buuctf初学者学习记录--[ACTF2020 新生赛]BackupFile

原创

pakho_C 已于 2022-02-03 23:45:23 修改 297 收藏

文章标签： php web安全 安全

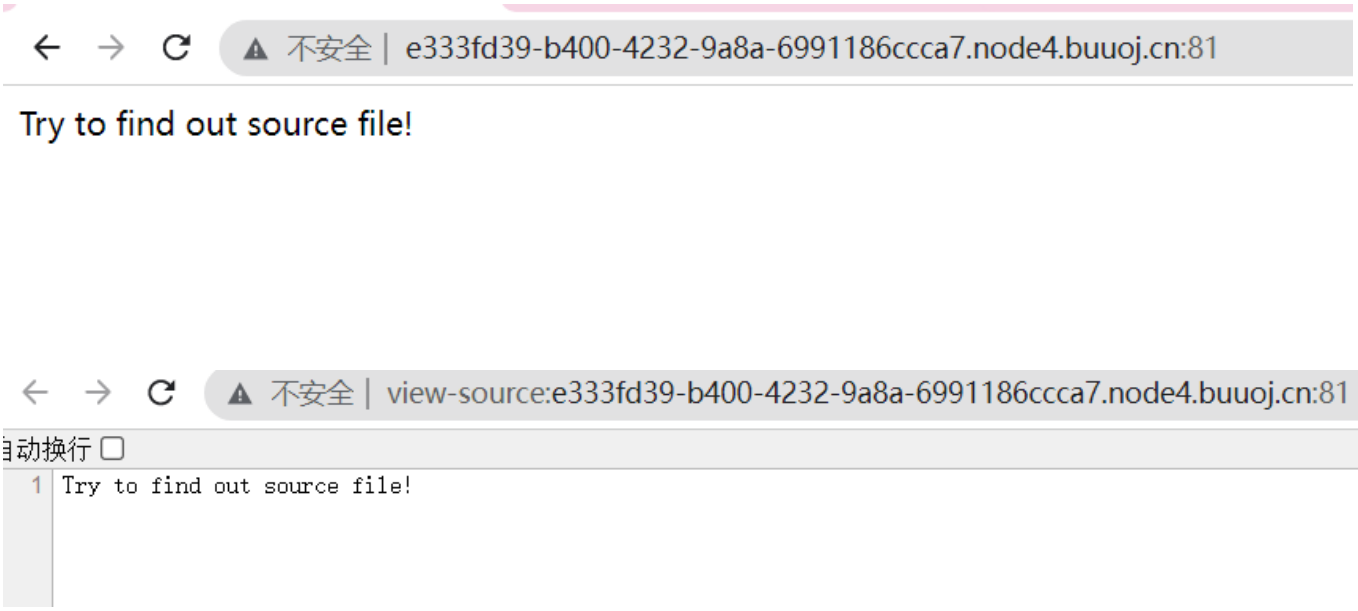
于 2022-02-03 23:45:00 首次发布

本文链接：https://blog.csdn.net/pakho_C/article/details/122779667

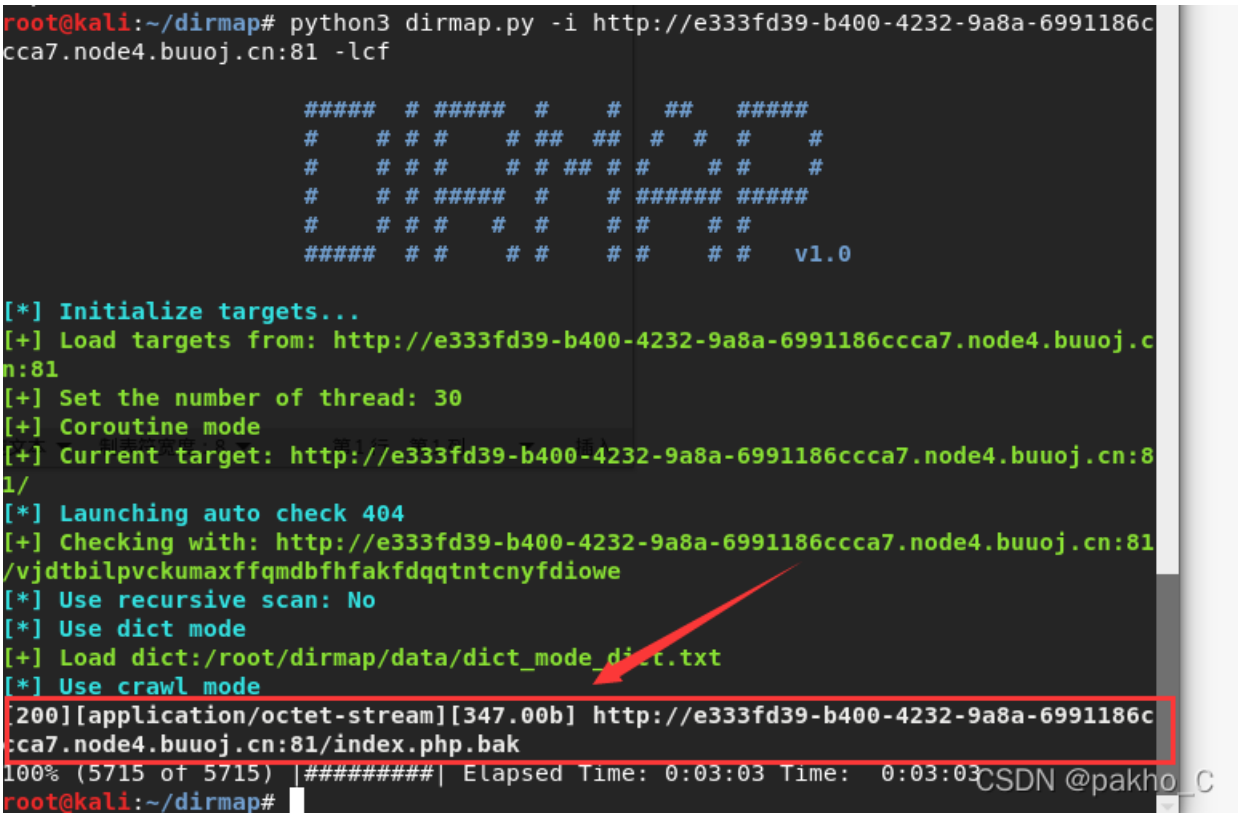
web第17题

[ACTF2020 新生赛]BackupFile

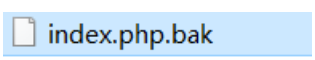
打开靶场



无任何提示，但是题目名为备份文件
常见备份文件名： .git ； .svn ； .swp ； .~ ； .bak ； .bash_history
