**SQL injection**

**اطلاعات پايه:**   
مربوط به بخش **Database** وب سايت هست   
هر جايي که ما فيلد داريم قطعا از پايگاه داده براي حفظ و نگهداري اطلاعات وارد شده استفاده ميشه ...  
همين باعث ميشه که فراگيري اين باگ از همه بيشتر باشه ... چون حتي کوچکترين وب سايت هايي که تنها از فيلد عضويت استفاده ميکنه هم ممکن هست اين باگ را داشته باشه ... تـا برسه به بزرگترين پايگاه داده ها شامل مهمترين اطلاعات افراد .  
  
ميزان گسترش و نفوذ پذيـري : **بسيار بالا**  
ميزان استفاده هکر ها از باگ : **بسيار بالا**  
  
**اهداف استفاده:**

اهداف ميتوانند متفاوت باشند .از بدست آوردن اطلاعات خصوصي افراد و سوء استفاده از آن (مانند سوء استفاده مالي از کارت هاي اعتباري) تـــا بدست آوردن username و password مديريت و نفوذ به سايت و ديفـــــيس (تغيير چهره)

**غالبا هم براي ديفيس ازش استفاده ميشه** .

این باگ از اشتباهات برنامه نویسان وب و صفحه هات وب به وجود میاد.

در SQL دیتابیس های زیادی هست که از مشهورترین آنها میشه به :

MySQL , MsSQL , oracle , MsAccess

inurl:news\_more.php?id=

تست آسیب پذیری:

سایت بدون هیچ تغییری لود میشه--------- باگ ندارد

صفحه سفید یا سیاه ظاهر شود -------- باگ دارد

یک عکس لود نشود و بقیه صفحه کامل لود شود------- باگ دارد

تغییر قسمتی از نوشته سایت ------ باگ دارد

پس نتیجه میگیرم هر تغییری در ظاهر سایت هرچند کوچک نشان از داشتن باگ sql است

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\'' at line 1