**Практическая работа № 18.**

**Список полей в SQL в PHP**

Иногда бывают ситуации, когда мы получаем от юзера имена полей. В этом случае их тоже просто так нельзя вставлять в запрос. А только после проверки по белому списку.

Давайте посмотрим на пример уязвимости. Пусть у нас есть следующий запрос:

<?php

$query = "SELECT id,login FROM users";

$res = mysqli\_query($link, $query);

?>

Пусть результат запроса мы выводим следующим образом:

<?php

for ($data = []; $row = mysqli\_fetch\_assoc($res); $data[] = $row);

var\_dump($data);

?>

Пусть имена полей приходят через GET-параметр:

<?php

$fields = **$\_GET**['fields'];

$query = "SELECT **$fields** FROM users";

$res = mysqli\_query($link, $query);

?>

Мы ожидаем, что пользователь будет передавать что-то такое:

?fields=id,login

А злоумышленник может добавить кое-что, чего мы бы не хотели показывать:

?fields=id,login,password

№1

Воспроизведите пример, приведенный в уроке. Проверьте наличие уязвимости. Устраните ее, воспользовавшись белым списком полей.

№2

Убедитесь, что ваш код защищен от SQL-инъекции.