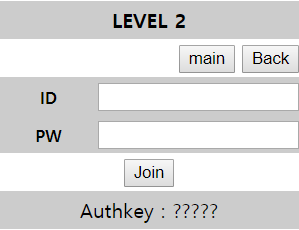
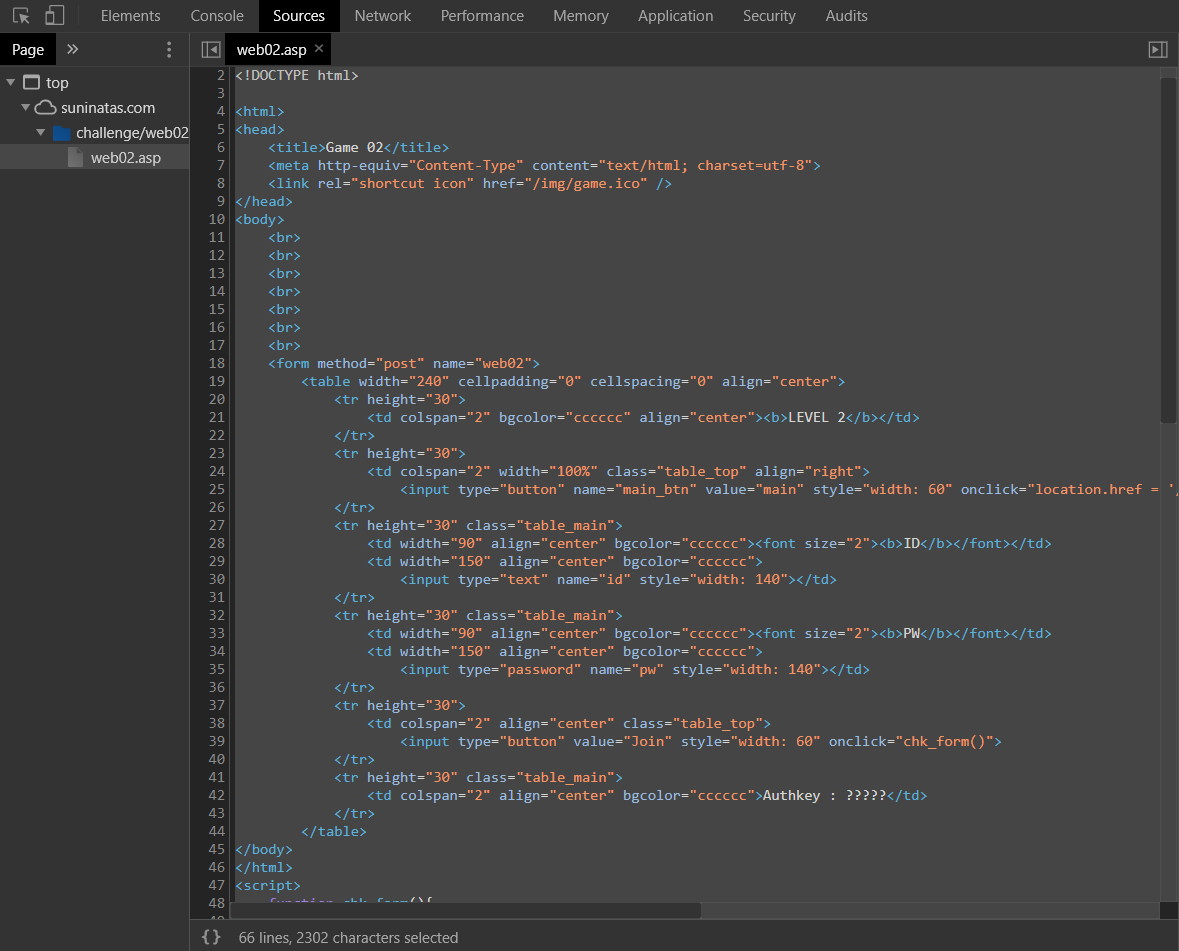
< 2번 워게임 풀이문서 >

김구민

다음 문제는 ID와 PW를 입력해서 Join해야

아래의 인증키를 얻을 수 있다.

