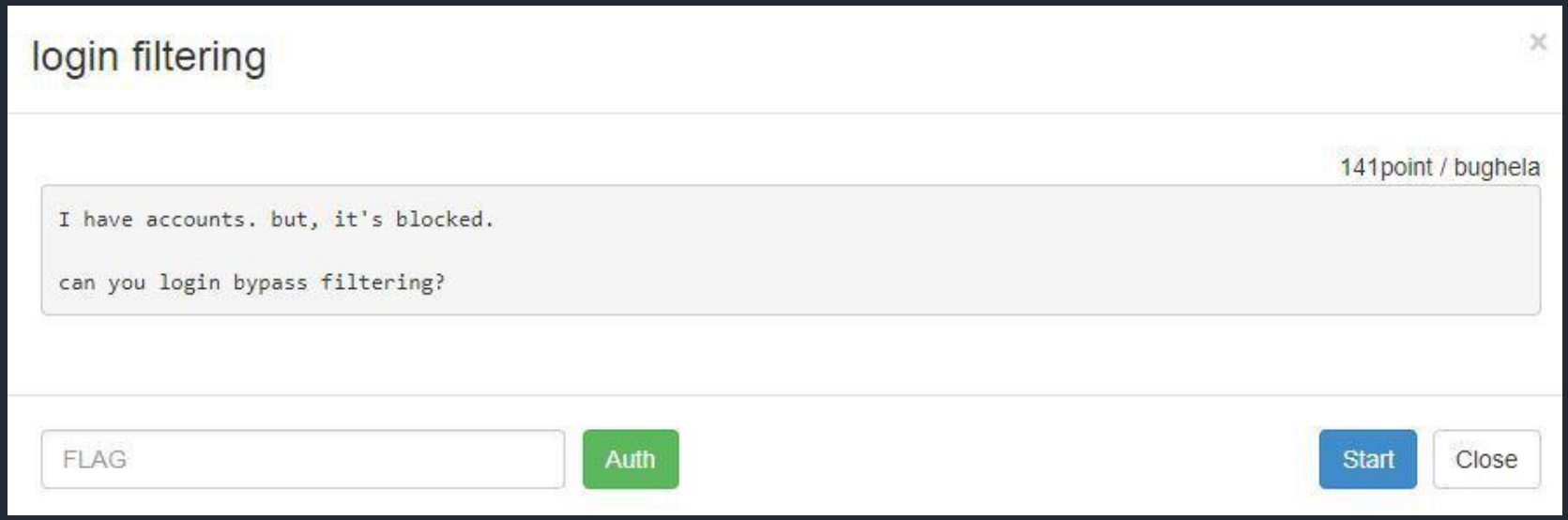
웹 초보의
웹 탈출기

Duni0107

Login Filtering 문제 풀이




ID
PW
login
get source

```php
if(isset($_POST['id']) && isset($_POST['ps'])){
 include("../lib.php"); # include for auth_code function.

 mysql_connect("localhost","login_filtering","login_filtering_pz");
 mysql_select_db ("login_filtering");
 mysql_query("set names utf8");

 $key = auth_code("login filtering");

 $id = mysql_real_escape_string(trim($_POST['id']));
 $ps = mysql_real_escape_string(trim($_POST['ps']));

 $row=mysql_fetch_array(mysql_query("select * from user where id='$id' and ps=md5('$ps')"));
```

mysql_real_escape_string이란?

➡ mysql_query에서 특수 문자열을 이스케이프 하기위해 사용되는 함수

➡ 쉽게 말해 sql injection 공격법을 방어하기 위한 함수

```php
if(isset($_POST['id']) && isset($_POST['ps'])){
 include("../lib.php"); # include for auth_code function.

 mysql_connect("localhost","login_filtering","login_filtering_pz");
 mysql_select_db ("login_filtering");
 mysql_query("set names utf8");

 $key = auth_code("login filtering");

 $id = mysql_real_escape_string(trim($_POST['id']));
 $ps = mysql_real_escape_string(trim($_POST['ps']));

 $row=mysql_fetch_array(mysql_query("select * from user where id='$id' and ps=md5('$ps')"));
```

mysql_real_escape_string이란?

