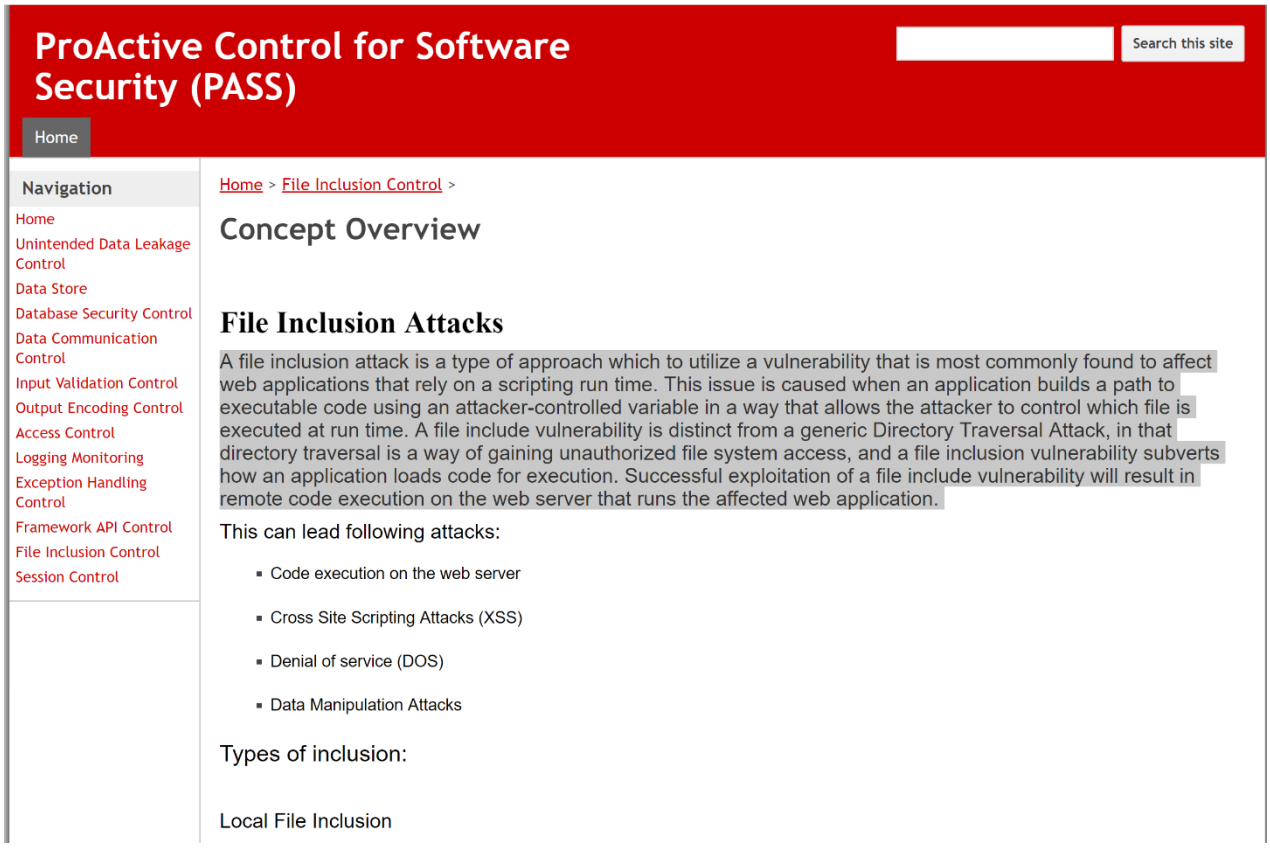
IT4863 – Asg 3: File inclusion
Total point: 100

