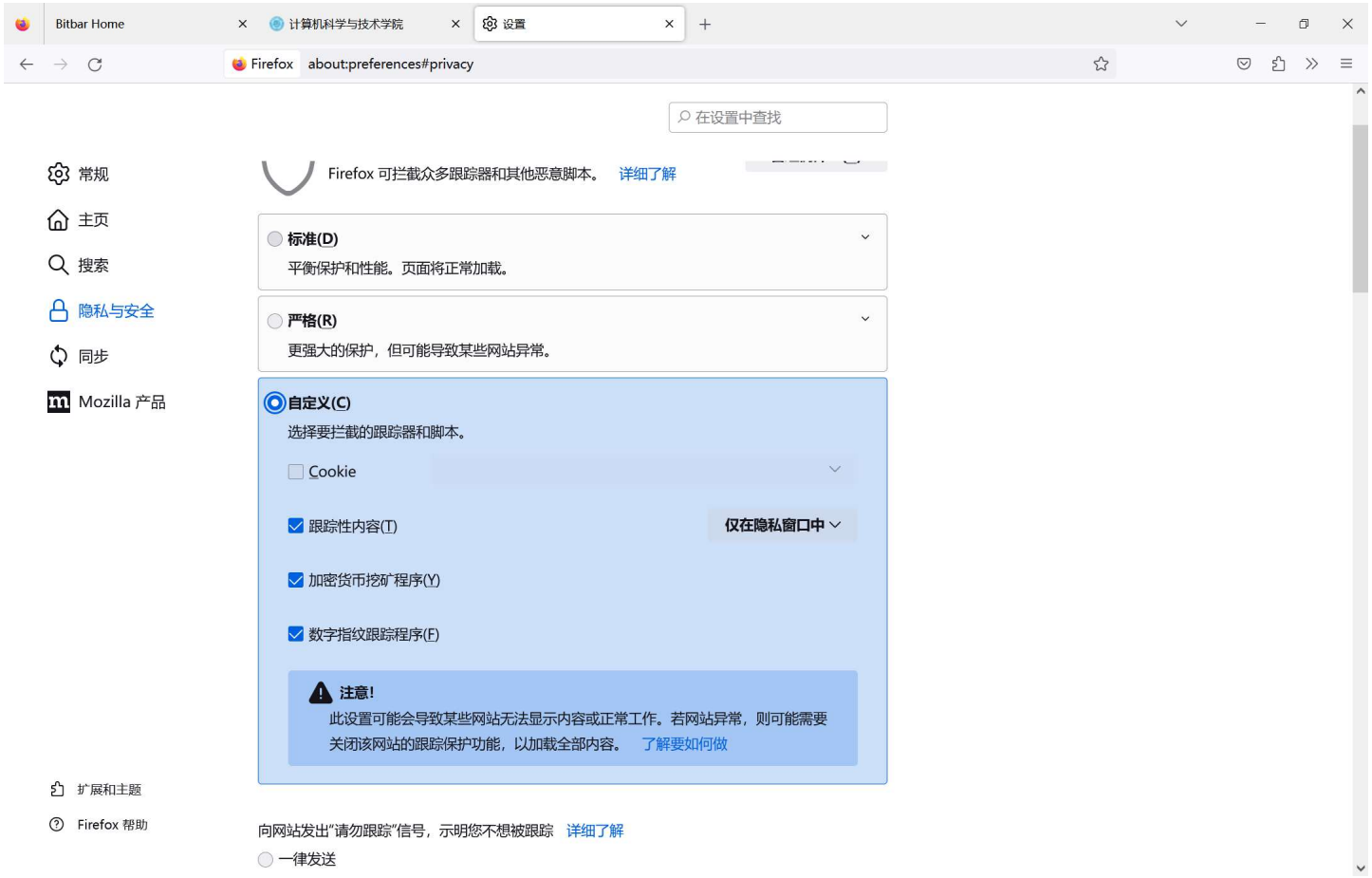
my analysis

这部分实验的原理是利用浏览器向服务器默认发送属于该服务器的cookie的性质。但是大多数浏览器会默认给cookie加上samesite属性，因此需要在浏览器设置取消拦截跨站请求的cookie。



这样一来，在b.html里面写入提交转账POST的代码，浏览器向服务器发送请求时会带上cookie，从而攻击成功。

如果cookie被拦截，则服务器端收到请求时，相当于没登录的状态，因此会得到 “You must be logged in to use this feature! ”这样的错误。

另外，还有个小细节。实验文档一开始说转10 bitbars，后来又说转15 bitbars。这应该是个笔误，不过对实验没什么影响，我这里以转15 bitbars为准。