

# 二向箔-百日打卡writeup 11-15

原创

beirry 于 2021-12-07 14:35:10 发布 162 收藏

分类专栏: [二向箔安全-百日打卡](#) 文章标签: [web安全](#)

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/beirry/article/details/121750854>

版权



[二向箔安全-百日打卡](#) 专栏收录该内容

6 篇文章 0 订阅

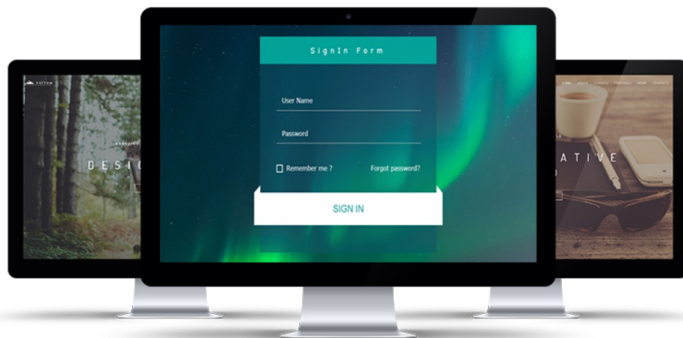
订阅专栏

## NO.11

根据提示可以知道是未授权访问

rimovni.exeeye.run 显示  
尝试登录并访问他人数据。

确定



## 伪装者

HELLO,HACKER.  
游戏已经正式开始了, 这个游戏最刺激的地方就在于没人会告诉你游戏规则, 你所在的就是一个真实的网页入口, 该怎么做, 发挥你的想象。

CSDN @beirry

登录默认账号

## 登录

默认帐号robber 密码twosecurity

用户:

密码:

## 伪装者

HELLO,HACKER.  
游戏已经正式开始了, 这个游戏最刺激的地方就在于没人会告诉你游戏规则, 你所在

确定 取消

就是一个真实的网页入口，该怎么做，发挥你的想象。

CSDN @beirry

跳转到这个页面，我先检查了一下按钮，发现都点不开，结果是发现根本就没有写链接

Robber

Home Little Game

## Robber

A lone Wolf in the wind.

About me...

More

CSDN @beirry

往下滑，看到只有三篇日记，点击More进去看看

rimovni.exeye.run/ne/diary/1

Robber

Home Little Game

## Busy Sunday

Last week , I had a busy Sunday.

I got up at six o'clock at first ,Then ,I must washed my face and brushed my teeth in ten minutes,Following,I need for breakfast . My breakfast was very delicious ,so I ate them fast.After this,I went out and went played basketball with my best friend ,Tom ,in the school playground .

We knew many tempering is good to health, so we can train each week together .

In the noon,I went home and cooked my lunch by myself ,then ate it .

In the afternoon ,I stayed at home .I read books and did my homework three hours .

I n the evening ,it is mountain in the sun ,I began to washed my dirty clothes .

At the o'clock ,I went to bed and had a rest.

How a busy day it is !

