

xxsj_web18

Note

[GZCTF-challenges/xxsj_web18](https://github.com/GZCTF/challenges/xxsj_web18)

查看网页源码可以看到 `js` 文件中有一个函数

```
1 function checkClearCondition() {
2     if (score > 120 && !game_over) {
3         (async () => {
4             const s = await (await fetch('?v=1')).text();
5
6             console.log("&#85;&#82;&#76;&#47;&#63;&#102;&#108;&#97;&#103;&#61;&#115;");
7             console.log(s);
8             message.textContent = "Reset:"+s;
9         })();
10        game_over = true;
11        updateScoreboard();
12    }
```

第一种方法

访问容器网页，按下 `F12` 打开开发人员工具，找到控制台。按下 `CTRL + R` 重新加载，然后依次输入以下内容

```
1 score=130
2 game_over=false
3 run()
```

会返回类似如下内容

```
1 &#85;&#82;&#76;&#47;&#63;&#102;&#108;&#97;&#103;&#61;&#115;
2 hsqjhpu0
```

URL/?flag=s Unicode解码出来就是
URL/?flag=s

访问 URL/?flag=hsqjhpu0 即可得到 flag

第二种方法

访问 URL/?v=1 得到 hsqjhpu0

访问 URL/?flag=hsqjhpu0 得到 flag