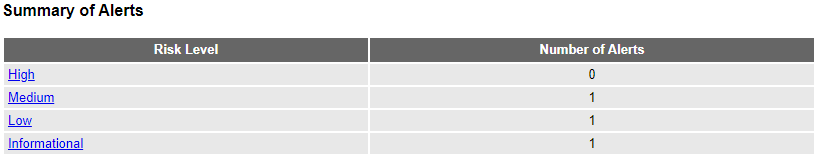
### Лабораторная работа №5

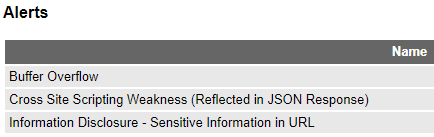
*Выполнил студент 4 курса, 12 группы*

*Лобко Артем*

В качестве веб-приложения для проверки послужил проект по курсу “Проектирование человеко-машинных интерфейсов” - Книжный онлайн-магазин.

По результатам проверки были выявлены следующие уязвимости:





* **Buffer Overflow**

Явление, возникающее, когда компьютерная программа записывает [данные](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5) за пределами выделенного в памяти буфера.

Переполнение буфера обычно возникает из-за неправильной работы с данными, полученными извне, и памятью, при отсутствии жесткой защиты со стороны подсистемы программирования (компилятор или интерпретатор) и операционной системы. В результате переполнения могут быть испорчены данные, расположенные следом за буфером (или перед ним).

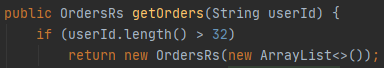
Переполнение буфера является одним из наиболее популярных способов взлома компьютерных систем, так как большинство языков высокого уровня использует технологию стекового кадра — размещение данных в [стеке](https://ru.wikipedia.org/wiki/%D0%A1%D1%82%D0%B5%D0%BA) процесса, смешивая данные программы с управляющими данными (в том числе адреса начала стекового кадра и адреса возврата из исполняемой функции).

Переполнение буфера может вызывать аварийное завершение или зависание программы, ведущее к *отказу обслуживания*. Отдельные виды переполнений, например переполнение в стековом кадре, позволяют злоумышленнику загрузить и выполнить произвольный машинный код от имени программы и с правами учетной записи, от которой она выполняется

**Как править:**



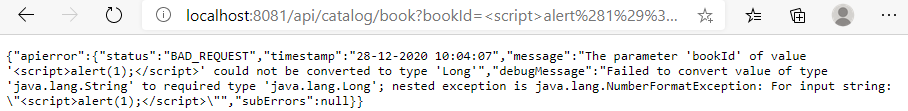
Собственно и была добавлена проверка на валидность длины входящего параметра:



* **Cross Site Scripting Weakness**

Уязвимость возникает, когда программное обеспечение не выполняет или неправильно выполняет нейтрализацию входных данных перед их отображением в браузере пользователя. В результате злоумышленник может внедрить и выполнить произвольный код HTML и скрипт в браузере пользователя в контексте уязвимого веб-сайта.

В отчете OWASP положила в параметр bookId значение, которое не может быть сконвертировано в числовой тип:

  
Исправлена путем проверки возможности конвертации значения входного параметра.

* **Sensitive Information in URL**

Была исправлена путем исправления параметра запроса:

