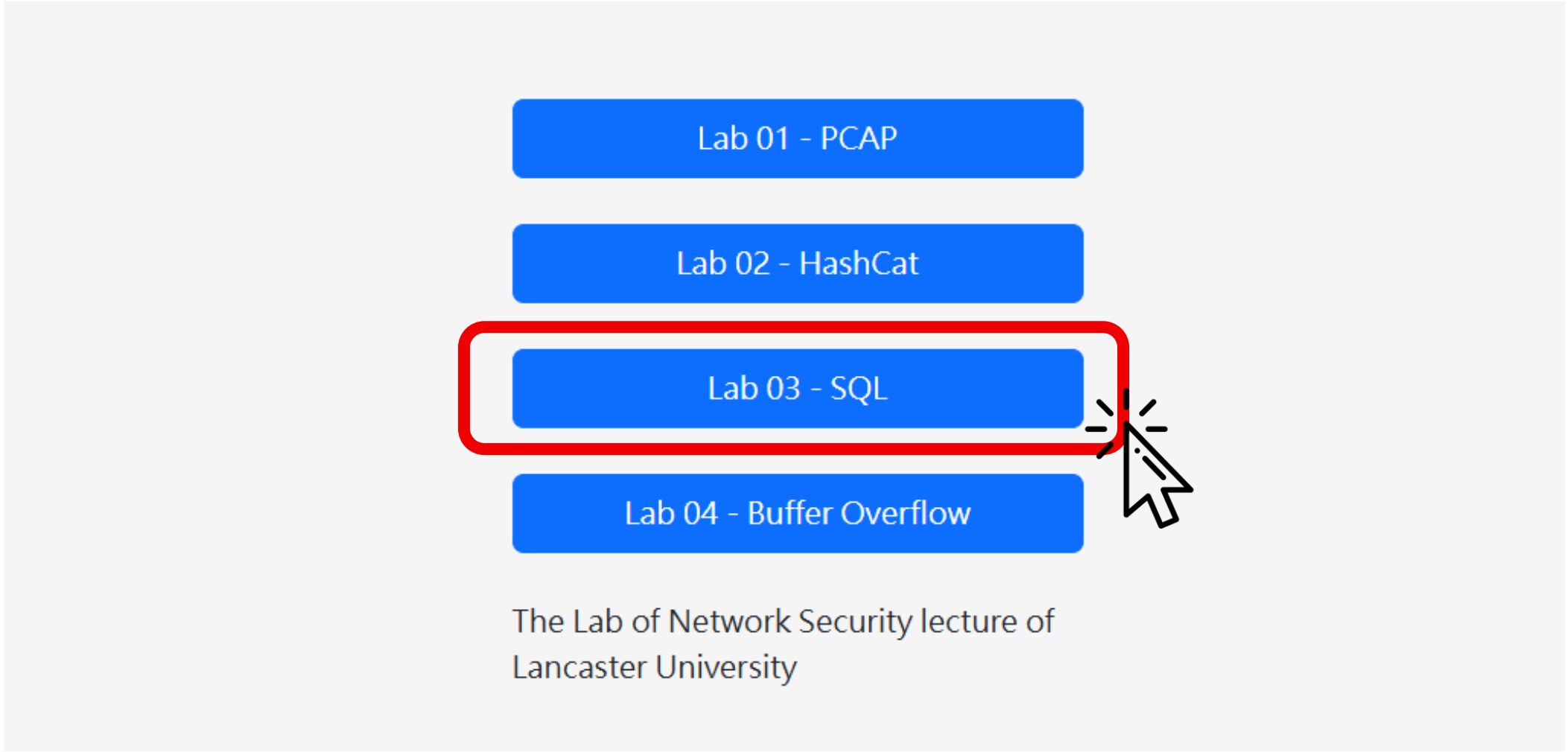
Lancaster University

Network Security Lab 03 Instruction

0. Open Lancaster.waynechiu.cc



1. Do some readings of SQL injection

WIKIPEDIA
The Free Encyclopedia

Search Wikipedia | Search

Donate | Create account | Log in | •••

SQL injection

41 languages

Article | Talk | Read | Edit | View history | Tools

Contents hide

Appearance hide

Text
- Small
- Standard
- Large

Width
- Standard
- Wide

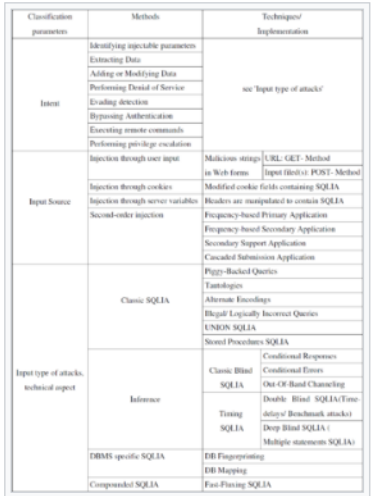
Color (beta)
- Automatic
- Light
- Dark

From Wikipedia, the free encyclopedia

In computing, **SQL injection** is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).[1][2] SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server. Document-oriented NoSQL databases can also be affected by this security vulnerability.[3]

