

به نام خدا

دانشجو: محمد مهدی رضائی

نام استاد: میثاق یاران

موضوع: امنیت در پایگاه داده (مورد تایید افتا و پدافند)

امنیت پایگاه داده:

فرآیندی ضروری برای حفاظت از اطلاعات حساس در برابر دسترسی غیرمجاز، افشا، تغییر یا تخریب است. این کار شامل طیف گسترده‌ای از اقدامات امنیتی، از جمله کنترل دسترسی، رمزگذاری، ممیزی و پشتیبان‌گیری می‌شود، در حالی که تهدیدات به پایگاه‌های داده دائماً در حال تکامل هستند، اقدامات اساسی متعددی وجود دارد که می‌توانید برای محافظت از داده‌های خود انجام دهیم:

1- کنترل دسترسی را به طور موثر پیاده‌سازی کنید:

الف- احراز هویت قوی: از گذرواژه‌های قوی و منحصر به فرد برای همه حساب‌های کاربری استفاده کنید و از احراز هویت چند عاملی برای افزایش امنیت بیشتر استفاده کنیم.

ب- مجوزهای حداقل: به کاربران و برنامه‌ها فقط مجوزهای دسترسی به داده‌هایی را که برای انجام وظایفشان ضروری است، اعطا کنیم.

ج- اصل کمترین امتیاز: کاربران و برنامه‌ها را با کمترین سطح مجوز لازم برای انجام وظایفشان پیکربندی کنیم.

2- داده‌های خود را رمزگذاری کنید:

الف- رمزگذاری در حال سکون: داده‌های ذخیره‌شده خود را با استفاده از الگوریتم‌های رمزگذاری قوی مانند AES یا RSA رمزگذاری کنیم.

ب- رمزگذاری در حال انتقال: از TLS/SSL برای محافظت از داده‌ها در حین انتقال بین سرورها و برنامه‌ها استفاده کنیم.

3-از داده‌های خود به طور منظم پشتیبان‌گیری کنید:

الف-پشتیبان‌گیری منظم: از پایگاه داده خود به طور منظم و در مکانی امن پشتیبان‌گیری کنیم.

ب-بازیابی در برابر فاجعه: یک برنامه بازیابی در برابر فاجعه را برای بازیابی داده‌ها و سیستم‌های خود در صورت بروز حادثه تدوین کنیم.

4- به‌روزرسانی‌ها و وصله‌های امنیتی را اعمال کنید:

الف-نرم‌افزار پایگاه داده: به‌روزرسانی‌های نرم‌افزار پایگاه داده خود را به طور منظم نصب کنید تا از آخرین وصله‌های امنیتی بهره‌مند شویم.

ب-سیستم عامل و برنامه‌ها: سیستم عامل و برنامه‌های مرتبط با پایگاه داده خود را به‌روز نگه دارید.

5-از داده‌های خود به طور منظم پشتیبان‌گیری کنید.