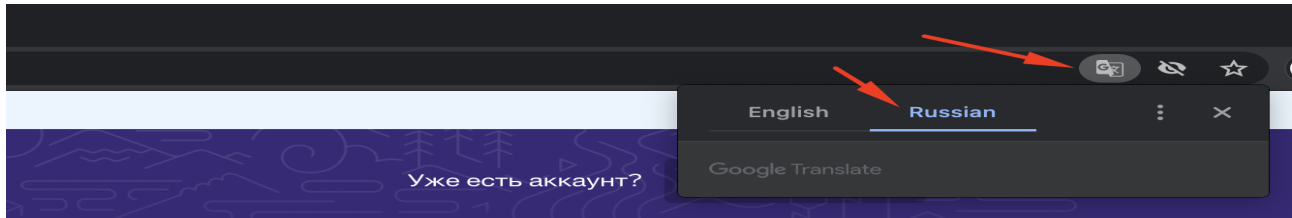


OWASP Juice Shop

Начало. Установка Heroku [~30 мин]

Для начала практики развернуть собственное веб-приложение. Для этого:

1. Зарегистрироваться на бесплатном ресурсе [Heroku: Cloud Application Platform](https://heroku.com). В случае сложностей можно воспользоваться встроенным в браузер переводчиком:



2. Зайти в Heroku с нового аккаунта и ввести в адресную строку браузера следующее:

<https://dashboard.heroku.com/new?button-url=https%3A%2F%2Fgithub.com%2Fbkimminich%2Fjuice-shop&template=https%3A%2F%2Fgithub.com%2Fbkimminich%2Fjuice-shop>

Так будут указаны системе, откуда брать данные для установки приложения.

3. Выбрать уникальное имя собственного приложения, затем **Deploy app**:

Create New App

Deploy your own
OWASP Juice Shop
Probably the most modern and sophisticated insecure web application
📄 [bkimminich/juice-shop#master](#)

App name

boris777-juice-shop ✓

boris777-juice-shop is available

Choose a region

🇪🇺 Europe

Add to pipeline...

Deploy app

4. Дождаться разворачивания (занимает около 15–20 минут). В конце должно получиться следующее:

Create app	✓
Configure environment	✓
Build app Show build log	✓
Run scripts & scale dynos	✓
Deploy to Heroku	✓

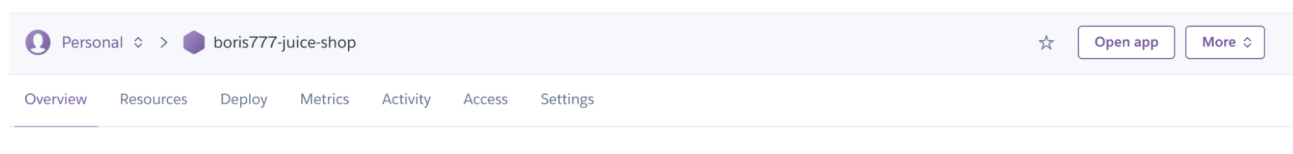
Your app was successfully deployed.

