# Sql Injection

للكاتب: الحقباني
رابط الموضوع على منتديات الفريق العربي للبرمجة:
http://www.arabteam2000-forum.com/index.php?showtopic=201325

طبعاً لغة السكول مخصصه لتعامل مع قواعد البيانات حيث تمكنك من الاستعلام عن بيانات معينه او انشاء جدول وعلاقات بين الجداول .... الخ

راح ناخذ مثال بسيط برنامج لإدارة شؤون الموظفين طبعاً راح يكون في جدول لحسابات المستخدمين زي ماتقول موظفين قسم شؤون الموطفين هم الي عندهم صلاحيه انهم يدخلون على النظام (يعني ماهوب من هب ودب دخل على النظام) طبعاً اخونا محمد كلفوه يصلح هالنظام وتوه متخرج من الجامعه علوم حاسب من قده الله يحرسه من العين بس ماعنده الخبره الكافيه طبعاً انشأ جدول للمستخدمين مكون من حقلين الحقل الاول اسم المستخدم والحقل الثاني كلمة المرور

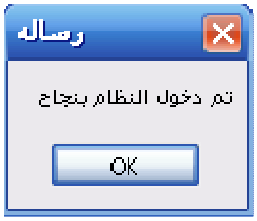
واضاف سجل في قاعدة البيانات للأختبار

اسم المستخدم: saleh

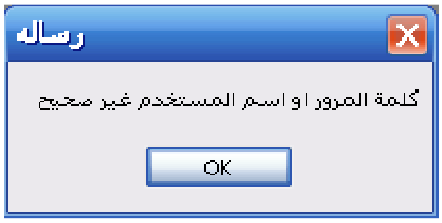
كلمة المرور :12345678

وصلح الواجهه الاول تطلب من المستخدم ادخال اسم المستخدم وكلمة المرور


طبعاً اذا ادخلت اسم مستخدم وكلمة مرور صحيحتان راح تطلع لك رساله تخبرك بان تم دخولك النظام بنجاح




اذا ادخلت اسم مستخدم او كلمة مرور غير صحيحه راح تطلع لك هالرساله (ياولد سكيورتي قوي)



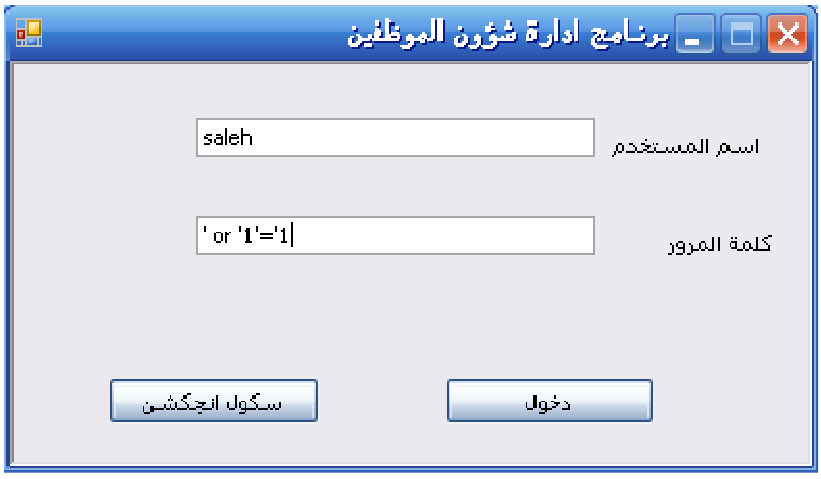

وفي يوم من الايام جانا هاك الهكرالي لاقبله ولا بعده في قسمنا وبدا يهايط ويتحدانا ويقول انه يقدر يدخل على النظام حقنا اذا عطيناه بس اسم مستخدم طبعاً ما صدقناه كيف والي مسوي النظام خوينا محمد خريج علوم الحاسب طبعاً عطيناه اسم مستخدم موجود عندنا من قبل وشغلنا النظام وطلعت لنا شاشة الدخول والتفتنا على خوينا الهكر وقلناله شف شغلك

بس بصراحه ياجماعه طلع هكر من جد شفت عجب العجاب

في خانة اسم المستخدم كتبSaleh:

في خانة كلمة المرور كتب:

‘ or ‘1’=’1




وضغط على دخول وبالفعل دخل على النظام وين السكيورتي حق اخونا محمد طلع فشنك

وبدا خوينا الهكر يتكلم عن السكول انجكشن ومكان الخلال في كود خوينا محمد

طبعاً كود ابو شباب كان مكتوب بشكل هذا

```
OleDbCommand cmd = new OleDbCommand("select * from users where
username='"+****Box1.****+"' and
password='"+****Box2.****+"'", conn);
```

طبعاً لو ان كلمة المرور او اسم المستخدم غير صحيحه ماراح يرجع لك الاستعلام اي شي

طيب نشوف شكل الاستعلام بالبيانات الصحيحه راح يكون بشكل هذا

```
Select * from user where username =’saleh’ and password
=’12345678’
```

الاستعلام صحيح وراح تطلع لك بيانات صالح

خوينا الهكر طلع ذكي من جد استفاد من الـ Or

True or false = true

طبعاً هو مايعرف كلمة المرور

```
Select * from users where username=’saleh’ and password=’’ or
‘1’=’1’
```

طبعاً هو ما ادخل كلمة مرور خالها فارغه بس الزياده الي سواه خلت الباسورد كأنه صحيح

وهذا مايسمى (بسكول انجكشن)

اطبعاً الدوت نت تغلبت على هذه المشكله باضافة بارامتر للكوماند

انظر للكود التالي (مافيه سكول انجكشن):

```
OleDbConnection conn = new
OleDbConnection("Provider=Microsoft.Jet.OLEDB.4.0;Data
Source=db1.mdb");



            OleDbCommand cmd = new OleDbCommand("select * from users
where username=@v2 and password=@v1", conn);
```

```
cmd.Parameters.AddWithValue("@v2", ****Box1.****);
cmd.Parameters.AddWithValue("@v1", ****Box2.****);
```

سابقاً البيانات المدخله من قبل المستخدم تعتبر كجزء من الـquery

وهاذي قصة خوينا محمد مع الهكر

ارجوا ان اكون قد وفقت في سرد القصه التي من نسج خيالي لكي اضفي عالموضوع شي من الدعابه والمرح

تحميل مشروع السكول انجكشن(sql injection)

رابط الموضوع بموقعي