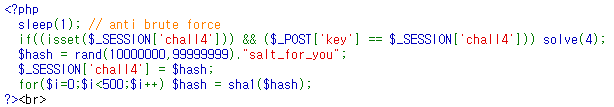
4번(300점)



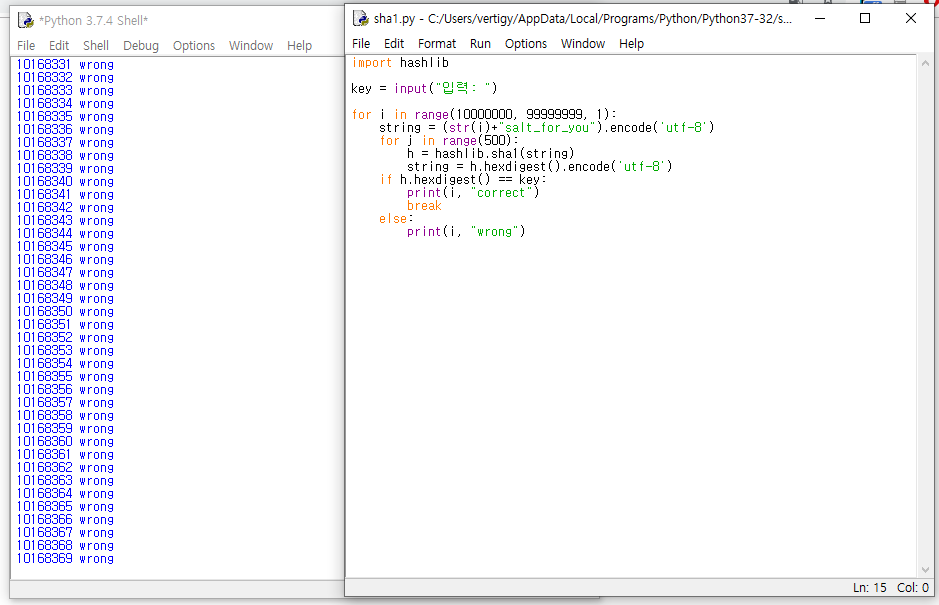
hash값과 post방식의 form이 주어진다.



‘chall4’ 라는 이름의 세션의 값이 post로 전송한 값과 같을 때 solve(4)가 실행된다.

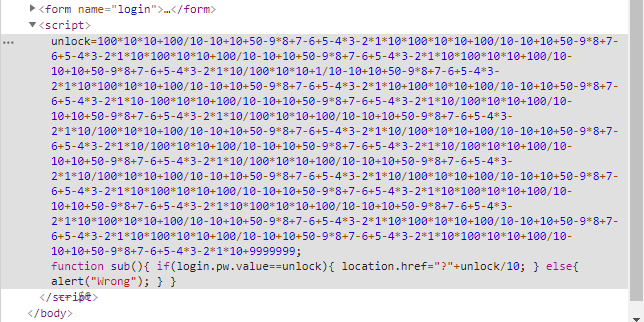
이 때 ‘chall4’ 세션에 저장되는 값인 hash는 10000000부터 99999999사이의 무작위 정수에 “salt\_for\_you”를 이어 붙인 문자열에 sha1 암호화를 500번 반복한 값이다.

sha1 복호화 사이트를 이용해 hash값을 복호화 해보려고 시도했으나 실패했고 검색해보니 sha1 해쉬는 일반적으로 복호화 되지 않는 것 같다.



파이썬의 hashlib 라이브러리를 사용하여 모든 8자리 정수를 sha1방식으로 500번 암호화하고 hash값과 비교하며 반복한다.

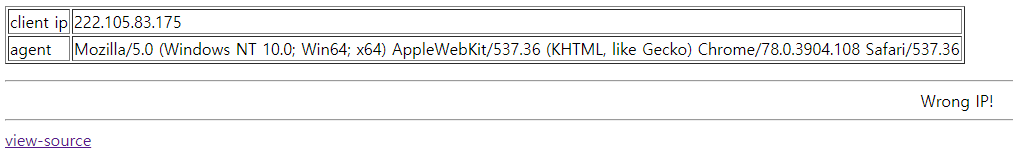
17번(100점)



unlock 변수의 값이 위와 같을 때 login 폼의 pw의 값이 unlock과 일치할 경우 location.href 함수를 통해 다른 페이지로 이동하게 되어있다.

스크립트를 그대로 복사 후 개발자도구 콘솔에서 실행해서 unlock의 값을 구한 후 form에 입력하면 성공

24번(100점)





$REMOTE\_ADDR은 접속자의 IP를 나타내는 PHP의 기본 변수인데, 이것을 ip라는 이름의 변수에 담은 후 “..”을 “.”으로 바꾸고 “12” “7.” “0.” 을 제거한다. Ip가 127.0.0.1 이 될 때 solve(24)가 실행되므로 4번의 str\_replace를 거치고 나서 ip의 값이 127.0.0.1이 되도록 REMOTE\_ADDR 값을 변조하면 해결된다.

자바스크립트를 이용해 쿠키의 REMOTE\_ADDR 값을 17.270.12.00.12.00.12.1 로 변조하면 성공