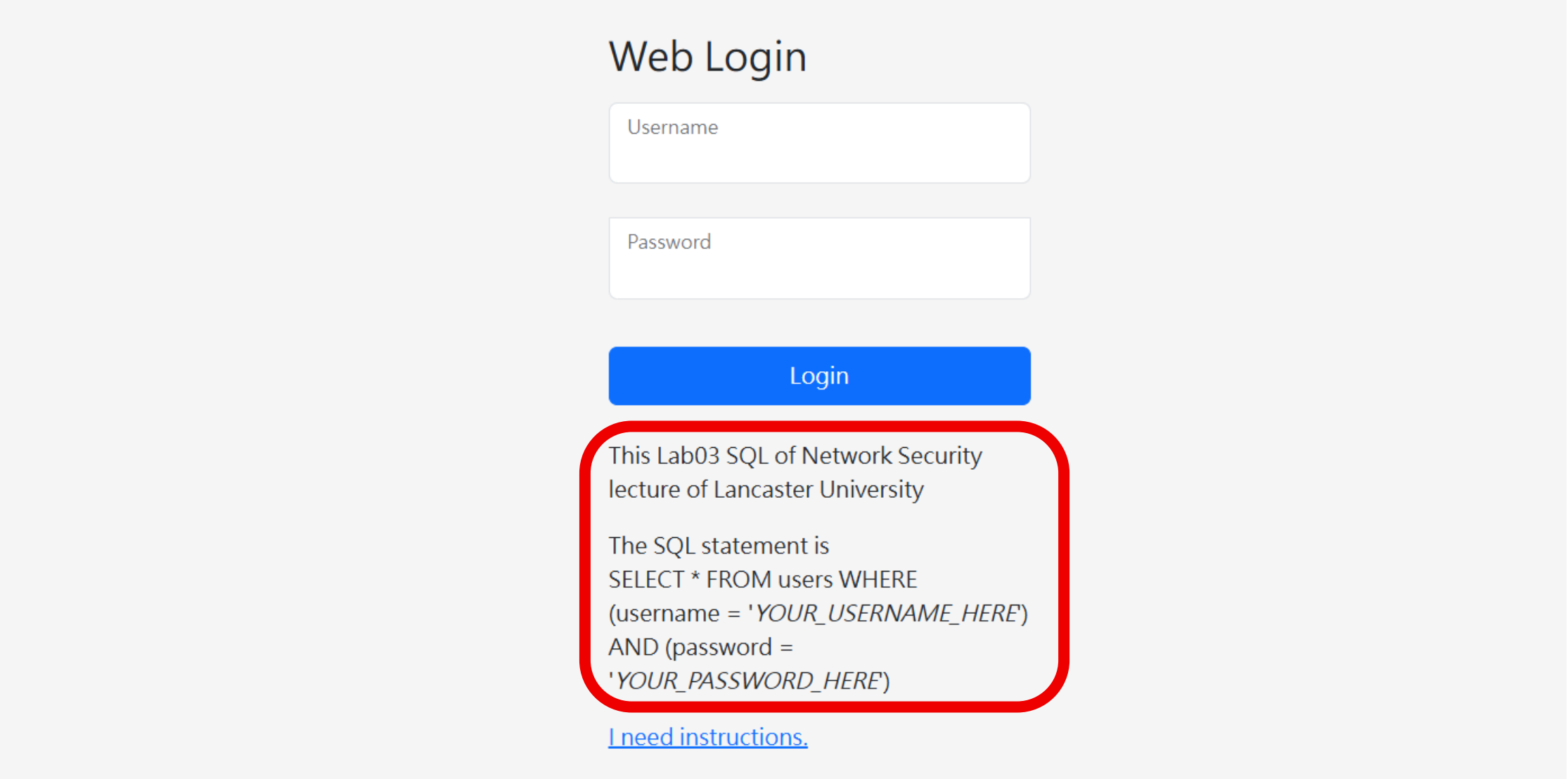
In a 2012 study, it was observed that the average web application received four attack campaigns per month, and retailers received twice as many attacks as other industries.[4]



