**SQL Injection**

تزریق دستورات مخرب بر روی پایگاه داده می تواند خطرات و هزینه های زیادی به بار بیاورد.

هکرها می توانند توسط **SQL injection** اقدام به اجرا کردن دستورات تخریب گر بر روی دیتابیس یک سایت کنند تا بتوانند نقض های امنیتی شدیدی ایجاد کنند.

شیوه ی کار SQL injection یا تزریق دیتابیس به این صورت است که فرد مهاجم یا هکر در فرم های تعبیه شده بر روی وب سایت و در فیلدهایی که به جمع آوری اطلاعات کاربران می پردازد اقدام به ورود کدهای مخرب SQL می کند. پس از ورود اطلاعات توسط کاربر در این فرم ها ، کدهای مخرب عمل می کنند و به جای اجرای SQL اصلی، کدهای مخربی که مهاجمین وارد کرده اند اجرا می شوند. روش SQL injection به شیوه های مختلف بر روی سایت ها اجرا می شود و به نوع [سرویس هاست](https://www.bertina.ir/host) و پایگاه داده ی تعبیه شده بر روی وب سایت بستگی دارد. چرا که به طور عمده برخی از بانک های اطلاعاتی حساسیت هایی بر روی کاراکترهای خاص دارند که هکرها با شناسایی این مساله می توانند اقدام به تولید و ورود آنها به بخش های مختلف وب سایت کنند.

https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/