Manage App

View

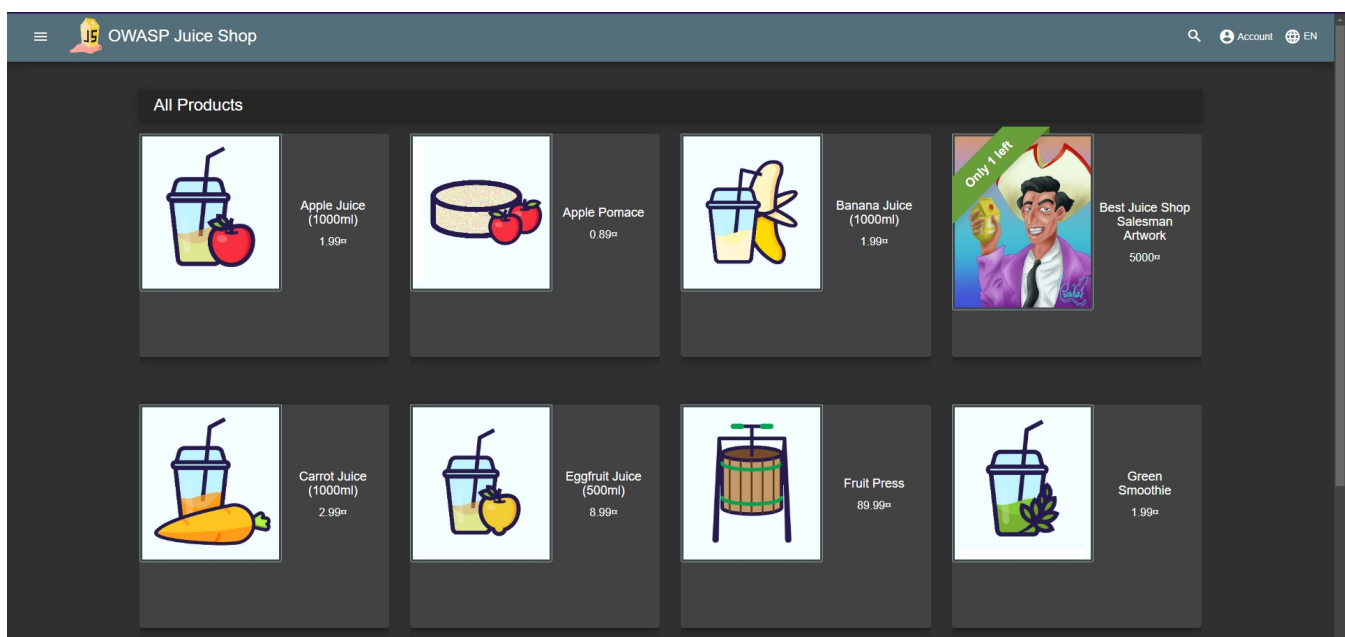
5. Нажать на кнопку View и посмотреть на созданное приложение.

Если приложением долго не пользуются, оно уходит в сон, тогда его нужно будет включить через **Open app** при входе в личный кабинет Heroku:



Вместо всего этого, я просто набрал в браузере данный доменом и всё:

<https://demo.owasp-juice.shop/>



Его интерфейс.

Task 2: Панель администратора [~10 мин]

Во время выполнения задачи 1 из урока 1 было показано, как находить пути к страницам из JS-файлов. Используя способ, описанный в видео задачи 1, найти путь к панели администратора веб-приложения Juice Shop.

Если найти путь верно (снова потребуются знания английского языка), должна возникнуть ошибка 403, так как не хватит прав доступа — не получится войти в личный кабинет администратора. Нужно это сделать в следующем задании в видеоразборе задачи 3.

Подсказка 1

Использовать «Инструменты разработчика» в браузере для чтения кода веб-приложения.

