Министерство науки и высшего образования Российской Федерации  
Федеральное государственное автономное образовательное учреждение высшего образования  
УРАЛЬСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ ПЕРВОГО ПРЕЗИДЕНТА РОССИИ Б. Н. ЕЛЬЦИНА  
(УрФУ)

ОЦЕНКА РАБОТЫ

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4  
по дисциплине «Разработка безопасных веб-приложений»

Дата Подпись Ф.И.О.

Преподаватель Мирвода С.Г.

Студент Малиновский А.А.

Студент Панькова А.С.

Студент Тимофеева В.В.

Специальность (направление подготовки) 10.05.02

Группа РИ-581220

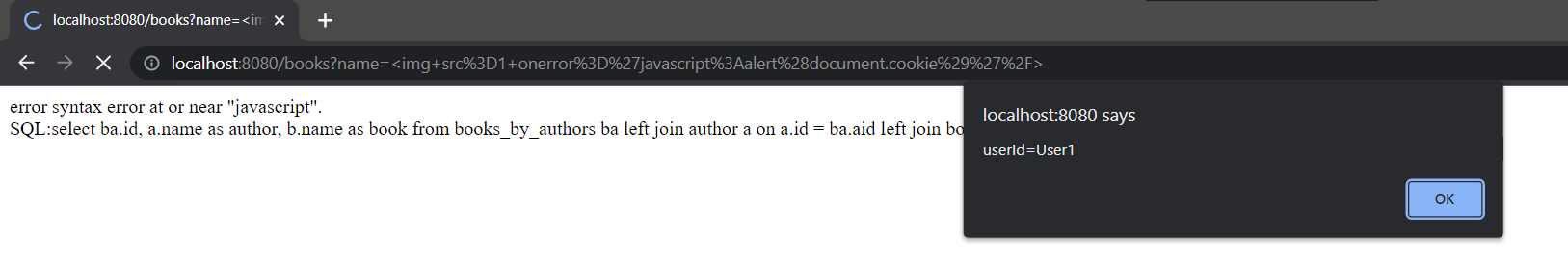
Екатеринбург 2022

## Reflected XSS

Используя строку поиска или напрямую через ссылку, можно сформировать следующий запрос:

<img src=1 onerror='javascript:alert(document.cookie)'/>

Это позволит украсть cookie жертвы, перешедшей по ссылке.