Last Name: Simmons **First Name:** Michael **Date:** 9/12/2021

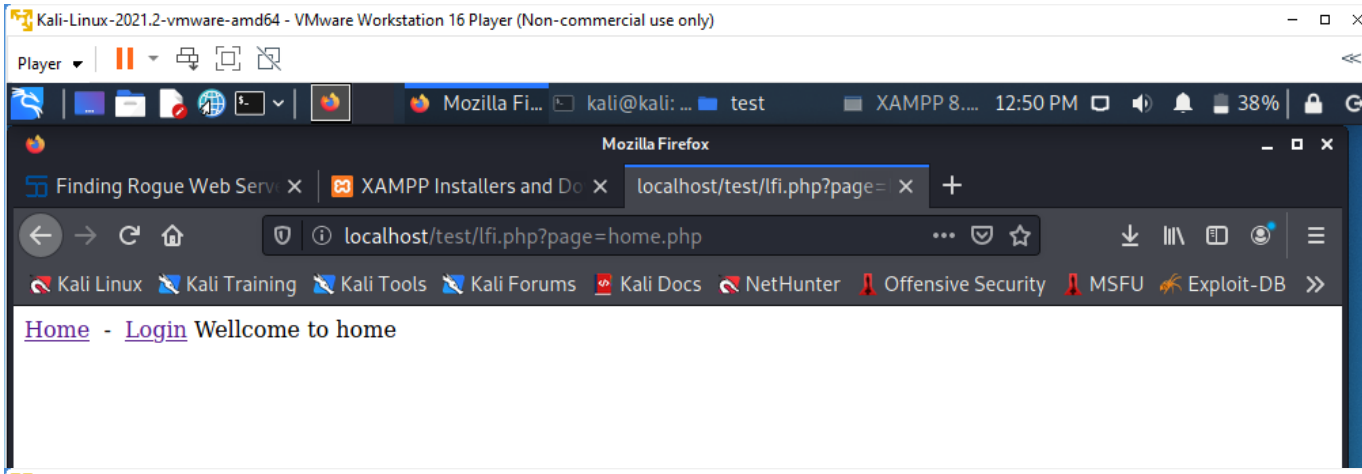
Goal:
A file inclusion attack is a type of approach which to utilize a vulnerability that is most commonly found to affect web applications that rely on a scripting run time. This issue is caused when an application builds a path to executable code using an attacker-controlled variable in a way that allows the attacker to control which file is executed at run time. A file include vulnerability is distinct from a generic Directory Traversal Attack, in that directory traversal is a way of gaining unauthorized file system access, and a file inclusion vulnerability subverts how an application loads code for execution. Successful exploitation of a file include vulnerability will result in remote code execution on the web server that runs the affected web application.

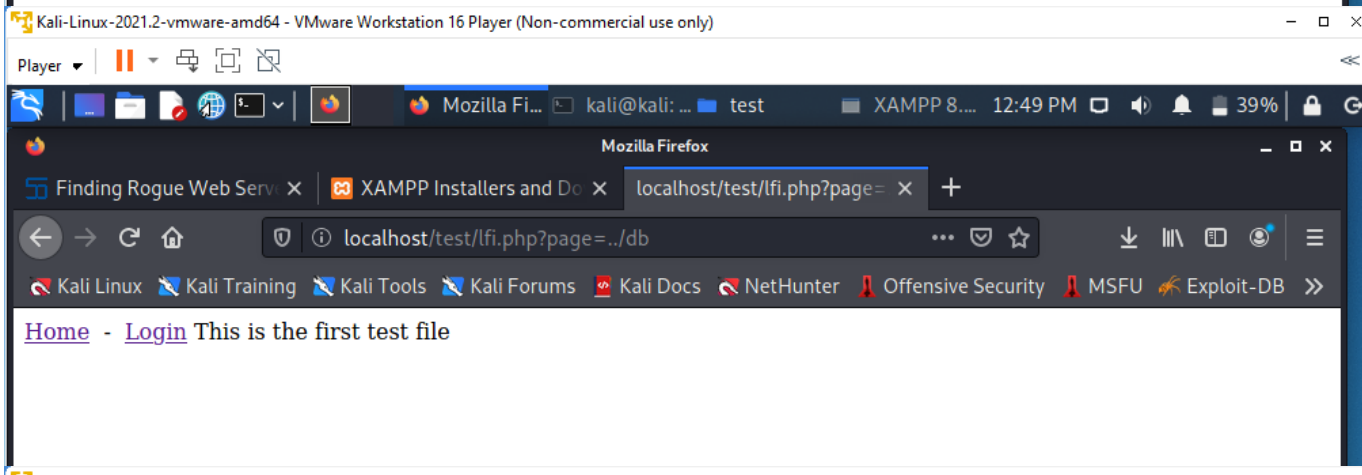
https://sites.google.com/site/proactivecontrolproject/home/file-inclusion-control/

