Report 4

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

Pwnable.kr 의 blackjack의 소스 코드 중 betting() 함수 부분이다.

해당 함수 부분을 분석해보면, 사용자에게 bet(배팅금액)을 입력받고, 해당 값이 cash(보유중인 금액) 보다 크면 재입력을 요청한다. 하지만, 해당 부분이 반복문이 아닌 단순 1회처리로 되어있어, 사용자가 bet을 cash보다 큰 값으로 2번 넣으면 사용자가 입력한 값으로 전달된다.

이를 통해 bet에 100000000을 2번 입력한 뒤 게임을 진행하면 FLAG를 얻을 수 있다.

텍스트, 폰트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

1000000000을 2번 입력하여 게임을 진행 한 모습.

텍스트, 폰트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

이후 게임에서 승리하면 FLAG가 되는 모습을 볼 수 있다.