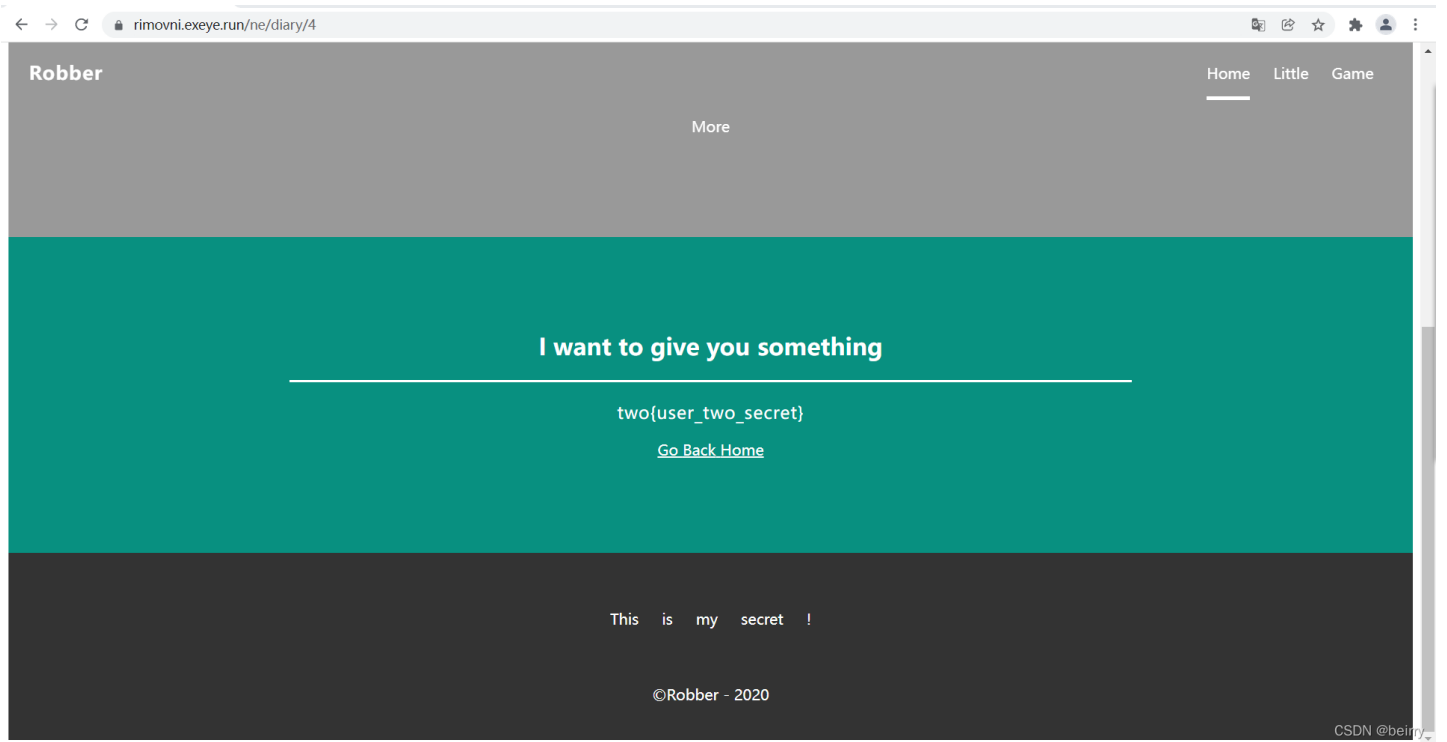
[Go Back Home](#)

This is my secret !

