BOB 웹해킹 문제
-SQL 인젝션-

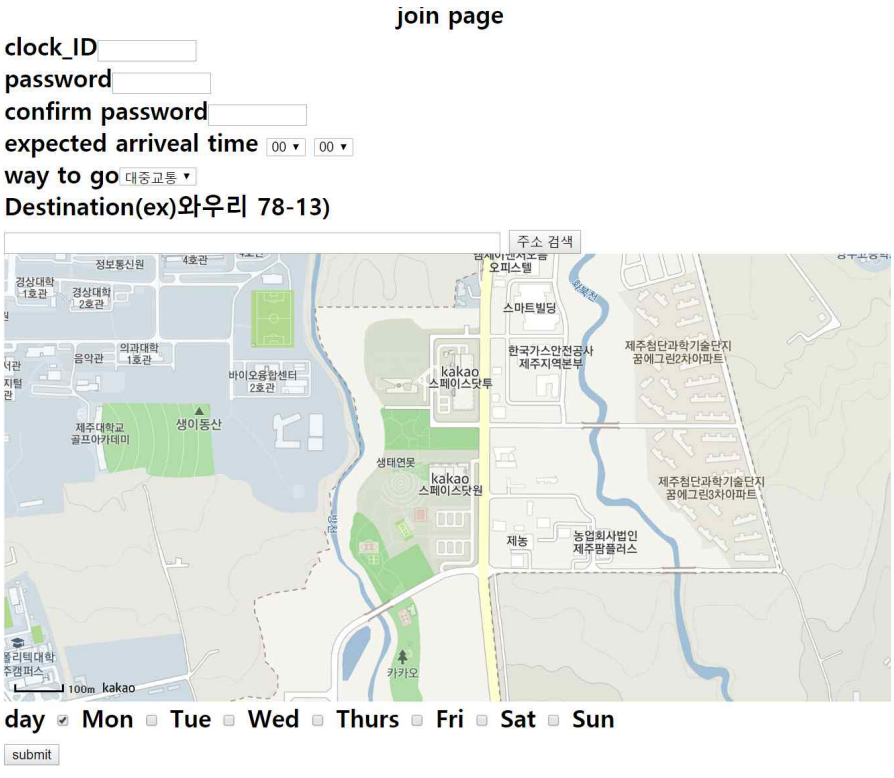
취약점 트랙
신현욱

문제

하루의 아침 이라는 일정 관련 웹페이지가 있다고 가정한다.

해커는 특정인의 ID에 대한 일정 정보 추출을 하고 경쟁업체 거래처 약속을 훼방 놓는 일을 하기로 했다. 특정인의 ID는 admin이라 가정한다.

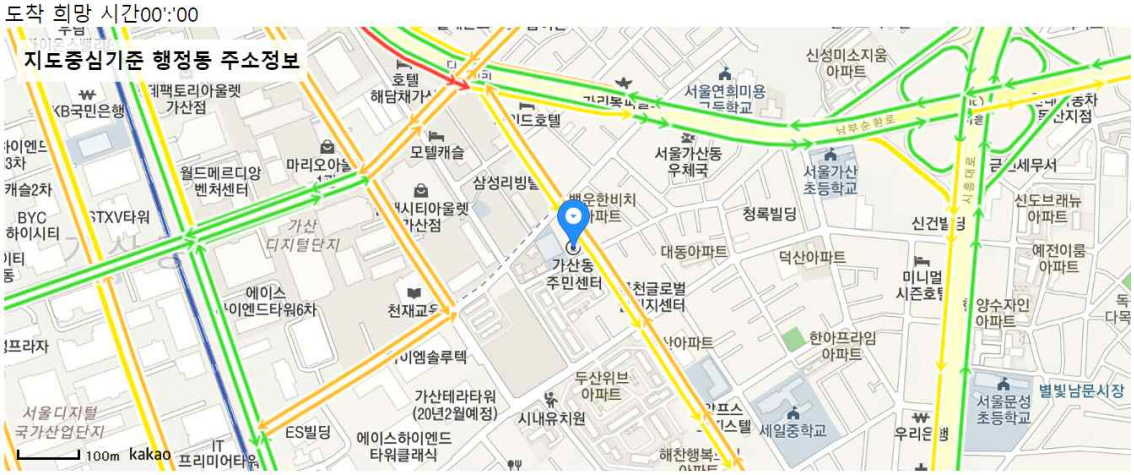
메인페이지는 위와 같다.



