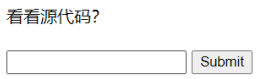
ctf web——源代码

原创

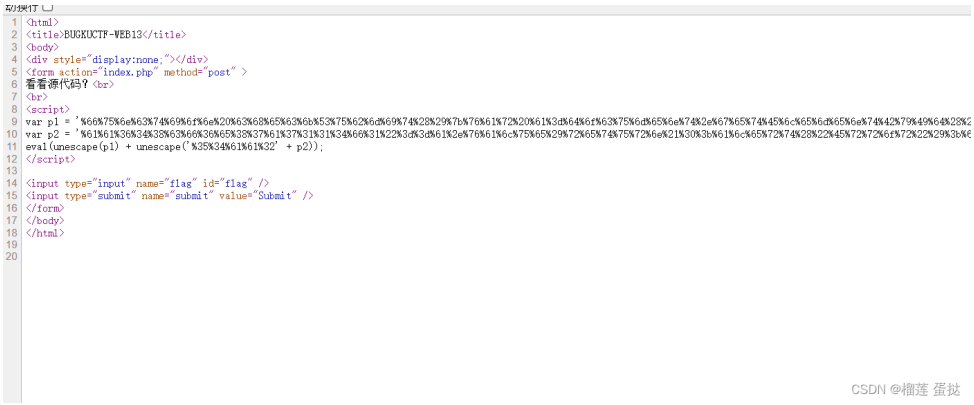
榴莲 蛋挞 已于 2022-03-28 14:54:46 修改 248 收藏
分类专栏： ctf 文章标签： 前端
于 2022-03-28 14:47:27 首次发布

本文链接：https://blog.csdn.net/god_001/article/details/123794891

打开题目网页：



于是查看网页源代码看到：



其中类似%66%75……的内容进行UnEscape解密（也可以用URL解码），解码后得到：

```
<script>
var p1='function checkSubmit(){var a=document.getElementById("password");if("undefined"!=typeof a){if("67d709b2b'
var p2='aa648cf6e87a7114f1"==a.value)return!0;alert("Error");a.focus();return!1}}document.getElementById("levelQuest").onsubmit=checkSubmit;'
eval(p1+'54aa2' + p2);
</script>
```


该脚本就相当于运行 函数checkSubmit()：

```
function checkSubmit(){
        var a=document.getElementById("password");
        if("undefined"!=typeof a){
                if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value)
                        return !0;
                        alert("Error");
                        a.focus();
                        return !1;
        }
}
document.getElementById("levelQuest").onsubmit=checkSubmit;
```


根据函数的含义，在网页中输入：67d709b2b54aa2aa648cf6e87a7114f1

得到结果：

看看源代码?

Submit

真实的flag: flag{2b0756f0962c23fa7f7c4db128c5de81}