SQL Serverでどーんといってみよう!

必ず役立つ現場のノウハウ

百田 昌馬
HYAKUTA, Shoma
Supported by 松本 美穂
http://www.ittraining.jp/

第5回 SQLインジェクション対策（ASP＋ADO編）

Level

1 2 **3** 4 5

Technology Tools

- ☑ Visual Basic
- ☐ Visual C#
- ☐ Visual C++
- ☑ SQL Server
- ☐ Oracle
- ☐ Access
- ☐ ASP.NET
- ☑ Other:
  - MSDE
  - Visual Studio 6.0

Samples

SQLインジェクションとは？

価格.comとOZmall、不正アクセスの被害にあった両サイトは、いずれも「SQLインジェクション」攻撃によるものだった。どちらもASP（Active Server Pages）によるWebサイトであり、バックエンドのデータベースサーバーにはSQL Serverを利用していたと言われている。したがって、データベースAPIには、ADOを使っていた可能性は非常に高いだろう。

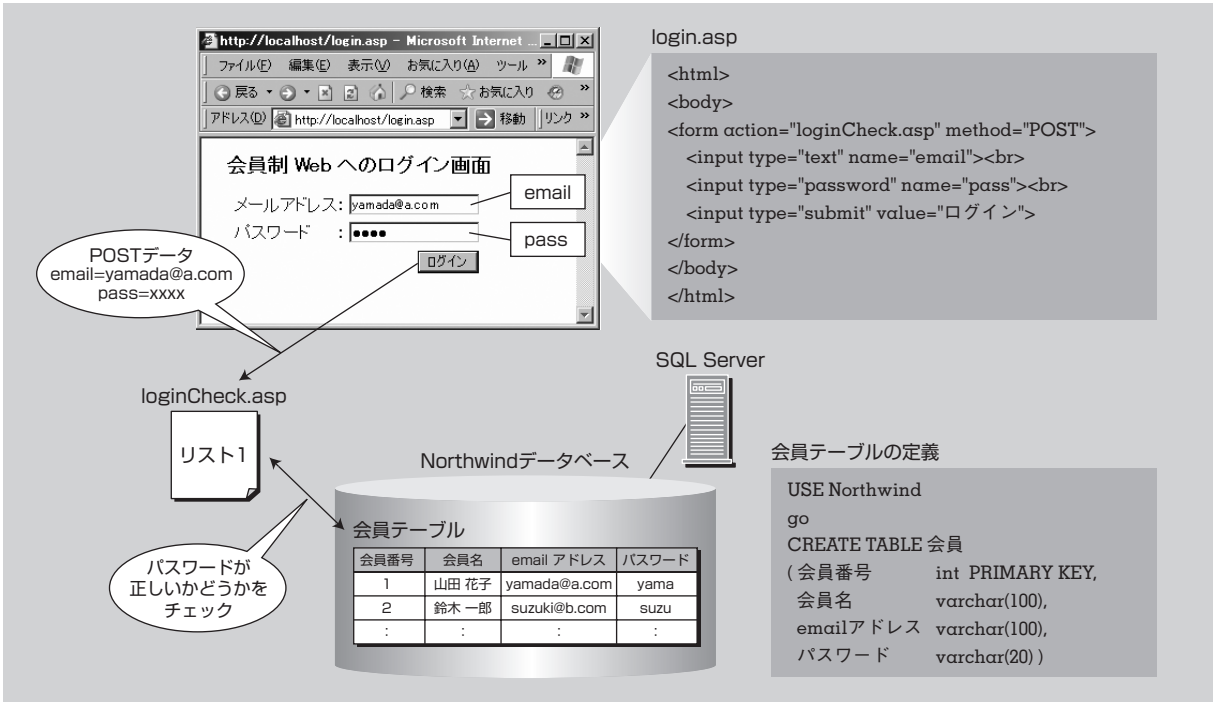
SQLインジェクションは、「ダイレクトSQLインジェクション」や「SQLコマンドインジェクション」とも呼ばれる。インジェクション（injection）は「注入」という意味である。この攻撃は、クエリ文字列（Query String）やPOSTデータに悪意のあるSQL文を埋め込んで不正に発行するという手法である。これを使えば、UNION SELECT文を埋め込んで顧客情報を入手したり、OR条件を追加して会員制のWebサイトに不正にログインしたり、OSコマンドを実行するための拡張ストアドプロシージャ「xp_cmdshell」を使ってOSを操作するといったことも可能になる。

SQLインジェクション対策を怠ると、企業の存続に関わる大きなダメージになりかねないので、しっかりと対策しておくべきである。

SQLインジェクションの具体的な攻撃手法

ここでは、図1のASPアプリケーションを例にSQLインジェクションを使った具体的な攻撃方法を説明する。このアプリケーションは、会員制のWebサイトにおけるログイン認証を想定したもので、試し

図1：会員制Webサイトのログイン画面



リスト1：ログイン認証（パスワードのチェック）

```
<%
' POSTで受け取ったメールアドレスとパスワードの取得
email = Request.Form("email")
pass = Request.Form("pass")

' Northwindデータベースへの接続
Set cn = Server.CreateObject("ADODB.Connection")
cn.Open "Provider=SQLOLEDB;" _
        & "Data Source=(local);" _
        & "Initial Catalog=Northwind;" _
        & "Integrated Security=SSPI;"

Set rs = Server.CreateObject("ADODB.Recordset")

' パスワードが正しいかどうかをチェック
rs.Open "SELECT 会員番号 FROM 会員 " _
        & " WHERE emailアドレス='" & email & "'" _
        & " AND パスワード='" & pass & "'", cn

If Not rs.EOF Then
   Response.Write "ログイン成功"
Else
   Response.Write "ログイン失敗"
End If

cn.Close
Set rs = Nothing
Set cn = Nothing
%>
```

やすくするために簡易構成にしている。

login.aspでは、ログイン画面（HTMLフォーム）を表示し、メールアドレスとパスワードを入力できるようにする。［ログイン］ボタンがクリックされると、「loginCheck.asp」が呼び出される。

loginCheck.asp（リスト1）では、SQL ServerのNorthwindデータベースへ接続し、あらかじめ作成しておいた「会員」テーブルに登録された会員情報を使ってメールアドレスとパスワードが正しいかどうかをチェックするようにしている。このチェックを行なうためのSQL文は、次のように文字列連結を使って動的に生成しているのがポイントである。

```
"SELECT 会員番号 FROM 会員 " _
& " WHERE emailアドレス='" & email & "'" _
& "   AND パスワード  ='" & pass & "'"
```