

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

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/god_001/article/details/123794891

版权



[ctf](#) 专栏收录该内容

23 篇文章 0 订阅

订阅专栏

打开题目网页:

看看源代码?

CSDN @榴莲 蛋挞

于是查看网页源代码看到:

```
1 <html>
2 <title>BUKEXCTF-WEB13</title>
3 <body>
4 <div style="display:none"></div>
5 <form action="index.php" method="post" >
6 看看源代码? <br>
7 <br>
8 <script>
9 var p1 = '%66%75%6e%63%74%6e%66%65%6e%63%75%62%6a%66%74%28%29%7b%76%61%72%20%61%3d%6e%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%
10 var p2 = '%1%61%3%63%4%3%63%6%63%65%3%8%3%7%61%3%7%3%1%3%4%6%6%31%2%2%3%3%4%61%2e%7%6%1%6c%75%65%2%9%7%2%6%6%21%3%0%3%61%6c%65%72%74%2%2%2%45%72%7%2%6%7%2%2%2%9%3%6%
11 eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
12 </script>
13
14 <input type="input" name="flag" id="flag" />
15 <input type="submit" name="submit" value="Submit" />
16 </form>
17 </body>
18 </html>
19
20
```

CSDN @榴莲 蛋挞

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>
```

CSDN @榴莲 蛋挞

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;
```

CSDN @榴莲 蛋挞

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

得到结果：

看看源代码？

真实的flag: flag{2b0756f0962c23fa7f7c4db128c5de81}

CSDN @榴莲 蛋挞