11.6.10 cookie、安全性和隐私

cookie 是可以禁止的，而且可以通过日志分析或其他方式来实现大部分跟踪记录，所以 cookie 自身并不是很大的安全隐患。实际上，可以通过提供一个标准的审查方法在远程数据库中保存个人信息，并将匿名 cookie 作为键值，来降低客户端到服务器的敏感数据传送频率。

但是，潜在的滥用情况总是存在的，所以，在处理隐私和用户跟踪信息时，最好还是要小心一些。第三方 Web 站点使用持久 cookie 来跟踪用户就是一种最大的滥用。将这种做法与 IP 地址和 `Referer` 首部信息结合在一起，这些营销公司就可以构建起相当精确的用户档案和浏览模式信息。

尽管有这么多负面的宣传，人们通常还是认为，如果能够小心地确认在向谁提供私人信息，并仔细查阅站点的隐私政策，那么，cookie 会话处理和事务处理所带来的便利性要比大部分风险更重要。

1998 年，计算机事故咨询能力组织（Computer Incident Advisory Capability）（美国能源部的一部分）编写了一份过分使用 cookie 的风险评估报告。下面是那份报告的摘要。

> CIAC I-034：因特网cookie
>
> （http://www.ciac.org/ciac/bulletins/i-034.shtml）
>
> - 问题
>
> cookie是Web服务器用来识别Web用户的小块数据。关于cookie功能的流行说法和谣言之间的比例已经达到了令人不解的地步，使用户恐惧，使管理者忧心。

> - 脆弱性评估
>
> 由于使用Web浏览器cookie使得系统被破坏或窃听，从而带来的系统脆弱性本质上并不存在。cookie只能告知Web服务器你以前是否到过某个网站，并在下次访问时将来自Web服务器的一些短小信息（比如用户编码）回送给它。大部分cookie只会持续到用户退出浏览器为止，然后就会被破坏掉。第二种名为持久cookie的cookie有一个过期日期，会在你的硬盘上存储到那个日期为止。无论用户何时返回一个站点，都可以通过持久cookie来识别其身份，以便跟踪用户的浏览习惯。你来自何处，以及访问过哪些Web页面等信息已经存储在Web服务器的日志文件中了，也可以用这些信息来跟踪用户的浏览习惯，只是使用cookie更简单一些罢了。