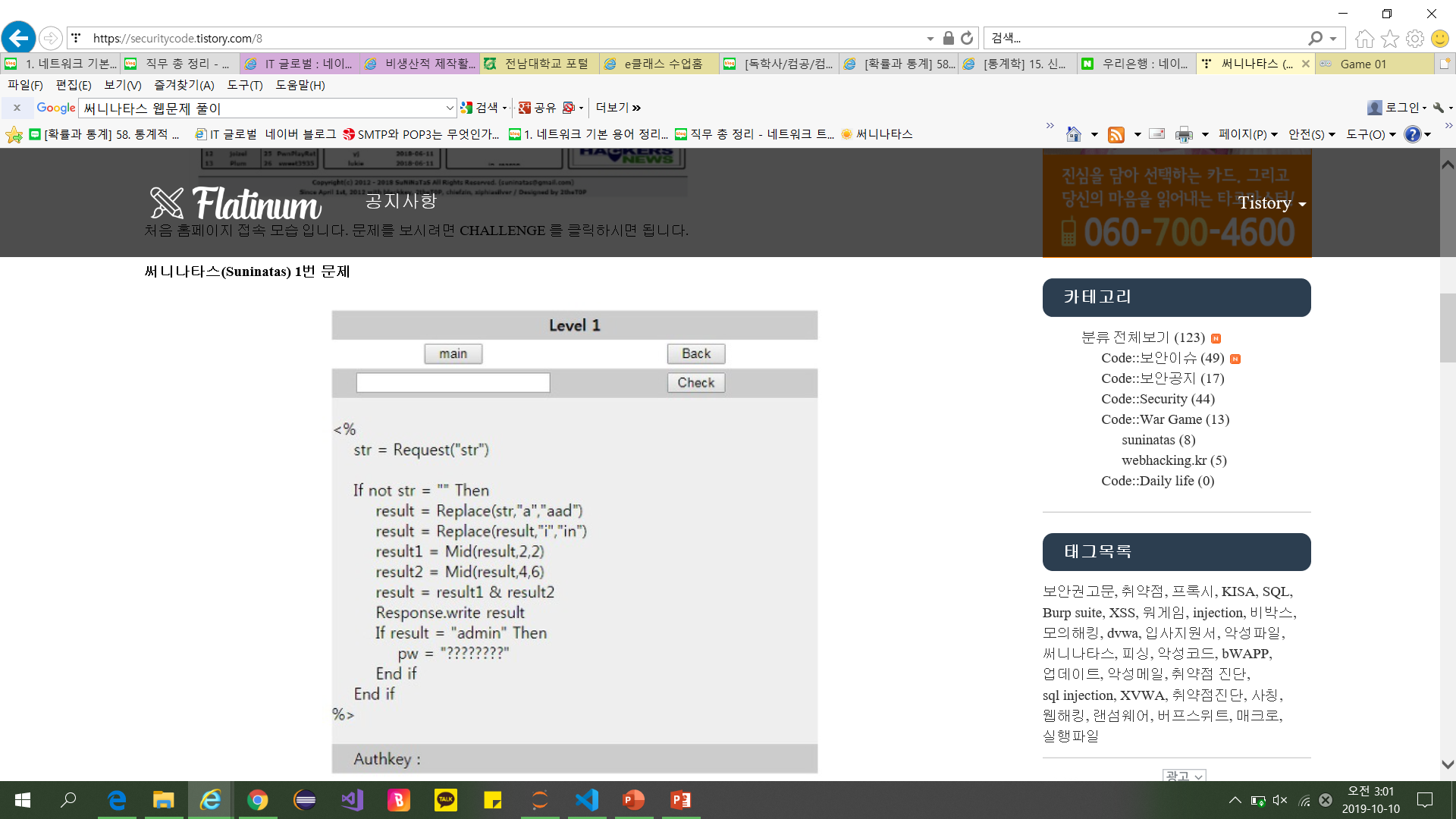
**써니나타스 워게임 문제 풀이**

**김사연**

**1번**

****

**현재 코드를 해석해보려고 검색하였다.**

**Replace 함수 - 해석을 해보면, 치환 함수**

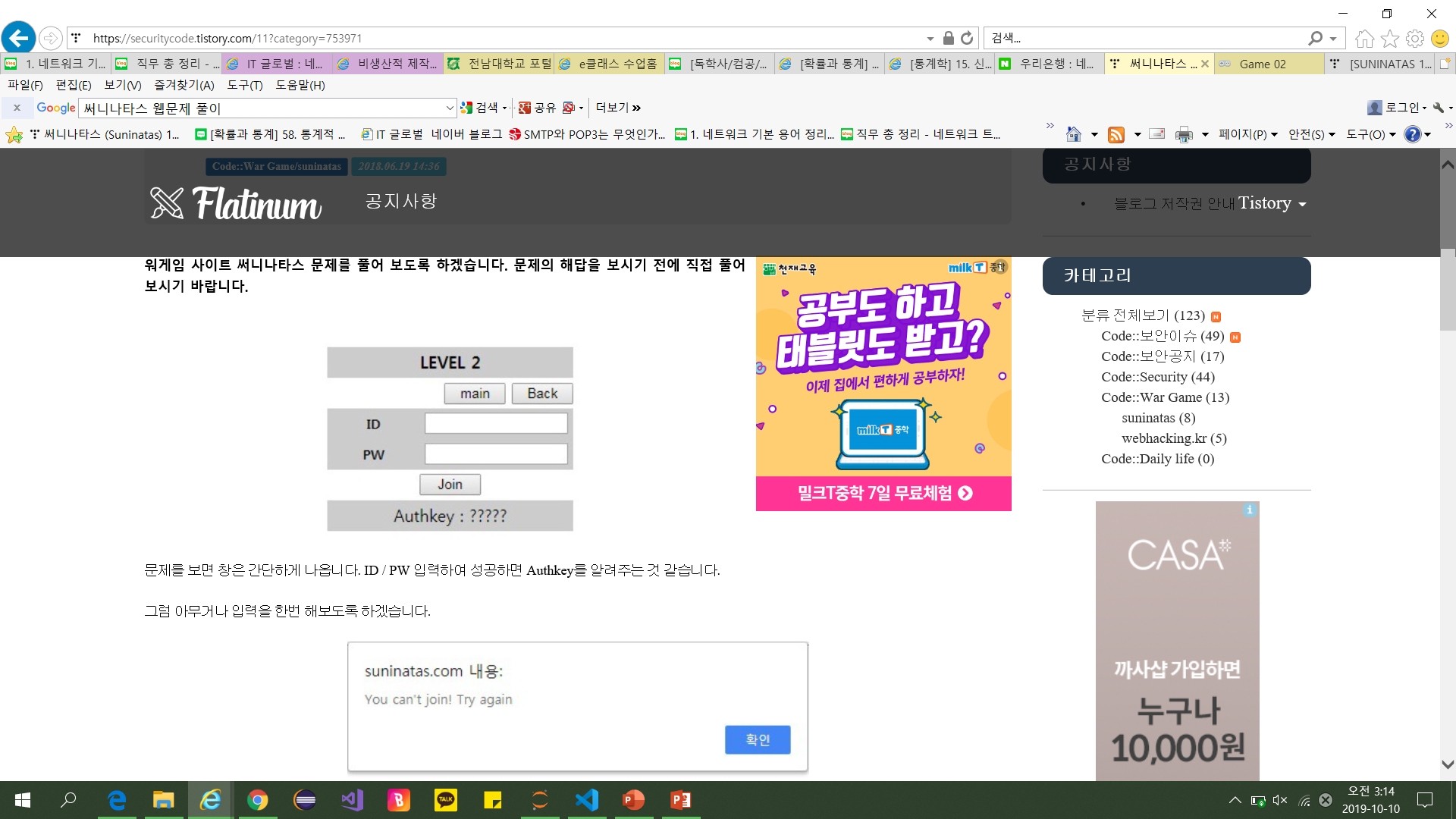
**Mid 함수 - 문자열 일부를 자르는 함수**

**->결과가 admin일 경우 pw를 반환하는 것으로 해석**

**So, ami를 입력하면 admin이 된다.