

别的网站对自己网站的影响，在用户不知情的情况下做的一些看似合理的请求

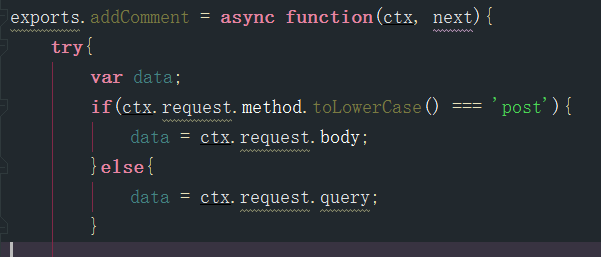
用户登录后，还没推出，发送合理请求，post提交一个表单



你啥也没看见就做了很多事情

最简单的是get请求，直接从参数中取值



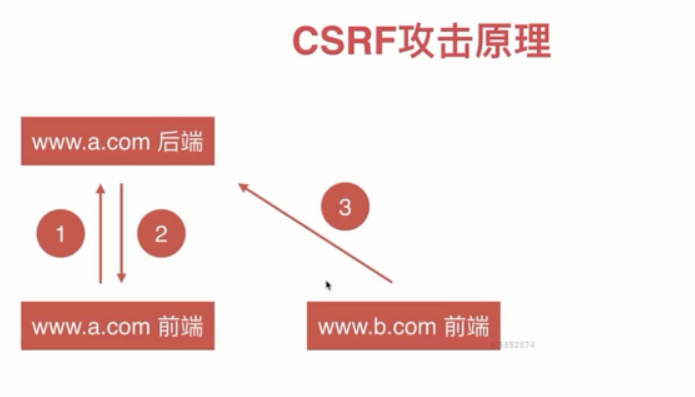


模拟请求发送



连环爆炸





登录后，发送到a后台，就会跳转，设置cookie, 登陆cookie



可以查看controller/use.js 的登陆操作 ,请求中带了登陆态；













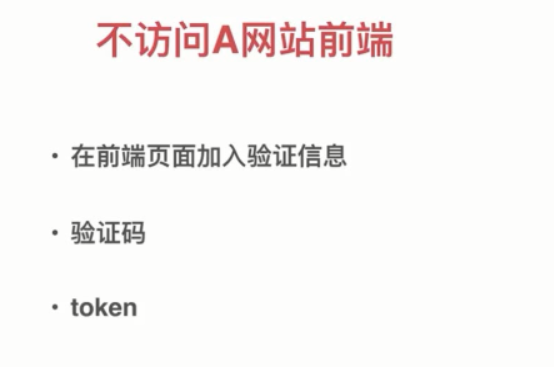
Same-site-strict lax





Koa 的cookie 模块并不支持 用原生的。

但是 same-site 属性的兼容性不是很好，但是以后会好的



后端验证码

Koa没有原生的，所以我们用第三方 ccap npm包

攻击者不访问你的前端就拿不到你的验证码，

可以cha



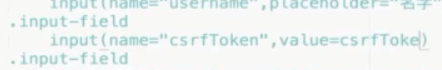


验证码，用户体验很差，验证码有误，啥的

让攻击者发起攻击时，不经过前端页面，无法得到token，同时也拿不到页面的cookie

Token是一个随机数，由后端生成：放到两个地方，放到页面的隐藏表单中，或者页面其他地方，另外还要放到cookie中。





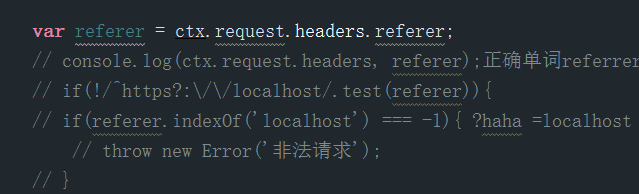
如果只有表单中的token,没有cookie中的token, 表单提交会会把token带过去，这样的话就无法验证；

如果没有表单中的token,只有cookie中的token,那么用户可以随意捏着一个cookie,也无法验证；

Ajax 请求，一般是将token放在meta中，在js中将meta中的token拿出来，发送给后端进行校验；

还要注意，如果用户打开多个页面，那么只有最后一个页面的token是有效的，那怎么办呢？可以思考；





但是有的网站可以指定不带referer,防盗链