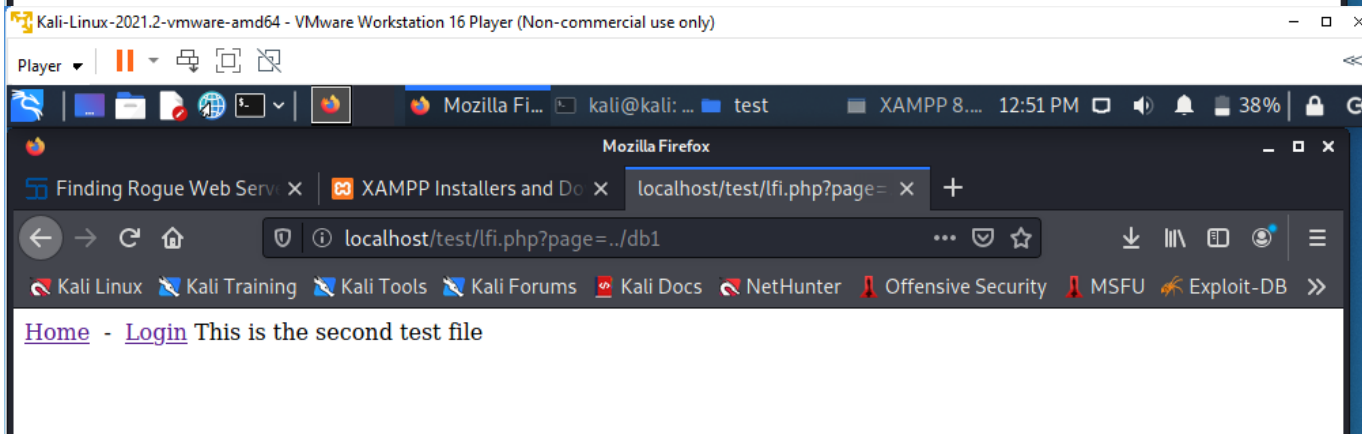
Complete the hands-on lab and provide screenshots for each of the steps.
You can run the lab by installing XAMPP and starting Apache service.

