MOCTF - WriteUp

转载

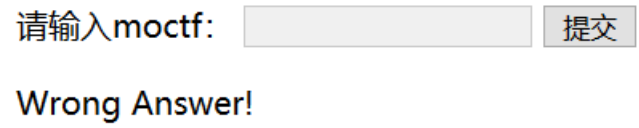
weixin_30655219 于 2018-11-17 19:33:00 发布 37 收藏
文章标签： php
原文链接：http://www.cnblogs.com/Rasang/p/9975244.html

最新更新已转移至个人博客http://rasang.site

1.一道水题

题如其名，查看源代码就可以看到flag

2.还是水题



Wrong Answer!

尝试输入，发现输入失败，于是F12直接修改数据

```
<html> event
▶ <head> ··· </head>
▼ <body>
  ▼ <form action="./index.php" method="post">
      请输入moctf:
      <input type="password" value="" disabled="disabled" name="password" maxlength="4">
      <input type="submit" value="提交">
    </form>
    Wrong Answer!
  </body>
</html>
```

直接删除disabled，修改长度为5

3.访问限制

```
<!DOCTYPE html>
<!--html lang="zh-CN">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
<?php

    $flag="moctf{**************}";

    if (isset($_GET['a'])&&isset($_GET['b'])) {
        $a=$_GET['a'];
        $b=$_GET['b'];


        if($a==$b)
        {
            echo "<center>Wrong Answer!</center>";
        }
        else {
            if(md5($a)==md5($b))
            {
                echo "<center>".$flag."</center>";
                echo "By:daoyuan";
            }
            else echo "<center>Wrong Answer!</center>";
        }

    }
    else echo "<center>濂藉儚灏戜簡鐐逛粈涔堬拷</center>";
?>
</body>
</html-->

```

只允许使用NAIVE浏览器访问!

很简单，使用tamper data修改firefox为NAIVE就可访问flag

4.机器蛇

```
2958
2959
2960
2961
2962
2963
2964
2965
2966
2967
2968
2969
2970
2971
2972
2973
2974
2975
2976
2977
2978
2979
2980
2981
2982
2983
2984
2985 <!--robots.txt-->
2986
```

直接进入源代码，发现下面有个提示，进入robots.txt文件查看

```
user-agent:
Disallow: /flag327a6c4304ad5938eaf0efb6cc3e53dc.php
Disallow: /index.html
```

访问flagxxxxxxxxxxxxxx.php的那个页面即可获得flag

5.php黑魔法

题目提示php~，访问index.php~ 发现源代码

```
<!DOCTYPE html>
<!--html lang="zh-CN">
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
</head>
<body>
<?php

    $flag="moctf{**************}";

    if (isset($_GET['a'])&&isset($_GET['b'])) {
        $a=$_GET['a'];
        $b=$_GET['b'];


        if($a==$b)
        {
            echo "<center>Wrong Answer!</center>";
        }
        else {
            if(md5($a)==md5($b))
            {
                echo "<center>".$flag."</center>";
                echo "By:daoyuan";
            }
            else echo "<center>Wrong Answer!</center>";
        }

    }
    else echo "<center>濂藉儚灏戝崟鐣逛粌涔<b>?</b></center>";
?>
</body>
</html-->

```

考察的是弱类型，md5无法加密数组，都返回false，因此构造?a=[]=1&b[]=2，得到flag

6.我想要钱

```
<?php
        include  "flag.php";
        highlight_file(__FILE__);

        if  (isset($_GET['money']))  {
                $money=$_GET['money'];
                if(strlen($money)<=4&&$money>time()&&!is_array($money))
                {
                        echo  $flag;
                        echo  "<!--By:daoyuan-->";
                }
                else  echo  "Wrong  Answer!";
        }
        else  echo  "Wrong  Answer!";
?>
```

阅读源代码可知要输入一个money，使其长度小于4，又要大于时间数（非常大），还不能是数组，于是就想到用科学计数法输入5e10，得到flag

7.登陆就对了

题目提示是一道sql注入题目，输入万能密码 'or '1' = '1' #

转载于:https://www.cnblogs.com/Rasang/p/9975244.html