설정 페이지는 다음과 같다.

가입 이후 내설정을 확인해보면

id:test
교통편 : 대중교통
요일 월
도착 희망 시간00':'00



37.47687631792999 126.89177947115427

이용 교통수단 일정정보 , 도착지 정보가 나오게된다.

목적지 설정 완료
clock_ID admin'#
password
설정 확인

admin’ #으로 sql 인젝션을 실행한다.

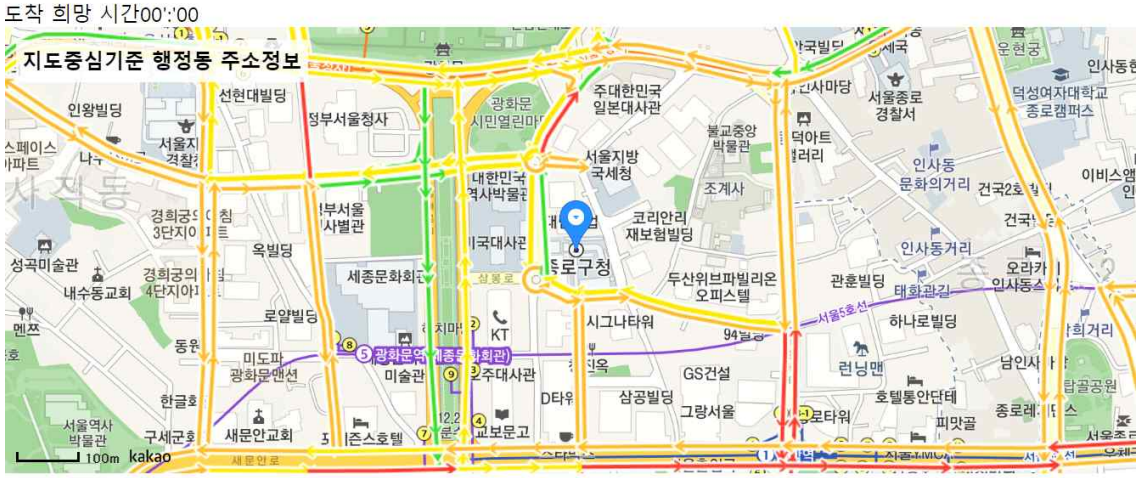
Congraturation. You hacked Admin account
but you have to change admin's destination to '종로' then you can find the flag

요일 월
도착 희망 시간00':'00

37.47687631792999 126.89177947115427

admin으로 접속은 했지만 admin의 destination을 종로로 바꿔 특정인을 속여야한다.
밑에 보면 x좌표와 y좌표가 나오므로 새로운 ID로 가입해 종로의 x좌표와 y좌표를 습득한다.

id:test2
교통편 : 대중교통
요일 월
도착 희망 시간00':'00



37.57312947159552 126.97923004370492

종로의 x좌표와 y좌표를 구했으므로 37.57312947159552 / 126.97923004370492 이므로
테이블 이름과 칼럼명을 모르므로 sql 인젝션 했던 곳 에서 union 인젝션을 통해 information_schema 트릭을 통해 테이블명과 칼럼명을 알아낸다.
테이블 명은 days_morning이고 x좌표와 y좌표의 칼럼명은 destinationX이고 destinationY 이다.
mysqli_multi_query로 이루어져있어 동시명령이 실행이 가능하다.
첫 번째로는, sql 인젝션을 통해 sql statement ; update statement로 admin의 id를 다른 id로 바꾸고 자신이 새로운 admin 아이디와 종로 목적지 기입으로 가능하고
두 번째로는, update 구문을 통해 admin의 destinationX와 destinationY를 위의 좌표로 바꿔준다.

Congraturation. You hacked Admin account
but you have to change admin's destination to '종로' then you can find the flag
flag is 808 h4ck th3 w0r1d
요일 월
도착 희망 시간00':'00

37.57312947159552 126.97923004370492

FLAG =808 h4ck th3 w0r1d