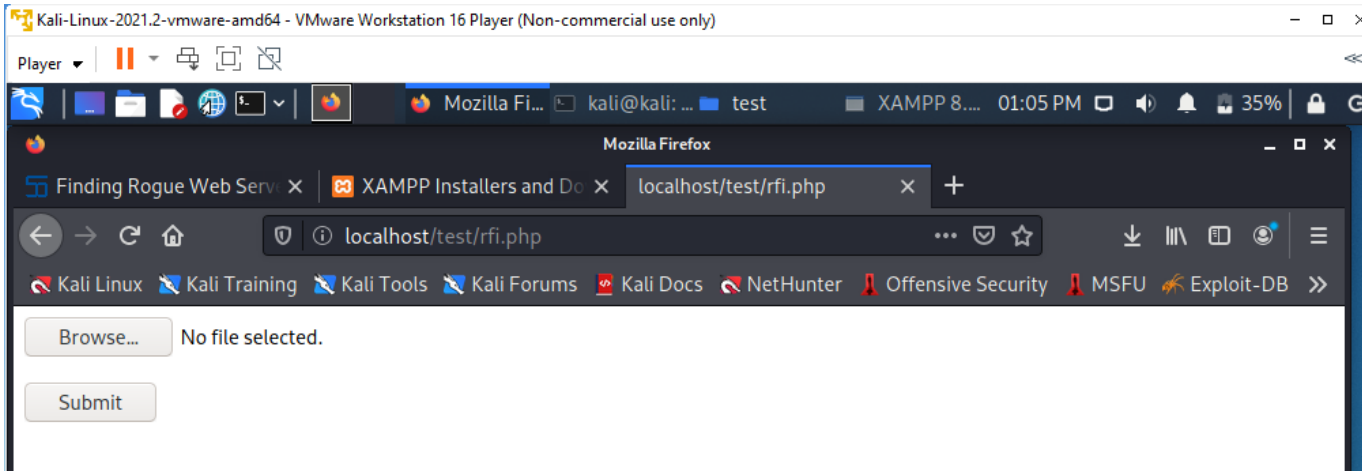


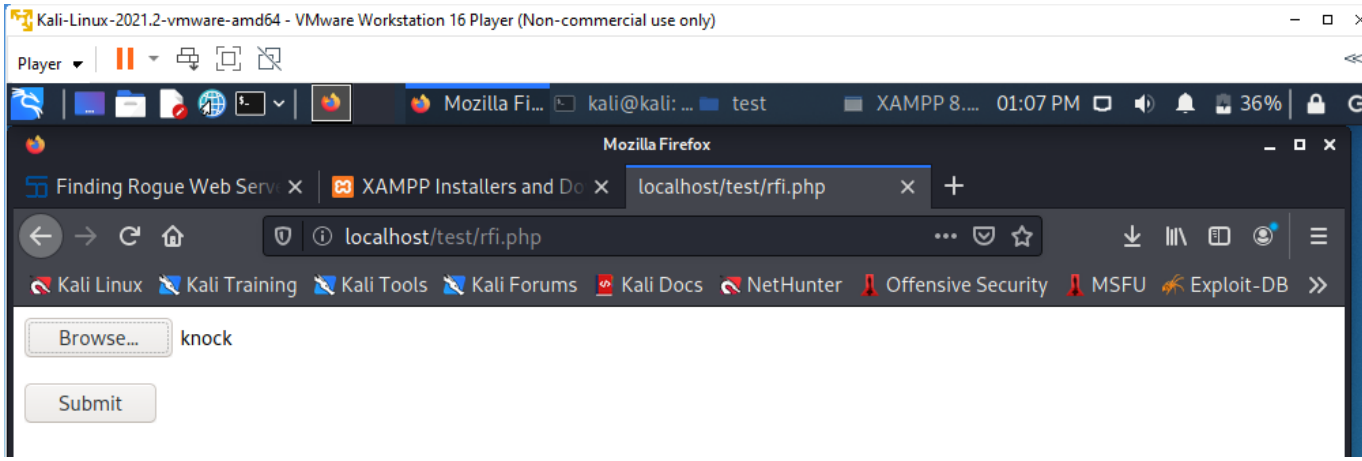
(a) Provide your screenshots for insecure vulnerable misuse case. [40 points]

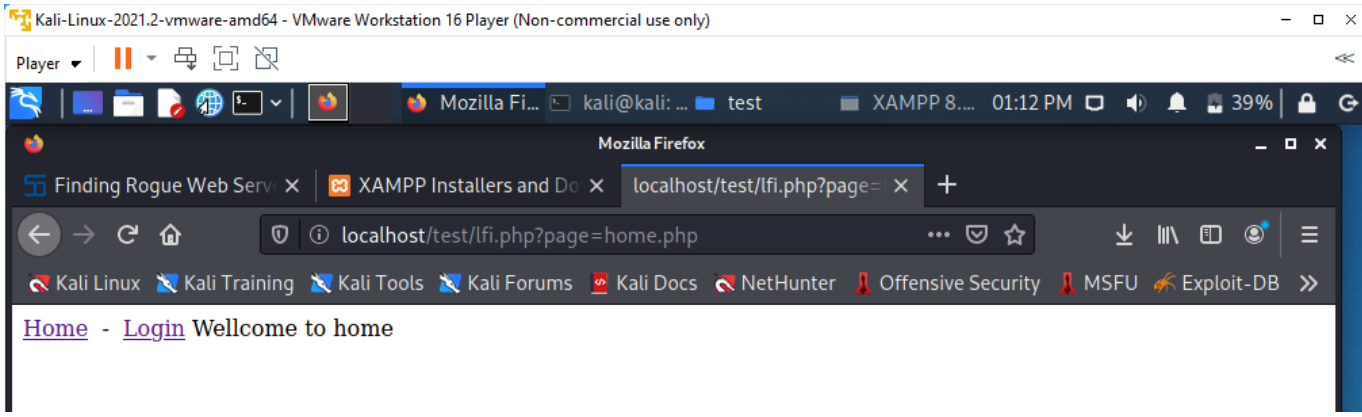

Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Fi... kali@kali: ... test XAMPP 8.... 12:50 PM 38%
Mozilla Firefox
Finding Rogue Web Serv
XAMPP Installers and Do
localhost/test/lfi.php?page=
localhost/test/lfi.php?page=home.php
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB
Home - Login Wellcome to home

