코드큐어 12주차

202321316 이승훈

1. SQL injection – simple\_sqli\_chatgpt

Dreamhack에 있는 문제인데, sql injection 이지만, 뭔가 다른 점이 있다고 하면 chatgpt를 이용하는 것이다.

문제 파일을 다운 받아서 풀어야 한다.

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

이런 글에서

if userid == 'admin' and userlevel == 0:

return f'hello {userid} flag is {FLAG}'

이런 코드가 있는 걸 확인할수 있다. 우선 chatgpt에게 물어보자.

텍스트, 스크린샷, 소프트웨어, 폰트이(가) 표시된 사진

자동 생성된 설명

여기서 깡통 로봇은 ‘ OR 1=’1’ –을 집어 넣으라 하는데, 이대로 집어넣으면 안된다.

이를 응용을 해서 집어 넣djdi 답이 나오는데, ' OR userid='admin' – 을 집어 넣어야 답이 나온다.

텍스트, 폰트, 스크린샷, 화이트이(가) 표시된 사진

자동 생성된 설명

헤헤…

이 문제는 sql 문을 단순하게 알고 있기만 하면 풀수 없다고 생각하고, 단순하게 아는 것이 아닌

응용을 할줄 알아야 이 문제를 풀수 있다고 생각한다.

1. Pathtraversal

이 문제를 설명하기 전에 cmd에서 경로를 찾아갈 때 쓰는 용어(?)같은 것이 있는데,

보통 cmd에서 경로를 찾아갈 때 / 을 쓴다.

. / : 현재 폴더  
../ : 이전 폴더

cd : 해당 경로로 이동

ls: 현재 내 위치의 모든 파일들을 출력.

etc/passwd : 사용자의 정보가 담겨있는 파일

한번 . / , ../ 에 대한 예시를 들어보자면,

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

자동 생성된 설명

내가 C 드라이브 안에 있는 vbios 라는 파일을 들어가고 싶다…

하면

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

이런식으로 이전 경로를 두번 해서 vbios로 들어가면 된다.

그리고 이 명령 프롬포트의 화면 처럼 cd ./vbios , cd C:/vbios가 있는데,

cd /vbios 가 상재적 주소, c:/vbios가 절대적 주소이다.

그 둘의 차이점은 그냥 읽는 형식일 뿐인데,

절대적 주소는 앞에 C 부터 시작해서 이동하고자 하는 파일의 경로(풀네임 경로)이고,

상대적 주소는 C 를 적지 않고도 C 에서부터 해당 주소로 이동하는 것 이구나를 알아서 스스로 그 위치로 찾아가는 것이다.

그냥 집주소를 말할 때 충청남도~~ 부터 시작하는 것이 절대적 주소이고, cu 건너서 바로 앞의 원룸. 으로 끝나는 것이 상대적 주소이다. 상대적이 절대적보다 더 간결하게 쓸수 있다.

이제 문제를 풀어볼까?

이 문제는 burp suite를 사용해야 하는 문제인데,

텍스트, 스크린샷, 라인, 폰트이(가) 표시된 사진

자동 생성된 설명

이런 사진이 있다. Guest를 입력하고 intercept를 해보면

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

이런 화면이 뜨는데, 우리는 이 userid를 조작해줘야 값이 나오게 된다.

우선 코드를 보게 되면,

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

이러 화면이 있다.

Api 안에 user 하고 flag 가 있다.

우리는 지금 user에 속해 있어서

텍스트, 폰트, 스크린샷, 라인이(가) 표시된 사진

자동 생성된 설명

이런 화면에서 자꾸 맴돌게 된다.

거기서 flag로 가면 키값이 나온다는 것을 아니까

Flag가 노출되도록 할려면 우리는 폴더를 한칸 뒤로 빼서 flag로 가게 하는것이다.

Userid=../flag를 입력하고 forward 하면

텍스트, 스크린샷, 라인, 폰트이(가) 표시된 사진

자동 생성된 설명

헤헤헤헤헤 풀어따…헤헿

이렇게 값이 나오게 된다.