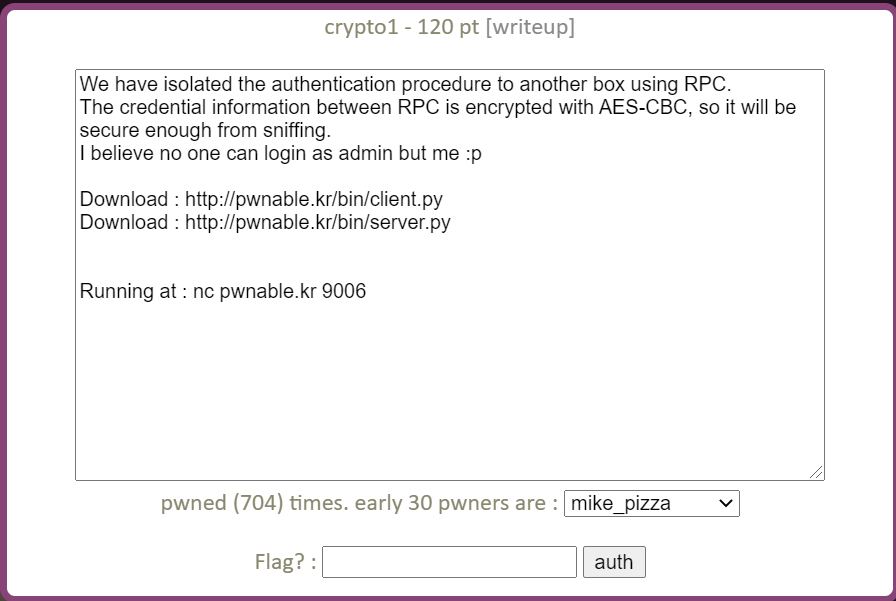
보안동아리 20주차 과제

크립토 문제(사실 아직도 잘 모르겠지만 구글링을 최대한 해서 80퍼센트 정도 이해함)..

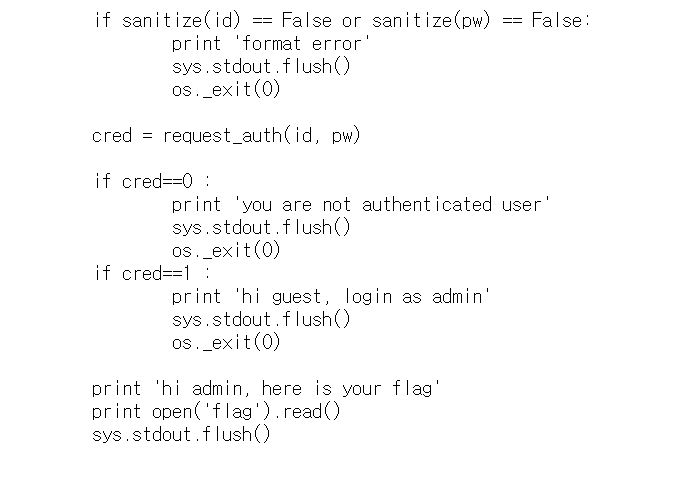


처음에 이렇게 뜬다.

저기 두개의 페이지로 들어가보자.

일단 클라이언트 부분 먼저





참고한 블로그:

<https://code1018.tistory.com/187>

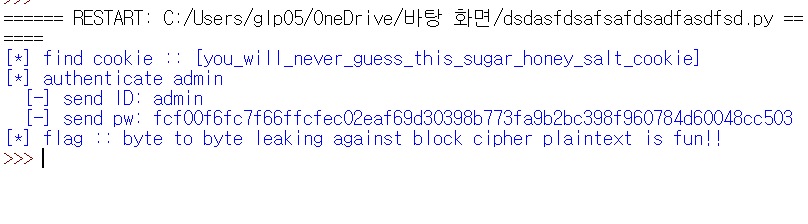
클라이언트 프로그램은 아이디와 비밀번호를 입력받아서 특정 형태의 문자열을 만든 후 그 문자열은 aes 암호화 과정을 한 패킷을 전송한다고 한다. 그리고 id-pw-cookie 이런 형태로 되어있어서 대쉬- 가 문자열을 구성해준다.



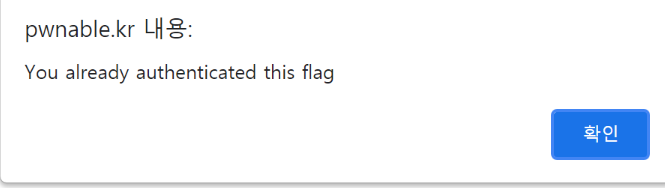
(서버 프로그램)

여기서 알 수 있는 점은 id와cookie 를 합하고 그것을 SHA-256 으로 해쉬한 값이 pw 와 일치한다는 것이다. 그래서 우리는 cookie 값을 알면 되는 것이라고 한다.

그래서 한글자씩 노출시켜 보아야 한다고 함.

