CTF/CTF练习平台 随机数运算验证【细节js文件查看】

原创

Sp4rkW 于 2017-08-16 09:02:49 发布 3519 收藏
文章标签： web ctf

原题内容：

http://120.24.86.145:8002/yanzhengma/

容我吐槽一句，这题真的非常坑！！！

好吧，来看题，首先，打开页面可以看到如下布局：

第一反应，我靠，欺负我智商，这题150，没毛病，开始输入，发现输入一个1之后就不能继续输入了，很明显，这题应该是卡住了输入框

查看源代码：

```
<span id="code" class="nocode">验证码</span> <input type="text" class="input" maxlength="1"/>
<button id="check">验证</button>
<div style="text-align:center;">
<p>来源:<a href="http://ctf.bugku.com/" target="_blank">BugKu-ctf</a></p>
</div>
```



```
</body>
```

maxlength=1，很明显

但是很重要的一点，这题没有表单，不知道大家有没有注意到，！！这就非常坑了，我瞬间被带坑，满脑子都在想怎么破maxlength的限制，google了一下都得从服务器配置或者上传脚本来改了

。。。想起在论坛讨论的，题库把防御措施几乎都关了，随意扫，别破坏，个人觉得应该不是修改服务器了，心疼这么一个免费靶场，还是不破坏好了

于是又开始了google，，，，无解

回到题目，既然没有表单，不是走表单判断的，那这题如果突破了maxlength的限制，那数据又是怎么验证呢？

js，没错，预感就是这个，js的函数

查看源代码，找js路径就去开始慢慢找，果然。。。。

！！！想想就气，真心坑，这么简单

```
$("#code").on('click',codes)

$("#check").click(function(){
    if ($(".input").val() == code && code != 9999) {
        alert("flag{CTF-bugku-0032}");
    } else {
        alert("输入有误!");
    }
});
```


代码自行理解，不说了！！！

总结，别激动，有时候线耐心把源代码的内容理解透了再动手