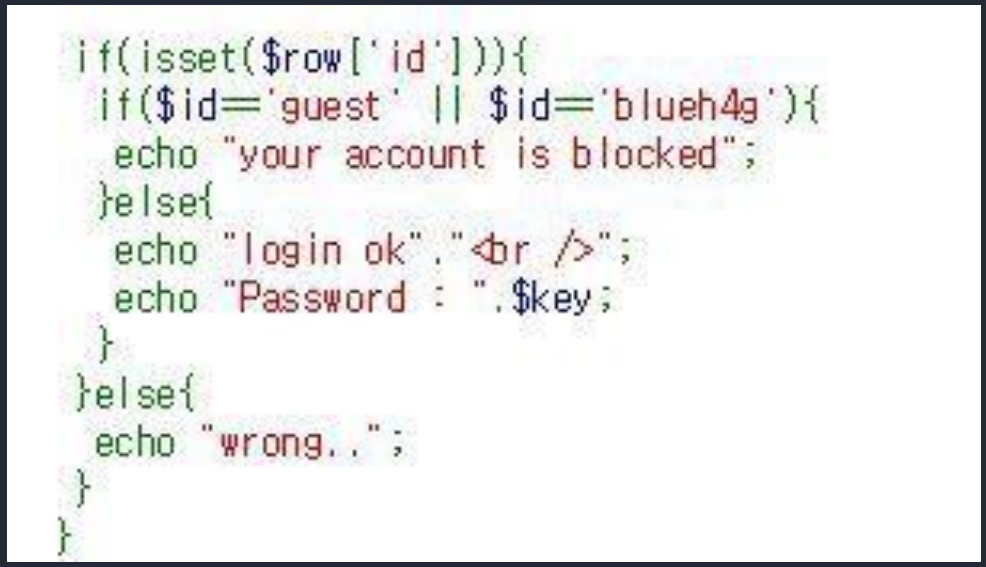
➡ mysql_query에서 특수 문자열을 이스케이프 하기위해 사용되는 함수

➡ 쉽게 말해 sql injection 공격법을 방어하기 위한 함수

VS

mysql_real_escape_string 우회 방법?

- 특정조건 하에서 가능 (멀티바이트를 사용하는 언어로 인코딩 할 시)
- ₩ 앞에 &a1_%fe 의 값이 들어가면 해당 값과 ₩에 해당하는 %5c가 합쳐져서 하나의 문자를 표현하게 됨
- sql injection 방어를 위해 생성한 ₩가 사라져서 공격이 가능해짐



```
if(isset($row['id'])){
 if($id='guest' || $id='blueh4g'){
  echo "your account is blocked";
 }else{
  echo "login ok"."<br />";
  echo "Password : ".$key;
 }
}else{
 echo "wrong..";
}
}
```

$row에 id 변수값이 존재할 경우
id가 guest이거나 blueh4g일 때 계정이 잠겨있다는 메세지가 출력

그것이 아니라면 key 값 나타남

$row에 id 변수 값이 존재하지 않을 경우 틀렸다는 메세지가 출력

→ %row에 id변수 값이 존재하면서 guest나 blue4g가 아닌 id를 입력해야겠다!

맨 아래 부분에 guest와 blueh4g의 비밀번호까지 쓰여있음
TMI일리는 없으니 이걸 이용하는게 확실하다!

결론 : 우회 방법을 찾던 중 php는 대,소문자를 고분하지만 쿼리문은 대,소문자를 구분하지 않는다는 것을 깨닫게 되었음

Id에 guest 대소문자를 섞어 Guest로 입력해주자 문제가 해결됨


느낀점 : php와 mysql_query의 특징을 잘
알면 바로 풀 수 있는 문제인데,, 그걸 몰라서,,
많이도 헤맸구나
공부를 진짜 열심히 해야겠구나..

11

Duni0107