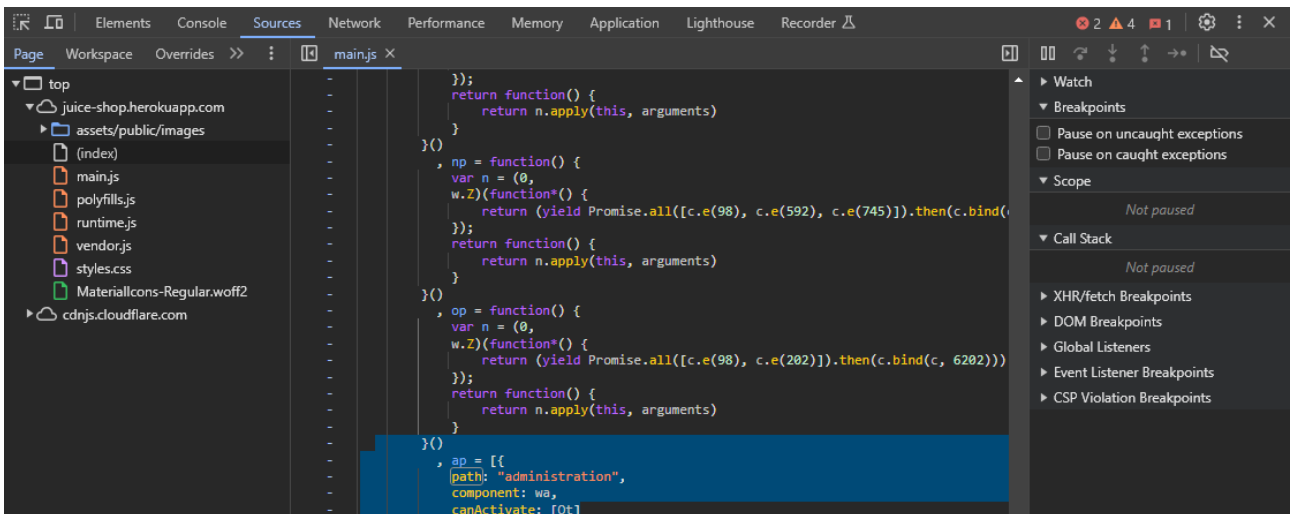
Подсказка 2

Помимо стандартного HTML-кода, страница подгружает файлы. Обратите внимание на вкладку Sources в панели инструментов разработчика в браузере.

Подсказка 3




















Прочитать код файла main*.js (удобно использовать при чтении кода Pretty View в составе браузера). Найти ключевое слово admin в его строках. В одном из вхождений будет указан путь (path) к странице счёта — administration.

В ответе на это задание указать путь/страницу, которую нужно добавить к основному домену (после символа #/), чтобы перейти на страницу входа в панель администратора.



В данном случае понадобится строка: path: "administration"

Вставив данную строку к домену: <https://demo.owasp-juice.shop/#administration>

Administration			
Registered Users		Customer Feedback	
 admin@juice-sh.op		1	I love this shop! Best products in town! Highly recommended! (**in@juice-sh.op) ★★★★★ 
jmg@juice-sh.op		2	Great shop! Awesome service! (**@juice-sh.op) ★★★★★ 
bender@juice-sh.op		3	Nothing useful available here! (**der@juice-sh.op) ★ 
bjoern.kimminich@gmail.com		21	Please send me the juicy chatbot NFT in my wallet at /juicy-nft : "purpose betray marriage blame crunch..." ★ 
ciso@juice-sh.op			Incompetent customer support! Can't even upload photo of broken purchase!... ★★ 
support@juice-sh.op			This is the store for awesome stuff of all kinds! (anonymous) ★★★★★ 
morty@juice-sh.op			Never gonna buy anywhere else from now on! Thanks for the great service! (anonymous) ★★★★★ 
mc_safesearch@juice-sh.op			Keep up the good work! (anonymous) ★★★ 
J12934@juice-sh.op			
wurstbrot@juice-sh.op			

И может вылезти данная страница с пользователями. Я говорю может, поскольку в первый раз у меня вылезла страница с 403 ошибкой.

Task 4: Вход из-под зарегистрированного пользователя [~10 мин]

В панели администратора (при переходе по ссылке, которая является решением задачи 2) можно увидеть всех пользователей. Используя техники задачи 3 (урок 2), попробовать зайти в учётную запись Бендера из зарегистрированных пользователей и посмотреть, что находится в его корзине.

В ответе на это задание указать итоговую сумму заказа корзины пользователя.

Подсказка


Так как имя пользователя известно, необходимо, чтобы часть проверки пароля отсеивалась. Для этого в поле логина нужно использовать уже известную комбинацию символов.

