

文章编号: 1000-5013(2007) 04-0382-03

OLAP 安全访问的层次化设计与实现

蔡榆榕, 陈维斌

(华侨大学 现代教育技术中心, 福建 泉州 362021)

摘要: 由于任何浏览 Web 站点的访问者都可以通过 HTTPS 使用联机分析处理(OLAP)数据源, 因此, 访问者的安全凭据是必需的. 针对 OLAP 的安全访问, 提出层次化设计方案, 通过给出分组实例程序, 阐述运用网上办公组件(Office Web Component, OWC)中的自行定制分组功能, 使各个级别的分析用户只能访问与自己相关的数据, 屏蔽与分析用户不相关的数据源. 对 OWC 组件的安全漏洞的威胁提出预防措施, 从而提高基于 Web 的 OLAP 访问的安全性.

关键词: 联机分析处理; 多维数据集; 网上办公组件; 安全访问

中图分类号: TP 393. 08 文献标识码: A

联机分析处理(Online Analytical Processing, OLAP)的安全性, 是指控制对分析服务器(Analysis Services)管理的数据进行访问. 对于获许通过分析管理人员(Analysis Manager)访问分析服务器数据和执行管理功能的管理员, 可以对其加以限制. 对于那些通过客户应用程序访问分析服务器上数据的最终用户, 同样可以进行限制, 可以指定哪些最终用户能访问数据, 以及他们能执行哪些类型的操作. 另外, 可以控制最终用户在各种分析服务器数据级别上的访问, 包括多维数据集、维度和多维数据集单元^[1-2]. 文中以网上评教及 OLAP 分析系统为例, 对用户可进行的 OLAP 操作作了分层、分级别的设定.

1 层次化安全体系的实现技术

本系统 OLAP 安全性的级别与提供的 OLAP 操作和操作人员, 如表 1 所示. 一般情况下, 可通过分析管理人员设置数据库角色或多维数据集角色, 直接实现用户访问数据视图权限的分层分级限制. 但是在本系统中, 分析客户端的登录用户并不等同与角色所对应的用户, 而出于对 Web 服务器安全性的考

表 1 OLAP 安全性级别与提供的 OLAP 操作和操作人员

Tab. 1 OLAP security level and relevant operators

| OLAP 安全性 | 可进行的 OLAP 操作 | 操作人员 |
|----------|---------------------------|-----------------|
| 管理员级别 | 对服务器上所有多维数据集和维度具有完全读取权限 | 教学管理的系统分析员 |
| 服务器级别 | 与评教数据有关的所有数据库数据分析 | 学校教学管理决策层 |
| 数据库级别 | 对评教数据库有关的多维数据集和维表具有完全读取权限 | 负责教学质量评估工作的教务人员 |
| 维度级别 | 可对与本院系有关的评教数据进行操作分析 | 人事管理部门或某院系 |
| 单元级别 | 与本人有关的数据进行分析比较 | 教师 |

虑, 又不可能允许一般管理用户直接在浏览器端对服务器进行操作. 因此, 方法缺少灵活性, 尤其是无法在客户端进行增加或删除管理用户, 必须要由系统管理员在分析服务器上进行操作. 利用 OWC 组件, 通过 Web 编程, 建立客户端浏览器登录用户与 OLAP 服务器角色之间的映射关系, 直接在浏览器中为管理用户提供角色权限指定的界面及操作. 具体有如下 5 个步骤. (1) 根据用户的分析级别, 创建分析服务器上的用户帐号和指定相应的角色. 分析服务器根据 Windows 用户帐户实现多维数据集的安全角色, 在服务器上创建 1 个或多个本地 Windows NT 用户帐户, 并将它们分配给 1 个 SQL Server

数据库角色. 然后, 将该数据库角色分配给多维数据集角色, 并为其分配特定的多维数据集^[1]. (2) 将客户分析端登录的用户根据分析级别进行归组, 建立用户到用户组的映射表. (3) 建立客户端用户组与分析服务器用户之间的映射表, 实现浏览器端到服务器端的用户转换. (4) 客户端浏览器登录用户与 OLAP 服务器角色之间的绑定. 由于多维数据集角色本质上继承了 Windows NT 用户 ID 与密码凭据. 将上面得到的用户 ID 与密码凭据添加到 OLAP 数据源连接字符串中, 就实现了客户端浏览器登录用户与 OLAP 服务器角色之间的绑定. 1 个 OLAP 数据源可能包含多个多维数据集. 通过将 OWC 组件中的 PivotTable 控件的< DataMember> XML 标记值设置为有效的多维数据集名称, 可以连接到特定的多维数据集, 给该多维数据集分配的角色必须对应于 OLAP 数据源连接字符串中的凭据^[3]. 以表 1 中的维度级别为例, 人事处的教师管理人员需要对各教师的评教情况进行分析, 因此, 必须保证最后绑定的角色对以教师职称、教龄等为维度的多维数据集具有访问权限, 同时将 OWC 的 PivotTable 控件的< DataMember> XML 标记值设置为相应的多维数据集名称, 相关代码如下:

```
Dim strOLAPConn As String = _
ConfigurationSettings.AppSettings("OLAPConnectionString")
objPT.ConnectionString = strOLAPConn
objPT.DataMember = "teacher"
//指定要访问的多维数据集
```

(5) 通过创建定制分组屏蔽其他数据访问. 通常当报表按照 college 字段来对评教各指标得分分组时, 院系依照各成员分组. 如果在定制的报表中限制用户只能访问与自己相关的数据, 可以使用 OWC 的 V10 控件^[3] 中的定制分组功能. 其实现方法是, 通过调用一个 JavaScript 函数, 使用 UseCustomGrouping Web 方法. 输入参数为当前加载的项目的 XMLData. 此 Web 方法将加载一个 PivotTable 控件并调用 UseCustom GroupField 方法定义定制分组.

