# URL相关安全问题

## 字形欺骗钓鱼攻击

通过相似字形，欺骗用户。

如 l 和1 非常相似，钓鱼网站利用相似的域名欺骗用户。

## 国际化域名字形欺骗 IDN

同样利用各种语系中字母外形相似的字母欺骗用户。

## 自纠错与Unicode字符分解映射

浏览器具有纠错功能

如会将。转换为 。

同时也会将某些Unicode字符通过其标椎化函数映射为ASCII字符

如在chrome中，会对host部分进行标椎化，如果发现它是一个类IDN,将会把它转换为ASCII(调用ICU--- Unicode国际化组件 的标准函数来分解 ),

## 登陆信息钓鱼

<http://www.qq.com:80@dongyuewu.com/>

这种用户名，密码登陆dongyuewu.com的链接，很容易认为是链接qq.com

# HTTP协议相关安全问题

由于http是明文传输，如果能控制到受害者网络，便可以轻易嗅探，修改http传输的内容。

http仅仅咋报文头部包含了数据的长度，而没有任何校验数据完整性的机制（Content-Length本身也能被修改）

## 注入响应头： CRLF

代码注入漏洞（回车换行）

原理：

如果某次响应的数据中，有一个字段的数据是用户输入的，而服务器没有做好过滤，用户就可以通过编码插入CR + LF及注入的新字段来发起攻击

## 攻击响应：HTTP 401钓鱼

基本就是Auth返回

也就是WWW-Authenticate中传递的提示信息，诱使用户提供隐私信息

## 源

源是由方案名称，主机名，端口号组成。

在客户端，绝大多数的安全策略都是通过限制源来实行的。