

# webhacking.kr 5번문제

Xero

박준혁 (한양대학교 신소재공학부 2학년 군휴학 중)

2016-03-28

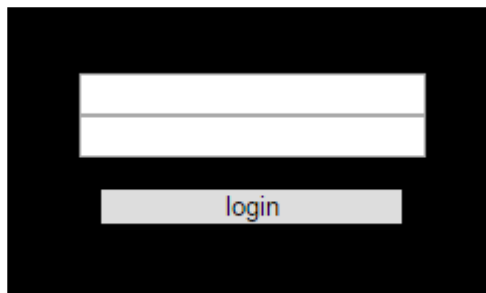
Email : wnsгурzxc@naver.com

Facebook : <https://www.facebook.com/wnsgurzxc>

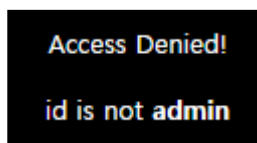
아래처럼 Login과 Join 버튼이 있다.



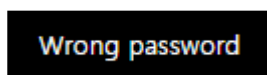
Login으로 들어가니 다음과 같이 Login하는 곳이 나왔다.



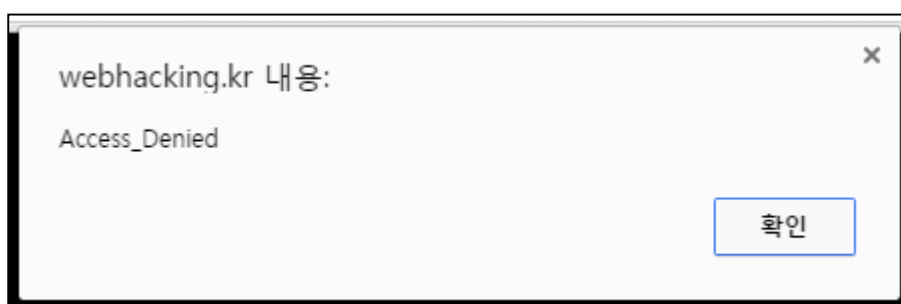
아무 값이나 넣고 로그인을 하니 id가 admin이 아니라고 한다.



아이디를 admin으로 로그인하니 비밀번호가 틀렸다고 한다.



뒤로 돌아가서 Join버튼을 눌러보면 안 들어가진다.



no()함수는 그저 접근을 거부시킨다.

[illegible]

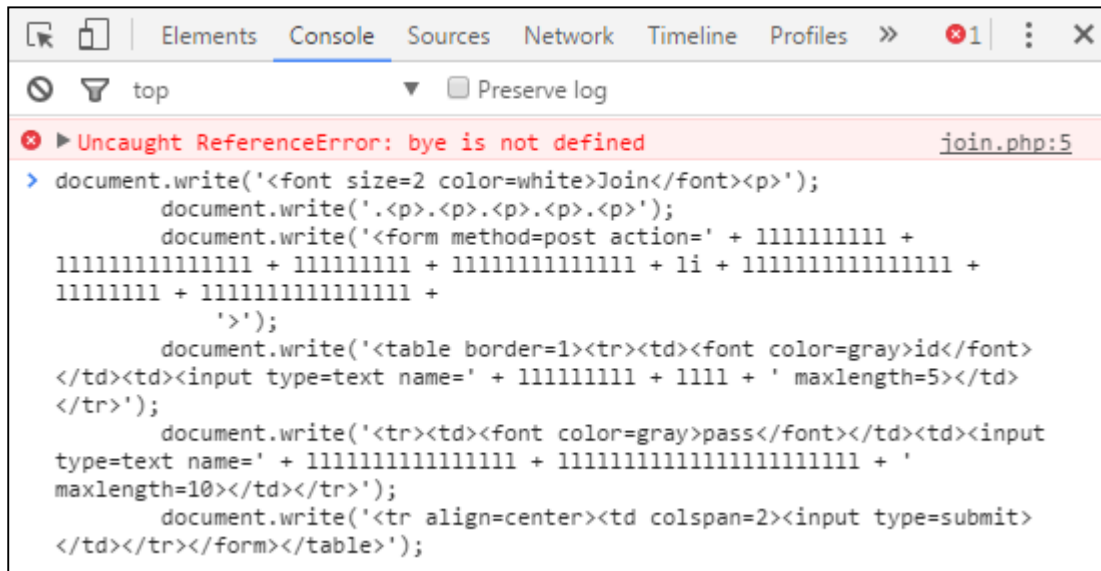
Join.php 페이지가 존재하고, 그저 검은 화면만 떠있다.

소스를 보면 다음과 같이 난독화 되어있다.

[illegible]

직접 치환을 해도 되겠지만 귀찮아서 그냥 소스를 대충 보니 앞쪽 if 문 두 개로 조건을 통과 못 하면 접근을 거부시킨다.

따라서 else 뒤쪽의 소스를 chrome의 개발자도구를 이용하여 console에 붙여넣었다.



```

Uncaught ReferenceError: bye is not defined
    at join.php:5

> document.write('<font size=2 color=white>Join</font><p>');
    document.write('<p>.<p>.<p>.<p>.<p>');
    document.write('<form method=post action=' + 1111111111 +
1111111111111111 + 1111111111 + 1111111111111111 + 1i + 1111111111111111 +
1111111111 + 1111111111111111 +
    '>');
    document.write('<table border=1><tr><td><font color=gray>id</font>
</td><td><input type=text name=' + 1111111111 + 1111 + ' maxLength=5></td>
</tr>');
    document.write('<tr><td><font color=gray>pass</font></td><td><input
type=text name=' + 1111111111111111 + 1111111111111111111111111111 + '
maxLength=10></td></tr>');
    document.write('<tr align=center><td colspan=2><input type=submit>
</td></tr></form></table>');
  
```

그러자 다음과 같이 정상적인 회원가입 창이 나왔다.



아이디를 admin으로 하고 비밀번호를 1234로 가입을 하니 다음과 같이 이미 존재한다고 한다.

**id 'admin' is already exists**

SQL구문이라고 생각하고 id 뒤에 공백을 하나 주기로 했다.

SQL구문의 INSERT문이라면 뒤에 공백이 있다면 제거하기 때문에 admin 뒤에 공백을 넣어서 회원가입 하더라도 admin 으로 인식되는 취약점을 이용한 것이다.

근데 소스를 보면 id의 maxLength가 5로 되어있다.

```
document.write('<table border=1><tr><td><font color=gray>id</font></td><td><input type=text
name=' + 1111111111 + 1111 + ' maxLength=5></td></tr>');
```

그래서 maxlength 값을 6으로 변경하고 id에 'admin' 값을 주어보았다.  
그러자 다음과 같이 sign up을 출력하고 회원가입이 되었다.

sign up

다시 login창으로 가서 id에 admin과 비밀번호를 입력하니 다음과 같이 클리어되었다.

You have cleared the 5 problems.

Score + 300