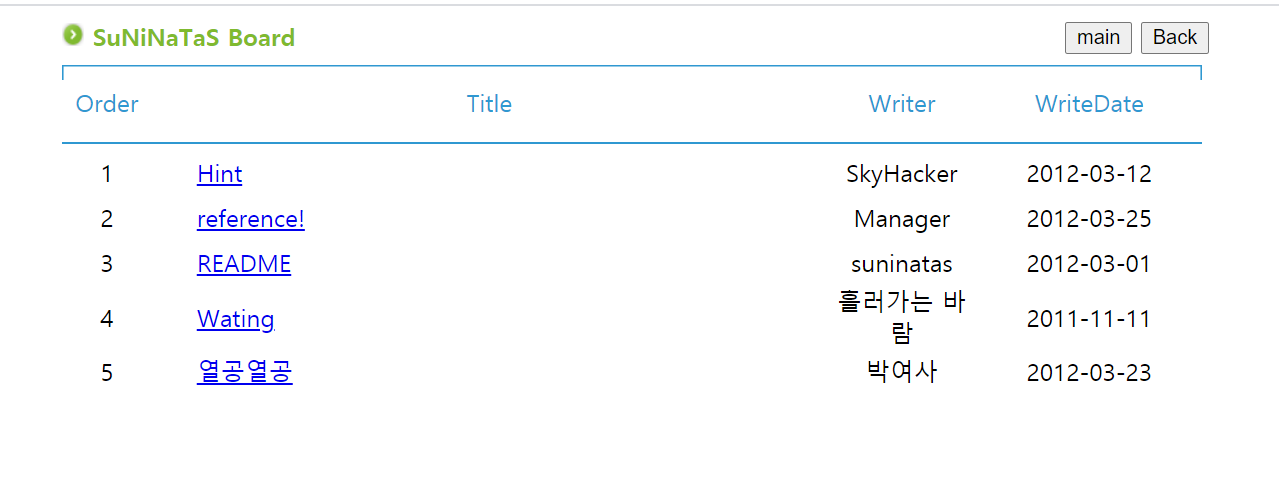


돌리면 이렇게 나오고



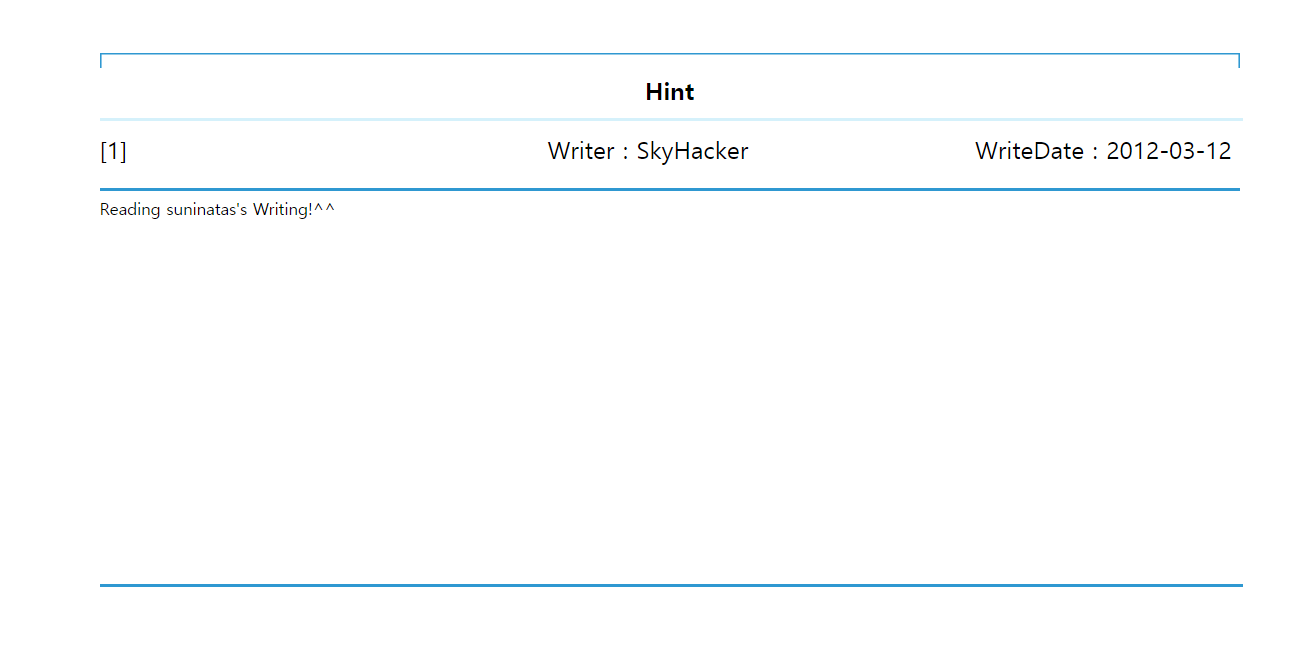
Flag 값 이렇게 넣어주면 완료…!

쿠키변조 문제 – 6번



첫 화면 이렇게 나옴

일단 Hint 부분에 들어가 보았다

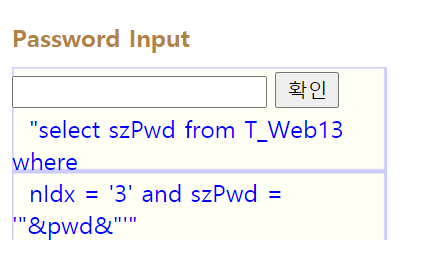


그리고

Reference!

