BUU[ACTF2020 新生赛]BackupFile

原创

SSDZLDL 于 2021-11-30 21:23:27 发布 234 收藏
文章标签： windows php

本文链接：https://blog.csdn.net/SSDZLDL/article/details/121642117

backup文件也叫系统备份文件，它的做作用是：拷贝到存储介质上的文件，可以帮助保护数据，以防其在系统硬件或存储介质出现故障时受到破坏。

那么搜索一下备份文件后缀名，如果网站存在备份文件，常见的备份文件后缀名有：“.git” 、“.svn”、“.swp”“.~”、“.bak”、“.bash_history”、“.bkf” 尝试在URL后面，依次输入常见的文件备份扩展名。这里也可以用御剑或者其他扫描文件得到后缀为.bak

加上index.php.bak后发现index的php代码：

```
<!--?php
include_once "flag.php";

if(isset($_GET['key'])) {//以GET形式获得KEY变量
    $key = $_GET['key'];
    if(!is_numeric($key)) {//判断key是否为数值或者数字字符串，无论十进制亦或十六进制也行
        exit("Just num!");
    }
    $key = intval($key);//intval – 获取变量的整数值
    $str = "123ffwsfwefwf24r2f32ir23jrw923rskfjwtsw54w3";
    if($key == $str) {//双等号是弱比较类型
        echo $flag;
    }
}
else {
    echo "Try to find out source file!";
}
```

php 弱类型总结 - Mrsm1th - 博客园

0x02 知识介绍

php中有两种比较的符号 == 与 ===

```php
<?php
$a = $b ;
$a===$b ;
?>
```

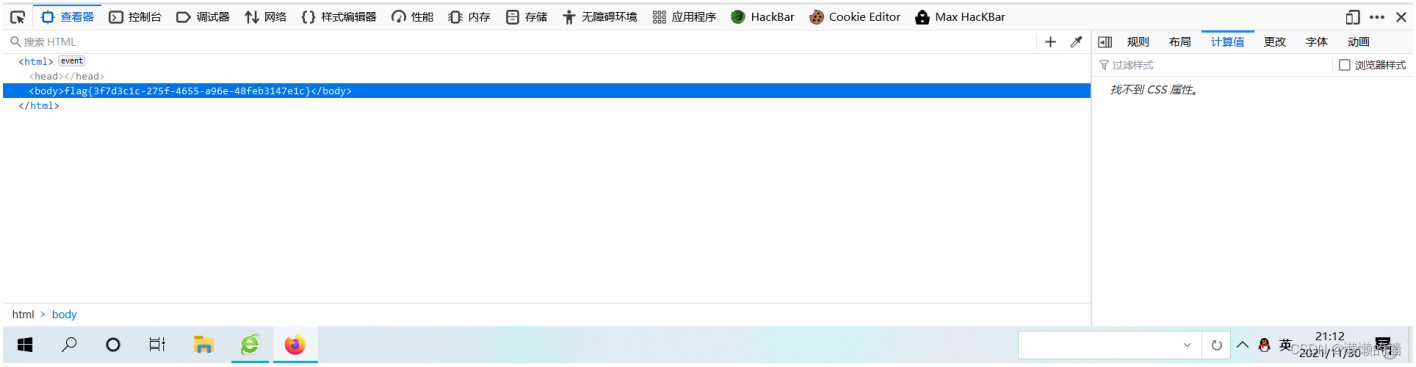
=== 在进行比较的时候，会先判断两种字符串的类型是否相等，再比较

== 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

这里明确了说如果一个数值和字符串进行比较的时候，会将字符串转换成数值

则str这里在进行弱比较时转化为了123，所以key=123即可得到flag




```
flag{3f7d3c1c-275f-4655-a96e-48feb3147e1c}
```