< 1번 워게임 풀이문서 >

김구민



첫 화면은 다음과 같이 php언어로 이루어진 소스 코드가 주어진다. 소스를 살펴보면

include “./config.php” 🡺 config.php 파일을 참조

login\_chk() 🡺 login\_chk() 함수를 이용해서 로그인 확인

dbconnect() 🡺 데이터베이스와 사이트를 연결

if(preg\_match('/prob|\_|\.|\(\)/i', $\_GET[id])) exit("No Hack ~\_~"); // do not try to attack another table, database! 🡺 preg\_match() 함수를 이용해서 id값을 필터링

if(preg\_match('/prob|\_|\.|\(\)/i', $\_GET[pw])) exit("No Hack ~\_~");

🡺 preg\_match() 함수를 이용해서 pw값을 필터링

*/prob|\_|\.|\(\).i- 는 테이블에 직접 접근을 제한하고, 추가적으로 information\_schema에 접근*

*prob, \_(underline), .(마침표), (\)를 필터링 하여 감지되면 No Hack을 출력*

$query = "select id from prob\_gremlin where id='{$\_GET[id]}' and pw='{$\_GET[pw]}'"; 🡺 쿼리문

echo "<hr>query : <strong>{$query}</strong><hr><br>"; 🡺 쿼리문 업데이트해서 상단에 출력

$result = @mysql\_fetch\_array(mysql\_query($query)); 🡺 mysql\_query() 함수와 쿼리를 이용해 mysql\_fetch\_array() 함수로 연관 배열에 접근하여 확인한 값을 result에 저장

if($result['id']) solve("gremlin"); 🡺 result에 id를 참조했을 때 pw가 맞으면 gremlin 문제 해결

highlight\_file(\_\_FILE\_\_); 🡺 ?

GET 방식의 메소드를 이용하는 사이트에서는 사이트 주소창에 입/출력을 하기 때문에 주소 창에 쿼리를 입력함으로써 진행할 수 있다.

url에 변수 값 수정시 php?[변수명]=[입력값] 방식으로 입력한다.

첫번째 변수 입력 후 두 번째 변수를 입력시 php?[변수명]=[입력값]&[변수명]=[입력값] 양식으로 입력한다.

id와 pw를 데이터베이스에 조회해서 존재하면 로그인하는 방식이다.

쿼리문이 참인지 거짓인지만 판단하기 때문에 id변수에 참을 입력해주면 해결할 수 있다.

pw변수의 경우에도 참이 되도록 입력해주면 해결할 수 있다.

초기 쿼리를 살펴보자.



id와 pw 변수에 이미 ‘ ‘(작은따옴표) 처리가 되어있음을 알 수 있다.

그렇기 때문에 ?id=1&pw=1’ or ‘1’ = ‘1을 입력하면 다음과 같이 해결할 수 있다.