**

**그래서 답을 ami를 입력하였더니 authkey가 나오고 이를 auth에 가서 입력하여 완료하였다.**

**2번**

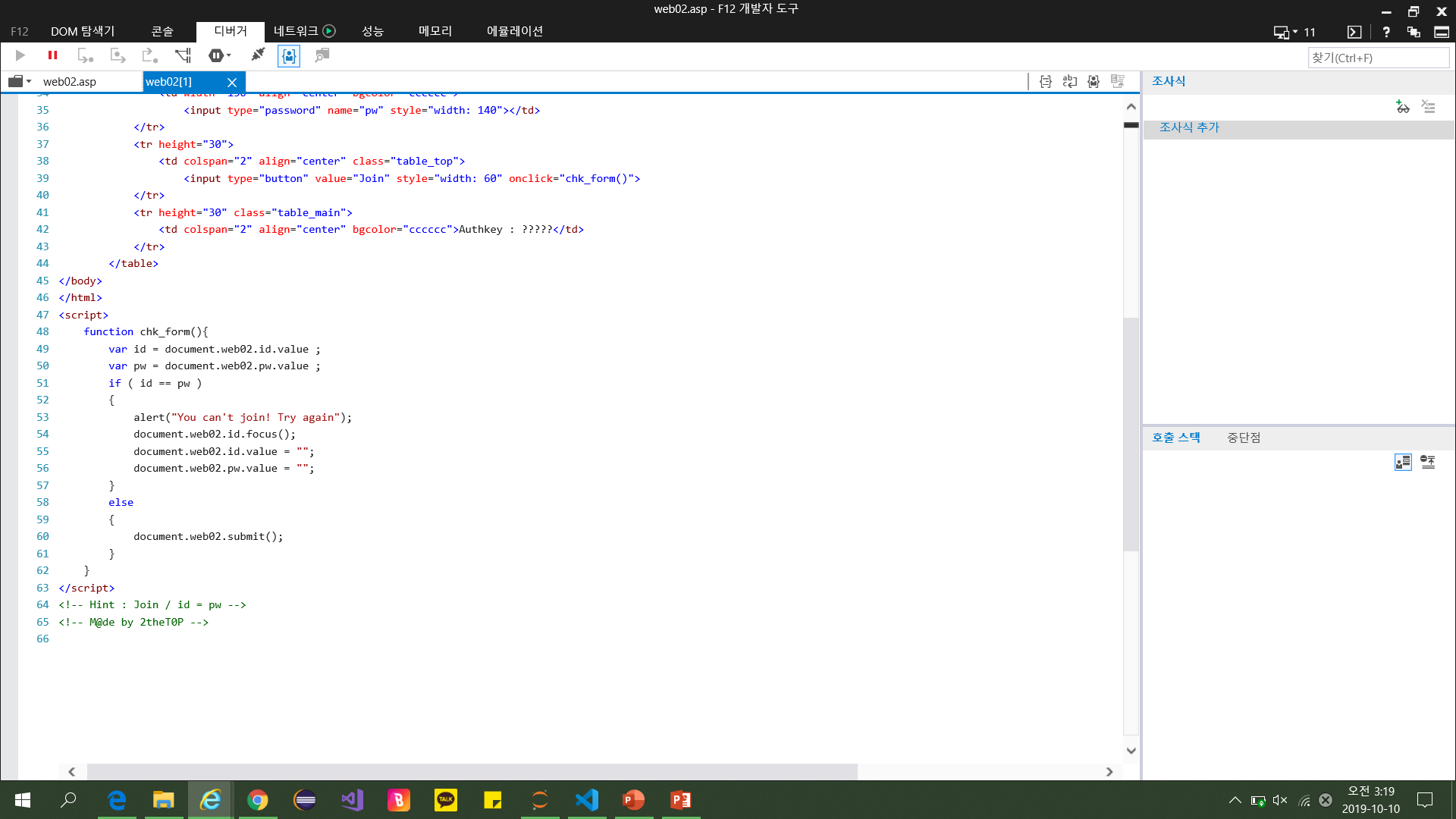
****

**아무거나 입력해도 반응 없음 그래서 써니나타스 아이디 비번도 눌러보고 goeh 반응이 없자,**

**그냥 입력없이 join만 눌렀는데, 이렇게 누르면 가입할수 없다는 경고창이 뜬다.**

**->결국 아무 동작도 하지않음.**

**그래서 소스보기를 눌러 보았다.**

****

**현재 script에 함수를 보니까 아이디 비번이 같으면 경고 