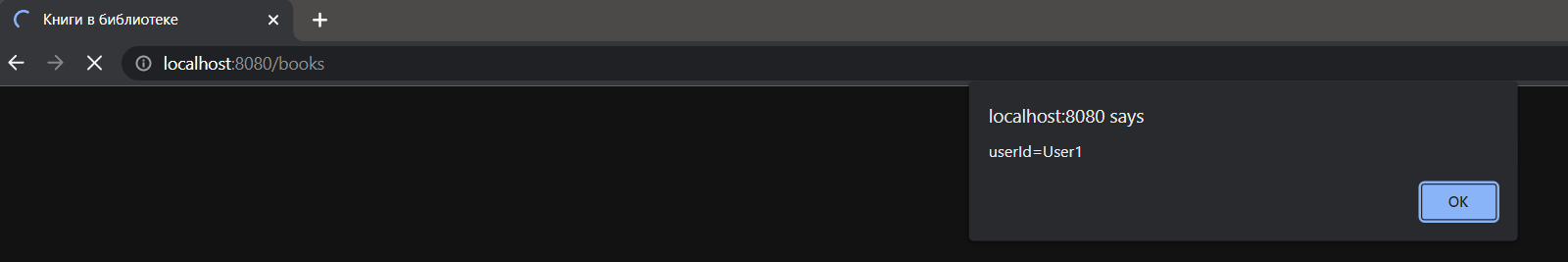


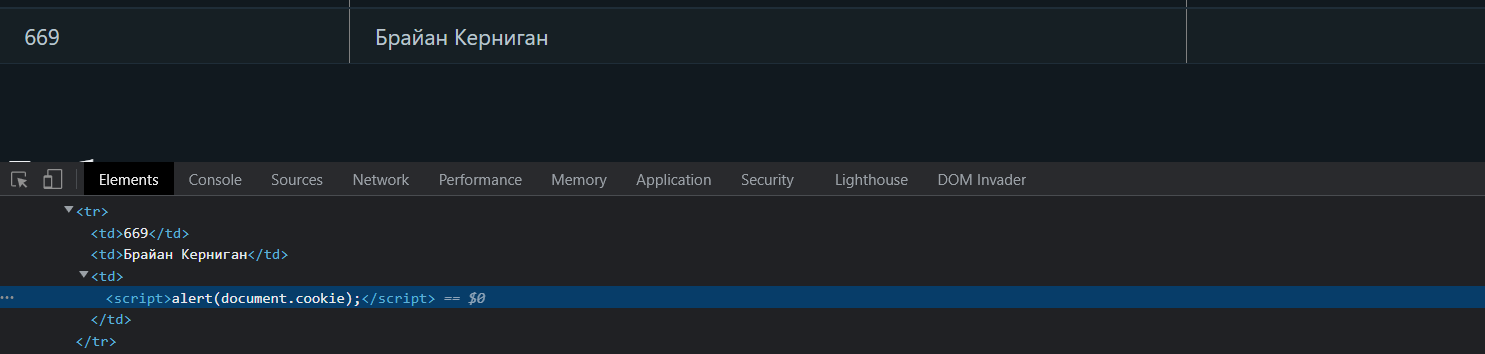
## Persisted XSS

В строке названия добавляемой книги можно записать следующий скрипт:

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

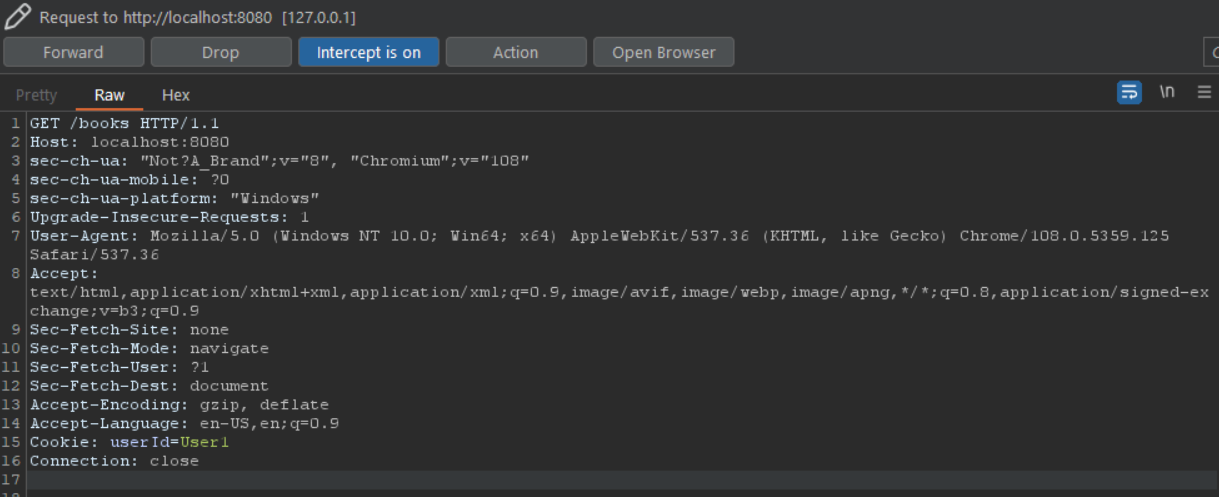
Он выполнится у любого зашедшего на страницу.

