SQL盲注

什么是盲注

盲注就是在sql注入过程中，sql语句执行select之后，可能由于网站代码的限制或者apache等解析器配置了不回显数据，造成在select数据之后不能回显到前端页面。此时，我们需要利用一些方法进行判断或者尝试，这个判断的过程称之为盲注。

通俗的讲就是在前端页面没有显示位，不能返回sql语句执行错误的信息，输入正确和错误返回的信息都是一致的，这时候我们就需要使用页面的正常与不正常显示来进行sql注入。

盲注的分类

- 基于布尔类型的盲注
- 基于时间类型的盲注

利用盲注的前提条件

首先页面没有显示位（如果有显示位可以选择union联合查询），并且没有返回sql语句的执行错误信息。

盲注的优缺点

优点：不需要显示位和出错信息。

缺点：速度慢，耗费时间长（可以用到bp等工具）。

基于布尔类型的盲注