창이 뜨고 초기화가 되는 것처럼 보여**

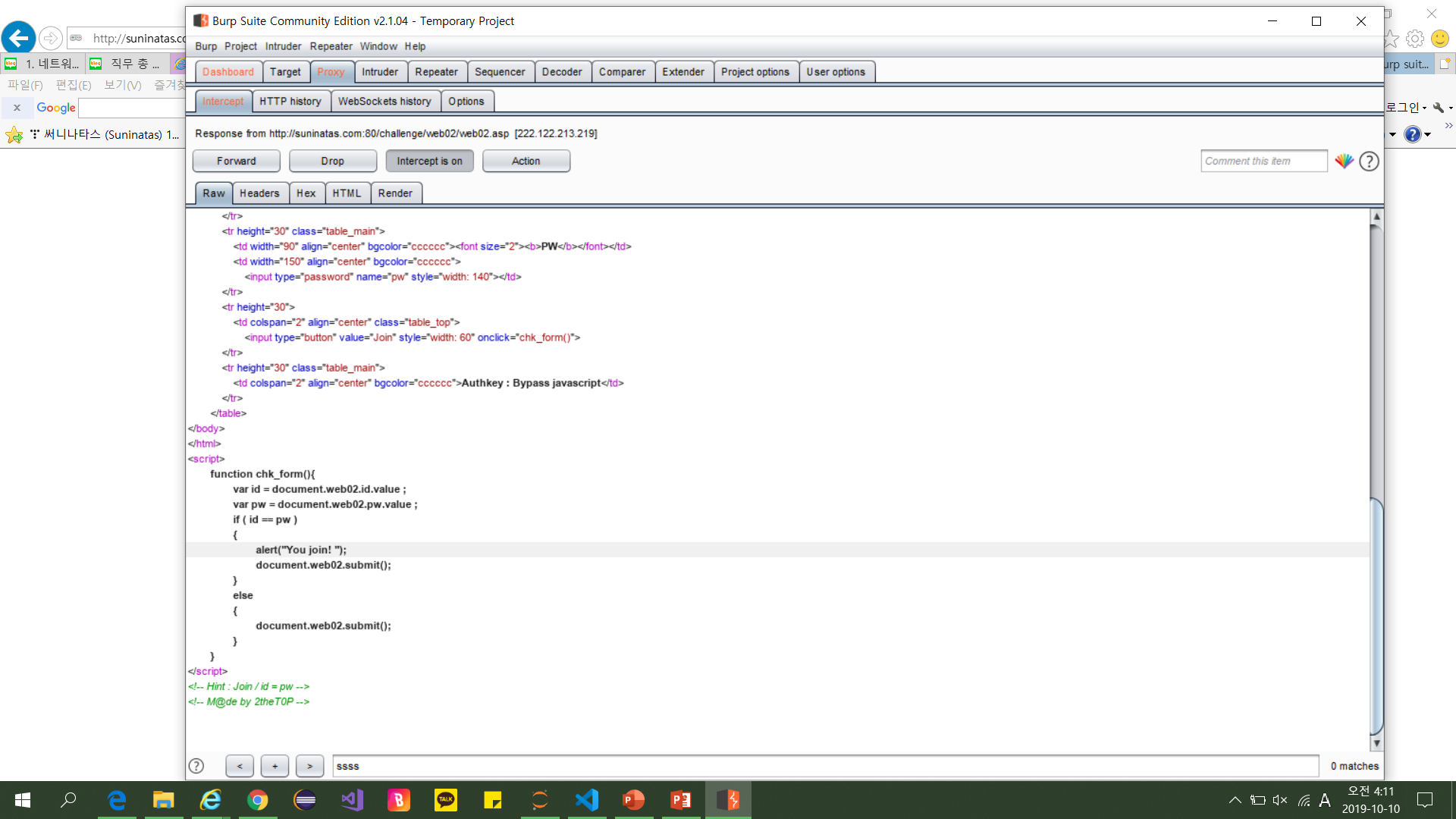
**이 부분을 수정해야겠다고 느낌**

**밑에 hint 부분에 id=pw일 때 join되도록 하라는 내용인거 같아서**

**alert경고창 부분을 you join!으로 바꾸고,**

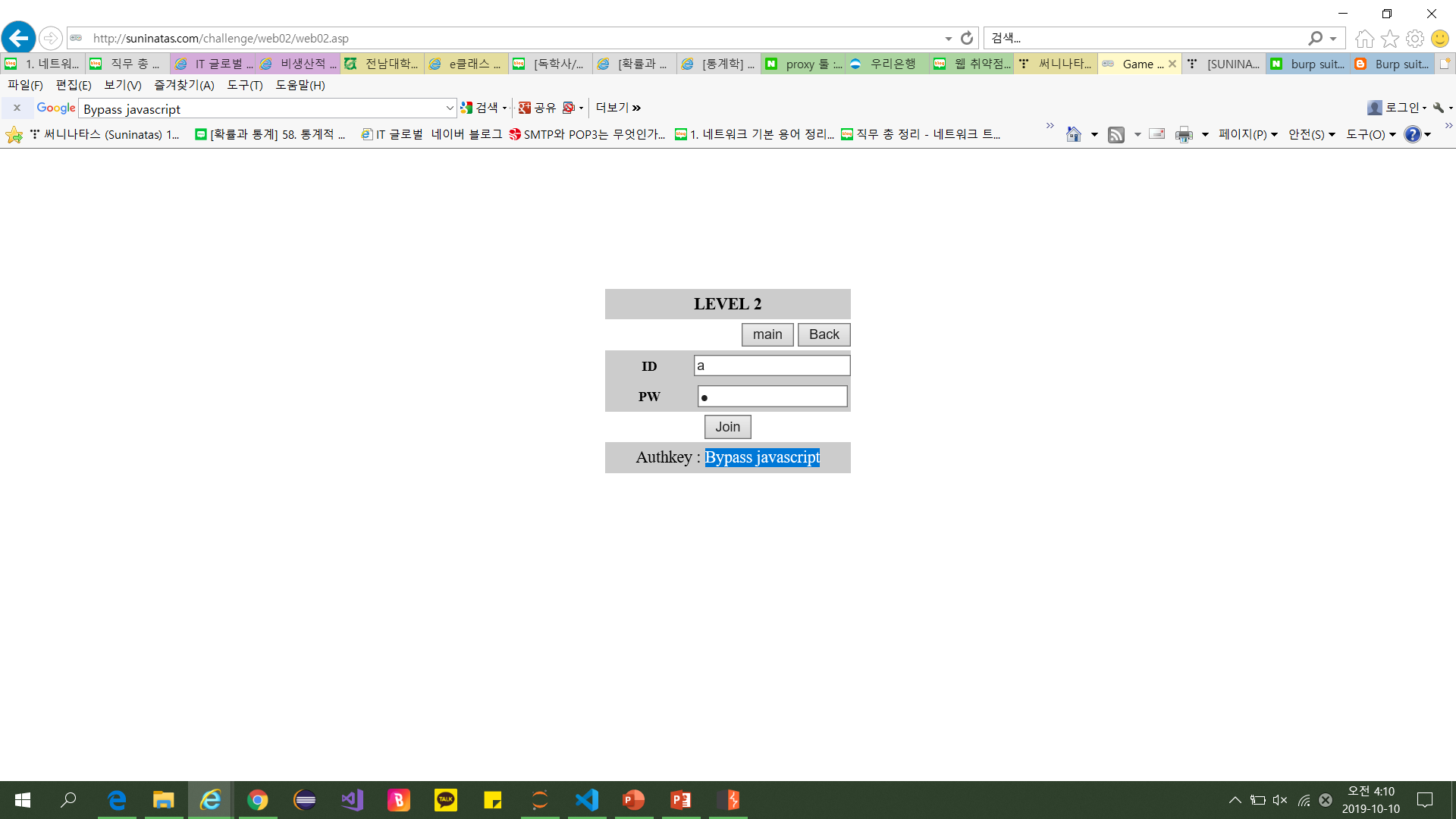
**document.web02.submit();으로 제출되게 하려고 하였다. 이를위해 script를 변경해야하는데 방법을 몰라서 인터넷에 참조하였다.**