对其使用dirsearch（报错429），然后使用dirmap工具进行目录扫描



扫出来一个index.php.bak文件，响应为200，就是备份文件，访问将其下载下来



文件内容是一个php代码

```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!";
}
```

这是一个弱类型比较的漏洞

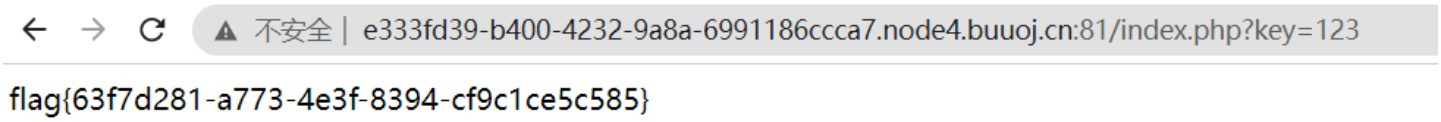
php 弱类型总结

这里涉及的原理就是==在进行比较时，会先将类型转换为相同再进行比较

这里是比较一个数字和字符串，则字符串会被转换为数字来进行比较，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。这里的str是123开头，那么它会被转换为123，那么就可以使key=123就可以输出flag

payload：

```
?key=123
```



flag{63f7d281-a773-4e3f-8394-cf9c1ce5c585}