HTTPS

HTTPS

`HTTPs = HTTP + SSL / TLS`. 服务端和客户端的信息传输都会通过 TLS 进行加密，所以传输的数据都是加密后的数据

- wireshark 分析 HTTPs

例题

> 题目：hack-dat-kiwi-ctf-2015:ssl-sniff-2

打开流量包发现是 `SSL` 加密过的数据, 导入题目提供的 `server.key.insecure`, 即可解密

```
GET /key.html HTTP/1.1
Host: localhost

HTTP/1.1 200 OK
Date: Fri, 20 Nov 2015 14:16:24 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Fri, 20 Nov 2015 14:15:54 GMT
ETag: "1c-524f98378d4e1"
Accept-Ranges: bytes
Content-Length: 28
Content-Type: text/html

The key is 39u7v25n1jxkl123
```

评论