**->web페이지 변경하기위해 , burp suite 툴을 설치.**

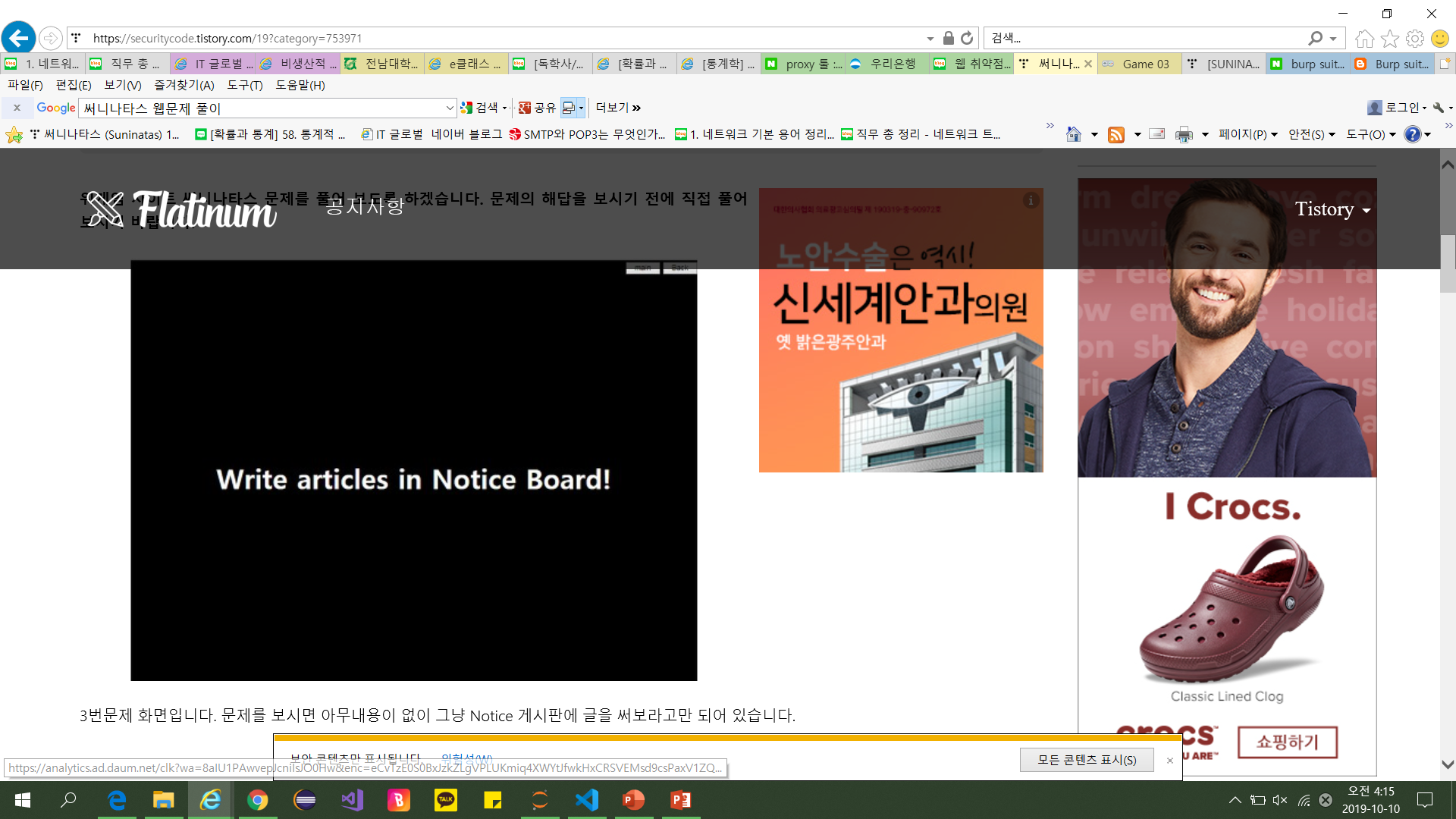
****

**처럼 변경하였다.**

**그리고 비번아이디를 서로 같게 a라고 입력하니,**

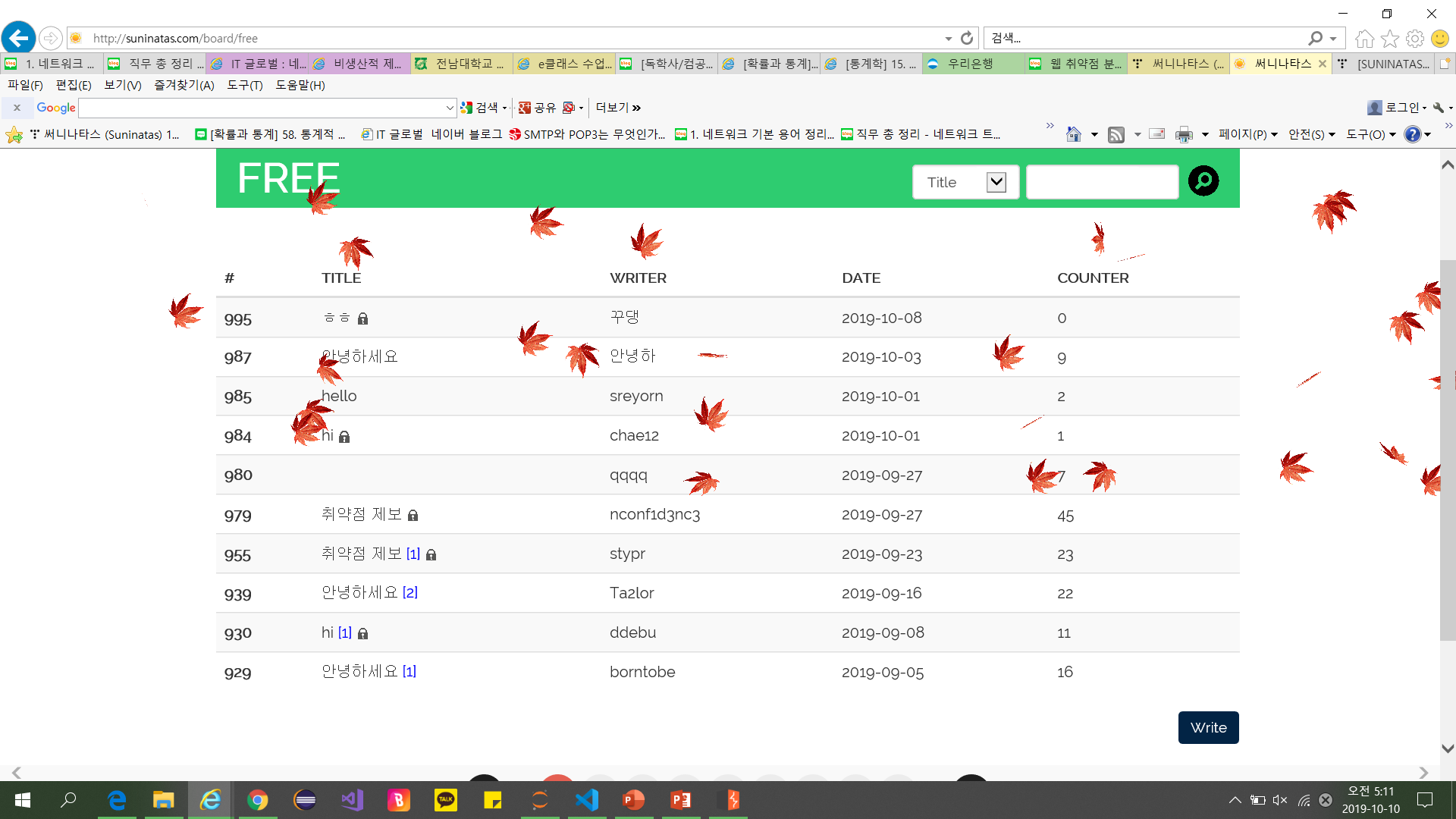
**라고 authkey가 뜨게 되고 이를 등록하였다.**

**3번**

****

**일단 무슨 창인지 몰라서 보다가 notice 창이 써니나타스에 있어서 main으로 빠져 나와 그곳에 글을 쓰려고 들어갔다.**

**그런데 글 작성 창이 없고, free 자유게시판에만 write부분이 있었다.**

****

**그래서 한참 동안 어떻게 해야 하는지 몰라서 페이지 만드는 방법에 대해 고민하다가**

**맨 위에 url 부분을 보니**

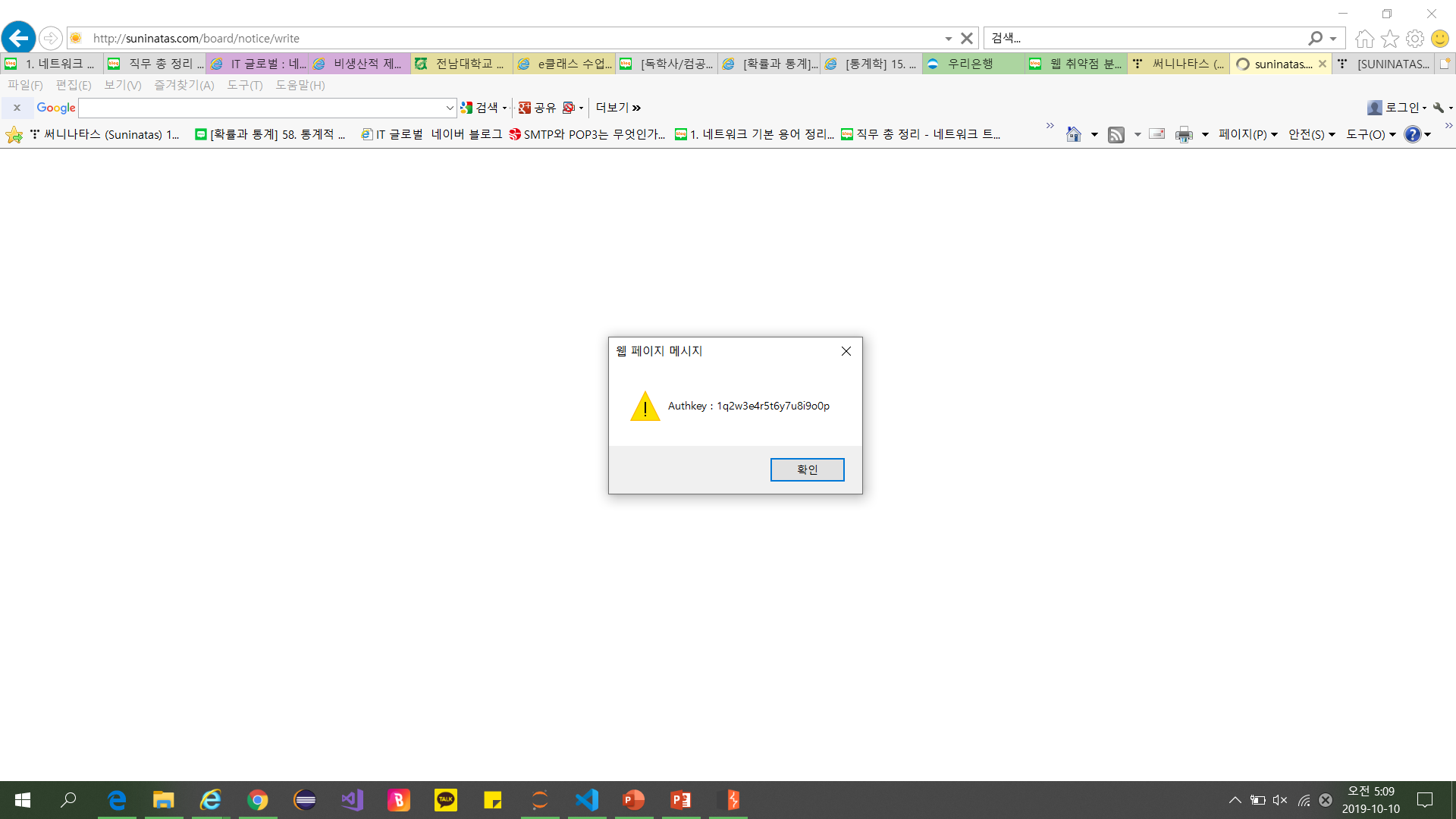
**http://suninatas.com/board/free/write**

