2020强网杯线上赛web Funhash writeup

原创

OceanSec 于 2020-10-15 08:58:48 发布

分类专栏： # CTF

本文链接：https://blog.csdn.net/q20010619/article/details/109090076

CTF 专栏收录该内容

66 篇文章 29 订阅

订阅专栏

```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();
?>
```

代码审计，考点是md4和md5的比较缺陷

1.md4的比较缺陷：

```
$_GET["hash1"] != hash("md4", $_GET["hash1"]
```

需要一个参数hash1的值和他的md4加密后的值相等的字符串

例如：0e001233333333333334557778889的md4值=0e434041524824285414215559233446

2.md5的比较缺陷：

当两个数组进行md5运算时结果都为null，所以相等，就可以绕过

例如：hash[]=1&hash[]=2

3.特殊的md5值：

md5加密，而ffifdyop md5($password,true)过后恰好结果是’or’6]!!r,!!b

```
$sql="select password from users where password=''or'<xxx>'"
```

最终payload
?hash1=0e001233333333333334557778889&hash2[]=1&hash3[]=2&hash4=ffifdyop

成功绕过。