php MD5值比较绕过

原创

执笔苦行僧 于 2021-05-31 23:48:09 发布

分类专栏： 网络安全攻防

本文链接：https://blog.csdn.net/qq_43580193/article/details/117432689

php MD5值比较绕过

关于 md5() 函数

> 在 php 程序中，md5($string,bool): 得到一个字符串散列值。其中第二个参数默认为false,表示该函数返回值是32个字符的十六进制数。若指定为true,则表示函数返回的是16字节的二进制格式（这样通过浏览器解析会出现乱码）。

== 绕过

示例：

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

绕过原理：

> 在 php 中，当字符串 以0e开头时，会被 php 识别成科学计数法，结果均为0，因此在比较两个以 `0e` 开头的字符串时，无论后面的字符时是什么，比较结果都为 True。

常用 MD5 值以 `0e` 开头的字符串：

字符串	MD5 值
QNKCDZO	0e830400451993494058024219903391
s878926199a	0e545993274517709034328855841020
s155964671a	0e342768416822451524974117254469

字符串	MD5 值
s214587387a	0e848240448830537924465865611904
s214587387a	0e848240448830537924465865611904
s878926199a	0e545993274517709034328855841020
s1091221200a	0e940624217856561557816327384675

payload：

```
a=QNKCDZO&b=s878926199a
```

=== 绕过

示例

```
if($_GET['a'] !== $_GET['b']){
    if(md5($_GET['a']) === md5($_GET['b'])){
     echo "flag";
    }
}
```

解析

在 php 中，`===` 代表着强比较，不仅仅会比较值，还会比较类型。因此这里不能在使用上面的方式进行绕过了。

要绕过此处的比较，需要向 md5() 函数中传入数组，md5() 函数中如果传入的不是字符串而是数组，不但md5()函数不会报错，结果还会返回null，在强比较里面`null=null`为 True 绕过。

payload：

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

MD5 碰撞

示例

```
if ((string)$_POST['a'] !== (string)$_POST['b'] && md5($_POST['a']) === md5($_POST['b'])) {
 echo $flag;
}
```