**라고 써져있는데 notice 부분은 단지** [**http://suninatas.com/board/notice**](http://suninatas.com/board/notice)

**라고만 써져있어서**

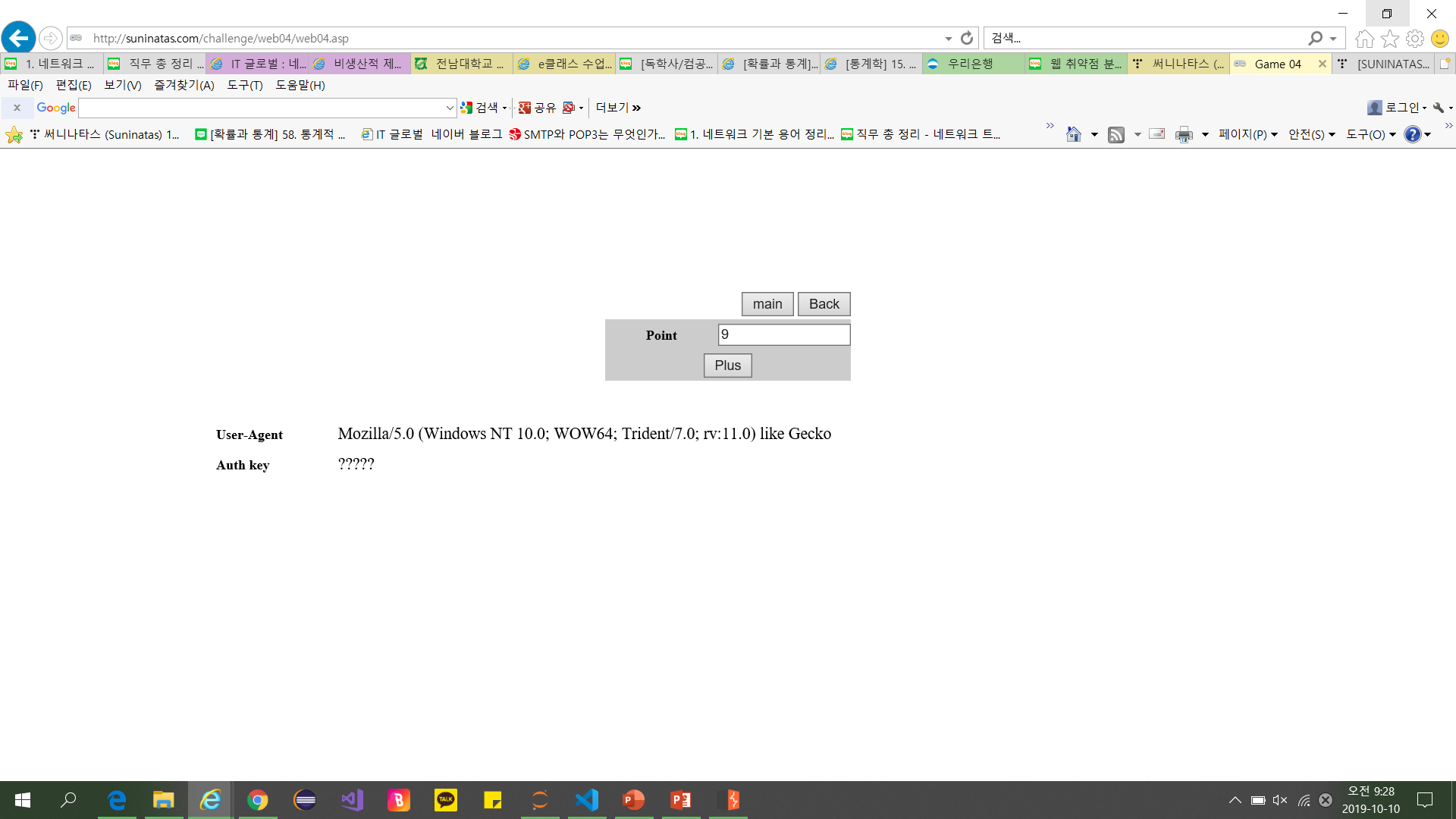
**혹시나 하고 옆에 슬쩍 /write를 썼는데 http://suninatas.com/board/notice/write**

