Cyber Security

2024

DVWA

Vathna.lay@cadt.edu.kh

Attack

- SQL injection Blind (low)
- SQL injection Blind (medium)
- SQL map

SQL Injection (Blind)

- **Content-Based Blind SQL Injection (Boolean-Based):**
  - **In this type, attackers structure their SQL queries to ask the database true or false questions.**
  - **By observing subtle changes in the application's response (e.g., different content, a successful login vs. failed login), attackers can infer whether their query evaluated to true or false.**
  - **Attackers repeatedly ask these questions to gradually extract information, like the database version, table names, column names, or even specific data.**

SQL Injection (Blind)

- Content-Based Blind SQL Injection (Boolean-Based):
  - Use boolean condition (AND)
  - find the length of database name:
  - find the name of the database:
  - find number of table in the database
  - find the length of each table in database
  - find the name of each table
  - Use the name of the table to find the column name

SQL Injection (Blind)

- **Content-Based Blind SQL Injection (Boolean-Based):**
  - **Find the number of the column in the table u want to know:**
  - **Find the length of each column:**
  - **Find the name of each column**
  - **Find the length of the data of the column you want to know**
  - **Last: find the all user**

SQL Injection (Blind)

- **Time-Based Blind SQL Injection:**
  - 1' and sleep(5)#
  - follow the same step, use condition statement

- Try to solve medium

SQLMap

- **SQLMap** is an automated tool for SQL injection and databse takeover
- -u <URL>: Specify the target URL.
- -r <REQUESTFILE>: Load HTTP request from a file.
- --data=<DATA>: Data string to be sent through POST.
- -p <PARAMETER>: Specify which parameter(s) to test for SQL injection.
- --cookie=<COOKIE>: Specify a cookie string to be sent to the target.
- --dbs: Enumerate databases.
- -D <DATABASE>: Specify the database to use.
- --tables: Enumerate tables.
- -T <TABLE>: Specify the table to use.
- --columns: Enumerate columns.
- --dump: Dump the contents of the database/table.
- --batch: Never ask for user input, use the default behavior.