A classification of SQL injection attacking vector as of 2010

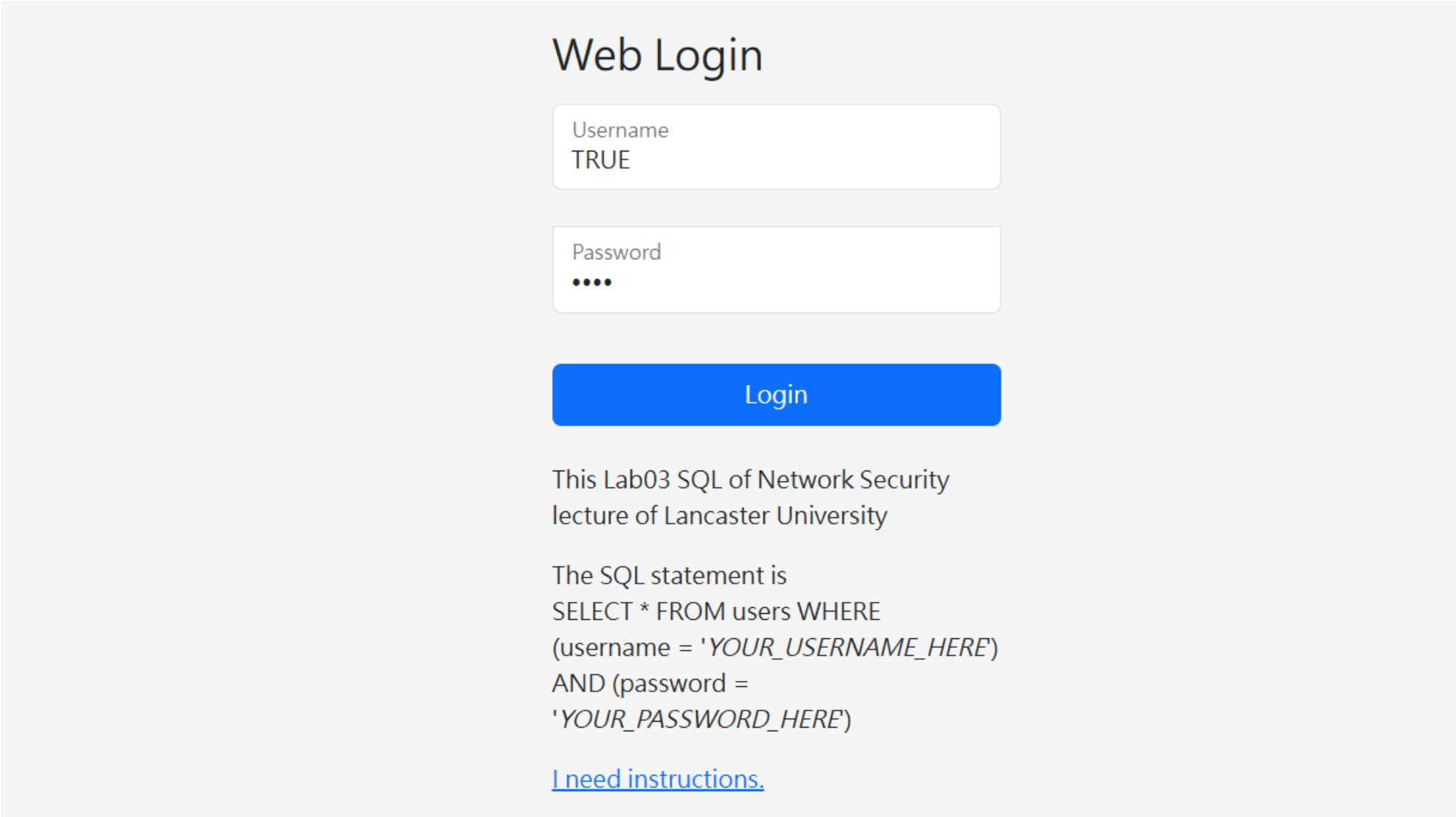
History [edit]

2. Reading the SQL query hint



Tips: Making the outcome of where clause true.

3. Try injecting



4. Congratulation!

```
Login successful!
The SQL statement is : SELECT * FROM users WHERE [redacted]
Which results in following query result :
Username = [redacted]    Password = [redacted]
Username = [redacted]    Password = [redacted]
Username = [redacted]    Password = [redacted]
```