BUUCTF [ACTF2020 新生赛]BackupFile

原创

维多利亚蜜汁鱼 于 2021-07-12 16:33:31 发布 106 收藏

分类专栏： Web CTF

本文链接：https://blog.csdn.net/CrotZZ/article/details/118678213


Web 同时被 2 个专栏收录

16 篇文章 0 订阅

订阅专栏


CTF

18 篇文章 0 订阅

订阅专栏

从题目看出是到备份文件题，第一次入手

备份文件可以进行后台扫描，起初使用御剑扫描，试了几次没成功返回想要的文件，看了其他人用的都是dirsearch，于是就去下了个进行扫描，后面参数一定要严格规定，不然扫出来东西会非常多。一般备份文件后缀有.rar.zip.7z.tar.gz.bak.swp.txt.html

```
D:\CTF\后台扫描\dirsearch-master>python dirsearch.py -u "ceb7b88f-521e-4dc4-902d-ccdec531345c.node4.buuoj.cn/" -t 5 -i 200 -e *

 v0.4.2

Extensions: php, jsp, asp, aspx, do, action, cgi, pl, html, htm, js, json, tar.gz, bak | HTTP method: GET | Threads: 5
Wordlist size: 15474

Output File: D:\CTF\后台扫描\dirsearch-master\reports\ceb7b88f-521e-4dc4-902d-ccdec531345c.node4.buuoj.cn-_21-07-12_16-04-12.txt

Error Log: D:\CTF\后台扫描\dirsearch-master\logs\errors-21-07-12_16-04-12.log

Target: http://ceb7b88f-521e-4dc4-902d-ccdec531345c.node4.buuoj.cn/

[16:04:13] Starting:
[16:06:24] 200 -    0B  - /flag.php
[16:06:29] 200 -  347B  - /index.php.bak

Task Completed

D:\CTF\后台扫描\dirsearch-master>                                    https://blog.csdn.net/CrotZZ
```

Index.php.bak就是想要的目标文件，加到url后面后下载这个文件

index.php(1).bak - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```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!";
}
```


可以看到输出flag的条件是

> key==str

，而这里是“==”，用到了php弱类型比较
加上?key=123，str的字符串转换为数字就是123，使得key和str相等

flag{44364d2f-747e-443a-94f3-1552dbabf068}

php中==是弱等于，不会比较变量类型；===是强等于，会先比较变量类型。
“0e"开头跟数字的字符串（例如"0e123”）会当作科学计数法去比较，所以和0相等；
“0x"开头跟数字的字符串（例如"0x1e240”）会被当作16进制数去比较；
布尔值true和任意字符串都弱相等。
当比较的一方是字符串时，会先把其转换为数字，不能转换为数字的字符串（例如"aaa"是不能转换为数字的字符串，
而"123"或"123aa"或"0x10"或"2e2"就是可以转换为数字的字符串）或null，被转换为0
在PHP中遇到数字与字符串进行松散比较时，会将字符串中前几位是数字且数字后面不是”.“，“e"或"E"的子串转化为数字，与数字进行比较，如果相同则返回为true，不同返回为false，后面的所有字符串直接截断扔掉。