安全-计算器（BugkuCTF）

原创

小狐狸FM 于 2021-07-06 09:39:21 发布 63 收藏

分类专栏： 安全 # CTF夺旗 文章标签： html css web 安全 ctf

本文链接：https://blog.csdn.net/smallfox233/article/details/118495737

安全 同时被 2 个专栏收录

91 篇文章 9 订阅

订阅专栏

CTF夺旗

38 篇文章 0 订阅

订阅专栏

文章目录

一、题目

原题链接

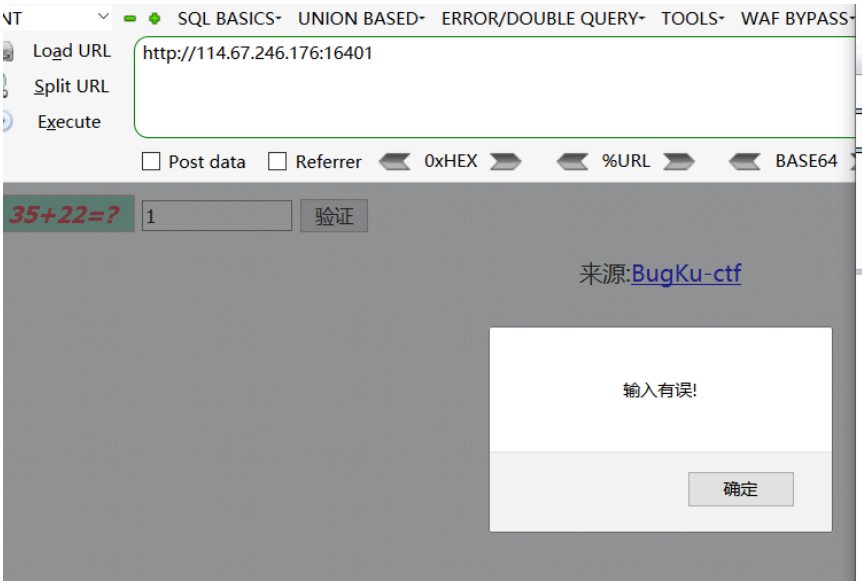
来源:BugKu-ctf

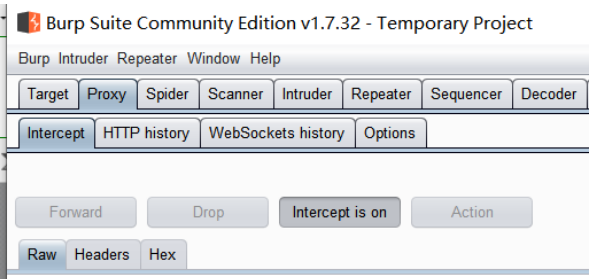
二、WriteUp

在输入数字的时候被限制了数字的长度

35+22=? 1 验证

使用 `burpsuite` 进行抓包时，发现没有抓到包，推测验证时是在本地验证的





右键页面先查看一下源码

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitio
nal.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>随机数字运算验证码</title>

<style type="text/css">
.nocode {
  display: inline-block;
    width: 100px;
    height: 25px;
}

.code {
  display: inline-block;
    color: #ff0000;
    font-family: Tahoma, Geneva, sans-serif;
    font-style: italic;
    font-weight: bold;
    text-align: center;
    width: 100px;
    height: 25px;
    line-height: 25px;
    cursor: pointer;
    border:1px solid #e2b4a2;
    background: #e2b4a2;
}

.input {
    width: 100px;

}
</style>

</head>

<body>

<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>
<script src="js/jquery-1.12.3.min.js"></script>
<script type="text/javascript" src="js/code.js"></script>

</html>
```

> 其中含有两个 `js` 文件

```
</body>
<script src="js/jquery-1.12.3.min.js"></script>
<script type="text/javascript" src="js/code.js"></script>
```

在 `js/code.js` 文件中发现了 `flag` 的信息

```
$(function() {
    var code = 9999;
    function codes(){

        var ranColor = '#' + ('00000' + (Math.random() * 0x1000000 << 0).toString(16)).slice(-6); //随机生成颜色
     // alert(ranColor)
     var ranColor2 = '#' + ('00000' + (Math.random() * 0x1000000 << 0).toString(16)).slice(-6);
      var num1 = Math.floor(Math.random() * 100);
        var num2 = Math.floor(Math.random() * 100);
        code = num1 + num2;

        $("#code").html(num1 + "+" + num2 + "=?");
        if ($("#code").hasClass("nocode")) {
            $("#code").removeClass("nocode");
            $("#code").addClass("code");

        }
        $("#code").css('background',ranColor);
         $("#code").css('color',ranColor2);

    }
    codes()

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

    $("#check").click(function(){
        if ($(".input").val() == code && code != 9999) {
            alert("flag{df7efb60253d7edf16f7b61a8f61624a}");
        } else {
            alert("输入有误!");
        }
    });
});
```

使用了 `if` 语句对输入的值进行判断，当 `code` 的值不为 `9999` 且值和输入的值相同时就会使用 `alert` 函数跳出弹窗显示 `flag`

```
$("#check").click(function(){
    if ($(".input").val() == code && code != 9999) {
        alert("flag{df7efb60253d7edf16f7b61a8f61624a}");
    } else {
        alert("输入有误!");
    }
});
```