Login

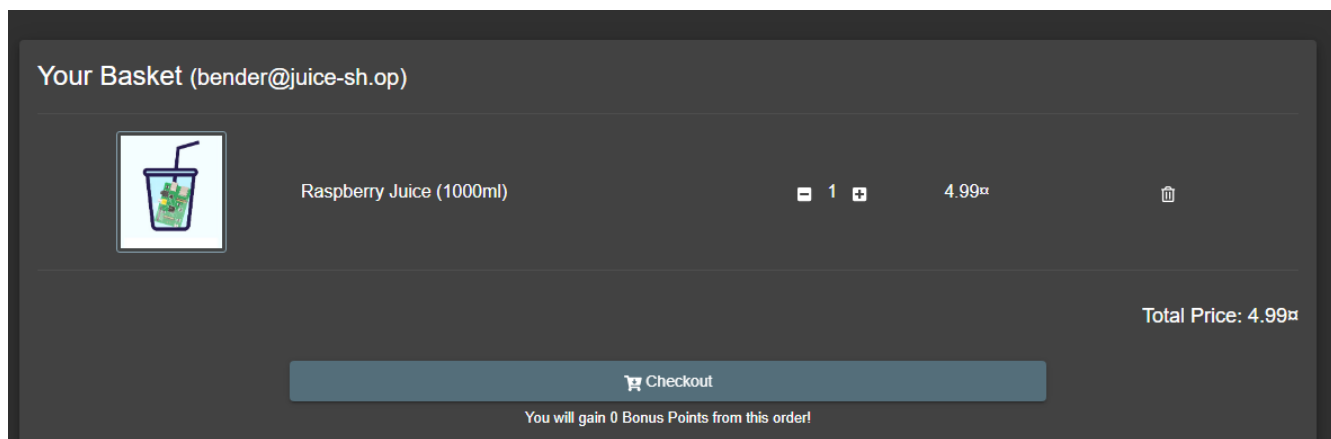
Email *

bender@juice-sh.op'—

Password *

.....


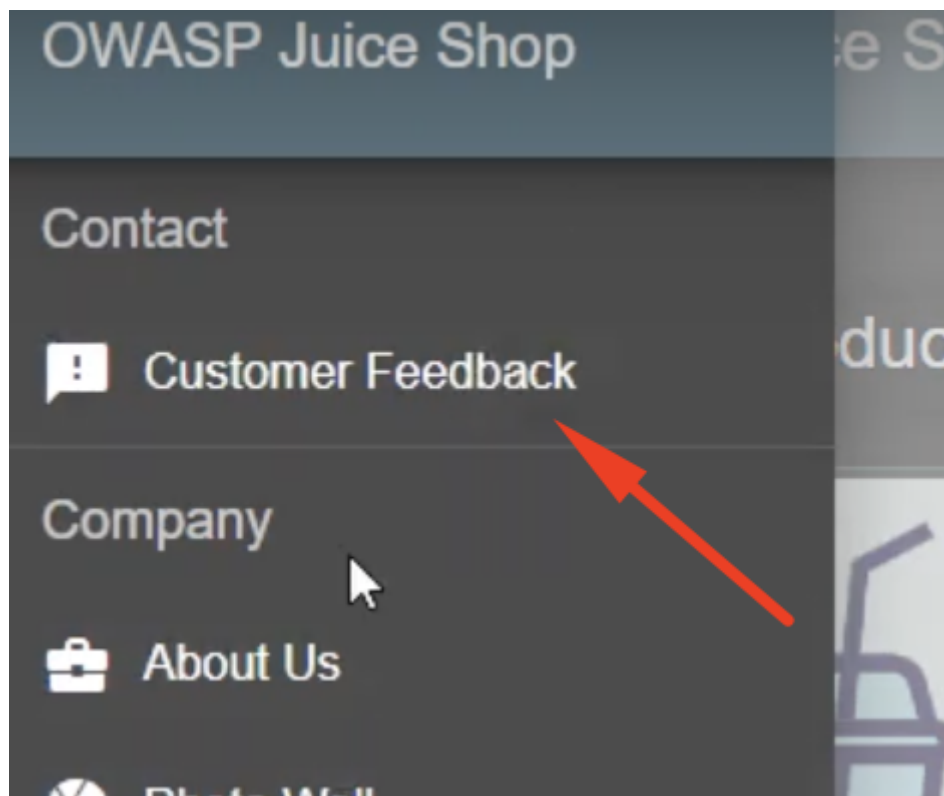
Для данной SQL-инъекции я ввёл данный почтовый адрес, а также «'--». До этого пытался вводить «'or TRUE--», но данная SQL-инъекция вводила только в аккаунт администратора.



У данного пользователя в корзине 1 малиновый сок.

Task 6: Оставляем нулевой фидбэк [~5 мин]

После выполнения всех предыдущих задач становится понятно, что магазин соков имеет множество уязвимостей, и это только вершина айсберга. Оставить негативный отзыв этому магазину! Зайти на ранее созданную учётную запись в магазине соков либо создать новую, затем в меню слева выбрать Customer Feedback:



Задача — выставить оценку с нулём звезд. Сложность в том, что такого параметра нет (ноль звезд). Такого рода уязвимости приложений называются Improper Input Validation.