**아니나 다를까 쓸수있는 창이 떴다…!**

****

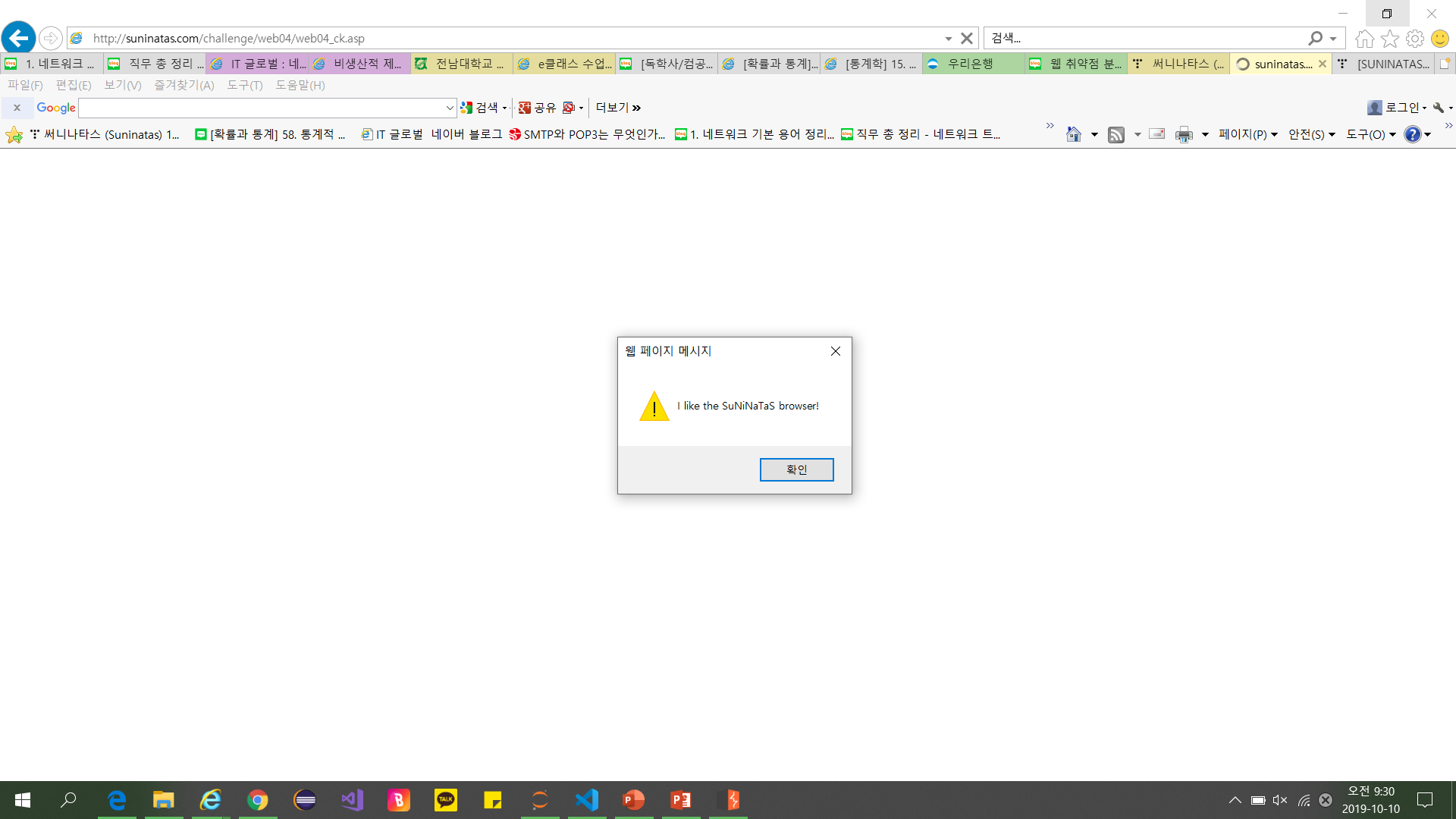
**그래서 authkey를 얻게 되었고 입력하였다.**

**4번**

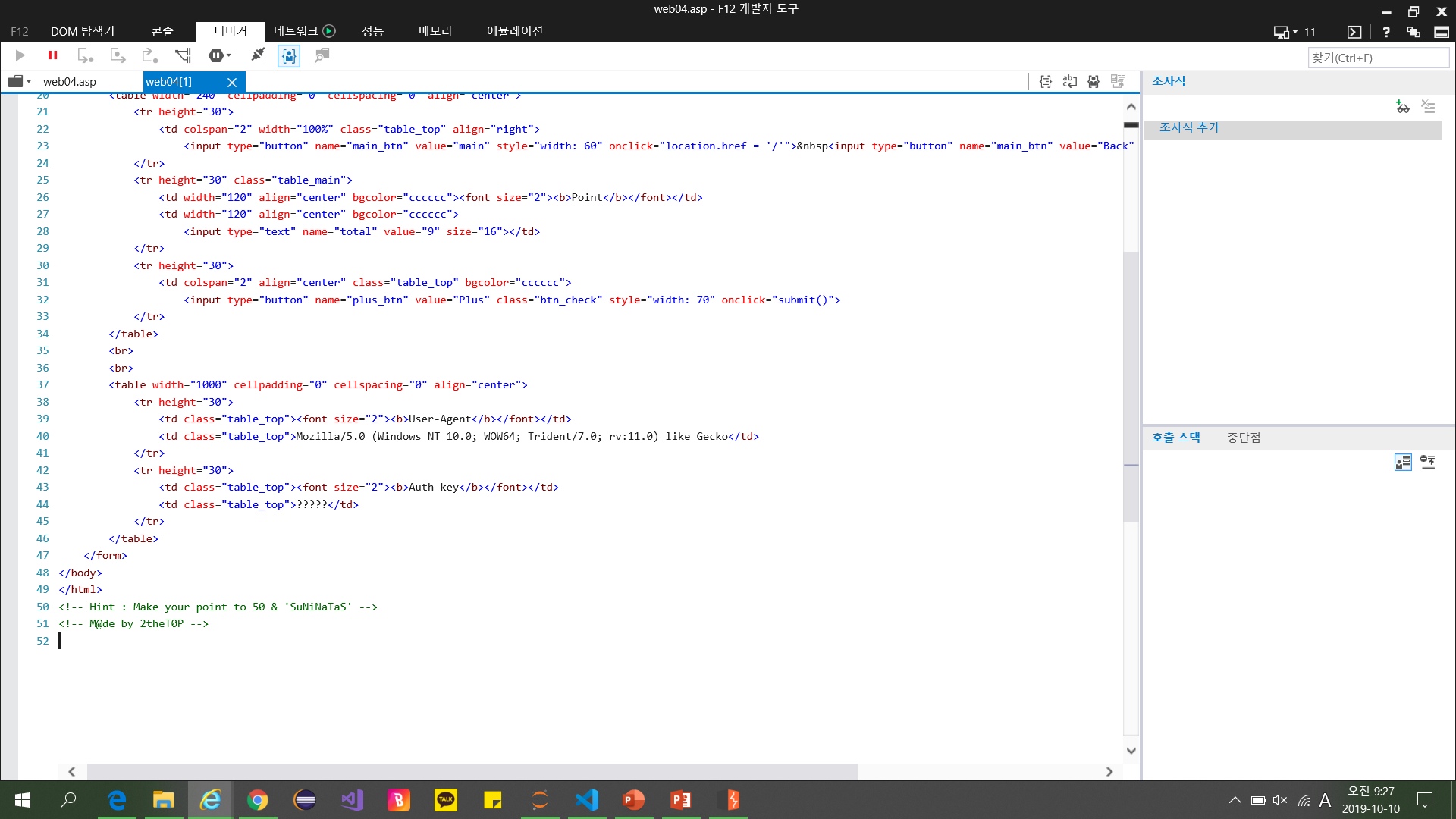
****

**문제를 보고 그냥 plus를 마냥 눌렀는데 숫자가 쭉쭉 증가하길래**

**무슨문제인지 생각하면서 하염없이 누르니까 25에 다다르니 경고창이 뜨고 더 이상 point가 증가하지 않았다.**

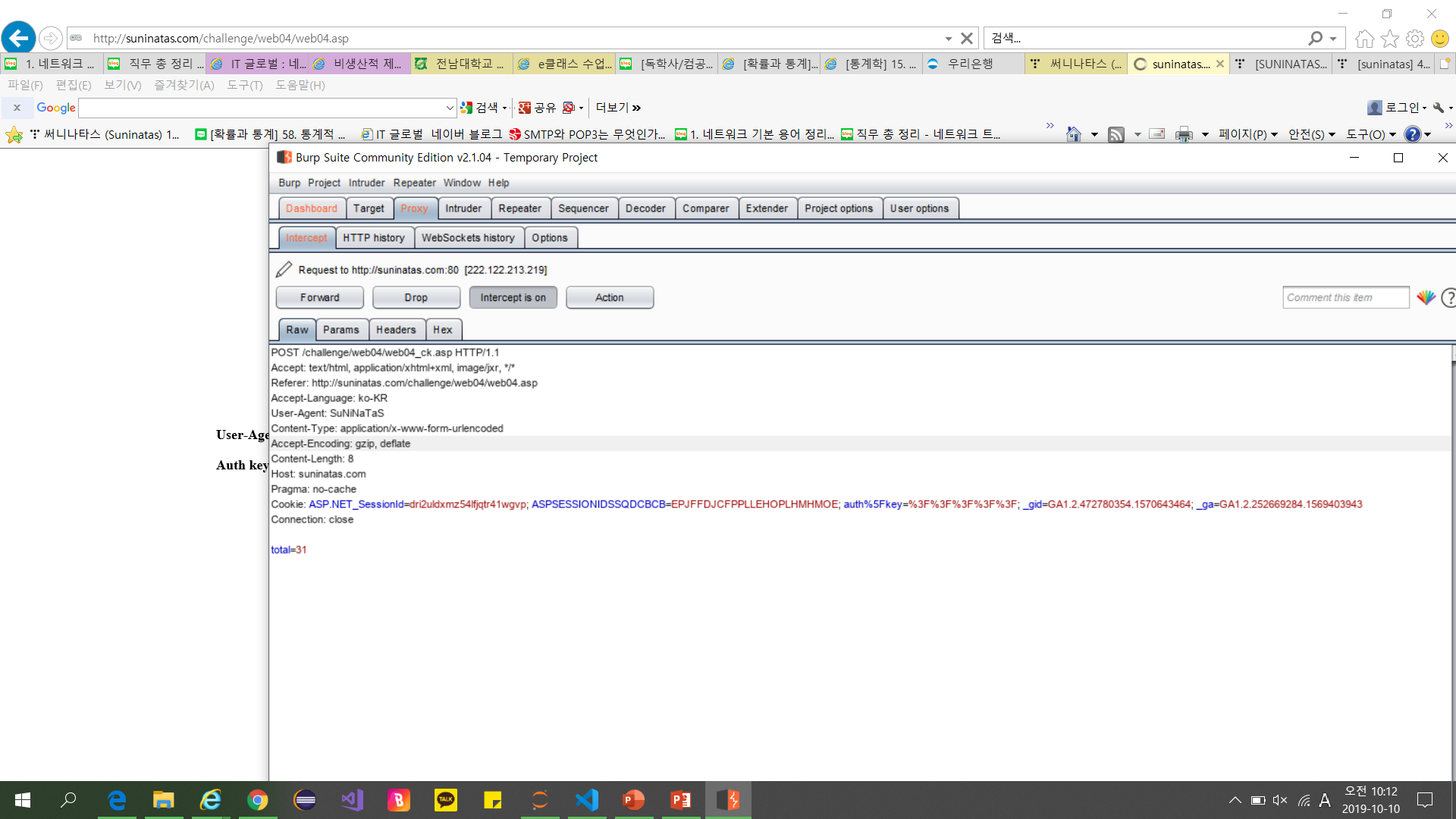
****

그래서 단순하게 소스보기를 봐서 어떤 힌트가 있을지 확인해 봤더니, 역시나 힌트가 있었따.



