Know, we will first view the source code.
Try all the medium level exploits with the difficulty set to HIGH, but you'll find that none of them work because the target is more secure and only accepts inputs beginning with "include.php" or "file." Any further attempts will result in "File not Found" being displayed.

File Inclusion Source

vulnerabilities/fi/source/high.php

```
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
if( !fnmatch( "file*", $file ) && $file != "include.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```

Step:-1 Change the URL from include.php to ?page=file:///etc/passwd or file/../../../../.../../../../etc/passwd