<https://md5hashing.net/>

뭔가 md5 해쉬를 쓰는 문제인 것 같다.



Readme는 이런식으로 되어있다. 뭔가 db 에서 가져오는 거 같음…

적절한 패스워드를 입력하게 되면, 테이블에서 nIdx 값이 3인 라인의 컬럼을 참조함.

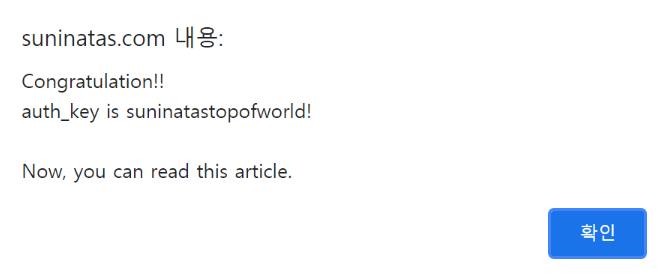
항상 써왔던 1 or ‘1’ = ‘1’—무조건 참이 되는 값을 입력해보자.



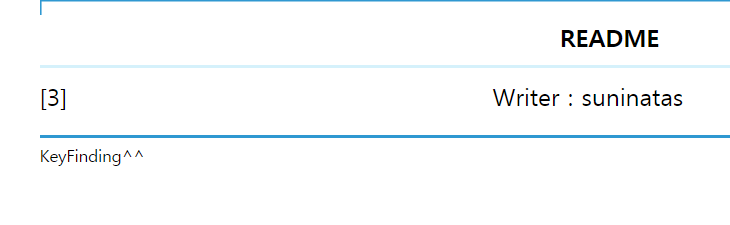
안댐 – 여러가지 문자열들이 필터링 되고 있음.

하지만 like 나 부등호는 가능했음. 따라서 필터링이 가능한 것들로 우회하면 됨.

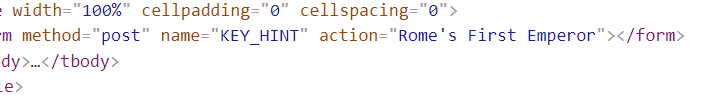
1’ or ‘1’ like ‘1’—이런식으로 우회하면 됨.



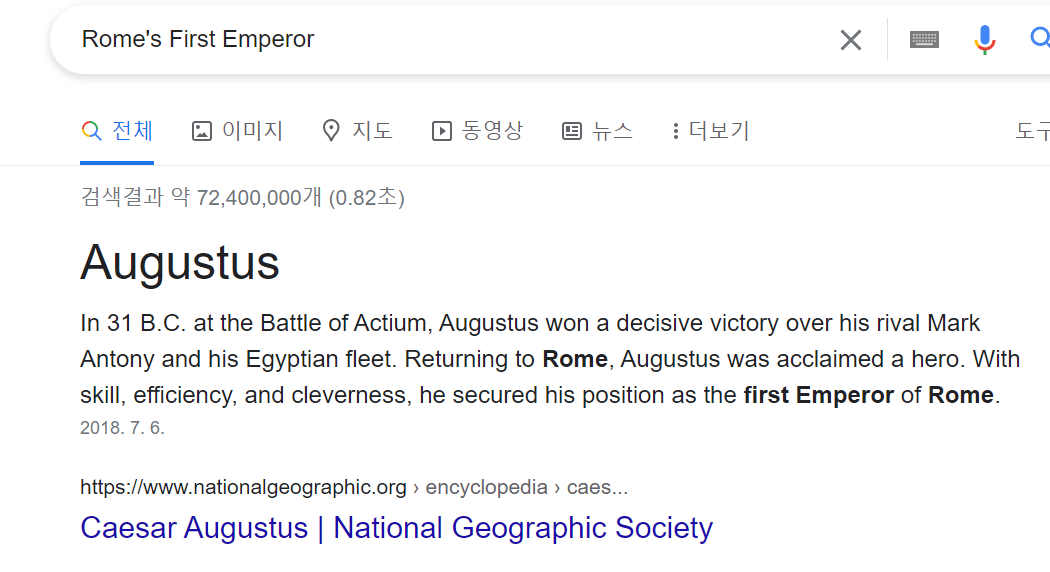
이런식으로 나옴



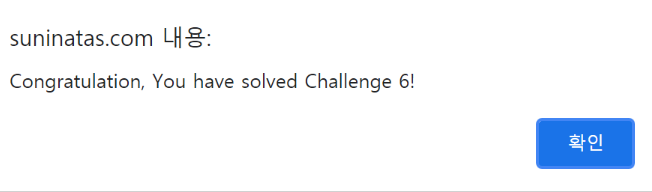
Keyfinding 을 하라고 함. 소스코드를 확인해 보자



Hint 에 action 부분에 뭐가 써져있음.



구글에 치니 이런 것이 나옴.



Auth 에 가서 치면 됨.