پیش نویس:

امنیت پایگاه‌های داده یکی از مهم‌ترین دغدغه‌های سازمان‌ها و شرکت‌ها در عصر دیجیتال است. با توجه به حجم بالای اطلاعات و داده‌هایی که در پایگاه‌های داده ذخیره می‌شوند، هرگونه نقض امنیتی می‌تواند عواقب جبران‌ناپذیری برای یک سازمان به همراه داشته باشد. یکی از رایج‌ترین پایگاه‌های داده‌ای که در بسیاری از سازمان‌ها و کسب‌وکارها مورد استفاده قرار می‌گیرد، SQL Server است. با وجود محبوبیت و قدرت بالای SQL Server، این پایگاه داده نیز در برابر تهدیدات مختلف امنیتی آسیب‌پذیر است. این تهدیدات می‌توانند شامل حملات دسترسی غیرمجاز، سوءاستفاده از نقص‌های نرم‌افزاری، و ضعف در پیکربندی‌های امنیتی باشند.

استانداردهای مرکز امنیت اینترنت (CIS) به عنوان یکی از معتبرترین منابع برای ایمن‌سازی سیستم‌ها و پایگاه‌های داده، مجموعه‌ای از دستورالعمل‌ها و بهترین شیوه‌ها را ارائه می‌دهند که به کمک آن‌ها می‌توان از امنیت بالاتری در برابر تهدیدات مختلف اطمینان حاصل کرد. استانداردهای CIS به طور خاص در زمینه‌های مختلف مانند پیکربندی‌های امن، دسترسی‌ها، رمزنگاری، و نظارت امنیتی برای پایگاه‌های داده مختلف از جمله SQL Server ، توصیه‌های مفیدی دارند.

با این حال، پیاده‌سازی این استانداردها در سیستم‌های SQL Server می‌تواند پیچیده و زمان‌بر باشد. در این راستا، نیاز به ابزاری کارآمد و جامع احساس می‌شود که پیاده‌سازی و نظارت بر استانداردهای CIS را به صورت خودکار و آسان انجام دهد. هدف این پروژه، طراحی و پیاده‌سازی ابزاری است که به صورت خودکار استانداردهای CIS را در SQL Server پیاده‌سازی کند و به سازمان‌ها کمک کند تا پایگاه داده‌های خود را در برابر تهدیدات مختلف مقاوم‌سازی کنند.

در ادامه در فصل 2 ، به بررسی آسیب‌پذیری‌های پایگاه های داده، معرفی و تحلیل استاندارد CIS پرداخته می‌شود، سپس ابزاری برای پیاده‌سازی این استاندارد در SQL Server طراحی و پیاده‌سازی خواهد شد. در نهایت، نتایج حاصل از استفاده از این ابزار بررسی و تحلیل خواهند شد. این تحقیق می‌تواند به بهبود امنیت پایگاه‌های داده SQL Server کمک کند و به عنوان مبنای مناسبی برای توسعه ابزارهای مشابه در دیگر سیستم‌های پایگاه داده عمل کند.

ساختار طبقه بندی هر ارزیابی بر اساس نحوه پیاده سازی:

|  |  |
| --- | --- |
| کد ارزیابی | نحوه ارزیابی |
| 0 | این نوع باید بصورت دستی کنترل شود و پرسمان ندارد |
| 1 | یک ردیف با چند ستون که مقادیر آن باید 0 یا 1 باشند |
| 2 | هیچ مقداری نباید برگردانده شود |
| 3 | مقدار برگشتی باید از مقدار ثابتی بزرگتر باشد |
| 4 | مقدار برگشتی شامل چند ردیف است که مقادیر خاصی باید در آن وجود داشته باشد. |
| 5 | مقدار برگشتی نباید یک مقدار ثابت باشد |
| 6 | یک یا چند ردیف که نباید مقدار یکی از فیلدهایشان یک مقدار ثابت یاشد. |
| 7 | یک یا چند ردیف که باید مقدار یکی از فیلدهایشان یک مقدار ثابت یاشد. |

ساختار طبقه بندی هر امن سازی بر اساس نحوه پیاده سازی:

|  |  |
| --- | --- |
| کد امن سازی | نحوه امن سازی |
| 0 | این نوع باید بصورت دستی کنترل شود و پرسمان ندارد. |
| 1 | پرسمان از نوع ساده. |
| 2 | کاربر باید با توجه به مقادیری که در پرسمان ارزیابی برگردانده میشود، مقداری را در پرسمان مقاوم سازی واردکند. (مانند username ، login\_name) |

پیکربندی و ورودی اطلاعات  
فایل ورودی اطلاعات در این برنامه .csv نام دارد که ساختار آن مطابق با جدول 1 است.

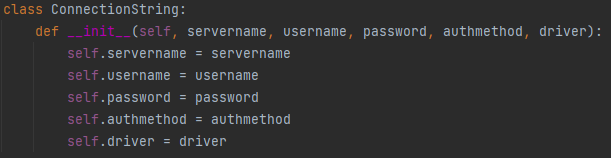
ساختار فایل csv:

|  |  |  |
| --- | --- | --- |
| ردیف | نام ستون | توضیحات |
| 0 | No. | شماره ردیف |
| 1 | Index | شماره امن سازی بر اساس دسته بندی CIS |
| 2 | Dsc | توضیحات |
| 3 | AuditQuery | پرسمان ارزیابی |
| 4 | AuditType | نوع پرسمان ارزیابی |
| 5 | ReturnNumbers | تعداد مقادیر برگشتی |
| 6 | Val1 | مقدار برگشتی 1 |
| 7 | Val2 | مقدار برگشتی 2 |
| 8 | Val3 | مقدار برگشتی 3 |
| 9 | RemType | نوع پرسمان امن سازی |
| 10 | numberOfTransitions | تعداد ترنزاکسن ها |
| 11 | ReplacementName | نام متغییر جایگزین |
| 12 | Tsql1 | ترنز اکشن 1 |
| 13 | Tsql2 | ترنزاکشن 2 |
| 14 | Tsql3 | ترنز اکشن 3 |
| 15 | title | عنوان |

جدول 1: ساهتار فایل

ساختار کلاس ها:

کلاس ConnectionString :  
در شکل 1-4مشخصات این کلاس مشاهده میشود، هر نمونه از این کلاس در واقعا اطلاعات مربوط به نام دیتابیس و نام کاربری و روش ورود را نگه داری میکند.



شکل 1-4

کلاس Login :

مشخصات این کلاس را در شکل 2-4 مشاهده میشود. این کلاس برای ساخت فرم ورود استفاده می‌شود.



شکل 2-4