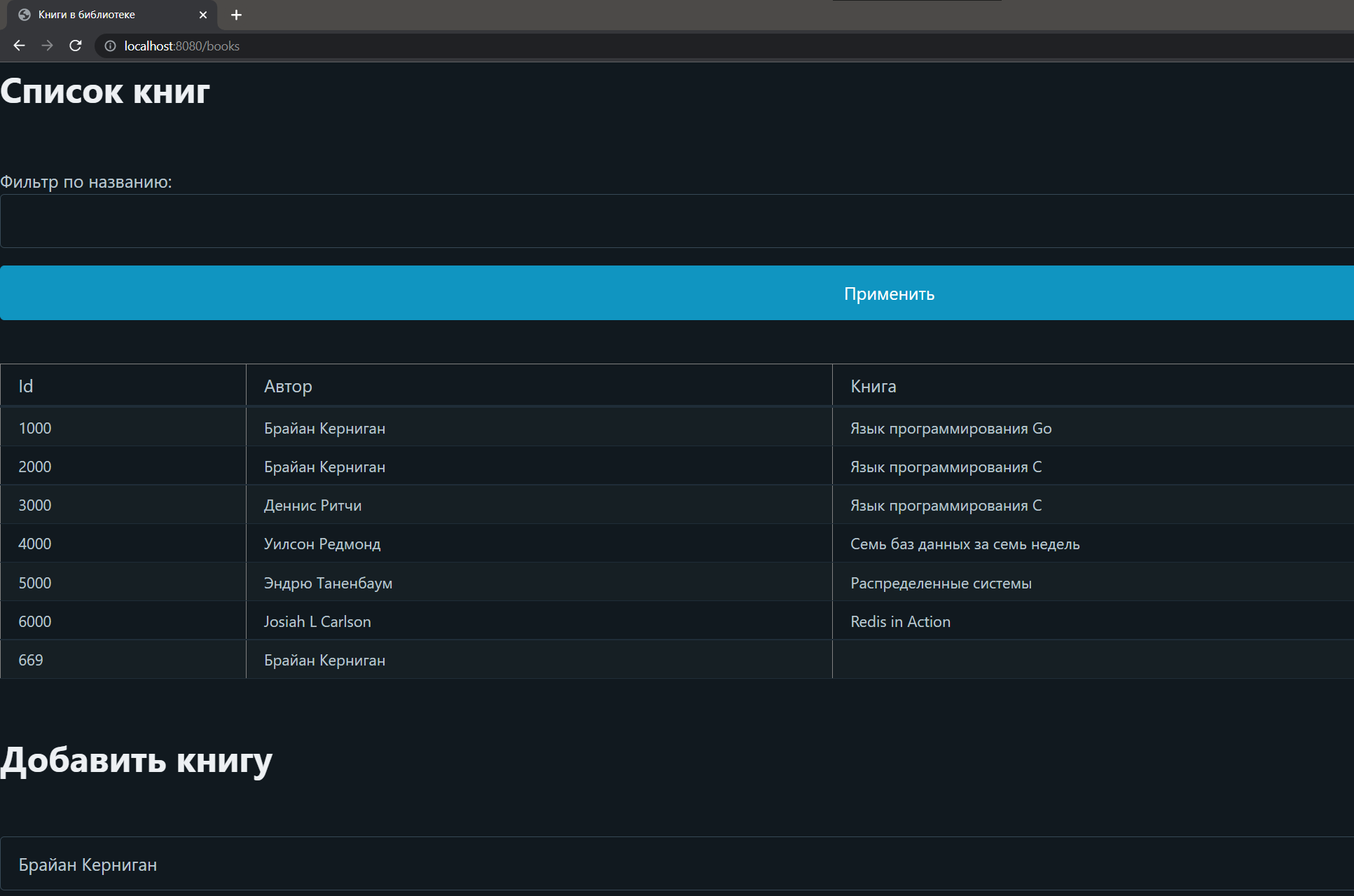




## Cookie Injection

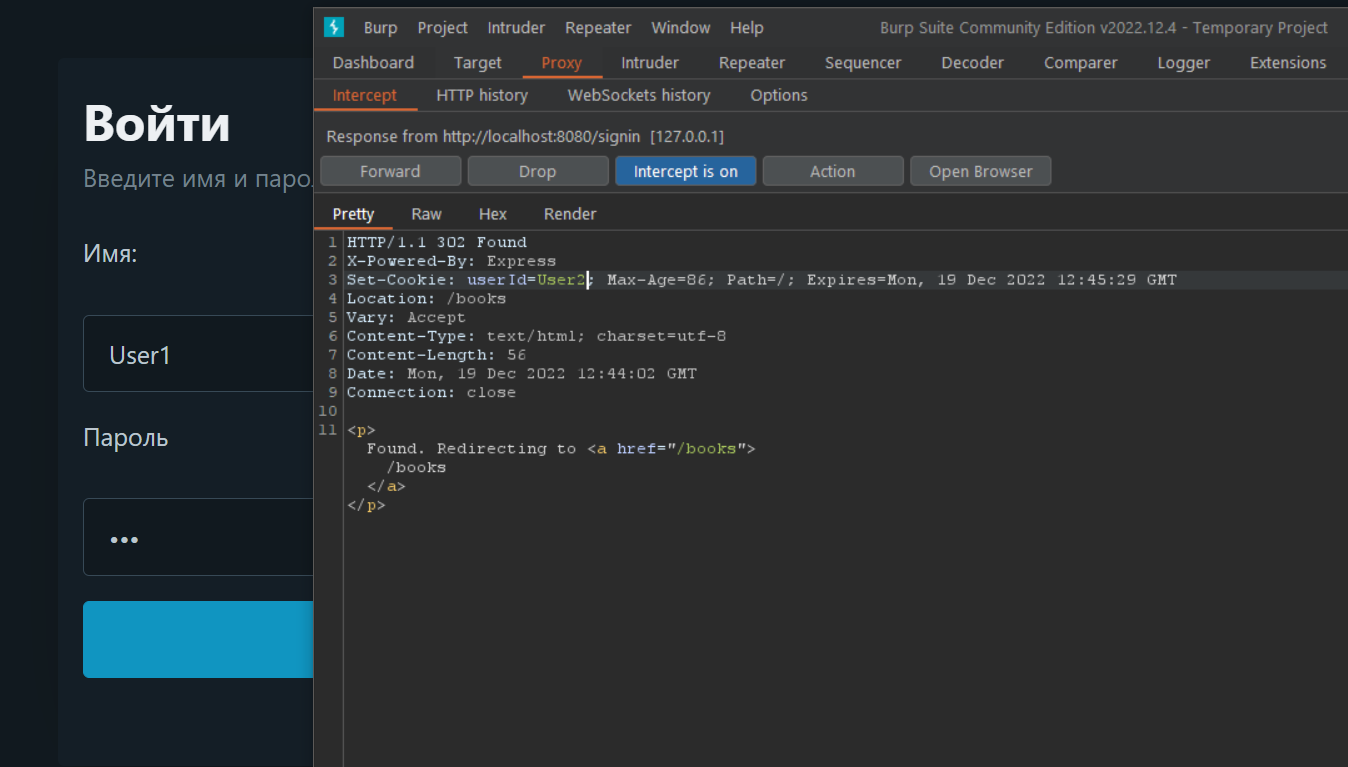
На сервер можно отправить запрос с хедером Cookie. Помимо подстановки значения cookie другого пользователя существует возможно подменить дополнительно установленные параметры.