Customer Feedback

Author

***is@juice-sh.op

Comment

Very Bad Shop Too many vulnerabilities !

Max. 160 characters

40/160

Rating

1★

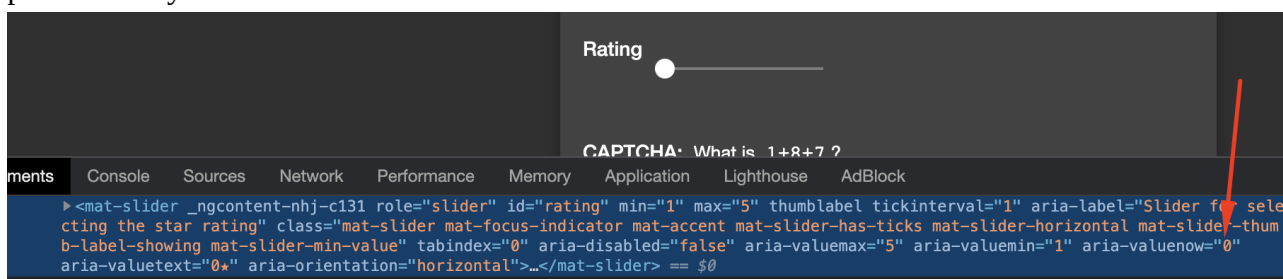
CAPTCHA: What is $1-9*8$?

Result

-71

Submit

Внимательно изучить код до и после ввода значений. Как видно, изначально рейтинг равняется нулю:

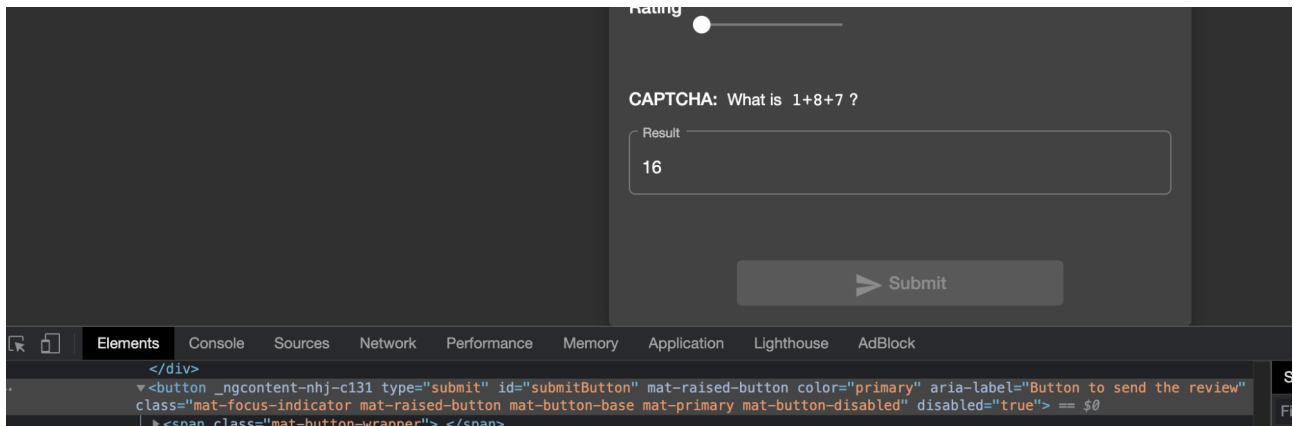


Но кнопка без выставления оценки не нажимается. Задача — исправить это.

