[ACTF2020 新生赛]BackupFile1

原创

cyphersec 于 2022-04-25 21:01:27 发布 662 收藏

分类专栏： buuctf 文章标签： web 网络安全

本文链接：https://blog.csdn.net/cuddlylm/article/details/124414365

Try to find out source file!

打开只有这句话，用dirsearch扫一下，发现了flag.php(空的)和index.php.bak

```
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/includes/fckedit
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/includes/fckedit
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/includes/fckedit
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/includes/fckedit
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/includes/fckedit
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/includes/fckedit
200    347B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/index.php.bak
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/index.temp
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/index.tmp
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/index.xml
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/index.vb
429    568B    http://41bde603-b1c7-40a6-b534-a6fb4ebbac3d.node4.buuoj.cn:81/index.zip
```

拿到备份文件打开

```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!";
}
```


get传参key
但是key的要求是只能数字，仔细看下面进行了php的弱类型比较，这样一比变量str就会变成123
所以只要传值
?key=123
就可以了
拓：

> 参考：php 弱类型总结：https://www.cnblogs.com/Mrsm1th/p/6745532.html

== 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
<?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
?>
```