**50의 포인트로 만들라는것인거같은데 SuNiNaTaS가 무슨 뜻인지 몰라서 한참고민하다가**

**User-agent부분이 SuNiNaTaS로 되야 하나 싶어서 User-agent를 SuNiNaTaS로 변경하니까 point가 올라간다.**

****

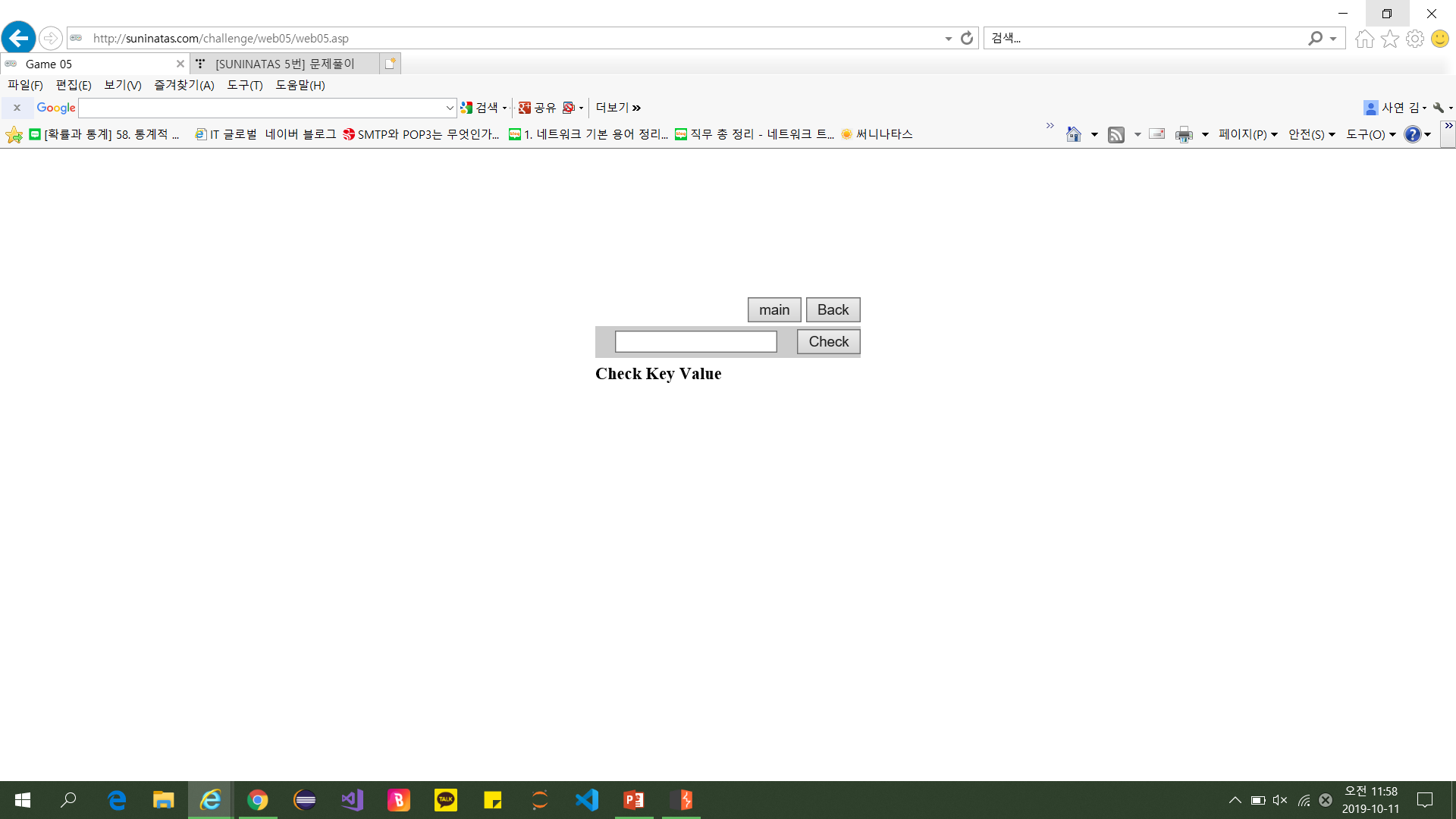
**역시나 웹 페이지를 변경해야 해서 burp suite 툴을 사용하였다.**

**근데 50으로는 어떻게 변경해야 하는지 몰라서 그냥 total부분에 50도 넣어보고 했는데**

**저거는 현재 plus를 눌렀을 때 변경된 숫자 값을 보여주는 부분 인 거 같았다.**

**그래서 다시 50이 될 때까지 계속 user-agent를 변경하면서 올렸더니, authkey가 나오고 이를 입력하였다.**

**5번**

****

**이문제도 check부분에 아무거나 쓰고 확인해보니 그냥 다시 reset되고 아무 효과도 일어나지 않아**

**웹 페이지 소스를 보았다.**

eval(function(p,a,c,k,e,r){e=function(c){return c.toString(a)};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]}];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('g l=m o(\'0\',\'1\',\'2\',\'3\',\'4\',\'5\',\'6\',\'7\',\'8\',\'9\',\'a\',\'b\',\'c\',\'d\',\'e\',\'f\');p q(n){g h=\'\';g j=r;s(g i=t;i>0;){i-=4;g k=(n>>i)&u;v(!j||k!=0){j=w;h+=l[k]}}x(h==\'\'?\'0\':h)}',34,34,'||||||||||||||||var|result||start|digit|digitArray|new||Array|function|PASS|true|for|32|0xf|if|false|return'.split('|'),0,{}))

**eval이란 부분에 함수가 묶여있는데 뭔지 몰라 코드를 그대로 검색해 보니**

**자바스크립트의 유명한 난독화 방법 중 하나였고, 그 중 packer 를 사용한 경우였다.**

**이 패킹에 사용된 문법에 대해 분석해 보고 문제를 해결하려고 찾아보았다.**

**p : 난독화 된 원래의 소스 코드**

**a : 원래 소스의 식별자의 개수입니다. 상수 처럼 쓴다.**

**c : 마찬가지로 원래 소스의 식별자의 개수입니다. 변수로 쓰입니다.**

**k : 원래 소스에 사용된 식별자의 배열.**

**e : 함수를 저장할 변수.**

**r : 난독화를 해제 하는 식별자를 담는 객체.**

**라고 한다.**

**while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);**

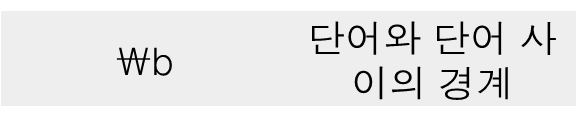
**소스 해석을 어렵게 하기 위해 트래시 코드가 추가 되어있는 부분이라고 한다.**

