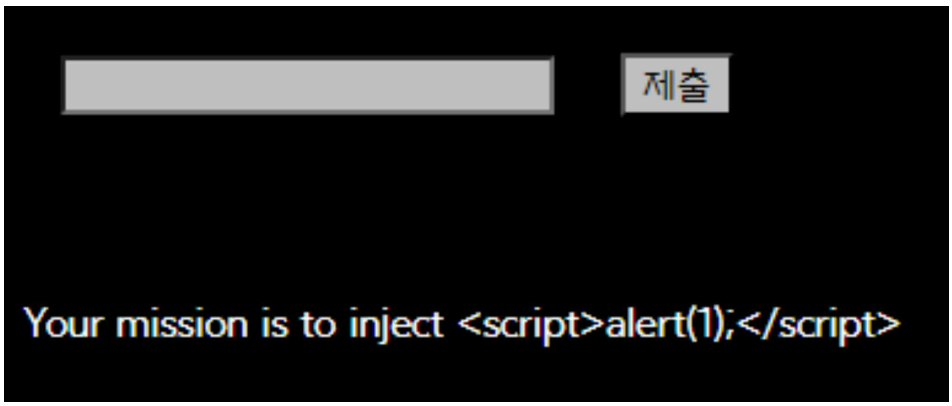
# WhiteHat School 1기

## Injection 문제 Write-up

Team: 과부화

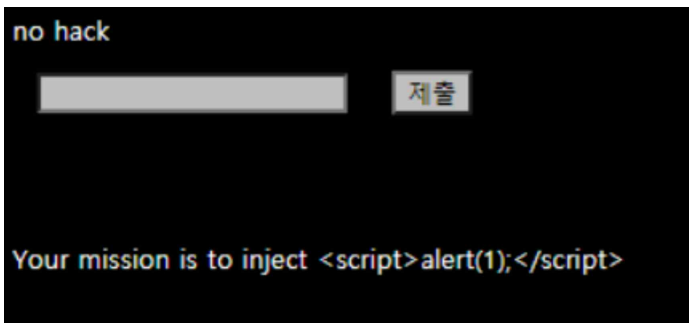
Writer: 김동규

# 문제분석




문제를 살펴보게 되면 텍스트를 입력할 수 있는 상자와 제출 버튼을 확인할 수 있다.
그 아래를 살펴보면 너의 임무는 <script>alert(1);</script> 구문을 삽입하는 것이라고 나와있다.

# 문제풀이




admin이라는 값을 넣어봤더니 no hack이라는 값을 출력한다.

webhacking.kr/challenge/bonus-3/index.php?code=<script>alert%281%29%3B<%2Fscript>

다른 값들을 입력해보면서 알아낸 결과, <script>alert(1);</script> 구문을 입력했을 시, 주소창에 역슬래시나 괄호들이 url 필터링이 되는 것을 보았다.

url 필터링을 회피하는 방법을 생각하다가NULL 필터링을 생각하였고 바로 사이사이에 %00, NULL 값을 넣어주었다.

->
%00<%00s%00c%00r%00i%00p%00t%00>%00a%00l%00e%00r%00t%00(%001%00);%00<%00/%00s%00c%00r%00i%00p%00t%00>%00

결과