WhiteHat School 1기

Injection 문제 Write-up

Team: 과부화

Writer: 정진교

문제분석

취약점… lssmsmam

SQL INJECTION

id : guest
pw : guest
제출

---

view-source

```
<?php
  include "../../config.php";
  if($_GET['view_source']) view_source();
?><html>
<head>
<title>Challenge 45</title>
</head>
<body>
<h1>SQL INJECTION</h1>
<form method=get>
id : <input name=id value=guest><br>
pw : <input name=pw value=guest><br>
<input type=submit>
</form>
<hr><a href=./?view_source=1>view-source</a><hr>
<?php
  if($_GET['id'] && $_GET['pw']){
    $db = dbconnect();
    $_GET['id'] = addslashes($_GET['id']);
    $_GET['pw'] = addslashes($_GET['pw']);
    $_GET['id'] = mb_convert_encoding($_GET['id'],'utf-8','euc-kr');
    if(preg_match("/admin|select|limit|pw|=|<|>/i",$_GET['id'])) exit();
    if(preg_match("/admin|select|limit|pw|=|<|>/i",$_GET['pw'])) exit();
    $result = mysqli_fetch_array(mysqli_query($db,"select id from chall45 where id='{$_GET['id']}' and pw=md5('{$_G
    if($result){
      echo "hi {$result['id']}";
      if($result['id'] == "admin") solve(45);
    }
    else echo("Wrong");
  }
?>
</body>
</html>
```

문제는 sql 문을 인젝션 하여 admin이 나오도록 하면 된다.
인젝션을 시킬 sql 구문은 다음과 같다.
select id from chall45 where id='{}' and pw=md5('%aa') or id like 0x61646d696e--
')

문제풀이

문제 코드를 분석해보면

1) id, pw 파라미터 값을 addslashes() 처리
2) id 파라미터 인코딩 방식을 'utf-8'에서 'euc-kr' 로 변경
3) id, pw 파라미터에 admin, select, limit, pw, =, <, > 가 들어가면 exit
4) id, pw 파라미터를 토대로 SQL 쿼리를 실행
5) 쿼리 결과의 id가 "admin" 이면 문제 해결

핵심은 addslashes()다.

addslashes()는 SQL Injection을 방지하기 위해 사용하는 함수로 ' , " , / 등을 이스케이프 시켜서 인젝션을 방지하는 함수다.

ex) select * from [table] where id=$id 라는 쿼리가 있다고 가정하자.

select * from [table] where id='WhiteHatSchool’ s Project'

$id에 위와 같이 입력된다면, 쿼리는 에러가 발생한다. 왜냐하면 id='WhiteHatSchool' 가 하나로 취급되고 나머지 부분은 ' 로 묶이지 않기 때문에 에러가 발생한다.

그렇다면, 'WhiteHatSchool's Project를 id로 쓰고싶으면 어떻게 할까?

select * from [table] where id='WhiteSchool\'s Project'

이렇게 ' 앞에 \(역슬래시)를 붙여주면 이스케이프 되면서 \뒤에 붙은 ' 는 $id의 일반문자로 취급받는다. 따라서 쿼리는 에러가 발생하지 않는다.

' 앞에 \(역슬래시)를 붙여주는 것을 이스케이프 처리한다고 한다.

결론적으로 id,pw 모두 이스케이프 되기 때문에 ' , " 문자를 이용한 인젝션은 힘들다.

그러나 mb_convert_encoding()를 통해 id 파라미터에 대한 인코딩 방식을 'utf-8' 에서 'euk-kr' 로 바꿔주고 있고 여기서 취약점이 발생한다.

'euk-kr'는 멀티바이트 환경의 언어셋으로 \(백슬래시) 앞에 %a1~%fe가 붙으면 2개의 문자를 하나의 문자로 취급해서 \를 없어지게 만든다.

정리하면, addslashes()를 통해 이스케이프 되면서 ' , " 문자 앞에 \(역슬래시)가 붙어서 인젝션을 방지하고 있는 상황이지만, mb_convert_encoding()에서 취약점이 발생하므로 \를 없애면서 인젝션을 수행할 수 있다.

select id from chall45 where id='1' or id like admin #' and pw=md5('{$_GET['pw']}')와 같은 구문을

->

selectid from chall45 where id='1%fe%27 or id like 0x61646d696e %23' and pw=md5('{$_GET['pw']}')로 둔갑시킬 수 있다.

결과