**Практическая работа № 20.**

**Просмотр чужих данных через SQL в PHP**

В данном уроке мы разберем уязвимость, связанную с возможностью просмотра закрытой информации. Пусть для примера у нас есть таблица notes, в которой хранятся заметки пользователей (см. тестовые таблицы в начале раздела). Пусть мы хотим сделать так, чтобы каждый пользователь мог просматривать только свои заметки.

Пусть на странице notes.php мы будем выводить ссылки на заметки пользователя. На этой странице мы будем выводить только заметки данного пользователя, беря его id из сессии:

<?php

$user\_id = **$\_SESSION**['id'];

$query = "SELECT \* FROM notes WHERE user\_id=**$user\_id**";

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

?>

Выведем ссылки на заметки:

<?php

foreach ($data as $key => $note) {

echo '<a href="note.php?id=' . $note['id'] . '"'>' . $key . '</a>';

}

?>

На странице note.php мы будем показывать конкретную заметку при переходе пользователем по ссылке:

<?php

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

$query = "SELECT \* FROM notes WHERE id=**$note\_id**";

?>

В чем же тут проблема? Дело в том, что мы выводим список записей юзера, рассчитывая, что он будет кликать на ссылки, попадая только на свои записи. Но ведь легко можно изменить значение GET-параметра и посмотреть любую запись, независимо от того, наша она или нет - мы никак это уже не проверяем.

Пофиксим проблему следующим образом:

<?php

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

$user\_id = **$\_SESSION**['id'];

$query = "SELECT \* FROM notes WHERE id=**$id** and user\_id=**$user\_id**";

?>

Так мы будем показывать запись:

<?php

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

if ($note) {

// показываем

} else {

// попытка обращения к чужой

// или несуществующей записи

}

?>

№1

Воспроизведите пример, приведенный в уроке. Проверьте наличие уязвимости. Устраните ее.

№2

Проверьте, нет ли в нашем коде проблем с SQL-инъекциями. Если есть, устраните проблему.

№3

В следующем пример автор кода выводит различные сообщения, когда запись несуществует и когда запись чужая:

<?php

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

$query = "SELECT \* FROM notes WHERE id=**$id**";

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

if ($note) {

$user\_id = **$\_SESSION**['id'];

if ($note['user\_id'] === $user\_id) {

// показываем запись

var\_dump($note);

} else {

echo 'запись с таким id вам не принадлежит';

}

} else {

echo 'запись с таким id нет';

}

?>

Объясните, почему так лучше не делать.