**Практическая работа № 14.**

**SQL инъекция в числовой параметр в PHP**

Давайте теперь рассмотрим SQL инъекцию, осуществляемую в числовой параметр. В этом случае наша длинная фунцкия mysqli\_real\_escape\_string не поможет, так как хакерском коде просто не будет кавычки - функции нечего экранировать.

Давайте посмотрим на практике. Пусть у нас есть следующая ссылка, с помощью которой осуществляется [GET-запрос](https://code.mu/ru/php/book/prime/forms/get-queries/):

<a href="?id=2">ссылка</a>

Пусть мы получаем содержимое GET-параметра в переменную:

<?php

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

?>

Пусть мы хотим достать из базы продукт с этим id:

<?php

$query = "SELECT name, cost FROM prods WHERE id=**$id**";

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

$row = mysqli\_fetch\_assoc($res);

?>

Обратите внимание на то, что, так как в переменной у нас числовое значение, то внутри запроса мы эту переменную не берем в одинарные кавычки. В этом и проявляется разница между строковыми и числовыми параметрами.

Наш GET-запрос содержится в адресе ссылки. Злоумышленник может как отредактировать ссылку в отладчике браузера, так и поменять значение GET-параметра в адресной строке браузера.

Давайте посмотрим, как злоумышленник сможет использовать эту уязвимость.

Вариант 1

Выполним безобидную атаку, просто чтобы проверить, что мы можем модифицировать SQL запрос. Изменим значение GET-параметра на следующее:

?id=-1 or cost=1000

В этом случае выполнится следующий запрос, который достанет продукт с заданной хакером ценой:

**SELECT** name, cost **FROM** prods **WHERE** id=-1 or cost=1000

Вариант 2

А теперь рассмотрим совсем не безобидную атаку. Злоумышленник может выполнить [UNION](https://code.mu/ru/sql/manual/union/) запрос и получить данные из любой таблицы! Вот так:

?id=-1 **UNION** **SELECT** login, password **FROM** users **WHERE** role=1

В результате выполнится следующий запрос, который достанет логин и пароль администратора (напомню, у него role в значении 1):

**SELECT** name, cost **FROM** prods **WHERE** id=-1

**UNION** **SELECT** login, password **FROM** users **WHERE** role=1

Если пароли на сайте хранятся не в [хешированном](https://code.mu/ru/php/book/prime/auth/hashing-function-password_hash/) виде или для хеширования используется устаревший [md5](https://code.mu/ru/php/book/prime/auth/hashing/), то все - сайт взломан.

При атаке через UNION запрос хакеру важно, чтобы количество полей в исходной выборке и в подключаемой совпадало. Но не переживайте, хакер легко подберет нужное количество, пусть и не сразу!

Защита

Как уже упоминалось ранее, защита через mysqli\_real\_escape\_string не работает в случае числовых параметров:

<?php

$id = mysqli\_real\_escape\_string($link, **$\_GET**['id']); // не работает

?>

В данной ситуации защита заключается в принудительном приведении значения параметра к числу:

<?php

$id = (int) **$\_GET**['id'];

?>

Практические задачи

№1

Опробуйте все описанные варианты использования уязвимости. Устраните уязвимость. Убедитесь, что она исчезла.

№2

Устраните уязвимость в следующем коде:

<?php

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

$query = "SELECT \* FROM products LIMIT **$from**";

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

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

var\_dump($data);

?>