解析

由于此处将得到的值强制转换为了字符串，因此使用数组的方式无法进行绕过。

此处只能利用 MD5 值计算方法本身的缺陷 —— 存在散列冲突，必然会有两个内容一样但是 MD5 值一样的序列。

内容不同值一样的序列：

```
$s1 = "%af%13%76%70%82%a0%a6%58%cb%3e%23%38%c4%c6%db%8b%60%2c%bb%90%68%a0%2d%e9%47%aa%78%49%6e%0a%c0%c0%31%d3%fb
%cb%82%25%92%0d%cf%61%67%64%e8%cd%7d%47%ba%0e%5d%1b%9c%1c%5c%cd%07%2d%f7%a8%2d%1d%bc%5e%2c%06%46%3a%0f%2d%4b%e9%
20%1d%29%66%a4%e1%8b%7d%0c%f5%ef%97%b6%ee%48%dd%0e%09%aa%e5%4d%6a%5d%6d%75%77%72%cf%47%16%a2%06%72%71%c9%a1%8f%0
0%f6%9d%ee%54%27%71%be%c8%c3%8f%93%e3%52%73%73%53%a0%5f%69%ef%c3%3b%ea%ee%70%71%ae%2a%21%c8%44%d7%22%87%9f%be%79
%6d%c4%61%a4%08%57%02%82%2a%ef%36%95%da%ee%13%bc%fb%7e%a3%59%45%ef%25%67%3c%e0%27%69%2b%95%77%b8%cd%dc%4f%de%73%
24%e8%ab%66%74%d2%8c%68%06%80%0c%dd%74%ae%31%05%d1%15%7d%c4%5e%bc%0b%0f%21%23%a4%96%7c%17%12%d1%2b%b3%10%b7%37%6
0%68%d7%cb%35%5a%54%97%08%0d%54%78%49%d0%93%c3%b3%fd%1f%0b%35%11%9d%96%1d%ba%64%e0%86%ad%ef%52%98%2d%84%12%77%bb
%ab%e8%64%da%a3%65%55%5d%d5%76%55%57%46%6c%89%c9%df%b2%3c%85%97%1e%f6%38%66%c9%17%22%e7%ea%c9%f5%d2%e0%14%d8%35%
4f%0a%5c%34%d3%73%a5%98%f7%66%72%aa%43%e3%bd%a2%cd%62%fd%69%1d%34%30%57%52%ab%41%b1%91%65%f2%30%7f%cf%c6%a1%8c%f
b%dc%c4%8f%61%a5%93%40%1a%13%d1%09%c5%e0%f7%87%5f%48%e7%d7%b3%62%04%a7%c4%cb%fd%f4%ff%cf%3b%74%28%1c%96%8e%09%73
%3a%9b%a6%2f%ed%b7%99%d5%b9%05%39%95%ab"

$s2 = "%af%13%76%70%82%a0%a6%58%cb%3e%23%38%c4%c6%db%8b%60%2c%bb%90%68%a0%2d%e9%47%aa%78%49%6e%0a%c0%c0%31%d3%fb
%cb%82%25%92%0d%cf%61%67%64%e8%cd%7d%47%ba%0e%5d%1b%9c%1c%5c%cd%07%2d%f7%a8%2d%1d%bc%5e%2c%06%46%3a%0f%2d%4b%e9%
20%1d%29%66%a4%e1%8b%7d%0c%f5%ef%97%b6%ee%48%dd%0e%09%aa%e5%4d%6a%5d%6d%75%77%72%cf%47%16%a2%06%72%71%c9%a1%8f%0
0%f6%9d%ee%54%27%71%be%c8%c3%8f%93%e3%52%73%73%53%a0%5f%69%ef%c3%3b%ea%ee%70%71%ae%2a%21%c8%44%d7%22%87%9f%be%79
%6d%c4%61%a4%08%57%02%82%2a%ef%36%95%da%ee%13%bc%fb%7e%a3%59%45%ef%25%67%3c%e0%27%69%2b%95%77%b8%cd%dc%4f%de%73%
24%e8%ab%66%74%d2%8c%68%06%80%0c%dd%74%ae%31%05%d1%15%7d%c4%5e%bc%0b%0f%21%23%a4%96%7c%17%12%d1%2b%b3%10%b7%37%6
0%68%d7%cb%35%5a%54%97%08%0d%54%78%49%d0%93%c3%b3%fd%1f%0b%35%11%9d%96%1d%ba%64%e0%86%ad%ef%52%98%2d%84%12%77%bb
%ab%e8%64%da%a3%65%55%5d%d5%76%55%57%46%6c%89%c9%5f%b2%3c%85%97%1e%f6%38%66%c9%17%22%e7%ea%c9%f5%d2%e0%14%d8%35%
4f%0a%5c%34%d3%f3%a5%98%f7%66%72%aa%43%e3%bd%a2%cd%62%fd%e9%1d%34%30%57%52%ab%41%b1%91%65%f2%30%7f%cf%c6%a1%8c%f
b%dc%c4%8f%61%a5%13%40%1a%13%d1%09%c5%e0%f7%87%5f%48%e7%d7%b3%62%04%a7%c4%cb%fd%f4%ff%cf%3b%74%a8%1b%96%8e%09%73
%3a%9b%a6%2f%ed%b7%99%d5%39%05%39%95%ab"

$s3 = "%af%13%76%70%82%a0%a6%58%cb%3e%23%38%c4%c6%db%8b%60%2c%bb%90%68%a0%2d%e9%47%aa%78%49%6e%0a%c0%c0%31%d3%fb
%cb%82%25%92%0d%cf%61%67%64%e8%cd%7d%47%ba%0e%5d%1b%9c%1c%5c%cd%07%2d%f7%a8%2d%1d%bc%5e%2c%06%46%3a%0f%2d%4b%e9%
20%1d%29%66%a4%e1%8b%7d%0c%f5%ef%97%b6%ee%48%dd%0e%09%aa%e5%4d%6a%5d%6d%75%77%72%cf%47%16%a2%06%72%71%c9%a1%8f%0
0%f6%9d%ee%54%27%71%be%c8%c3%8f%93%e3%52%73%73%53%a0%5f%69%ef%c3%3b%ea%ee%70%71%ae%2a%21%c8%44%d7%22%87%9f%be%79
%ed%c4%61%a4%08%57%02%82%2a%ef%36%95%da%ee%13%bc%fb%7e%a3%59%45%ef%25%67%3c%e0%a7%69%2b%95%77%b8%cd%dc%4f%de%73%
24%e8%ab%e6%74%d2%8c%68%06%80%0c%dd%74%ae%31%05%d1%15%7d%c4%5e%bc%0b%0f%21%23%a4%16%7c%17%12%d1%2b%b3%10%b7%37%6
0%68%d7%cb%35%5a%54%97%08%0d%54%78%49%d0%93%c3%33%fd%1f%0b%35%11%9d%96%1d%ba%64%e0%86%ad%6f%52%98%2d%84%12%77%bb
%ab%e8%64%da%a3%65%55%5d%d5%76%55%57%46%6c%89%c9%df%b2%3c%85%97%1e%f6%38%66%c9%17%22%e7%ea%c9%f5%d2%e0%14%d8%35%
4f%0a%5c%34%d3%73%a5%98%f7%66%72%aa%43%e3%bd%a2%cd%62%fd%69%1d%34%30%57%52%ab%41%b1%91%65%f2%30%7f%cf%c6%a1%8c%f
b%dc%c4%8f%61%a5%93%40%1a%13%d1%09%c5%e0%f7%87%5f%48%e7%d7%b3%62%04%a7%c4%cb%fd%f4%ff%cf%3b%74%28%1c%96%8e%09%73
%3a%9b%a6%2f%ed%b7%99%d5%b9%05%39%95%ab"
```

如果需要对特定值构造，那么也可以使用下面这个神器快速构建字符串：

内容参加：如何用不同的数值构建一样的MD5 - 第二届强网杯 MD5碰撞 writeup - 先知社区 (aliyun.com)