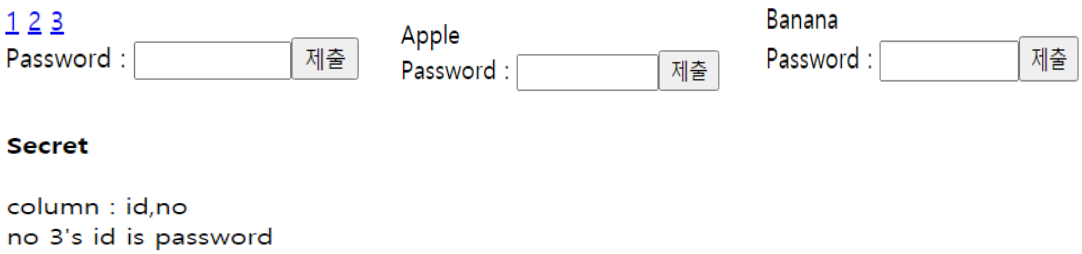
[웹해킹 9번&22번]

2020111318 김수현



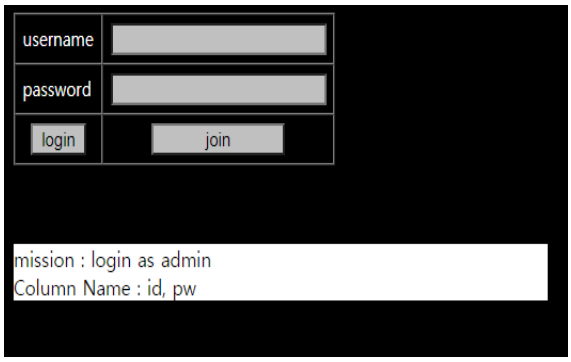
9번 문제는 1 2 3 과 함께 패스워드를 입력하는 창이 떴다. 처음에 1을 눌러보니 Apple, 2를 눌러보니 Banana, 3을 눌러보니 Secret no 3's id is password라고 쓰여져 있었다. 이는 no 파라미터에 수업시간에 배운 Blind SQL Injection을 활용하는 문제인 것 같다. No와 id가 함께 주어진 것으로 보아 no의 값은 변경할 수 있지만 id의 값을 우리가 알아내는 것이 중요한 것 같다. No의 값을 변경하여 SQL injection 을 통해 id의 값을 알아낼 수 있을 것 같다.

No의 값을 변경하기 위해서 사용되는 함수가 substr과 length 함수가 있다. 구글링을 한 결과, substr은 문자열,시작위치,길이를 인자 값으로 받는 질의어 함수이다. if문은 조건을 받아 참일 경우 1, 거짓일 경우 0을 반환하는 구문이다. 하지만 각 케이스별로 커스텀된 결과 값을 반환하게 만들 수 있다고 한다.

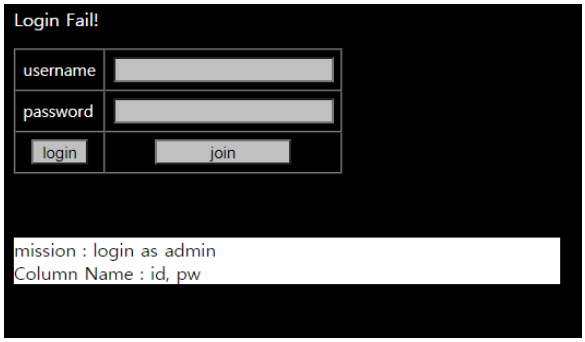
substr과 if 문을 이용하여 id를 substr하여 나온 결과값이 모든 아스키 코드와 같은 지 판별하고 같다면 3 같지 않다면 0을 반환하게 만든다. (if(substr(id,1,1)=0x61,3,0))의 형태로 만든다. 하지만 = 연산자는 필터링 되어 사용할 수 없다고 수업시간에 들었다. 그래서 = 대신 like를 활용해보았다.

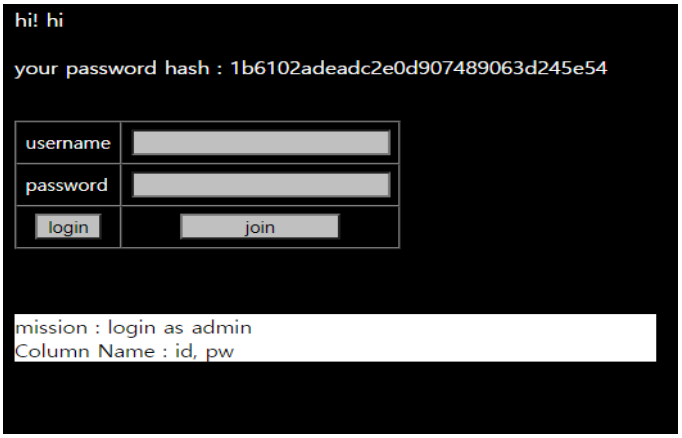
no=if(substr(id,1,1)like(0x41),3,0)으로 완성하였다. 하지만 이 다음부터 무엇을 해야 될 지 모르겠다.뒤에 3,0은 if문의 기본 형식에 따라서 앞의 값이 참이면 3을 반환, 거짓이면 0을 반환 하는 것인데, 이와 같은 과정을 어떻게 반복해야 될 지 잘 모르겠다.

22번 문제)



22번 문제도 9번 문제와 비슷한 것 같다. Username과 password 칸이 있고, admin으로 로그인을 해야 하는 것 같다. 그래서 일단 아무거나 입력하고 로그인을 해보았는데, 아래와 같이 Login Fail 창이 떴다.





그래서 일단, username은 hi password도 hi로 하고 join을 해주었더니 위와 같은 창이 뜨면서 password에 대한 해시 값이 떴다. 그래서 이게 문제의 힌트라고 생각이 들었다. 하지만 그 이후부터 어떻게 접근을 해야 될 지 모르겠다. Admin' and 1=1#을 username 창에 입력하고 비밀번호를 다른 것을 입력하였더니 아래와 같이 wrong password창이 떴다. 똑같이 username과 비밀번호에 admin' and 1=1#을 입력해도 같은 결과가 나왔다. 그래서 이 문제도 9번 문제와 같이 풀지 못했다.