CSDN @beirry

一般日记都是一些私人敏感的事件，那么尝试去看4的日记

修改url: <https://rimovni.exeye.run/ne/diary/4>



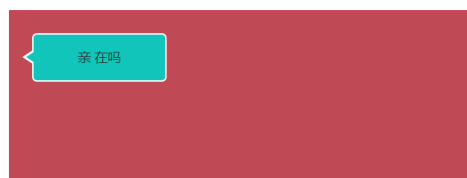
得到flag

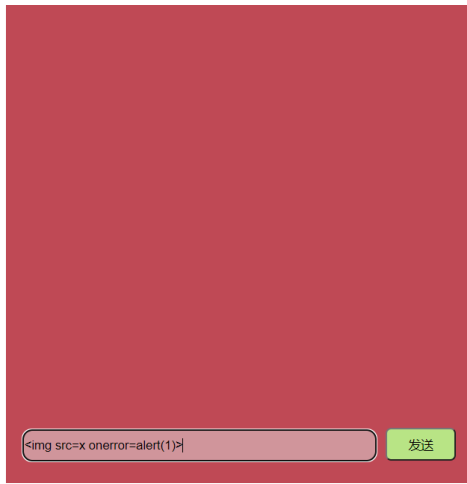
## NO.12

这个提示也是非常明显了，就是测试xss无疑了



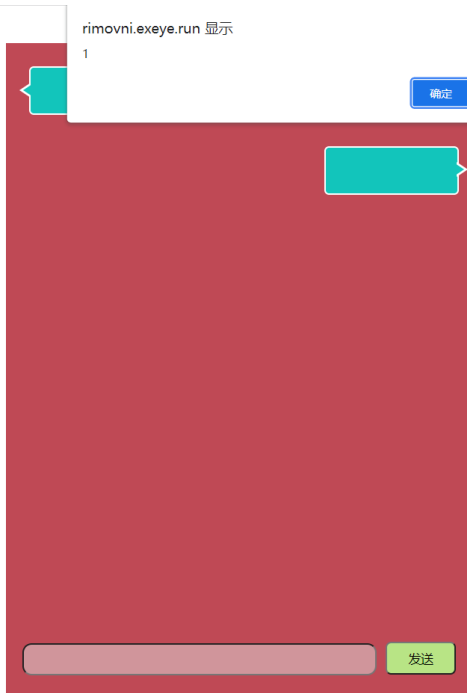
直接测试 `<img src=x onerror=alert(1)>`





CSDN @beirry

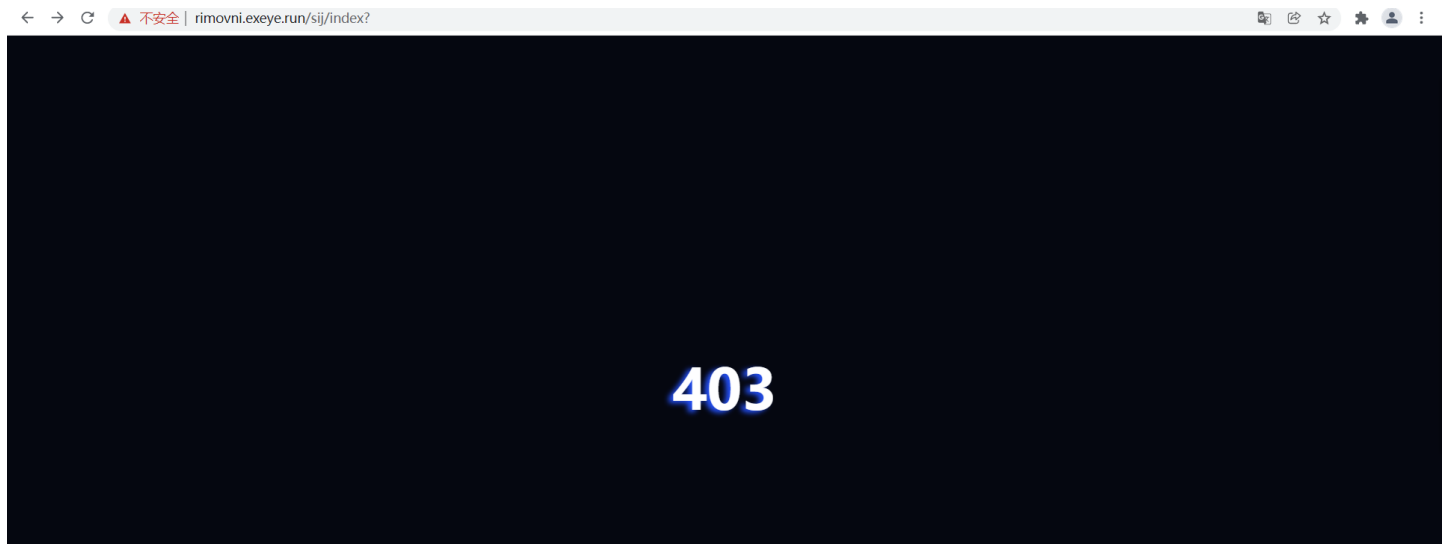
触发弹窗



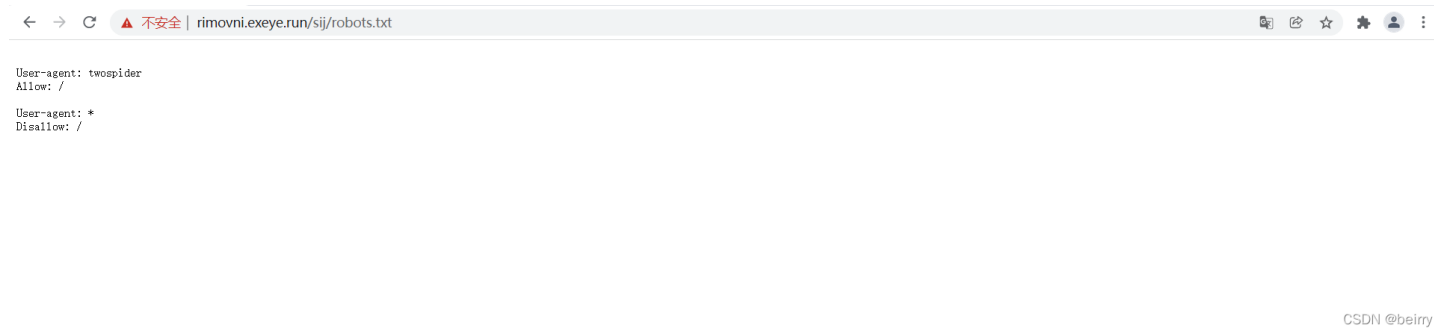
CSDN @beirry

## NO.13

进入页面发现报403的错误



这个时候就查看一下robots.txt文件，看是不是做了哪些策略



清晰明了了，通过burp抓包，修改user-agent值

The screenshot shows the Burp Suite interface with a request and response view. The request shows a User-Agent of 'twospider'. The response shows a User-Agent of 'two (d0nt\_uSer\_Agent)' highlighted in red. The Inspector panel on the right shows the selected text 'twospider' and the decoded response 'two (d0nt\_uSer\_Agent)'.

