1. [另存为 PDF](https://success.coupa.com/@api/deki/pages/555/pdf/Vulnerability%2bReporting%2bPolicy.pdf?stylesheet=default)

**概览**

在 Coupa，我们认识到独立安全研究人员在保持互联网安全方面所起的重要作用。 保持客户数据的安全是我们的首要任务，我们鼓励负责任的报告任何漏洞，可能会发现在我们的网站或应用程序。我们致力于与安全社区合作，以验证和回应任何潜在的漏洞报告给我们，我们承诺不发起法律行动，对安全研究人员渗透或试图渗透我们的系统，只要他们遵守以下条件。

**安全漏洞测试**

只对我们的在线服务的试用实例进行漏洞测试，以最小化对客户数据的风险。在测试时，我们不允许进行以下类型的安全研究：

* 导致或试图导致拒绝服务（DoS）条件
* 访问或试图访问不属于你的数据或信息
* 毁灭或腐蚀或企图破坏或破坏不属于你的数据或信息

**报告潜在的弱点**

与我们私底下分享可疑的漏洞的细节，通过发送电子邮件到[security@coupa.com](mailto:security@coupa.com)如果你想发送加密的消息，你可以用这个[PGP 密钥](https://success.coupa.com/Trust/Security_Policies/04_Coupa_Security_Team_PGP_Key)提供被怀疑的漏洞的全部细节，以便我们的安全团队能够验证和重现问题。

包括下列资料：

* 概念证明和/或 URL 显示漏洞
* 问题类型（跨站点脚本、缓冲区溢出、SQL注入等）
* 复制问题所需的任何特殊配置
* 这个问题的影响包括攻击者如何利用这个问题

**我们的安全承诺**

对于所有遵循 Coupa 漏洞报告政策的安全研究人员，我们的安全团队承诺：

* 及时答复，确认收到你的报告
* 为解决漏洞提供一个估计的时间框架
* 当漏洞被修复时通知报告个人

我们认真对待安全问题，并将迅速作出回应，以解决可验证的安全问题，然而，我们的一些产品是复杂的，可能需要一些时间来更新。

**补偿**

虽然我们赞赏独立安全研究人员所做的工作，但我们不提供报告安全漏洞的补偿。任何要求赔偿的行为都将被视为违反上述条件。在这种情况下，Coupa保留其所有的法律权利。