HashTeam web_MD55555 writeup

原创

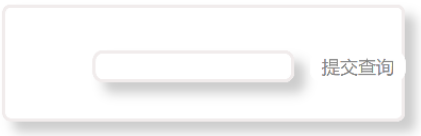
Mitch311 于 2020-12-29 22:33:13 发布 158 收藏
分类专栏： CTF 文章标签： unctf

HashTeam web_MD55555

原题链接

key:md5&sql注入+md5函数绕过

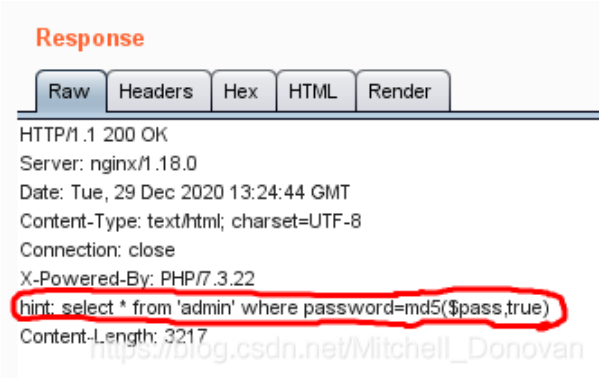
①原题页面长这样式的□



提交查询无回显，查看源码无提示，尝试抓包

（其实当时给了hint:抓包有惊喜）

②尝试抓包，可以看到回送报文中有hint字段



应该是后台对我们提交的处理sql语句：

```
select * from 'admin' where password=md5($pass,true)
```

语句的意思是从表admin中取出所有密码等于我们提交的$pass经过md5函数处理后取值的项

> 知识补充：md5函数的用法
>
> **语法**
>
> ```
> md5(string,raw)
> ```
>
> | 参数 | 描述 |
> | --- | --- |
> | *string* | 必需。规定要计算的字符串。 |
> | *raw* | 可选。规定十六进制或二进制输出格式：
• TRUE - 原始 16 字符二进制格式
• FALSE - 默认。32 字符十六进制数 |
>
> **技术细节**
>
> | | |
> | --- | --- |
> | 返回值： | 如果成功则返回已计算的 MD5 散列，如果失败则返回 FALSE。 |
> | PHP 版本： | 4+ |
> | 更新日志： | 在 PHP 5.0 中，*raw* 参数变为可选的。 |
>
>
>
> （1）如果添加的**raw**字段为**true**，就会返回字符串的原始二进制格式**md5**值
>
> （2）如果不添加**raw**字段或者**raw**字段为**FALSE**的话，就会返回对应字符串的**32** 字符十六进制格式**md5**值

> **md5&sql**注入的问题，一般我们会利用的字符串是**ffifdyop**
>
> 该字符串经过**md5**加密后若**raw**字段是**true**则会返回**'or'6xxxxxx**（**x**表示没什么用的部分）

这样如果和整个sql语句合并的话就是如下sql语句：

```
select * from 'admin' where password=''or'6xxxxxxx'
```

如此一来，返回值的引号和前面的引号形成了闭合

> 在**mysql**中，在用布尔型判断时以数字开头的字符串会被当做整型数

所以就相当于 '' or 1,这样的布尔值肯定就是true，就会返回整个admin表的内容，这样就达到了注入

提交查询**ffifdyop**，进入下一关

③第二关的界面长这样式的□

Do You Like MD5?

在源代码中发现php代码

```
$a = $_GET['a'];
$b = $_GET['b'];
if($a != $b && md5($a) == md5($b)){
    //almost there!!!
```

md5函数绕过问题，**==弱比较，思路有两个**

一是传md5值是0e开头的字符串，比如QNKCDZO和s214587387a（网上能搜到好多payload）

> 知识补充：
>
> **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**
>
> **所以如果两个不同的密码经过md5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**
>
> **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**

二是利用函数松散性，因为

> **向md5函数传递数组会返回NULL**

显然NULL是等于NULL的，所以传两个数组也可以进行绕过

补充一句，如果是===强比较的话就必须用数组绕过了

get传参**?a=QNKCDZO&b=s214587387a**或者**?a[]=1&&b[]=2**，进入下一关

④最后一关界面是一段PHP代码，内容如下□

```php
 <?php
error_reporting(0);
highlight_file(__FILE__);

if((string)$_GET['hash']!==(string)$_GET['ctf']&&md5($_GET['hash'])===md5($_GET['ctf'])){
    eval(system("cat flag.php"));
}
```

可以看到这里我们还是get方式提交两个字段，先将两个字段的值强行转为字符串，再要求两个字段的值严格不相等并且两个字段的md5值相等

此时如果上传数组就会被强行转为字符串ARRAY，所以数组显然不行

建议跟着下面这篇大佬博客里最后一条学习一下

> 知识补充：md5碰撞大全

问题过于复杂，就不赘述了

get传参?
hash=M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C
%18%AF%BF%A2%00%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1U%5D%83%60%FB_%07
M%C9h%FF%0E%E3%5C%20%95r%D4w%7Br%15%87%D3o%A7%B2%1B%DCV%B7J%3D%C0x%3E
F%BF%A2%02%A8%28K%F3n%8EKU%B3_Bu%93%D8Igm%A0%D1%D5%5D%83%60%FB_%07%FE

⑤传完这一大串参数后在新页面的源代码里找到flag