得到flag

## NO.14

又是未授权访问

rimovni.exeye.run 显示  
尝试登录并访问他人数据。

确定



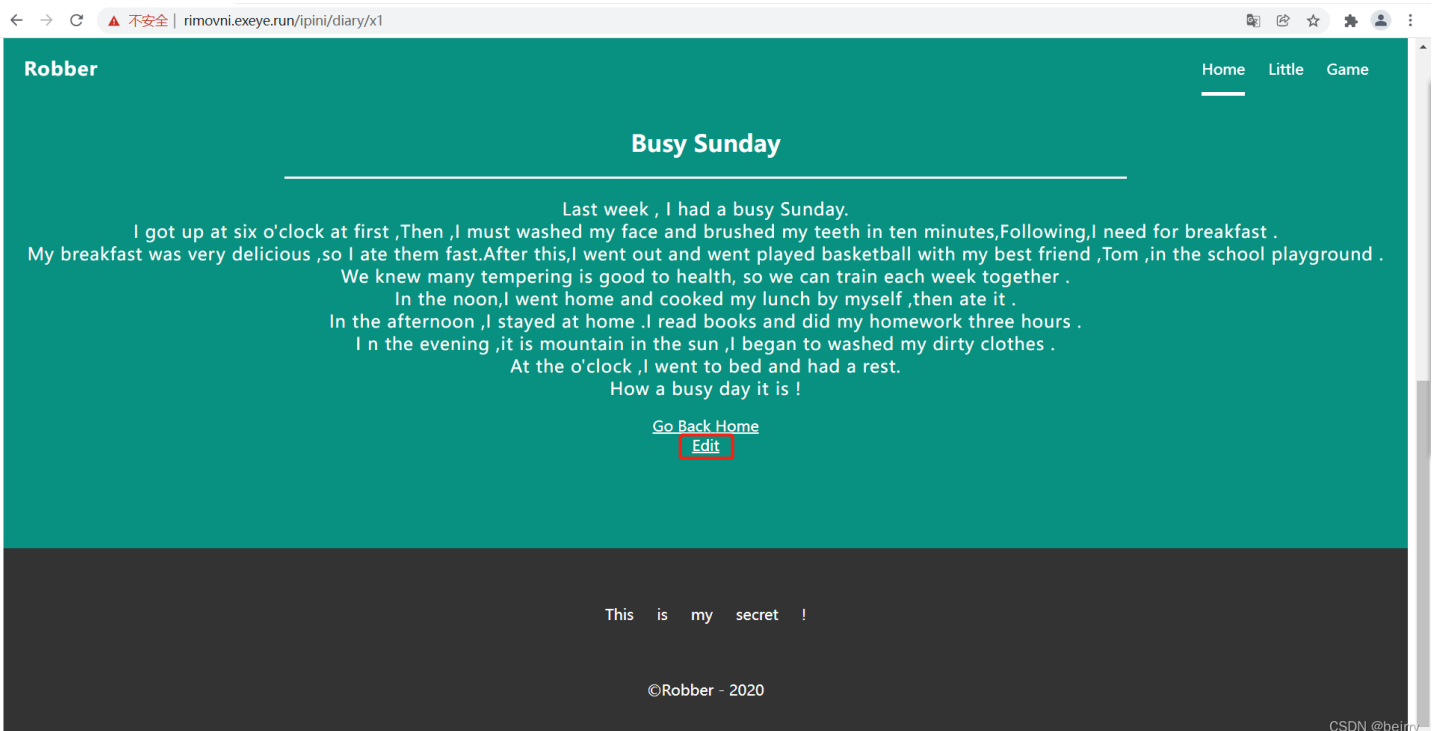
## 伪装者

HELLO,HACKER.

游戏已经正式开始了,这个游戏最刺激的地方就在于没人会告诉你游戏规则,你所在的就是一个真实的网页入口,该怎么做,发挥你的想象。

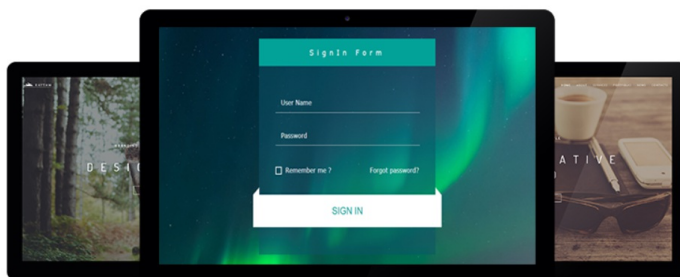
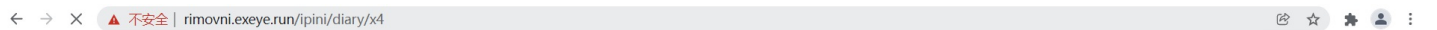
CSDN @beirry

