

**Домашнее задание № 7**

***Типы атак I, OWASP top 10***

CVE, CWE, CAPEC, Injection, SQL

**1. Изучить SQL запросы.**

* [Пройти как можно больше заданий в SQLBOLT](https://sqlbolt.com)

**2. Лабораторные работы по OWASP TOP 10.**

* Выполнить 2 лабораторные работы из практики Brocken Access Control
  + [Lab Broken Access Controll 1](https://portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter)
  + [Lab](https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter) [Broken Access Controll](https://portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter)\_[2](https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter)
* Выполнить 1 лабораторную работу из практики Injections
  + [Lab Injection 1](https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data)
* Выполнить 1 лабораторную работу из практики Server-Side Request Forgery
  + [Lab SSRF 1](https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-localhost)

1. **Тренировка поиска уязвимостей на примере OWASP Juice Shop**

* [**OWASP Juice Shop**](https://spy-soft.net/owasp-juice-shop/)

Ссылки на дополнительные ресурсы

* [Тренировка написания SQL запросов в SQLBOLT](https://sqlbolt.com)
* [Lab Broken Access Controll 1](https://portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter)
* [Lab](https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter) [Broken Access Controll](https://portswigger.net/web-security/access-control/lab-user-role-controlled-by-request-parameter)\_[2](https://portswigger.net/web-security/access-control/lab-user-id-controlled-by-request-parameter)
* [Lab Injection 1](https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data)
* [Lab SSRF 1](https://portswigger.net/web-security/ssrf/lab-basic-ssrf-against-localhost)
* [OWASP Juice Shop](https://spy-soft.net/owasp-juice-shop/)