

inget



说实话这道题最开始让我从id去get, 我首先就是想到去爆破目录

然后是之前ssti, 或者文件泄露, 但是都没有

然后想到id的传参可能直接到数据库, 有数据库注入, 但是使用 `'', sleep(5)` 的时间盲注都没有效果

偷看了一下wp, 还真是sql注入, 直接构造出

```
' or 1=1 -- '
```

得到答案

backup

首先界面是一个很简单的让我爆破目录



首先wget一下php文件看看有什么吧, 得到没啥有用信息

就直接gobuster爆破吧, 可以-x加一个php, index进行增加索引

爆破到一个bak的目录，index.php.bak 懒得解压，直接wget

```
File Actions Edit View Help
(kali@kali) ~
$ wget http://61.147.171.105:61980/index.php.bak
--2024-08-05 11:41:07-- http://61.147.171.105:61980/index.php.bak
Connecting to 61.147.171.105:61980... connected.
HTTP request sent, awaiting response... 200 OK
Length: 500 [application/x-trash]
Saving to: 'index.php.bak'

index.php.bak 100% |#####| 500
2024-08-05 11:41:08 (68.9 MB/s) - 'index.php.bak' saved [500/500]

(kali@kali) ~
$ ls
Desktop Documents Downloads index.php index.php.bak login.html Music Pictures Public pmdbg shell.php Templates tplmap venv2 Videos
(kali@kali) ~
$ cat index.php.bak
<html>
<head>
<meta charset="UTF-8">
<title>备份文件</title>
<link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
<style>
body{
margin-left:auto;
margin-right:auto;
margin-top:200PX;
width:20em;
}
</style>
</head>
<body>
<h3>你知道 index.php 的备份文件名吗？</h3>
<?php
$flag="Cyberpeace{855A1C683401294C86604CCC988DE334}";
?>
</body>
</html>
```

上一题

下一题

随机一题

backup

GFSJ0477

积分 1

金币 1

261 最佳Writeup由 沐一清 提供

收藏

反馈

难度: 1

方向: Web

题解数: 354

解出人数: 69611

题目来源: Cyberpeace-n3k0

题目描述: X老师忘记删除备份文件，他派小宁同学去把备份文件找出来,一起来帮小宁同学吧!

题目场景: http://61.147.171.105:61980

100%

倒计时: 3时51分31秒

延时

删除场景

题目已回答正确