[ACTF2020 新生赛]BackupFile

原创

Wuuconix 于 2021-03-11 11:01:40 发布 49 收藏

文章标签： web 安全漏洞 php

Wuuconix wanna a girlfriend!

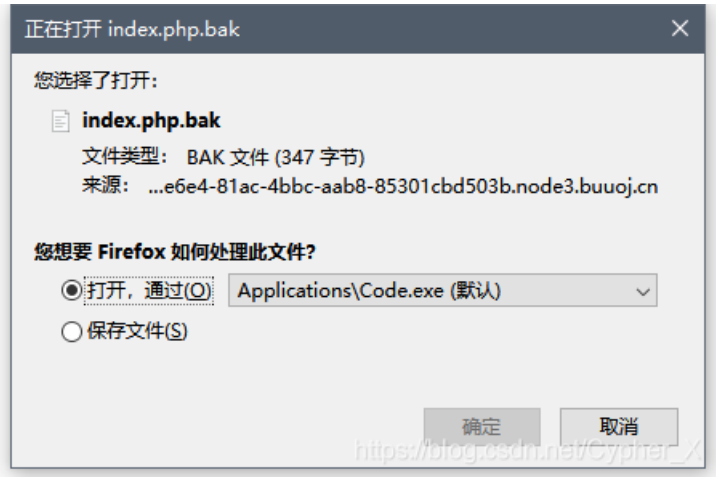
[ACTF2020 新生赛]BackupFile

考点： `php备份文件名` `php弱类型绕过`

主界面提示我们找找到`source file`，再结合题目，肯定是备份文件

常见php文件备份后缀名：`.git .svn .swp .~ .bak .bash_history`

果然，成功下载到`index.php.bak`



进行代码审计

```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!";
}
```

我们需要用`get`方式传一个key的值，这个key必须得是数字，不然就会exit，它需要和`$str`弱相等。

查阅资料后，我们知道

> 弱比较：如果比较一个数字和字符串或者比较涉及到数字内容的字符串，则字符串会被转换成数值并且比较按照数值来进行，在比较时该字符串的开始部分决定了它的值，如果该字符串以合法的数值开始，则使用该数值，否则其值为0。所以直接传入key=123就行

```
payload: index.php?key=123
```

flag{db85500a-f6ac-4368-9509-53b03f01c1d0}

成功获得flag。

参考链接

- [ACTF2020 新生赛]BackupFile
- [ACTF2020 新生赛]BackupFile