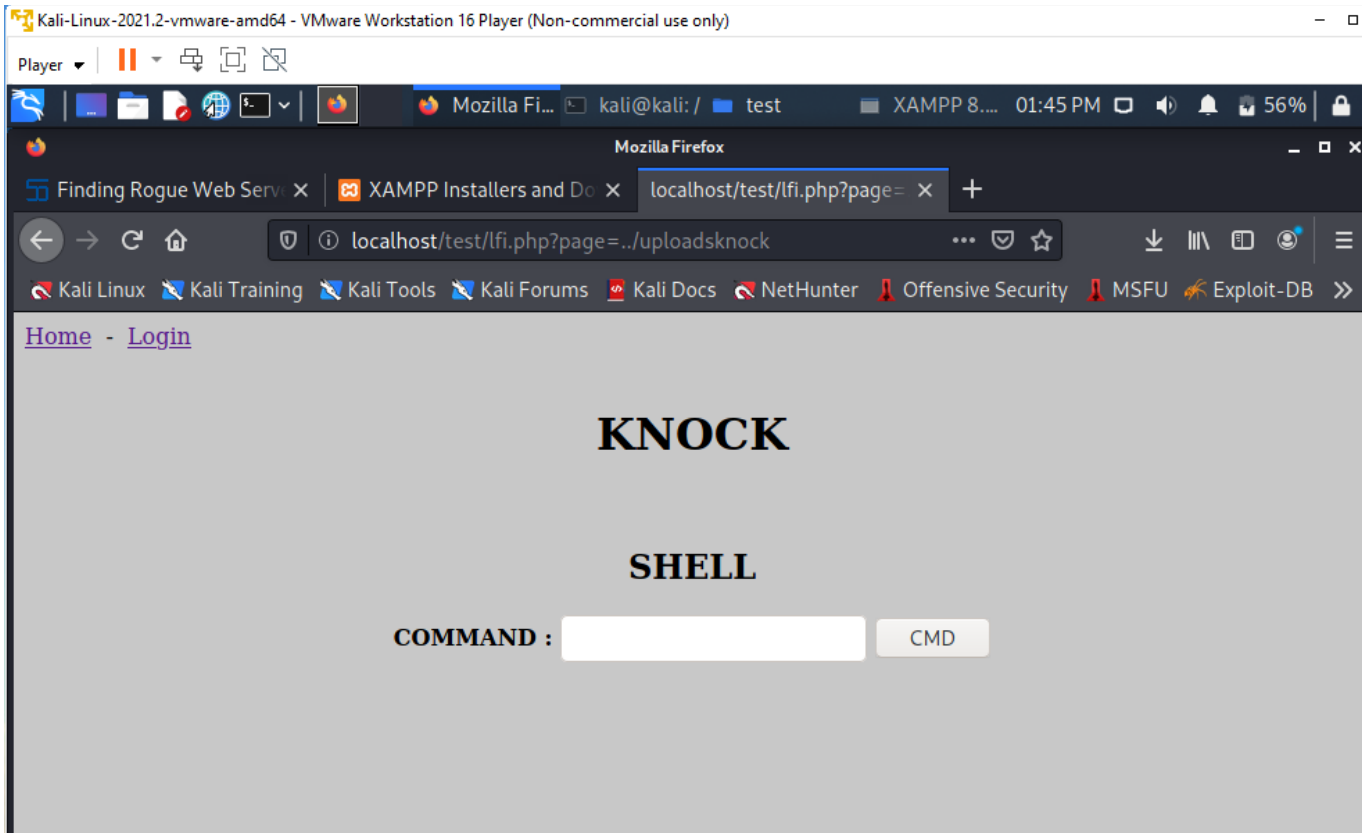

Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Fi... kali@kali: ... test XAMPP 8.... 12:49 PM 39%
Mozilla Firefox
Finding Rogue Web Serv
XAMPP Installers and Do
localhost/test/lfi.php?page=
localhost/test/lfi.php?page=../db
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB
Home - Login This is the first test file