现以某院系教学管理人员的分析为例. 在这里, 只允许访问本院系和其他院系平均综合指标的数据, 即添加一个到两个成员("mycollege", "othercollege") 的定制分组以涵盖全部的院系成员. 调用 AddCustomGroupMember 方法以添加上述的定制成员. 当 Web 页面上的函数执行时, ChartSpace 控件可以自动将定制分组功能反映到条形图表中——这也是使用 OWC 的优点. 即将其他院系作为一个成员, 本院系作为一个成员, 相关代码^[4] 如下:

```
< WebMethod() > Public Function UseCustomGroup( ByVal _
strReportXMLData As String, collegename as string) As String
Dim m_xml As String
Dim objPT As PivotTableClass = New PivotTableClass
Dim objPTView As PivotView
Dim fscollege As PivotFieldSet
Dim fscollegigroup As PivotField

Try
objPT.XMLData = strReportXMLData
objPTView = objPT.ActiveView\设置学院变量
fsTime = objPTView.FieldSets("college") \将组' group1' 添加到学院字段中
fscollegigroup.AddCustomGroupField("CustomGroup1", "CustomGroup1", "college")
fscollegigroup.AddCustomGroupMember ( fscollege.Member..Name, _
New Object() {"collegename"}, "mycollege")
fscollegigroup.AddCustomGroupMember( fscollege.Member..Name, _
New Object() {"college1", .., "collegem"}, "othercollege") \ 不允许用户展开' 学院' 的组成员
fscollegigroup.Expanded = False
m_xml = objPT.XMLData
objPT = Nothing
```

⋮
End Function

2 OWC 组件的安全漏洞和预防措施

OWC 的安全漏洞主要包括以下 3 方面。(1) 能够让黑客读取受害用户的本地文件。(2) 即使脚本功能被禁用的情况下也能运行脚本,同时还能让黑客看到剪贴板的内容。(3) 在处理.xls 和.xla 文件组合时存在问题,其 Spreadsheet 组件的 Host() 函数中存在 1 个漏洞可用以写任意文件,通过嵌入包含=host().saveas(“arbitraryfilename”)形式的代码到 Spreadsheet 对象,远程攻击者可以利用这个漏洞在目标用户系统中建立任意文件^[5]。而上述 3 方面的恶意攻击,都要求攻击者必须直接登录服务器。

由于目前还无法得到微软关于这几个安全漏洞的补丁,暂时可以从以下两方面来进行防范。(1) 在 Web 服务器端加强 Web 服务的身份认证,拒绝攻击者直接登录服务器,使恶意脚本无法在浏览器端因为运行 OWC 组件而读取分析用户的本地文件,防止攻击者在分析用户的系统中建立任意文件。(2) 由于 OWC 组件的安全漏洞主要集中在 Spreadsheet 组件的 Host(), Copytext, List 等函数中,因此在分析页面中,尽量避免运行该组件,将 Pivottable 中的分析报表通过分析日志文件动态生成分析表,绑定到其他数据库服务器控件,如 Datagrid, Datalist 等,实现分析报表的显示和输出,从而降低其组件运行带来的安全威胁。

3 结束语

本文以网上评教及 OLAP 分析系统为例,通过建立浏览器端到 OLAP 服务器端的用户映射关系,提出了基于 Web 的 OLAP 安全访问的层次化设计方案,并结合运用 OWC 组件,实现了各分析用户按其功能级别与相应的多维数据集的捆绑。通过采用上述安全性措施,在保证分析服务器及评教数据源安全性的前提下,可以更加灵活地对用户指派角色,同时,对 OWC 组件的安全漏洞采取了一定的预防措施,减少了系统的安全隐患,从而达到提高基于 Web 的 OLAP 访问安全性的目的。

参考文献:

[1] GUNDERLOY M. SQL Server 开发指南——OLAP(联机分析处理)[M]. 张伟,等译. 北京:电子工业出版社, 2001: 45-53.
[2] 汤姆森. OLAP 解决方案——创建多维信息系统[M]. 2 版. 朱建秋,译. 北京:电子工业出版社, 2004: 8-10
[3] 唐贤伦, 张学旺. OWC 组件在 Web 图表统计中的应用[J]. 计算机应用, 2003, 23(S2): 437-438
[4] 东方人华. SQL Server 2000 与 Visual Basic. NET 数据库入门与提高[M]. 北京:清华大学出版社, 2002: 159-176
[5] 王大印, 刘在强, 姜中华. Windows 安全漏洞与黑客防范[M]. 北京:电子工业出版社, 2005: 151-166.

The Layer Design and Realization of OLAP Security Visit

CAI Yurong, CHEN Weibin

(Centre of Modern Education and Technology, Huaqiao University, Quanzhou 362021, China)

Abstract: Because any interviewer can use online analytical processing (OLAP) data source through HTTPS, therefore the interviewer authentication is necessary. Aiming the OLAP, the layer design scheme is proposed. Thought proposing the grouping example program, the authors elaborate the function of ordering grouping by oneself using office web component (OWC) which made each level operator only can visit the relevant data himself and shield unrelated data. In addition, some protective measures about OWC security holes are given to improve the OLAP security visit.

Keywords: online analytical processing; multi-dimension data; office Web component; security visit

(责任编辑: 黄仲一)