

## 2

**LEVEL 2**

ID

PW

Authkey : ?????

2번 문제에 들어가보면 로그인 창이 보인다. SQL인젝션이 의심되어 몇몇 값을 넣어보았다.

**LEVEL 2**

ID

PW

Authkey : ?????

**LEVEL 2**

ID

PW

Authkey : ?????

별다른 반응이 없는 것 같아서 소스코드를 살펴보았다.

```

▼<form method="post" name="web02">
  ▶<table width="240" cellpadding="0" cellspacing="0" align="center">...</table>
  ▼<script>
    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();
      }
    }
  </script>
  <!-- Hint : Join / id = pw -->
  <!-- M@de by 2theT0P -->
</form>

```

form부분을 보면 javascript로 작성된 코드를 볼 수 있고, 주석으로 힌트가 있는 걸 확인할 수 있다.

힌트에는 id와 pw가 같아야된다고 되어있는데 chk\_form함수를 보면 두 값이 같으면 빈칸으로 변경되어 풀리지 않는다.

따라서 console에서 값을 변조하여 두 값을 같게 만들어 준 후 submit하면

```

> document.web02.id.value = 1;
< 1
> document.web02.pw.value = 1;
< 1
> document.web02.submit();|

```

**LEVEL 2**

main

Back

ID

PW

Join

Authkey : Bypass javascript

authkey가 뜨게 된다.

I N P U T A U T H K E Y

Bypass javascript

SUBMIT

suninatas.com 내용:

Congratulation, You have solved Challenge 2!

확인