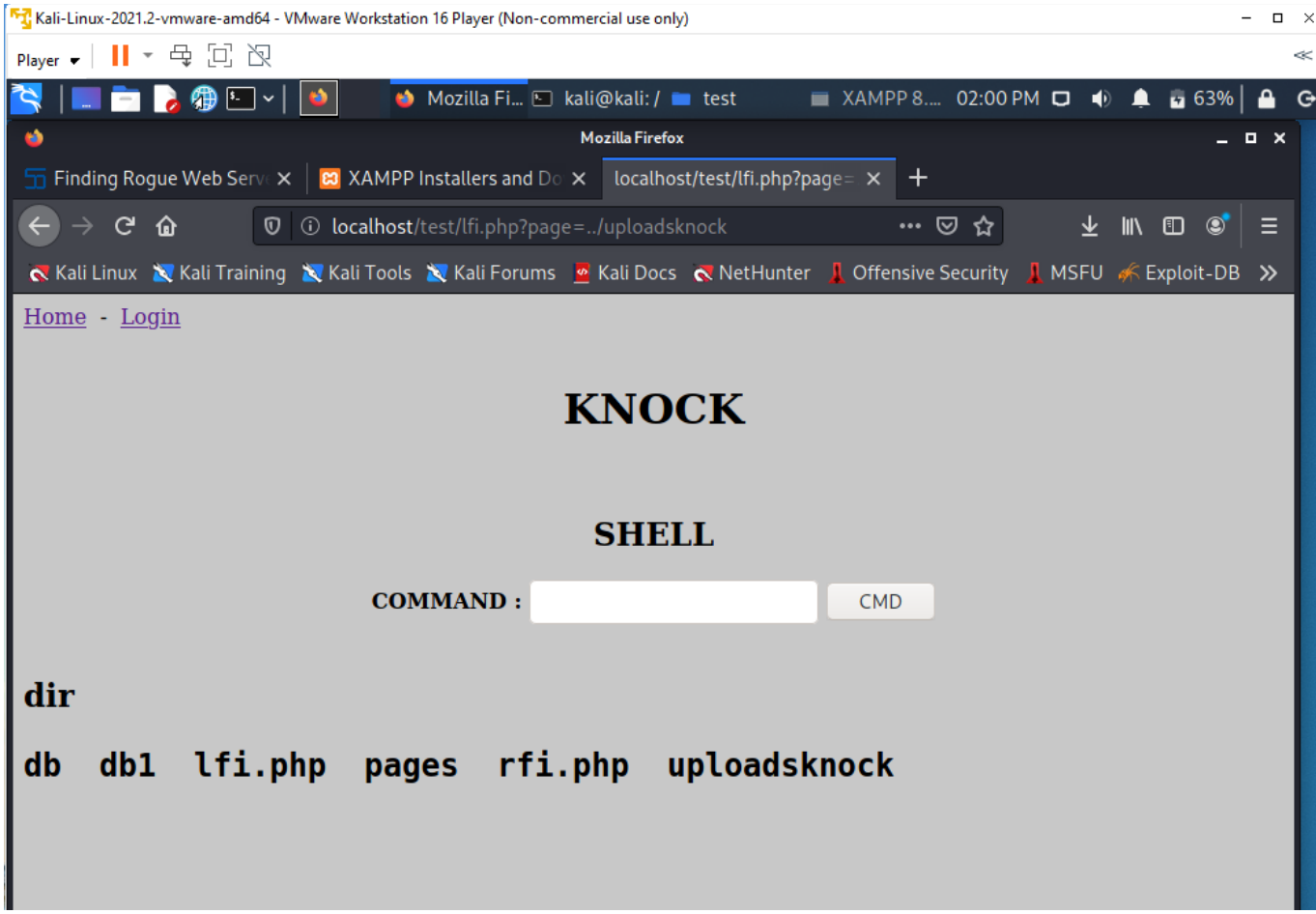

Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Fi... kali@kali: ... test XAMPP 8.... 12:51 PM 38%
Mozilla Firefox
Finding Rogue Web Serv
XAMPP Installers and Do
localhost/test/lfi.php?page=
localhost/test/lfi.php?page=../db1
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB
Home - Login This is the second test file


Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Fi...
kali@kali: ...
test
XAMPP 8....
01:05 PM
35%
Mozilla Firefox
Finding Rogue Web Serv
XAMPP Installers and Do
localhost/test/rfi.php
localhost/test/rfi.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Browse...
No file selected.
Submit


Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Fi...
kali@kali: ...
test
XAMPP 8....
01:07 PM
36%
Mozilla Firefox
Finding Rogue Web Serv
XAMPP Installers and Do
localhost/test/rfi.php
localhost/test/rfi.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Browse...
knock
Submit

