Is Voyager susceptible to blind SQL injection vulnerabilities?

- **Product:** Voyager
- **Product Version:** 8.0.0

Question

Is Voyager susceptible to blind SQL injection vulnerabilities?

- A required security audit may flag the OPAC interface for this vulnerability
- A blind SQL injection is when a remote attacker uses a front-end interface to execute SQL commands on the back-end database, possibly leading to password retrieval, authentication bypass, unauthorized data access, or unauthorized data modification.

Answer

No.

SQL injection attacks are not possible within the Voyager system. Voyager uses pre-compiled SQL cursors, which are not dynamically parsed and no strings are sent back from WebVoyage (the Web interface) to the database (Oracle).

Any “command” which is entered as a parameter of a URL or in a search field is executed as the “subject” of a select query. The value and type of the user input is validated and only values expected by the application are allowed. Voyager uses stored procedures to abstract data access so that users do not directly access tables or views

Input is sanitized to the extent possible, given that some of the symbols are part of the search interactions and can not be sanitized

---

- **Article last edited:** 26-Nov-2013