WhiteHat School 1기

Injection 문제 Write-up

Team: 과부화

Writer: 정진교

문제분석

화이트햇스쿨 정도원 멘토(rubiya)님이 제작하신 사이트인 los.rubiya.kr에서
문제를 하나 골라와봤다.

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)|#|-/i', $_GET[pw])) exit("No Hack ~_~");
  if(strlen($_GET[pw])>6) exit("No Hack ~_~");
  $query = "select id from prob_nightmare where pw=('{$_GET[pw]}') and id!='admin'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) solve("nightmare");
  highlight_file(__FILE__);
?>
```

이번 코드에서 살펴볼 점은 preg_match 함수와 strlen 함수 그리고
pw 쿼리를 괄호로 묶었다는 점이다.

저번 Write-Up 풀이에서 설명했듯이
preg_match 함수는 문자열 안에서 특정한 정규식 패턴의 존재 여부를 찾는데
유용한 함수로
prob _ . () # - 이 정보들을 id와 pw 입력 값에서 필터링을 한다는 것이다.

strlen 함수를 보게 되면 pw의 입력 길이가 6이 넘어가면 안된다는 조건이 있다.
(strlen($_GET[pw])>6)

즉, 6자 이내로 id!=’admin’을 우회하는 것이 문제의 핵심이라는 것을 알 수 있다.

id!=’admin’을 주석처리를 하기 위해 몇 가지 주석 처리 방법을 생각해보았다.
#을 쓰는 방법과 –을 쓰는 방법은 preg_match 함수에 의해 필터링이 되어 불가능했다.

다른 방법으로는 ;%00이 있다.
mysql에서는 ;%00을 입력할 시 쿼리의 마지막으로 생각해 뒤를 읽지 않기 때문에 이 구문을 사용하였다.

해당 문제를 푸려면 자동 형 변환에 대한 이해가 필요하다.

자동 형 변환이란 조건절에 있는 데이터 타입이 다르면 '우선 순위가 있는 쪽'으로 '형 변환'이 내부적으로 발생하게 되는 것을 말한다.

자동 형 변환의 규칙은 다음과 같다.

1. 묵시적 형 변환으로 풀 테이블 스캔(테이블의 내용을 전체 다 살펴봄)이 발생한다.
2. 기본적으로 문자열은 0으로 치환된다. 따라서 문자와 숫자 0을 비교하면 참이다.
3. 문자열과 숫자를 비교할 때 가장 처음 글자와 숫자가 일치하는지 비교한다.
   일치하면 참, 다르면 거짓이다.

idx(INT UNSIGNED)	name(VARCHAR)	id(VARCHAR)	password(VARCHAR)
1	name1	id1	password1
2	name2	id2	password2
3	1name	1id	1password
4	2name	2id	2password
5	0	0	0
6	1	1	1
7	0name	0id	0password
8	name0	id0	password0

위 테이블(testtable)을 예시로 들어보고자 한다.
SELECT * FROM testtable WHERE id=0; 쿼리를 짜보았을 때,
1,2,5,7,8번 컬럼이 나오게 된다.

id 컬럼의 문자열과 숫자를 비교하여 나타난 결과 중, 1,2,8번 컬럼은 첫 번째 글자가 문자이기 때문에 문자는 0으로 변하게 된다는 규칙에 따라 참이 된다.

1. 컬럼의 첫 문자 'i'
2. 숫자와 비교하기 위해 이를 0으로 변환
3. 0으로 변한 'i'와 0이 같은가?
4. 같으므로 참
5. 검색 결과에 반영

SELECT * FROM testtable WHERE id=1; 쿼리를 사용하게 된다면?

idx(INT UNSIGNED)	name(VARCHAR)	id(VARCHAR)	password(VARCHAR)
3	1name	1id	1password
6	1	1	1

위의 결과가 나타나게 된다.

1. 컬럼의 첫 문자 '1'
2. 첫 문자가 숫자이므로 숫자로 변경한다.
3. 첫 문자 '1은 숫자 1로 치환되었다.
4. 치환된 숫자와 비교할 숫자 1이 일치하므로 참
5. 검색 결과에 반영

나머지 컬럼은 문자 == 0이거나 첫 번째 숫자가 1이 아님과 같은 이유로 거짓이 되어 검색되지 않는다.

문제풀이

자동 형 변환의 규칙 중 문자열은 숫자 0과 같다라는 점을 이용해
값을 넣어주게 되는데 (%27 = 싱글쿼터)
주소?pw=%27)=0;

위와 같은 값을 넣게 되면 다음과 같은 쿼리 형태가 된다.
select id from prob_nightmare where pw=('')=0;') and id!='admin'

select id from prob_nightmare where pw=('')=0; 의 깔끔한 쿼리를 위해서
%00 즉, NULL 값을 넣어준다.
주소?pw=%27)=0;%00
select id from prob_nightmare where pw=('')=0;') and id!='admin'
첫 번째 페이지에서 설명한 주석 처리 방법 중 %00을 선택한 것이다.

결과

query : **select id from prob_nightmare where pw=('')=0;') and id!='admin'**

NIGHTMARE Clear!

```php
<?php
  include "./config.php";
  login_chk();
  $db = dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)|#|-/i', $_GET[pw])) exit("No Hack ~_~");
  if(strlen($_GET[pw])>6) exit("No Hack ~_~");
  $query = "select id from prob_nightmare where pw=('{$_GET[pw]}') and id!='admin'";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysqli_fetch_array(mysqli_query($db,$query));
  if($result['id']) solve("nightmare");
  highlight_file(__FILE__);
?>
```