[ACTF2020 新生赛]BackupFile 1

原创

succ3 于 2022-01-28 19:56:27 发布 321 收藏

分类专栏： BUUCTF 文章标签： web安全

本文链接：https://blog.csdn.net/shinygod/article/details/122735498


```
考点：
1、php弱类型
```

Try to find out source file!

题目提示我们查找目录，我们就扫一下呗

200 347B http://35ee6c54-04f6-4f9a-99ca-6cfb56cfda98.node4.buuoj.cn:81/index.php.bak

找到一个index.php.bak,下载一下

```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!";
}
```

只要我们使$key == $str就可以拿到flag，并且双等于为弱比较

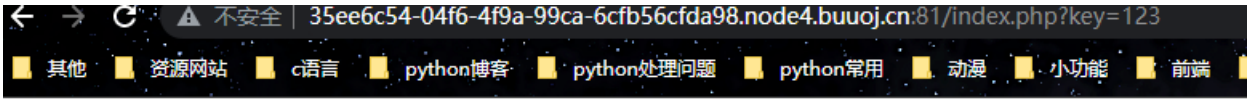
```
== 在进行比较的时候，会先将字符串类型转化成相同，再比较

//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
```

PHP弱类型详细介绍.

```php
<?php
var_dump("admin"==0);  //true
//将admin转化成数值，强制转化,由于admin是字符串，转化的结果是0
var_dump("1admin"==1); //true
//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
var_dump("admin1"==1) //false
//不是以数字开头所以为admin1为0
var_dump("admin1"==0) //true
var_dump("0e123456"=="0e4456789"); //true
//"0e123456"=="0e456789"相互比较的时候，会将0e这类字符串识别为科学技术法的数字，0的无论多少次方都是零，所以相等
?>
```

而$str化为数值为123，所以只要使key=123即可。



flag{488b418a-cc9a-4a0d-b151-7447243dfea8}

用dirsearch遇到的问题

Error:No matching distribution found for cryptography

```
pip3 install cryptography -i http://pypi.douban.com/simple/ --trusted-host pypi.douban.com
```

```
命令：
python dirsearch.py -u "网址" -e *
```