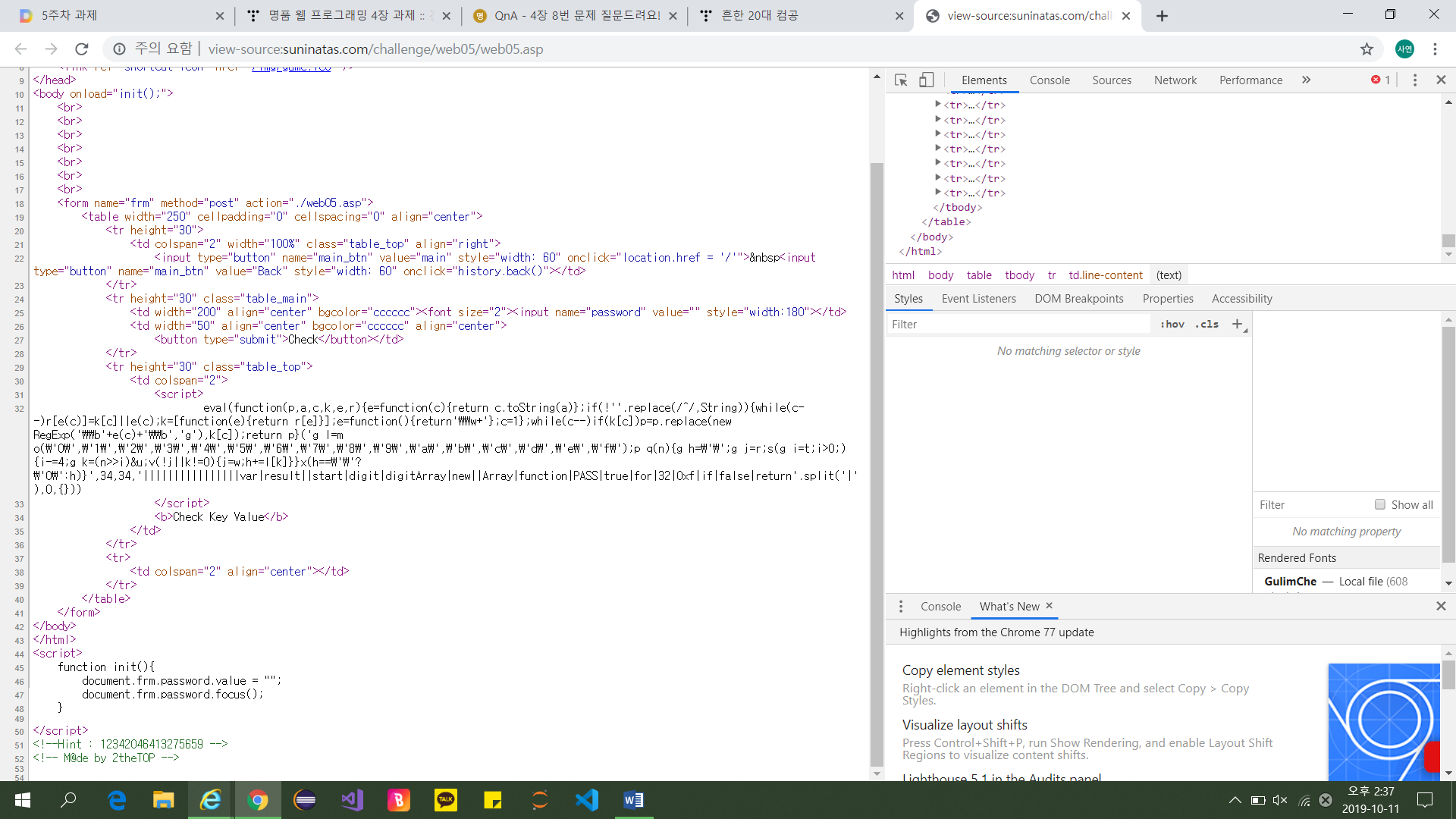
**이는, p=p.replace(/\b\w+\b/g,k[c]); 처럼 나타낼 수 있다고 한다.**

**이때 regexp가 무엇인지 찾아보았다.**

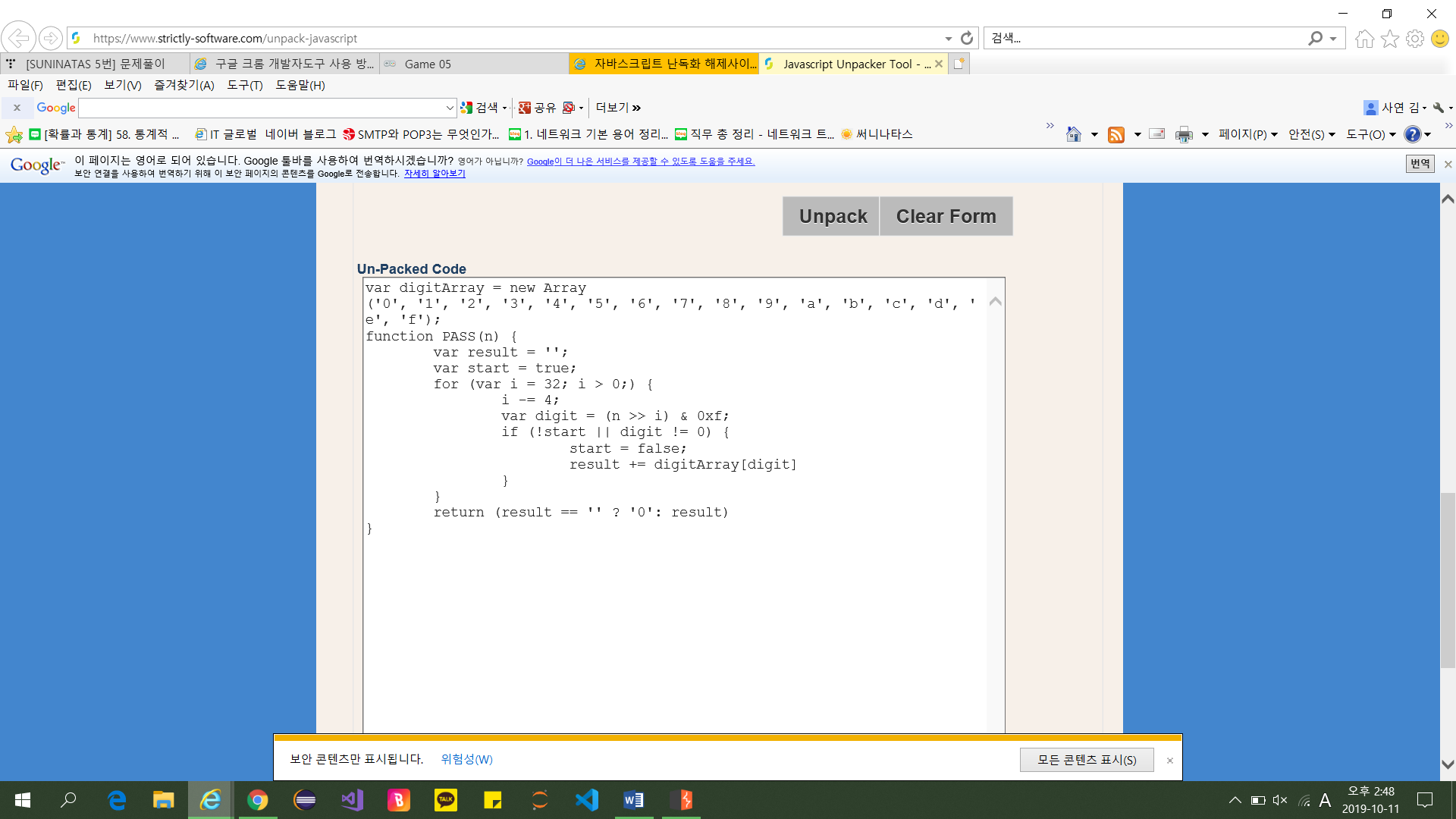
**이는 Regular Expression이고 줄여서 Regex, Regexp 등으로 불린다.**

**->특정한 규칙을 가진 문자열의 집합을 표현하기 위해 쓰이는 형식언어**

****



**마지막에 힌트 부분을 보니 저렇게 입력하면 된다는 거 같아서**



**Unpacking 하고,**

**프록시 툴로 변경하려 하니까 변경이 안돼서 풀지 못한 상태이다.**