# 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）

## session会话相关攻击

由于：http无状态，为了位置一个可识别的状态，需要session.攻击者捕获合法用户的session，用户身份验证。

### 攻击者获取session方法

①暴力破解

基本不可能成功

②预测--针对非随机方式生成的session

③窃取

通过网络嗅探，XSS攻击

④固定会话

会话固定（Session fixation）是一种诱骗受害者使用攻击者指定的会话标识（SessionID）的攻击手段。这是攻击者获取合法会话标识的最简单的方法。（让合法用户使用黑客预先设置的sessionID进行登录，从而是Web不再进行生成新的sessionID，从而导致黑客设置的sessionId变成了合法桥梁。）

## 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

CRLF可以可以导致多种问题

1. 注入set-cookie,指定固定会话，攻击者也可以通过注入http头关闭浏览器xss保护。

具体方式：

一、js修改 --- 适用于非httponly的session 和 有安全漏洞的浏览器

document.cookie = ‘PHPSESSID=12345

1. 在head标签中添加set-Cookie标签

<meta http-equiv='Set-Cookie' content='PHPSESSID=22333'>

三、在响应头部写入set-cookie

1. 如果攻击者在响应中写两个%0d%0a，这相当于将后面的实体展示在浏览器中，如果我们直接在响应实体中写脚本，这个脚本也会在浏览器中直接执行。

## 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。

# DNS

浏览器DNS缓存 --》 系统DNS缓存 --》 路由器DNS缓存 -》 ISP DNS缓存 -》 递归搜索模式

DNS查询基于 UDP 且没有任何认证机制，因此DNS十分容易被篡改，攻击者扮演‘中间人’。

## DNS攻击

### 劫持

ISP(Internet Server Provider)中很常见，ISP会劫持某个域DNS（投放广告）

### 污染

# XSS

反射型

Reflected XSS

存储型

Stored XSS

# CSRF

跨域请求伪造

就是在攻击者网站 访问本地登录的网站。

Get 请求设置数据，更容易被攻击。

Post请求也能通过form提叫的方式攻击。

一般来说，最好有验证码，提交。（感觉还能验证，origin）