特定的**域名**（或**IP地址**）**、协议和端口号**称为一个**源**(Origin), 现代浏览器所共同遵守的一个规范，即不同源的客户端脚本（如js,as等）在没有明确授权的情况下不能读写对方资源的原则称为**同源策略**(Same Origin Policy). 现代所有支持js的浏览器都实现了这一策略。同源策略**隔离了不相关的网站**所提供的内容，因而是浏览器最核心、最基本的安全功能。

假设没有同源策略，则当我们打开A网站并登录时，另一个网站B可以不受限制地**跨域**读取我们在A上的所有账号数据。

在浏览器中，<script>,<img>,<iframe>,<link>等带有"src"的标签可以跨域**加载**资源，但实际上是由浏览器发起了一次GET请求，因此不能读写返回的内容，本质上只是一种**引用**。

XMLHttpRequest可以访问来自同源对象的内容，

御剑（想念初恋）是一款路径扫描软件，通过扫描网站后台的路径寻找网站的薄弱点。实践中我们已经利用御剑直接拿到了福建省青少年科技活动中心数据库（设计的太烂了，数据库文件路径一旦被找到，不需要权限就可以随意下载）；不过比较尴尬的一点是我们测试了附小和启明的网站，但频率超过一定次数以后都被安全狗拦截了，无法完成完整的扫描工作，因而对于有安全狗存在的网站可能需要走一波代理IP池（僵尸网络）。

awvs是一款web漏洞扫描软件。

dvwa是专门为web安全设计的一套模拟系统，安全研究员可以使用dvwa来进行渗透测试的练习。需要主机上预装有apache+php+mysql环境.

IBM Security AppScan, 曾用名IBM Rational AppScan（从8.6版本起才改为现在的名字）,后面简称为**RA**, 是IBM[[1]](#footnote-0)公司的Rational Software部门开发的一款Web安全的测试工具.

RA采用三种彼此互补的扫描方法：**动态分析**、**静态分析**和**交互分析**（或者称为“黑盒扫描”、“白盒扫描”和"glass box扫描"），动态分析是主要的方法，将页面视为一个黑盒，只考虑request-response反应，静态分析是完整的上下文环境中分析JavaScript代码的先进技术，能够直接看出JS代码中可能存在的漏洞，最后的玻璃盒GlassBox(GB)技术是RA8.5版本引进的技术，这个似乎是一种很高端的路线（仅在RA中才有，其他扫描器中都没有使用），暂时不进行原理分析，参见

GB的本质是一种安装在Java服务器上的**代理程序**（在RA9.0以后也可以安装在.NET服务器上）

http://www.2cto.com/article/201209/152567.html

RA的扫描分为“探索”和“测试”两个**阶段**，在探索阶段RA通过模拟用户点击链接、填写表单的行为来探索站点，分析所每一个请求所返回的相应，从中寻找出可能存在安全漏洞的相应，并且基于这些响应方式来创建测试请求，在测试阶段中则发送这些先前创建的测试请求，并进一步分析其中的响应，从而确定目标网站的漏洞情况.

值得注意的是，在测试阶段过后可能会发现更多的新链接和安全问题，因此执行新一轮的探索—测试是有必要的，我们把一次的“探索—测试”称为一个**过程**，在第一个过程之后AppScan会自动进行第二个过程，阶段的个数是可以人工设定的，默认情况下执行4个阶段，也就是2个过程.

1. 国际商业机器公司 [↑](#footnote-ref-0)