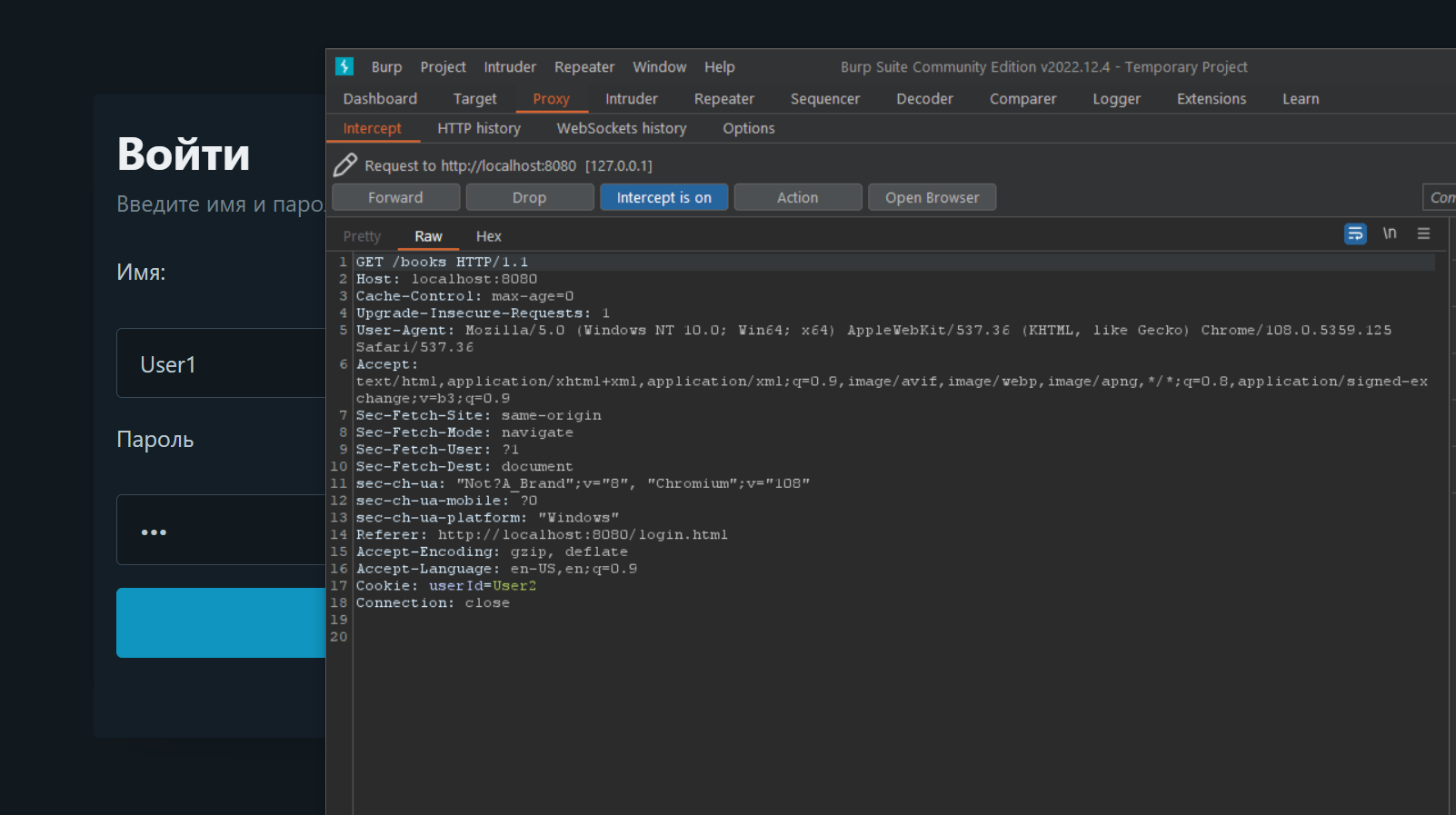


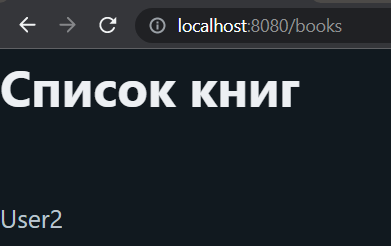


## Session hijacking

Так как на сервере не используется шифрование cookie могут быть перехвачены. Помимо этого, значение cookie может быть подобрано брут форсом или если алгоритм формирования значения недостаточно случайный.

