Queryهای آماده و برنامه های ذخیره شده

ما طراحی منطقی و فیزیکی را بررسی کرده ایم. اکنون زمان آن رسیده تا از دیتابیس داده بگیریم. روش های انجام این کار چه هستند؟

توضیحات

روش ها و فن آوریهایی برای انتشار query وجود دارند (به عنوان مثال ,LINQ ,Hibernate). بدون توجه به روش انتخابی مهم است که اطمینان حاصل کنید که وضعیت های query شما در مقابل حمله های SQL Injection ایمن و قابل استفاده مجدد می باشند. انتشار query آماده یا فراخوانی های برنامه ی ذخیره شده یک راه طولانی در تکمیل این اهداف می باشند.

مثال زیر یک وضعیت آماده را در مقابل یک وضعیت غیرآماده قرار می دهد.

به query مربوط به برنامه ی زیر توجه کنید.

```
// Get a connection to SQL Server 2005
Class.forName("com.microsoft.sqlserver.jdbc.SQLServerDriver");
conn = DriverManager.getConnection(connectionUrl);

// Via the connection, mimic user requests by looping through the table
// and retrieving rows 1 at a time up to 20 rows;
// SalesOrderHeader id's start at 43659
for (int id = 43659; id < 43679; id = id + 1) {

    // Get the id and execute the query
    SQL = "SELECT c.FirstName, c.LastName, oh.SalesOrderID, "
        + "oh.OrderDate, oh.DueDate, oh.TotalDue "
        + "FROM Sales.SalesOrderHeader oh "
        + "JOIN Person.Contact c on c.ContactID = oh.ContactID "
        + "WHERE SalesOrderID = " + id;

    stmt = conn.createStatement();

    // Execute the query
    rs = stmt.executeQuery(SQL);
```

این query غیرآماده برنامه ی حافظه ی پنهان را با تعداد زیادی query های مجزا پر می کند، مانند زیر:

	usecounts	cacheobjtype	objtype	text
1	1	Compiled Plan	Adhoc	
2	1	Compiled Plan	Adhoc	found in the procedure cache -- select qs.usecounts, cacheobjtype, objtype, qt.text
3	2	Parse Tree	View	
4	2	Parse Tree	View	ET(TABLE FNGETSQL, @handle)
5	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43659
6	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43660
7	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43661
8	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43662
9	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43663
10	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43664
11	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43665
12	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43666
13	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43667
14	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43668
15	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43669
16	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43670
17	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43671
18	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43672
19	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43673
20	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43674
21	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43675
22	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43676
23	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43677
24	1	Compiled Plan	Adhoc	Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = 43678

نگران کننده تر در مورد عبارت WHERE این است که query هایی شبیه به این برای تزریق SQL بسیار کامل می باشند. از طریق UI یک یوزر زیرک می تواند به طور بالقوه به عبارات SELECT, DELETE, INSERT, or UPDATE متوسل شده تا اینکه یک رشته ورودی متغیر منجر به یک شکاف امنیتی شدید می شوند.

اکنون به query دقت کنید که مانند یک عبارت آماده به شکل زیر نوشته شده است:

```
// Get a connection to SQL Server
Class.forName("com.microsoft.sqlserver.jdbc.SQLServerDriver");
conn = DriverManager.getConnection(connectionUrl);

// Via the connection, mimic user requests by looping through the table
// and retrieving rows 1 at a time up to 20 rows;
// SalesOrderHeader id's start at 43659
 for (int id = 43659; id < 43679; id = id + 1) {
   // Create and execute a PREPARED SQL statement that returns some data
   // Get the id and execute the query
   SQL = "SELECT c.FirstName, c.LastName, oh.SalesOrderID, "
         + "oh.OrderDate, oh.DueDate, oh.TotalDue "
         + "FROM Sales.SalesOrderHeader oh "
         + "JOIN Person.Contact c on c.ContactID = oh.ContactID "
         + "WHERE SalesOrderID = ?";

   // prepare the statement with the integer value we want to find
   stmt = conn.prepareStatement(SQL);
   stmt.setInt(1, id);

   // Execute the query
   rs = stmt.executeQuery();
```

Query آماده ابتدا یک برنامه ی اجرایی دریافت میکند، اجرا می کند، و همه ی اجراهای بعدی مجددا از این برنامه استفاده می کنند. به علاوه پتانسیل برای تزریق SQL Server به شدت کاهش می یابد.

	usecounts	cacheobjtype	objtype	text
1	1	Compiled Plan	Adhoc	
2	2	Parse Tree	View	
3	1	Compiled Plan	Adhoc	qs.plan_handle) as qt order by qt.text
4	20	Compiled Plan	Prepared	rderHeader oh JOIN Person.Contact c on c.ContactID = oh.ContactID WHERE SalesOrderID = @P0
5	2	Parse Tree	View	PENROWSET(TABLE FNGETSQL, @handle)

از آنجایی که برنامه های حافظه ی پنهان (cache) در حافظه ذخیره شده اند، مشاهده ی چگونگی کاهش در حافظه ی برنامه ی شما آسان می باشد.

برنامه های ذخیره شده همچنین می توانند به همراه یا به جای query های آماده استفاده شوند تا دسترسی به داده ی منطقی و انتزاعی را خارج از برنامه، فشرده کنند (encapculate). مزیت این دیدگاه این است که به توسعه دهنده ی دیتابیس آزادی می دهد برای ایجاد تغییرات ساختاری در دیتابیس بدون اینکه نگران شکست برنامه باشد. نظریه مطرح شده در اینجا این است که ورودی های برنامه ی ذخیره شده و خروجی query منسجم هستند و ویژگی های دسترسی به داده برای برنامه ناشناخته است. به علاوه برنامه نباید به همه ی مراجع مربوط به جدول یک دیتابیس اختصاص داده شود که ممکن است در ساختار تغییر کرده باشد.

آدرس آموزشگاه : تهران - خیابان شریعتی - بالا تر از خیابان ملک - جنب بانک صادرات - پلاک 651 طبقه دوم - واحد7

88146323 - 88446780 - 88146330

http://www.tahlildadeh.com/