https://zhidao.baidu.com/question/587951165640935605.html

为什么站点使用https加密之后还能看到相关数据

https://iknowpc.bdimg.com/static/question-new/widget/ask/replyer/img/gift.7b31617.gif?1545372916 我来答

分享

[举报](javascript:void(0))浏览 718 次

2个回答

[#热议# 考研在即，你如何看待大学生蜂拥考研的现象？](https://zhidao.baidu.com/question/653747516622936565.html?entry=hottopic)

热心网友   
2016-12-16

为什么站点使用了https加密之后，还是能够用firebug之类的软件查看到提交到的信息，并且还是明文的?例如说这样：  
  
这是因为:https(ssl)加密是发生在应用层与传输层之间，所以在传输层看到的数据才是经过加密的，而我们捕捉到的http post，是应用层的数据，此时还没有经过加密。这些明文信息，其实就是你的本地数据。  
  
加密数据只有客户端和服务器端才能得到明文，客户端到服务端的通信过程是安全的。  
  
可能有些读者会对此表示担忧了：这样的话密码不是会被本地恶意软件截获么?只能说的确存在这样的可能。不过在银行电商等安全防护程度较高的网站，除了https加密外，还有安全控件加密，用户必须下载安全控件后才能输入密码，以支付宝为例：通过下图可以发现就算在本地也无法查看账号信息。  
  
针对这个问题，沃通CA建议：行政、金融、电商等需要高安全防护的站点在实行https加密外，还应该部署沃通客户端证书，以强身份认证的方式替代不安全的账号密码认证，确保登录过程中的安全无忧，同时还能弱口令漏洞，最大程度保护用户信息安全。  
  
此外，针对使用安全控件辅助登录的站点，沃通还建议使用代码签名证书，以保证安全控件在下载传输过程中没有被篡改及破坏。从而保证代码的完整性，保护用户不会被病毒、恶意代码和间谍软件所侵害，真正做到全面安全防护。

**5**

 评论

分享

[举报](javascript:void(0))收起

匿名用户   
2016-12-16

加密数据只有客户端和服务器端才能得到明文，客户端到服务端的通信过程是安全的。  
可能有些读者会对此表示担忧了：这样的话密码不是会被本地恶意软件截获么?只能说的确存在这样的可能。不过在银行电商等安全防护程度较高的网站，除了https加密外，还有安全控件加密，用户必须下载安全控件后才能输入密码，以支付宝为例：通过下图可以发现就算在本地也无法查看账号信息。