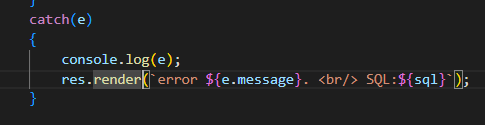


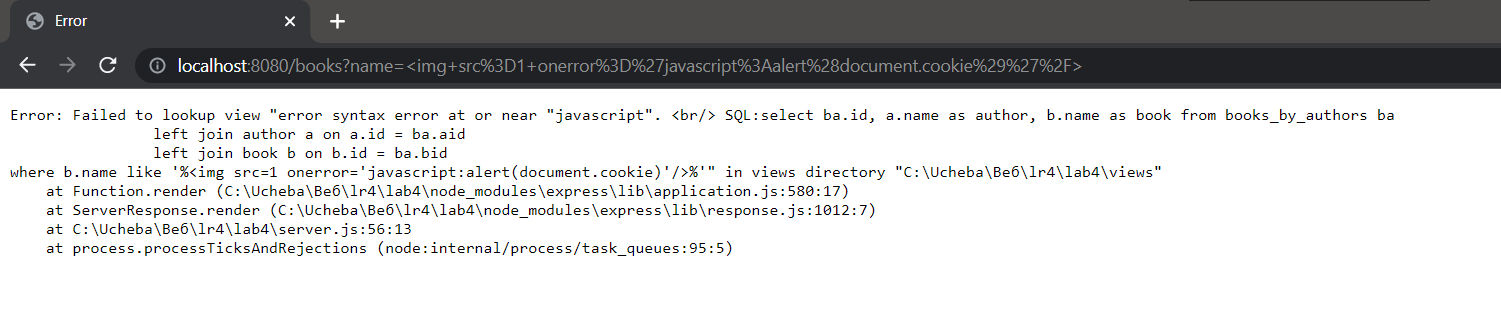




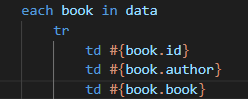
## Защита

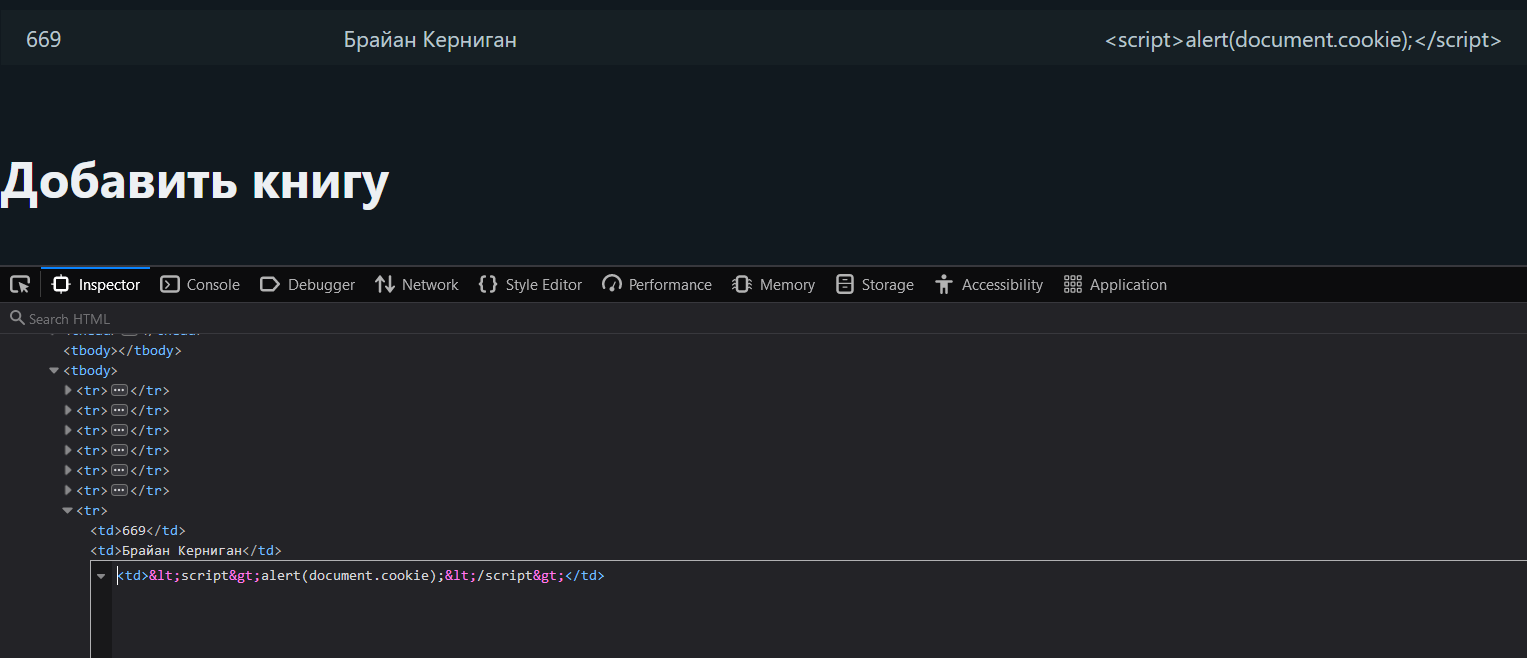
Для защиты от Reflected XSS следует доработать функцию обработки ошибок и заменить функцию res.send() на res.render().





Для защиты от Persisted XSS следует доработать шаблон Pug и заменить знак «!» на «#».





Также для запрета доступа JavaScript к файлу cookie следует установить атрибут httpOnly. Если бы сервер работал на HTTPS, то следовало бы установить атрибут Secure.

