Cross-Site Request Forgeries: Exploitation and Prevention

跨站点请求伪造：开发和预防

William Zeller\* and Edward W. Felten\*†

\*Department of Computer Science

\*Center for Information Technology Policy

†Woodrow Wilson School of Public and International Affairs

Princeton University

fwzeller,felteng@cs.princeton.edu

修订10/15/2008：注意到“纽约时报”已经修复了下面所述的漏洞。 另外澄清了我们的服务器端CSRF保护建议并不能阻止[17]中描述的主动网络攻击。

本文的最新版本可以在这里找到

<http://citp.princeton.edu/csrf/>

摘要  
跨站点请求伪造（CSRF）攻击发生在恶意网站导致用户的Web浏览器对受信任站点执行不必要的操作时。这些攻击被称为基于Web的漏洞的“睡眠巨人”，因为互联网上的许多站点都不能对其进行保护，因为它们在很大程度上被Web开发和安全社区忽视。我们提出了四个严重的CSRF漏洞在四个主要网站上发现，包括我们认为是首次发布的涉及金融机构的攻击。这些漏洞允许攻击者从用户银行帐户中转账，获得用户电子邮件地址，侵犯用户隐私和妥协用户帐户。我们推荐能够完全保护站点免受CSRF攻击的服务器端更改（我们已经实现的）。我们还描述了服务器端解决方案应该具有的功能（缺少这些功能导致CSRF保护不必要地破坏了典型的Web浏览行为）。此外，我们还实施了一个客户端浏览器插件，即使站点没有采取措施保护自身，也可以保护用户免受某些类型的CSRF攻击。我们希望提高CSRF攻击的意识，同时向负责的Web开发人员提供保护用户免受这些攻击的工具

1.简介  
跨站点请求伪造1（CSRF）攻击发生在恶意网站导致用户的Web浏览器对受信任站点执行不必要的操作时。 这些攻击被称为基于Web的漏洞的“睡眠巨人”[23]，因为互联网上的许多站点都不能对其进行保护，因为它们在很大程度上被Web开发和安全社区忽视。 CSRF攻击不会出现在Web Security Threat Classification [12]中，很少在学术或技术文献中进行讨论.2 CSRF攻击简单易于诊断，易于开发，易于修复。 它们存在是因为Web开发人员对于CSRF攻击的原因和严重性没有受过教育。 Web开发人员也可能会受到错误的印象，即针对更好的跨站脚本（XSS）问题的防御也可以防范CSRF攻击。

在第3节中，我们介绍了四个主要站点发现的四个严重的CSRF漏洞。 这些漏洞允许攻击者从用户银行帐户中转账，收获用户电子邮件地址，侵犯用户隐私和妥协用户帐户。

—————————————————

1跨站点请求伪造攻击也称为跨站点参考伪造，XSRF，会话骑乘和混淆副攻击。我们使用术语CSRF，因为它似乎是这种攻击最常用的术语。  
2在ACM数字图书馆搜索“跨站脚本”（与CSRF不同）返回72篇论文，搜索“xsrf OR csrf”只返回四篇论文。 在Safari Books Online上搜索“xss”（收集了4752本技术书籍），该书出现在96本书中，而“csrf OR xsrf”只出现在13本书中。

在第4.1节中，我们建议可以完全保护站点免受CSRF攻击的服务器端更改（我们已经实施）。这些建议具有优于先前提出的解决方案的优点，因为它们不需要服务器状态，并且不会破坏典型的Web浏览行为此外，我们实施了一个客户端浏览器插件，可以保护用户免受某些类型的CSRF攻击（第4.2节）。服务器端保护允许站点完全保护自己免受CSRF攻击，而客户端保护允许用户采取主动措施来保护自身免受许多类型的CSRF攻击，即使站点没有采取措施保护自身。我们希望提高CSRF攻击的意识，同时向负责的Web开发人员提供保护用户免受这些攻击的工具。