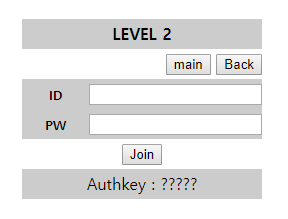
써니나타스 풀이 문서

이진하

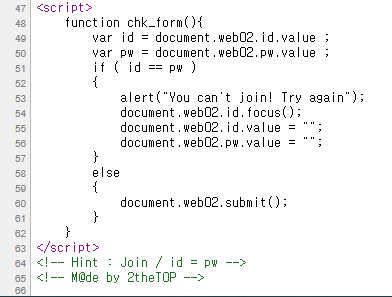
문제 2번



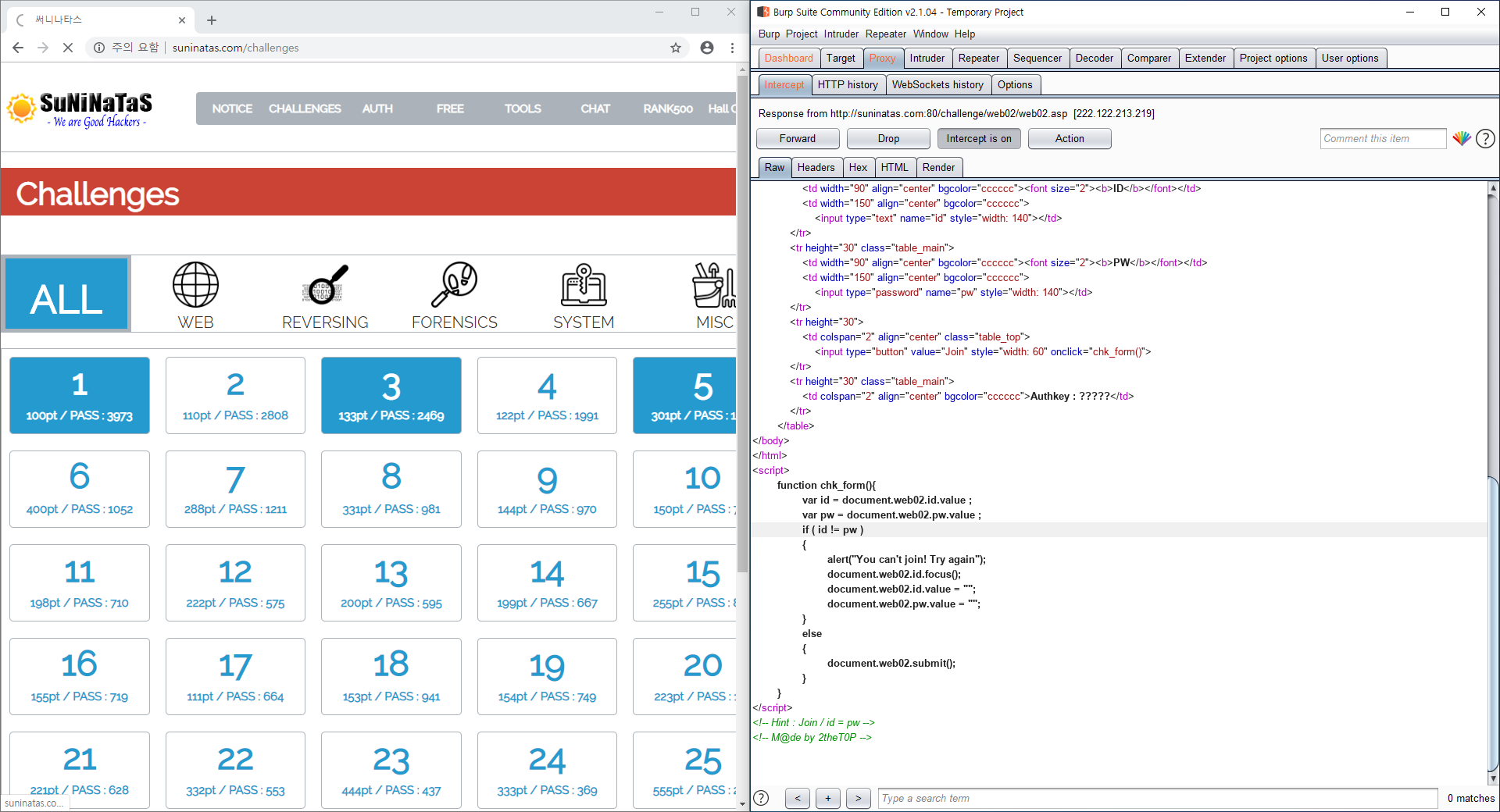
ID와 PW를 입력하면 Authkey를 얻을 수 있다.