登录默认账号  
直接访问日记



CSDN @beirry

修改url/x4, 报错

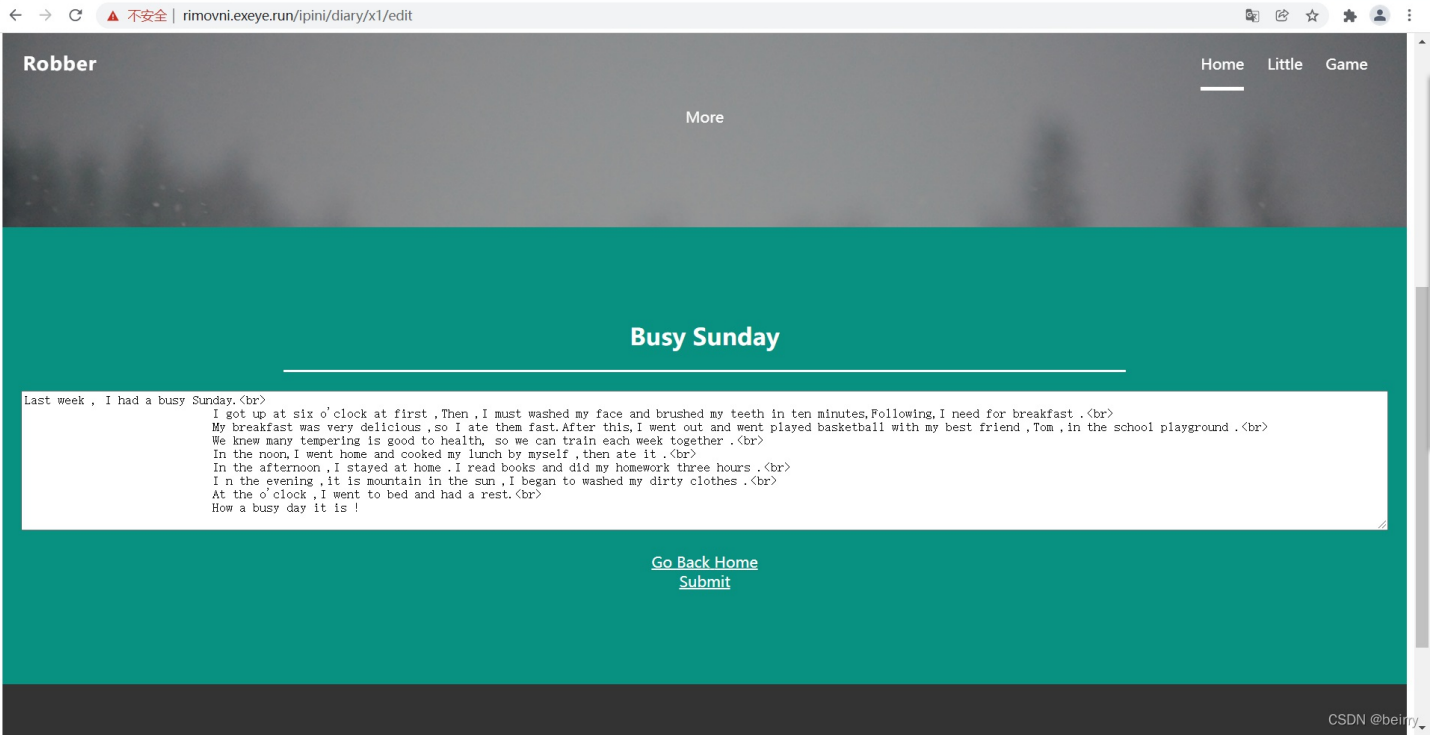


## 伪装者

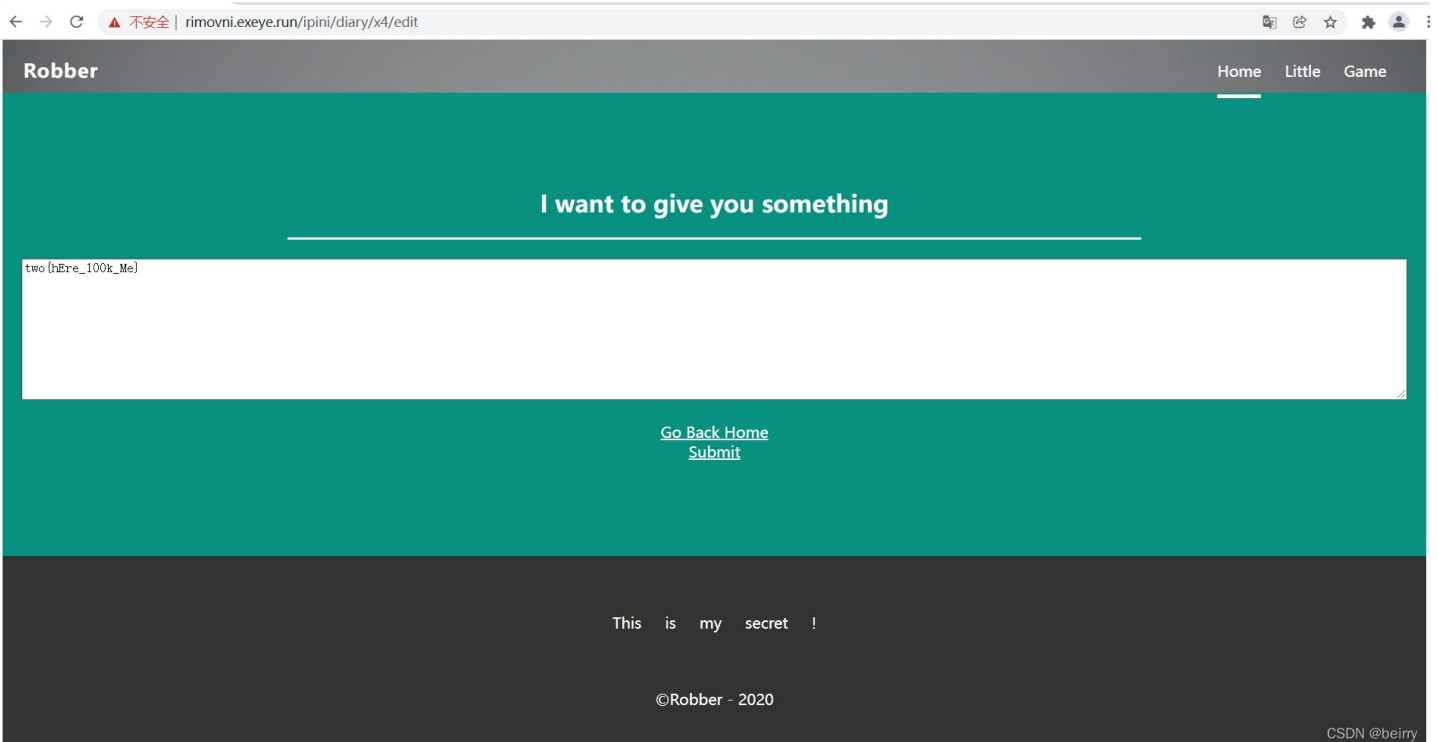
系统异常返回



返回到日记页面可以看到多了一个edit，直接点击访问



再改url

