**Identifying the SQLi**

|  |  |  |  |
| --- | --- | --- | --- |
| SQLi Tests | Goal | Notes | Example Probes |
| **Reflected Output** | See whether or not the DB will perform / eval the operation we entered, or merely return our string input | Only works if our input is directly reflected onto the webpage (or returned somewhere in the HTTP response). | **Standard Eval**  <http://website.php?id=1+1>  Test if 1+1 evals to 2  **Wildcard**  [http://website.php?id=%](http://website.php?id=%25)  Causes a vuln site search to return all available results. |
| **Error based** | Attempt to get the server to return some sort of SQL related error by giving it input containing malformed SQL syntax. | Presence of an error tells us the server is trying to parse input as legitimate SQL syntax.  Also gives us extra information about the database through error msgs. | <http://website.php?id>=’  <http://website.php?id>= SELECT \* FROM \* |
| **Blind SQL** | Most of the time, output won’t be returned in the form of an eval / error.  Use of **sleep** command to get around lack of info. | **Sleep** tells the server to wait for a given amount of time before handling our request. |  |

**Escalating the attack**

^See cheat sheet bookmarks for more information.