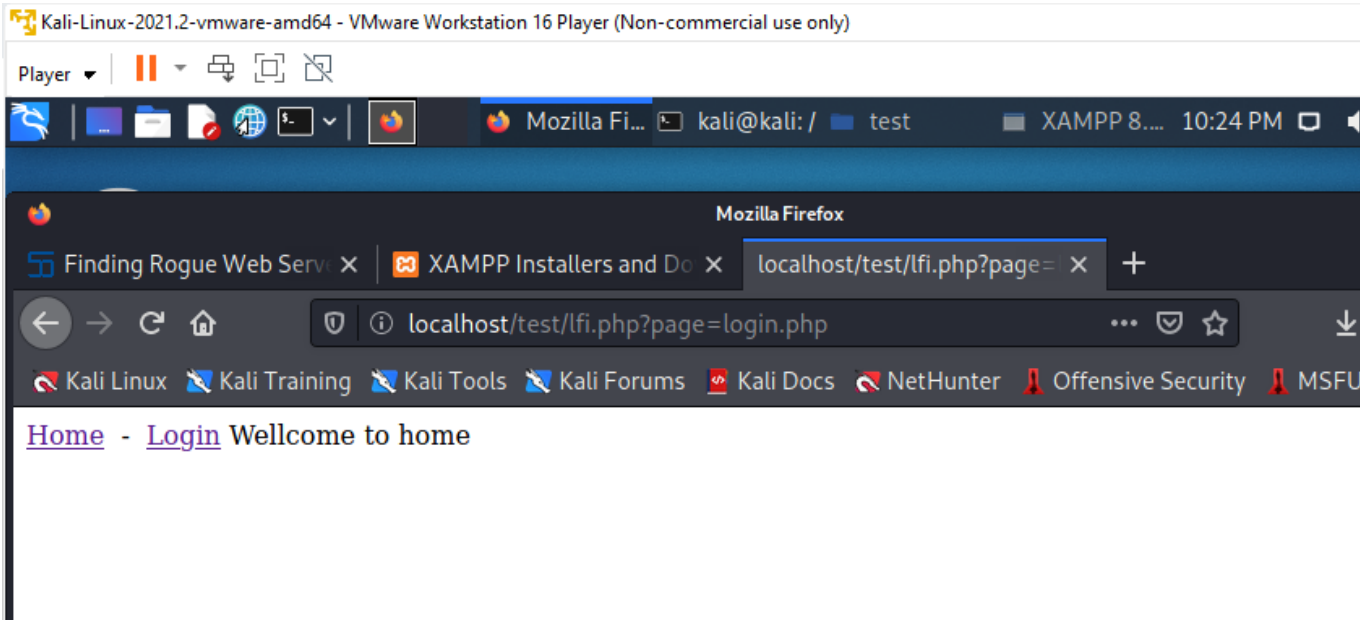

Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Fi...
kali@kali: ...
test
XAMPP 8....
01:12 PM
39%
Mozilla Firefox
Finding Rogue Web Serv
XAMPP Installers and Do
localhost/test/lfi.php?page=
localhost/test/lfi.php?page=home.php
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Home - Login Wellcome to home


Kali-Linux-2021.2-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
Mozilla Fi...
kali@kali: /
test
XAMPP 8....
01:45 PM
56%
Mozilla Firefox
Finding Rogue Web Serv
XAMPP Installers and Do
localhost/test/lfi.php?page=
localhost/test/lfi.php?page=../uploadsknock
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Home - Login
KNOCK
SHELL
COMMAND :
CMD



(b) Provide screenshots for secure use case. [40 points]

```php
<?php
$page='pages/home.php';
if (isset($_GET['page']))
{
  switch($_GET['page'])
  {
    case 'home' :
    case 'login': $page='pages/'.$_GET['page']; break;
  }
}
?>
<a href="?page=home.php">Home</a> - <a href="?
page=login.php">Login</a>
<?php
include ($page);
```



(c) What is the difference between RFI and LFI? How would you prevent them in web applications? [20 points]

LFI (Local File Inclusion) is a vulnerability of files on the current server that be used to execute attacks. LFI commonly leads to RFI (Remote File Inclusion). RFI is a vulnerability that allows an attacker to add their own code or remote file to be executed on another server, commonly a web server using PHP files.

To prevent LFI or RFI in a web application, we can reference OWASP for a full list of mitigation standards. Some of the best practices include:

Strong Input Validation
A whitelist of acceptable inputs
Run code using least privileges
Environment hardening
Configure PHP applications to not use register globals