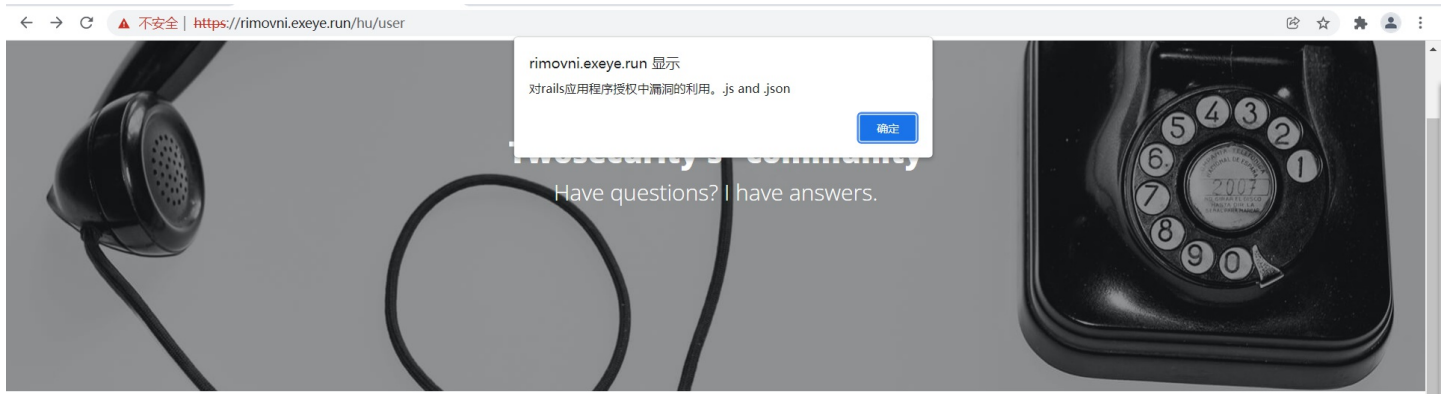


得到flag

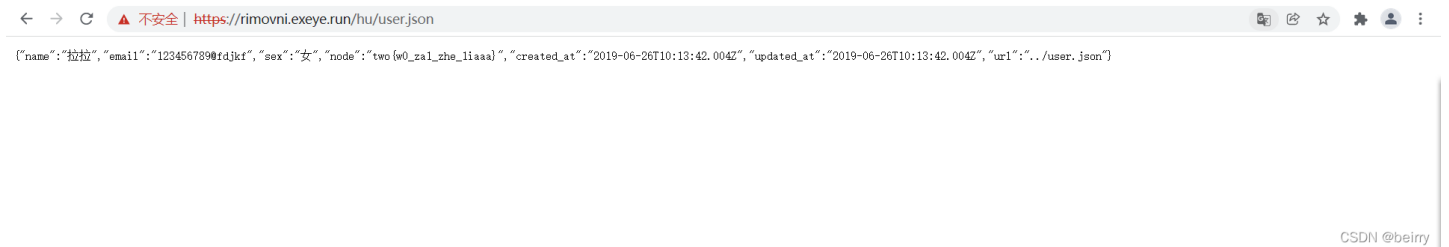
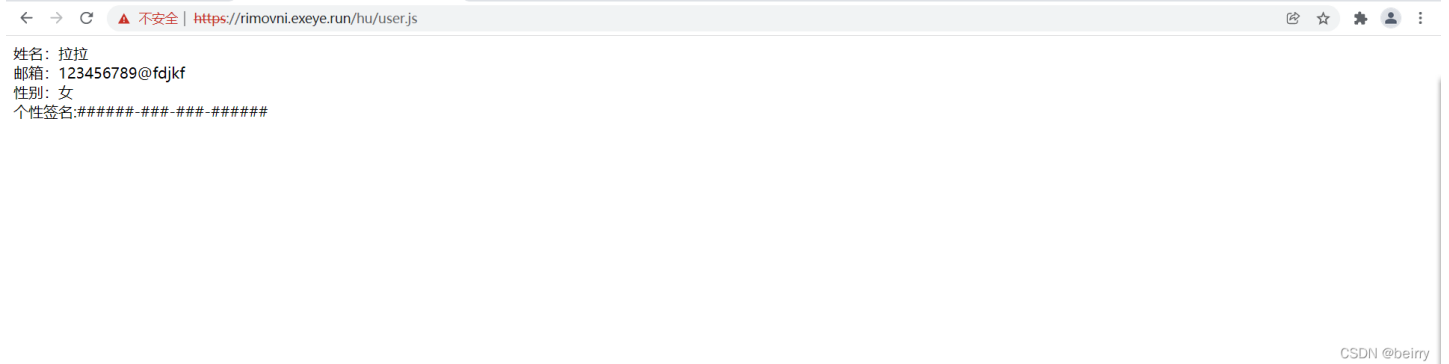
NO.15



根据提示，我去网上搜索了一下有关于对rails应用程序授权漏洞原理及利用方法



但都是以失败告终，又看了下后面的.js and .json，这个页面又是个人信息，猜测名字邮箱性别都是调用js文件，但是查看源码也没发现能利用到的js文件，做了半天一点思路也没有。最后随手测试了一下去访问user.js和user.json，发现flag



这道题其实我的思路并没有错，个人信息确实是从js和json文件中调取。这个也算是一个未授权访问的漏洞。但我至今也没想明白它给的提示前半句话是啥意思。。。