[풀이]

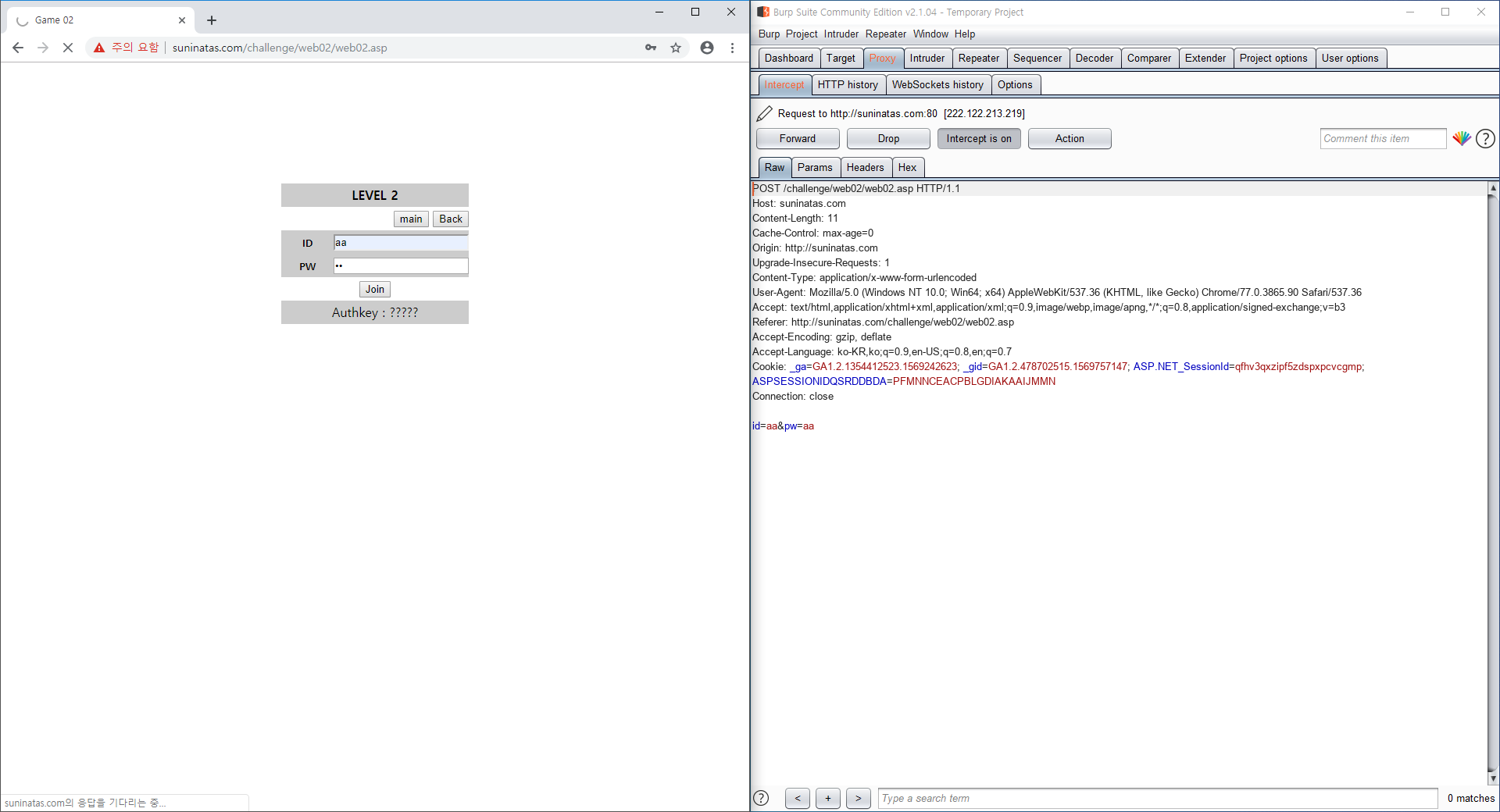
먼저 풀이를 위해 소스 코드를 열어 보았다.



chk\_form 함수를 보면 id와 pw가 같으면 “You can’t join! Try again”이 출력된다고 하는데 힌트에서는 로그인을 위해서는 id와 pw가 같아야 한다고 했다. 따라서 프록시 툴을 이용하여 입력 값을 우회해 보려고 했다.



burp suite에서 chk\_form 함수를 수정하여 id != pw 일 때 알림 창이 뜨도록 수정하였다.



burp suite에서 id, pw에 전달하는 값이 동일한 것임을 확인했고, forward를 하여 Authkey를 얻었다.

