Bugku web16 writeup(2021)

原创

Sprint#51264 于 2021-03-11 17:37:25 发布 44 收藏

分类专栏： 靶场 Web

本文链接：https://blog.csdn.net/qq_45837896/article/details/114674357

版权

靶场 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏

Web

12 篇文章 0 订阅

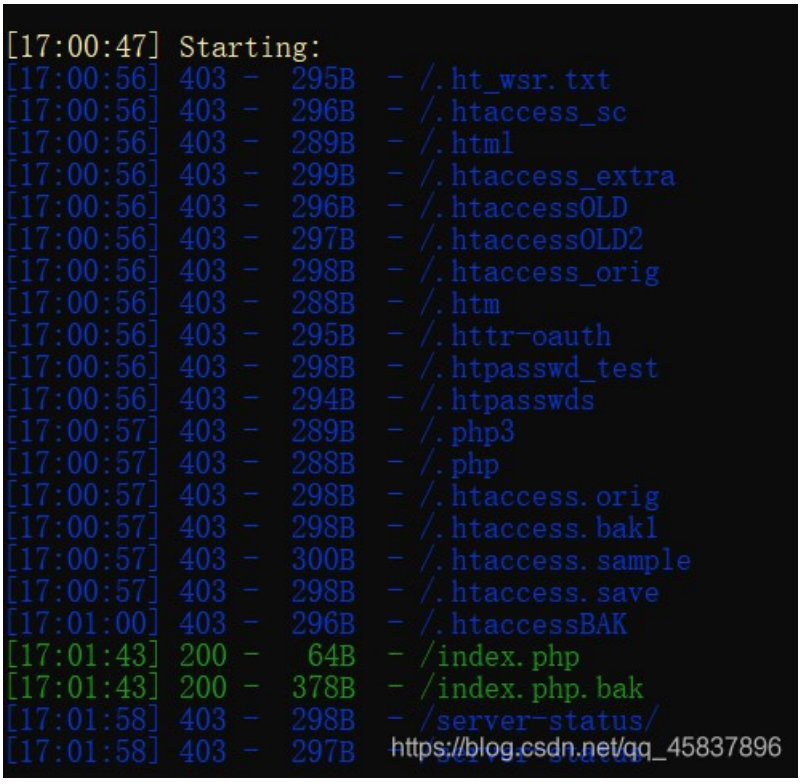
订阅专栏

题目提示说备份，我们可以知道有备份文件存在

扫描

用御剑扫描没有dirsearch快，于是乎使用了dirsearch

扫描结果



看到index.php.bak就是主页的备份文件

哦对了，提一下在主页看到一串字符串，当时猜测就是加密后的数据。

下载

url后面输入备份文件路径进行下载
可以把bak后缀删掉，也可以直接用记事本打开，随心所欲。

审计

对这个主页源码仔细观察~


```php
<?php
/**
 * Created by PhpStorm.
 * User: Norse
 * Date: 2017/8/6
 * Time: 20:22
*/

include_once "flag.php";
ini_set("display_errors", 0);
$str = strstr($_SERVER['REQUEST_URI'], '?');
$str = substr($str,1);
$str = str_replace('key','',$str);
parse_str($str);
echo md5($key1);

echo md5($key2);
if(md5($key1) == md5($key2) && $key1 !== $key2)
    echo $flag."取得flag";
}
?>
```

包含文件flag.php，猜测flag就在这个文件里

> strstr($str1$,str2)函数：检测str2是不是str1的子字符串，如果是的话就截取str2直到str1结尾的字符串

这里也就是截取url中?之后的所有数据

> substr()截取字符串的某一个部分

这里是截取str中?之后的字符串

> str_replace()字符替换函数

此处是检测字符串中的key关键字，并替换为空，可以考虑双写绕过

> parse_str()函数，把查询字符串解析到变量中

此处，如果字符串中有赋值语句就会执行，例如key=xxxxx

> 然后用md5对key进行加密

最后有个判断，要求key1的md5值和key2的md5值相等并且它们两个原先不相等
此处可以考虑弱比较类型(松散比较)。
通过查阅php手册知道如果是数组的话数组之间使用松散比较是可以成功的
于是乎~

步骤

传值?kekeyy1[]=alksdjld&kekeyy2[]=asfasf32131
传什么值就随意发挥吧
就能看到flag了√

菜是原罪