[ 사이트 소스 코드 ]



아래 코드를 보고 처음에 ID와 PW가 같을 때만 로그인이 되지 않을 것으로 예상하고 ID와 PW를 다르게 입력해보았으나 실패했다.

function chk\_form(){

var id = document.web02.id.value ;

var pw = document.web02.pw.value ;

if ( id == pw )

{

alert("You can't join! Try again");

document.web02.id.focus();

document.web02.id.value = "";

document.web02.pw.value = "";

}

else

{

document.web02.submit();

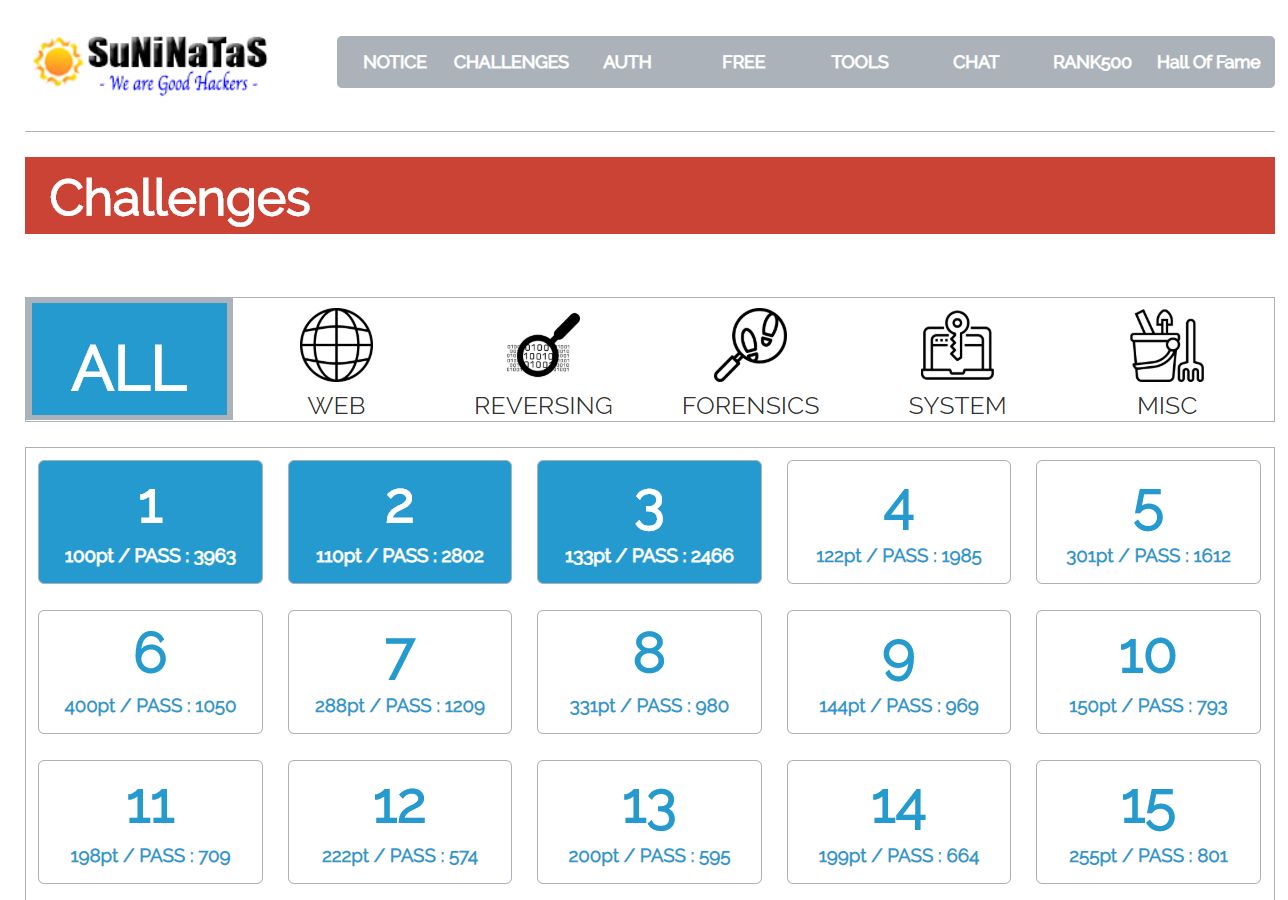
}

}

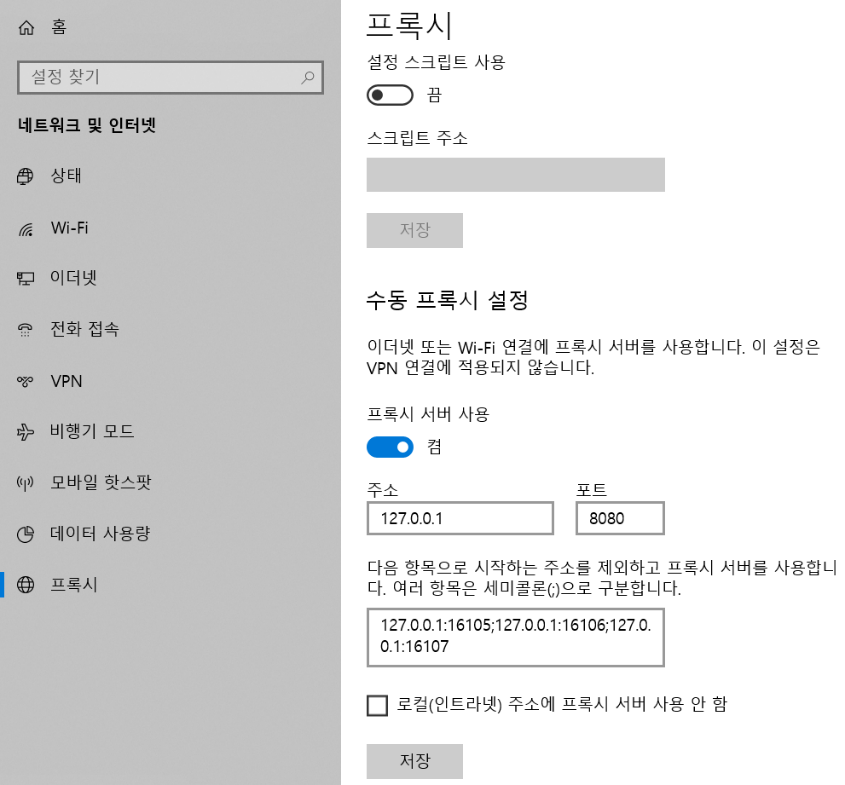
그러다가 else문에 web02.submit(); 구문을 보고 ID와 PW가 다를 때 로그인이 되지 않도록 소스 코드를 바꾸고 실행해보기로 했다.

소스 코드를 바꾸고 실행하기 위해서는 인터셉트 해주는 프로그램이 필요하다.

그래서 본인은 Burp Suite 라는 프로그램을 사용했다.

일단 문제 화면 직전 화면으로 이동한다. 

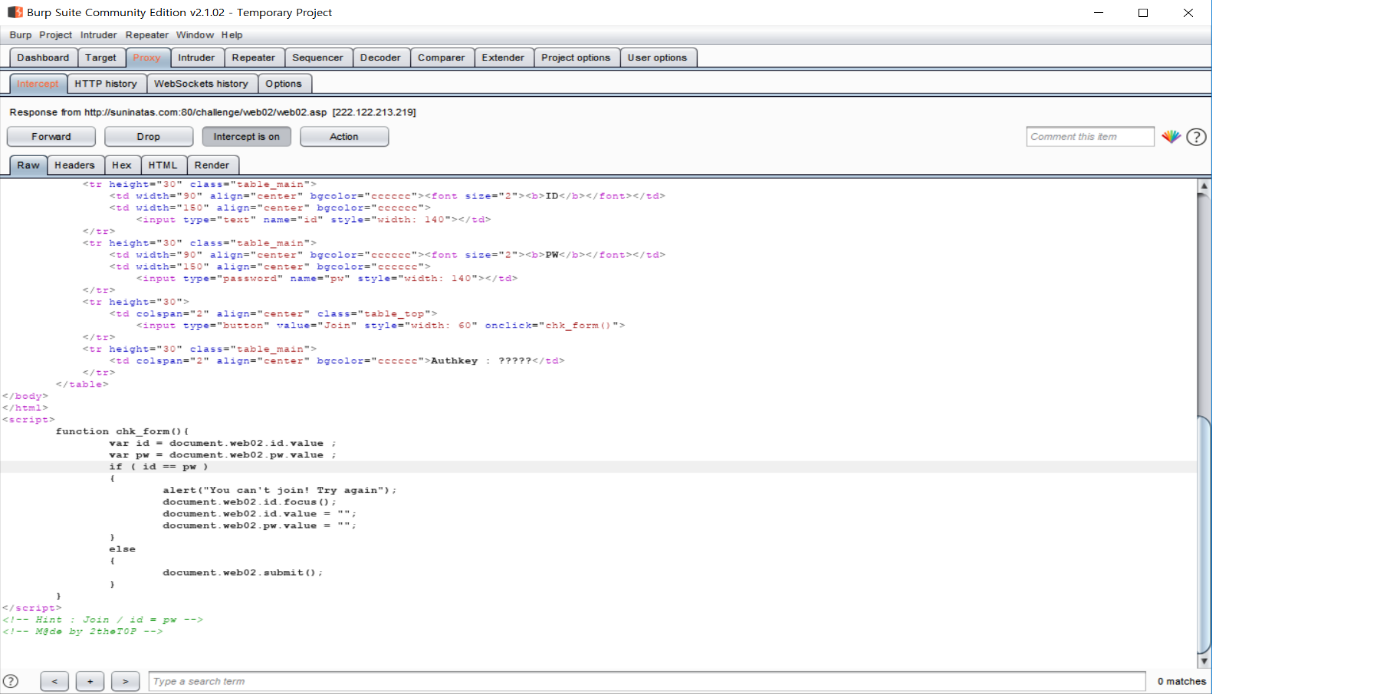
그 다음 프록시를 켜준다.



