Lab 2.2 - File Inclusion Vulnerabilities

💀A local file inclusion vulnerability allows the attacker to specify a file local to the target server for either display or rendering. For instance, a poorly constructed web application could allow the attacker to display the underlying source code of a page or an arbitrary file like /etc/passwd. If the vulnerability allows the attacker to specify a remote source for inclusion, this allows things like a remote web shell to be included.

Local File Include (LFI) setup

- Create a directory on kali like ~/sec335/file-inclusion
- Create the following index.php file

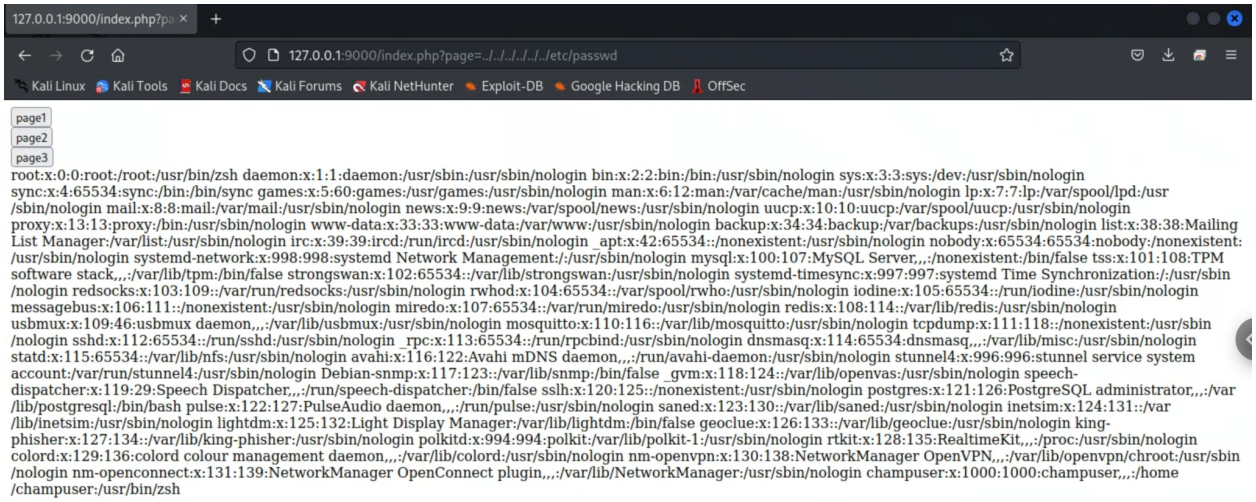
```
<a href="index.php?page=page1.html"><button>page1</button></a><br/>
<a href="index.php?page=page2.html"><button>page2</button></a><br/>
<a href="index.php?page=page3.html"><button>page3</button></a><br/>
<?php
$page = $_GET['page'];
echo "<div>";
if(isset($page))
{

  include("$page");
}
else
{
  echo "<p>select a page</p>";
}
echo "</div";
?>
```

- Create page1.html,page2.html,page3.html each with arbitrary content of your choice

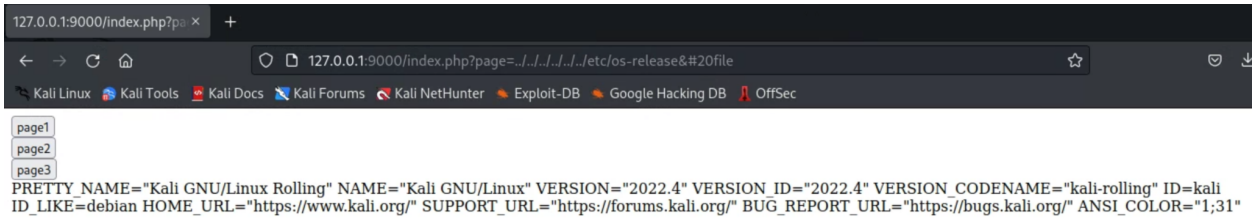
php -S

💡You are probably familiar with using python to host an adhoc-web server for file transport. If not, ask the question. The php program installed on kali has a similar feature but more importantly, it can interpret php code. It is useful for local testing, particularly if you are able to acquire a snippet of code from a target.

