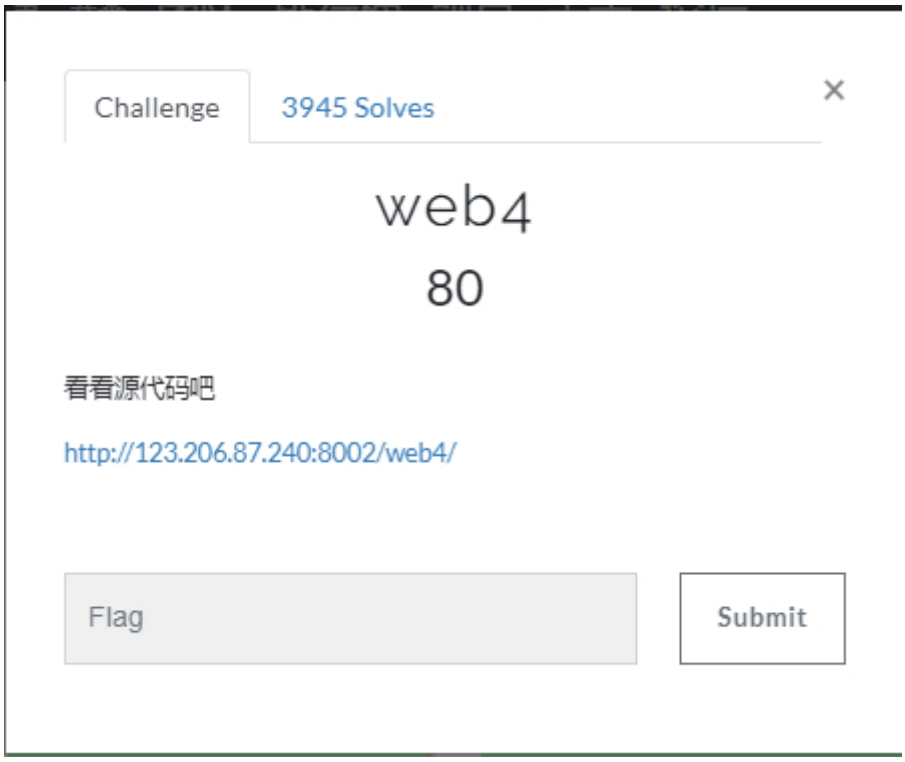
WEB4-writeup

打开题目



访问链接，提示看看源代码？查看源代码

得到一串经过escape编码的代码

```
<html>
<title>BKCTF-WEB4</title>
<body>
<div style="display:none;"></div>
<form action="index.php" method="post" >
看看源代码？ <br>
<br>
<script>
var p1 =
'%6f%75%6e%63%74%69%6f%6e%20%63%68%65%63%6b%53%75%62%6d%69%74%28%29%7b%76%61%72%20%61%3d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%70%61%73%73%77%6f%72%64%22%29%3b%69%66%28%22%75%6e%64%65%66%69%6e%65%64%22%21%3d%74%79%70%65%6f%66%20%61%29%7b%69%66%28%22%36%37%64%37%30%39%62%32%62',
var p2 =
'%61%61%36%34%38%63%66%38%36%65%38%37%61%37%31%34%66%31%22%3d%3d%61%2e%76%61%6c%75%65%29%72%65%74%75%72%6e%21%30%3b%61%6c%65%72%74%28%22%45%72%72%6f%72%22%29%3b%61%2e%66%6f%63%75%73%28%29%3b%72%65%74%75%72%6e%21%61%7d%7d%64%6f%63%75%6d%65%6e%74%2e%67%65%74%45%6c%65%6d%65%6e%74%42%79%49%64%28%22%6c%65%76%65%6c%51%75%65%73%74%22%29%2e%6f%6e%73%75%62%6d%69%74%3d%63%68%65%63%6b%53%75%62%6d%69%74%3b';
eval(unescape(p1) + unescape('%35%34%61%61%32' + p2));
</script>

<input type="input" name="flag" id="flag" />
<input type="submit" name="submit" value="Submit" />
</form>
</body>
</html>
```

进行escape解码后

```
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}}docume
nt.getElementById("levelQuest").onsubmit=checkSubmit;';
eval(unescape(p1) + unescape('54aa2' + p2));
```

主要看这一句

eval(unescape(p1) + unescape('54aa2' + p2))

```
eval() 函数可计算某个字符串，并执行其中的的 JavaScript 代码。
语法
eval（string）
string-必需。要计算的字符串，其中含有要计算的JavaScript表达式或要执行的语句
```

p1+p2连接整理后的代码

```
function checkSubmit(){
    var a=document.getElementById("password"); //匹配ID名为password的元素，并赋值给a
    if("undefined"!=typeof a){  //判断a的类型是否undefined
        if("67d709b2b54aa2aa648cf6e87a7114f1"==a.value) //判断a的元素的value值是否为67d709b2b54aa2aa648cf6e87a7114f1（67d709b2b+54aa2+aa648cf6e87a7114f1）
            return!0;
        alert("Error"); //弹框“Error””
        a.focus();  //获取焦点时，向元素添加特殊的样式（改变背景颜色）
        return!1  //! 表示取反运算，js 为弱类型语言，所有非0的int值都为 Bool 值的 True，所以 !1就是取 True的反，即False。
    }
}
document.getElementById("levelQuest").onsubmit=checkSubmit;  //获取id为levelQuest文档元素，点击submit时执行checkSubmit函数，onsubmit再点击submit时发生，若返回真提交表单
```

```
var
声明（创建）JavaScript变量

escape() 函数
定义和用法
escape() 函数可对字符串进行编码，这样就可以在所有的计算机上读取该字符串。
语法
escape(string)
string-必需。需要转义或编码的字符串

unescape() 函数
定义和用法
unescape() 函数可对通过 escape() 编码的字符串进行解码。
unescape(string)
string-必需。要解码或反转义的字符串

typeof
操作符返回一个字符串，表示未经计算的操作数的类型
详情点击：https://developer.mozilla.org/zh-CN/docs/Web/JavaScript/Reference/Operators/typeof#%E5%8F%82%E6%95%B0
```

分析完代码后，表单的id值为levelQuest，通过审查元素将输入框的id值更改为password，输入框输入67d709b2b54aa2aa648cf6e87a7114f1点击submit

看看源代码?

Submit

KEY{J22JK-HS11}