Burp Suite 설정 완료 후 Proxy > Intercept 화면에서 Intercept on으로 설정

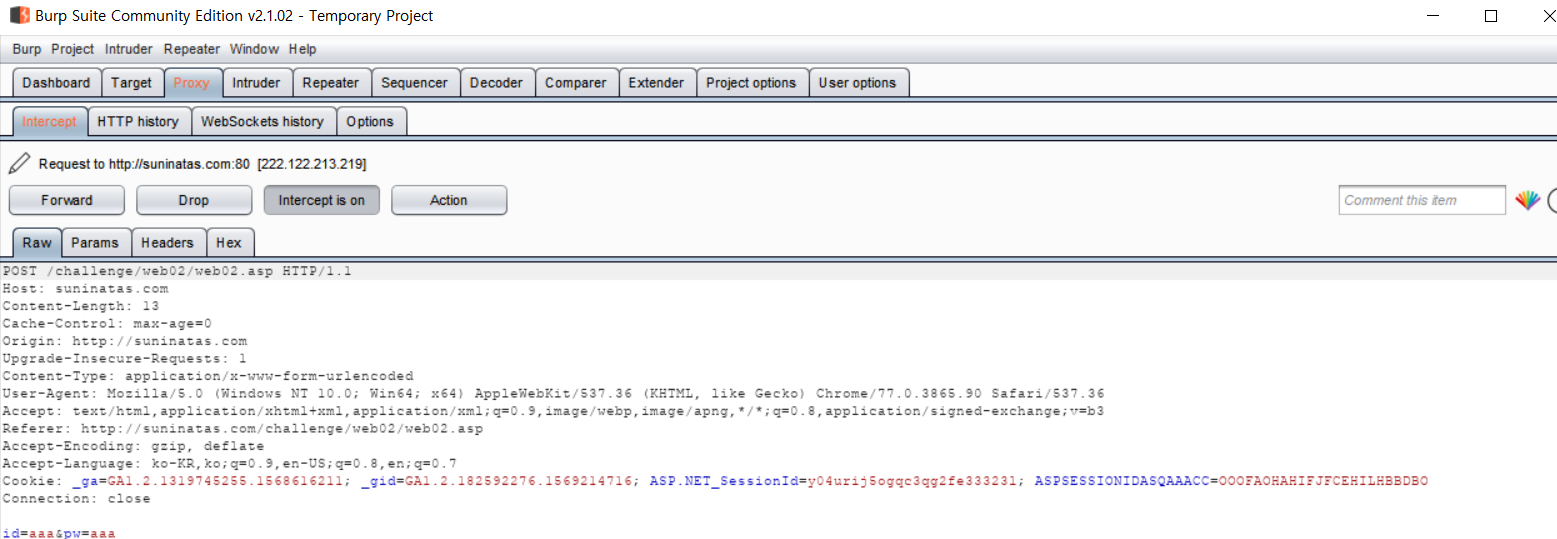
문제 화면을 클릭하고 Forward를 누르면 이동할 사이트의 소스 코드가 나온다.

이 순간 인터셉트가 진행되는 것으로 보인다.



그리고 id == pw 코드를 id != pw 로 변경한 후 Forward 해준다.

그러면 문제 화면으로 이동하게 되는데 ID와 PW를 입력하고 join 을 클릭하면

다음과 같이 입력된 값들이 나온다.

그런 후 프록시 설정을 꺼주고 join을 다시 한번 해주면 아래와 같이 인증키가 뜨면서 성공한다.