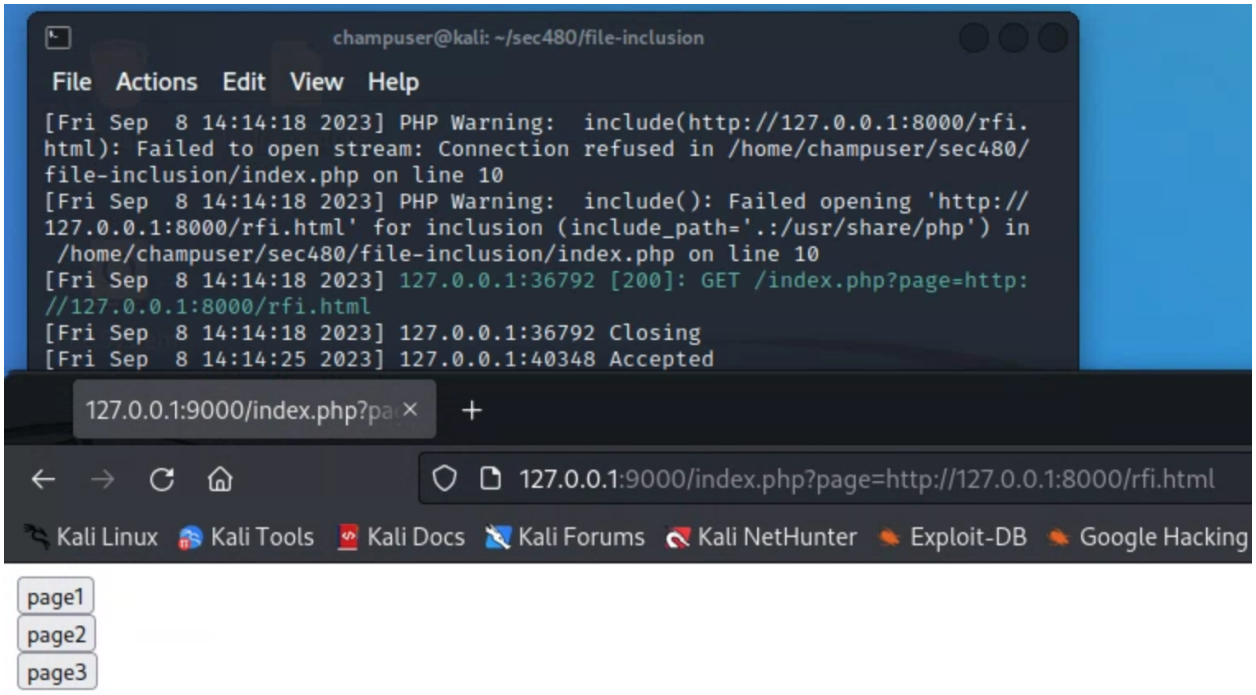
Deliverable 1. See if you can display kali's /etc/passwd. Provide a screenshot that shows the url used as well as output similar to the content below.



Deliverable 2. Figure out how to display the file that shows the current version of linux. OR display the php code associated with index.php.

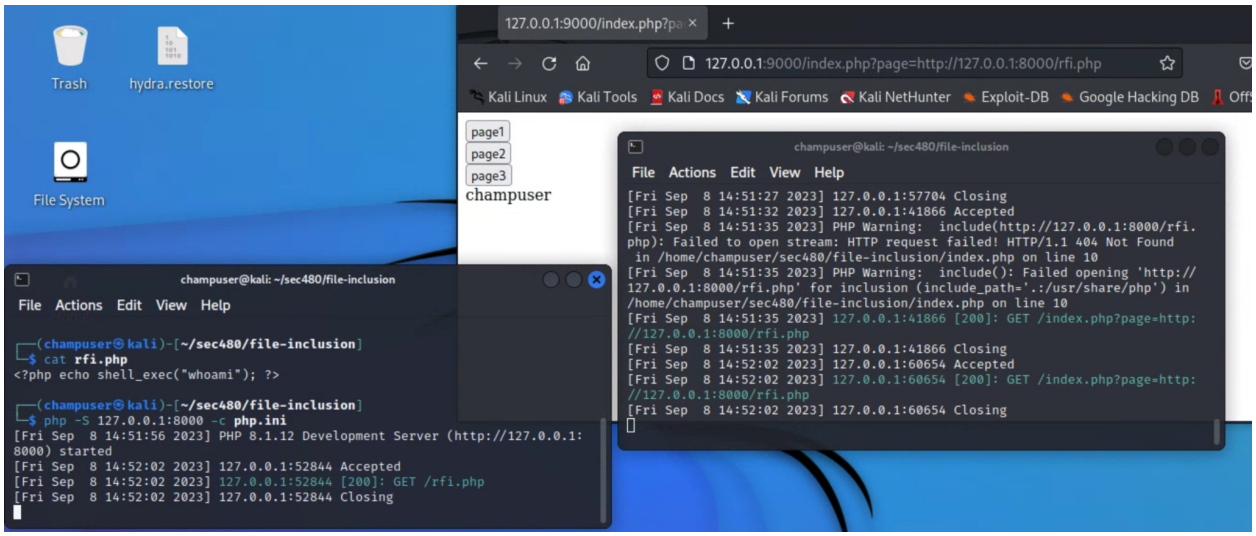


Deliverable 3. Figure out how to include rfi.html as shown below. Provide a screenshot that shows this.



No text on the file but it works based on the console response

Deliverable 4. Figure out how to include a rfi.php that executes a single command of your choice. The example executes ifconfig.



Challenge: Repeat this exercise with a partner where the remote file is stored on your partner's server.

```
Deliverable 5.  Create a technical article on php server usage as
illustrated in this lab.  We will make use of this functionality for
several targets in Middle earth.  Provide a link to this article.
```

https://github.com/dthomsen116/SEC-480/wiki/Lab-2.2-%E2%80%90-File-Inclusion-Vulnerabilities