//Mozilla Security Bug Bounty Program是Mozilla的2004年开始的漏洞举报奖励制度，谷歌也于2010年初启动的Chrome浏览器Bug报告奖励计划

一般奖励说明：

Mozilla会奖励发现各客户端与服务的漏洞，细则如下：

- 安全漏洞必须是之前未被发现的
- 安全漏洞必须是属于被远程利用的
- 提交者不能是有漏洞的代码的作者或贡献者
- Mozilla员工不算数

如果您是出于工作目的参与了Mozilla代码的研究，我们希望您不要申请奖励，我们会很感激，因为基金总数是有限的，我们希望把机会留给其他无偿参与Mozilla项目的人。
Mozilla有权取消有损用户利益的申请者的奖励权利。
如果多人同时申请同一个bug奖金平分。

客户端奖励说明：

高危漏洞提交者奖励现金3000美金+T恤一件，予以奖励的严重/高危漏洞必须满足下面的要求：

- 安全漏洞必须是主要产品的Mozilla公司发布的，最新开发版(i.e., Aurora, Beta or EarlyBird, and nightly mozilla-central releases)，或者Firefox, Thunderbird, Firefox for Android的正式版，或者可以使用户受这些产品损害的Mozilla服务
- 由第三方软件/插件，比如flash等，引起的安全漏洞不算数

更多关于该奖励制度的FAQ，

Web应用与服务奖励说明：

与Web应用/服务相关的的安全漏洞，我们会奖励至少500美金一个高位漏洞，至多3000美金一个极其严重的安全漏洞，外加一件T恤。
预计奖励的高危/严重安全漏洞的要求如下：

- 划定为Web应用的安全漏洞必须满足Web Application Security Bounty FAQ的界定
- 安全漏洞属于奖金奖励Sites名单中，查看Web Application Security Bounty FAQ中的合格bug部分关于具体Sites名单。

更多信息查看Web Application Security Bounty FAQ，

提交方法：

//文件化bug，
邮件通知Mozilla安全组，
下面省略不翻译了