**前提了解：**

**2017年WannaCry病毒(撞库/暗网)**

网络安全：网络空间是信息时代人类赖以生存的信息环境，是所有信息系统的集合。

网络空间安全：网络空间安全学科是研究信息获取，信息存储/信息传输和信息处理过程中的安全保障问题的新兴学科。

**web应用的基本架构**

**客户端(浏览器) —— 传输协议(HTTP) —— 服务端(应用服务器数据库服务器)**

HTTP是一个**应用层协议**，是由请求和响应构成，是一个标准的客户端服务器类型，HTTP是一个无状态的协议。

# WEB常见安全问题

## 尽量不要从URL、document.referrer、document.forms等这种DOM API中获取数据直接渲染。

1. 尽量不要使用eval，new Function()，document.write()，document.writeIn()，window.setInterval()，window.setTimeout()，innerHTML，document.createElement()等可执行字符串的方法；
2. Content-Security-Policy文档
3. 提交参数时进行转码encodeURI()和encodeURIComponent()

两者区别：encodeURI()不会对本身属于URI的特殊字符进行编码，例如冒号、正斜杠、问号和井字号；而encodeURIComponent()则会对它发现的任何非标准字符进行编码

1. window.open

var aa = window.open('http://127.0.0.1:3000/border.html')；

aa.opener == window // true

aa.opener.history