NCTF Challenges 解题历程实录 Web#1

原创

Herman_Lien 于 2018-02-14 23:58:33 发布 300 收藏

分类专栏： ctf 文章标签： ctf

本文链接：https://blog.csdn.net/Herman_Lien/article/details/79327227

NCTF Challenges 解题历程实录 Web#1

签到题

题面：

> 这一定是最简单的
> 传送门：题目地址
> 分值：50

历程：

- 主页面干净光洁，那么view-source[**Ctrl-U**] 或inspect[**Ctrl-Shift-I**]（on Chrome），看到key

```
    <a style="display:none">nctf{flag_admiaanaaaaaaaaaaa}</a>
```

知识点：
css: 设置display属性为none来隐藏网页内容

md5 collision

题面：

源码

```
<?php
$md51 = md5('QNKCDZO');
$a = @$_GET['a'];
$md52 = @md5($a);
if(isset($a)){
if ($a != 'QNKCDZO' && $md51 == $md52) {
echo "nctf{*****************}";
} else {
echo "false!!!";
}}
else{echo "please input a";}
?>
```

传送门：题目地址
分值：50

历程：

- 主页面只显示`please input a`,php源码中也只用$_GET获取a的值,那么就直接在url后加`?a=`传入a;
- 题面源码要求`$a != 'QNKCDZO' && $md51 == $md52`，难道要我构造冲突？？？百度：MD5 构造冲突。emmm王小云教授挺强的。。。exm？？真要我构造冲突？？啊啊啊啊还是看writeup吧。
- 看完writeup恍然大雾！！首先，MD5散列值长度是128位（16字节）且用十六进制表示(32字符)。
  这里`QNKCDZO`的MD5值（怎么查？问度娘！）`$md51`为`'0e830400451993494058024219903391'`（形式上就是个科学计数法的数！）。
  而 php 如果比较一个数字和字符串或者**比较涉及到数字内容的字符串，字符串会被转换为数值并且比较按照数值来进行**，因而此字符串不严格等于(`==`，区别于`===`)`float(0)`。同理我们也只要构造一个字串a，使其MD5值同为`0exx...`格式即可。
- 怎么构造呢。。。我也没了解到，还是先看别人整理好的吧[传送门]。
  这里我就改url为`http://chinalover.sinaapp.com/web19/?a=240610708`
- 噔噔噔~得到flag：`nctf{md5_collision_is_easy}`。easy？题目做下来感觉和MD5碰撞一点关系都没有，只觉得是php的不严格比较和MD5的'特殊'散列值碰撞擦出的漏洞。。。

知识点：
php：php中的@作用：屏蔽函数执行过程中遇到问题而产生的一些错误、警告信息，使其不输出到浏览器。
php：比较运算符：其中有字符串比较时的详细例子和贴心链接，推荐
编程语言：强/弱类型：本题体现了php作为一种**弱类型**编程语言的特点（类型检查更不严格，如偏向于容忍隐式类型转换）
http：http的GET请求类型，通过url[?a=...&b=...]传入数据。HTTP POST GET 本质区别详解
密码：单向散列函数MD5

> 单向散列函数又称哈希函数或杂凑函数，是将任意长度的消息M转换成一个固定长度的散列值h的函数H：h = H(M)，散列值也叫做消息摘要（Message Digest）。这说明一定有多个输入具有相同的输出，这叫做碰撞，但对好的单向散列函数来说在可接受的时间内是找不到这样的输入的，因而可以认为输入与输出一一对应。

小心得

1. 当初做题的时候找的writeup写得太差劲了，心态也不好，于是照着‘做出’答案来了依旧对相关的知识点半知不解，当时觉得实在是费时又不讨好。写这篇时又认真查了一遍，竟然很快就查到好资源，这才把这道题的相关知识了解得很详细了，现在想想要通过ctf题来学新知识的话还是——既然决心翻writeup了就把它翻透来！
2. php手册真的是个好东西！学习php查阅必备
3. 这么水的博文写了我3小时，吐血。。。