**Hardening Web Applications Using a Least Privilege DBMS Access Model**

**摘要翻译**

**20152180 王帆 15-计算机1班**

**ABSTRACT**

Within the last three years hundreds of millions of private data records have been compromised in high-profile data breaches, resulting in billions of dollars in economic losses and unrecoverable loss of privacy. One commonality is that attackers obtained administrative-level access to records on a central database. We argue that the widespread practice of highest privilege design and configuration is a significant contributor, where users and applications are given the highest level of privilege needed to execute the union of all needed tasks. One problematic common practice is, in a web-based application, for front-end and middleware processes to have root privileges to the complete DBMS back-end database. This practice is in stark opposition to the well-known secure design principle of least privilege introduced 40 years ago. Enforcing least privilege at all levels of a web application would help prevent future all-lost cyber-compromises. Here we introduce Hierarchical Policy (HPol), a formal access control modeling tool used in modeling web application database security.

**摘要**

在过去三年中，数以千计的私人数据记录在频发的数据泄露问题中受到影响，这已导致约数十亿美元的经济损失和无法估量的个人隐私问题。这些问题的共同点，是攻击者获得了对中央数据库记录的管理员级别访问权限。我们认为，最高权限设计和配置的广泛实践是一个关键问题，其中，用户和应用程序被赋予执行所有任务所需的最高级别的权限。在基于Web的应用程序中，一个常见的且具有争议性的做法是授予前端与中间件进程完整的数据库管理系统的root权限。这种做法，同40年前著名的最低特权安全设计原则完全相悖。在Web应用程序的各层级实施最低权限，将有助于防止潜在的网络攻击。这里，我们介绍一种用于Web应用程序数据库安全性建模的通用访问控制工具——分层策略（HPol）。