<https://dreamhack.io/wargame/challenges/1/>

1. admin으로 로그인 했을 때, FLAG 값을 탈취할 수 있다.

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

1. 코드를 봣을 때, DB에 admin 값을 생성하지 않는다.

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

1. 다만 flag값을 탈취하기 위해선 uid 값에 admin을 넣어야 한다.

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

1. 쿼리를 실행했을 때, uid에 admin을 넣어줘야 하는데, DB에 만들어진 admin이 없으므로, admin 더미 데이터를 만들어 반환한다.

스크린샷, 텍스트이(가) 표시된 사진

자동 생성된 설명

1. 다만 sqli\_filter 부분에 필터링할 문자열이 등록되어있는데 해당 필터링을 우회해야한다.

텍스트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

1. 따라서 admin을 우회할 수 있는 쿼리를 만든다.
2. SELECT uid FROM users WHERE uid='x' and upw='x' and level=9 union values(admin, ‘x’, 9);
3. **uid=test&upw=test&level=1/\*\*/union/\*\*/values(char(97)||char(100)||char(109)||char(105)||char(110))**

**/\*\*/ <- 공백대신 사용, 주석을 의미, admin을 아스키값으로 포장, || <- sqlite에서 문자 이어붙이기**

텍스트, 스크린샷, 소프트웨어, 번호이(가) 표시된 사진

자동 생성된 설명