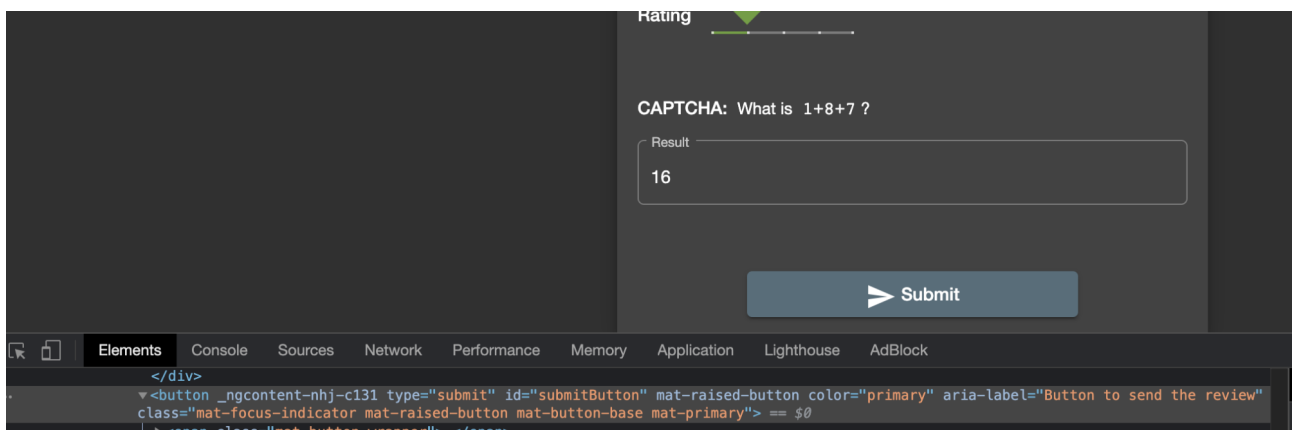
В ответе на это задание указать, какой именно класс CSS нужно удалить, чтобы кнопка нажалась и опубликовался отзыв.

Подсказка 1

Какие теги и классы появляются или пропадают? Код кнопки до выставления рейтинга:



Код после выставления рейтинга:

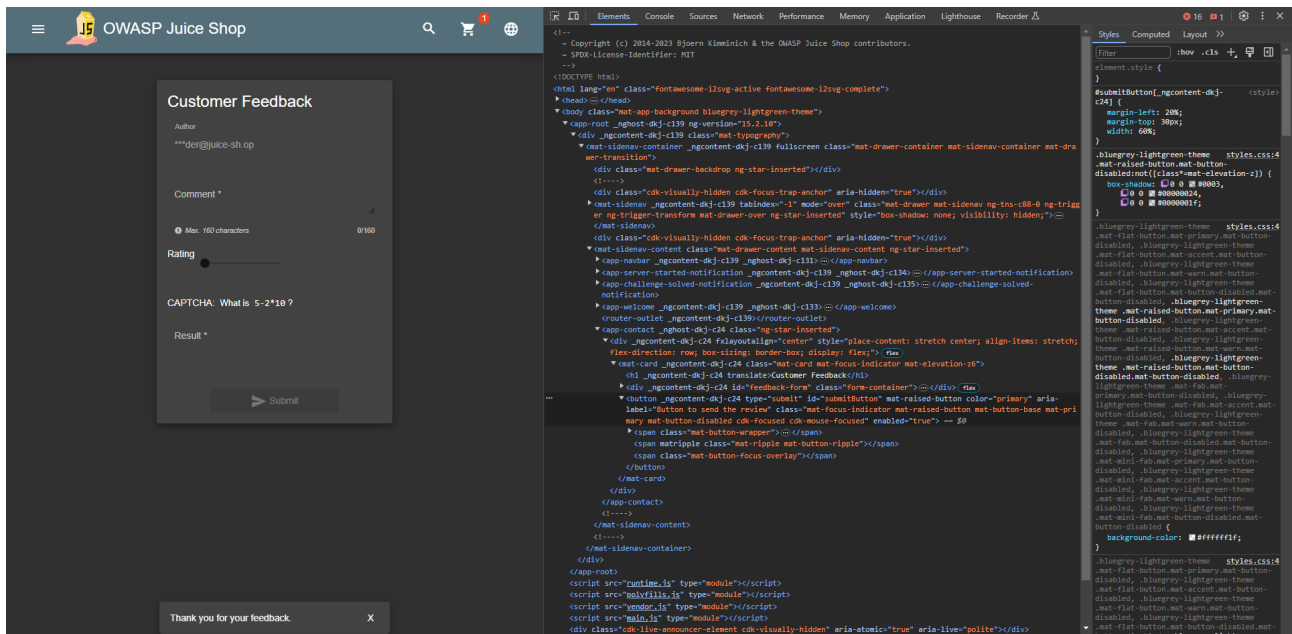


Подсказка 2

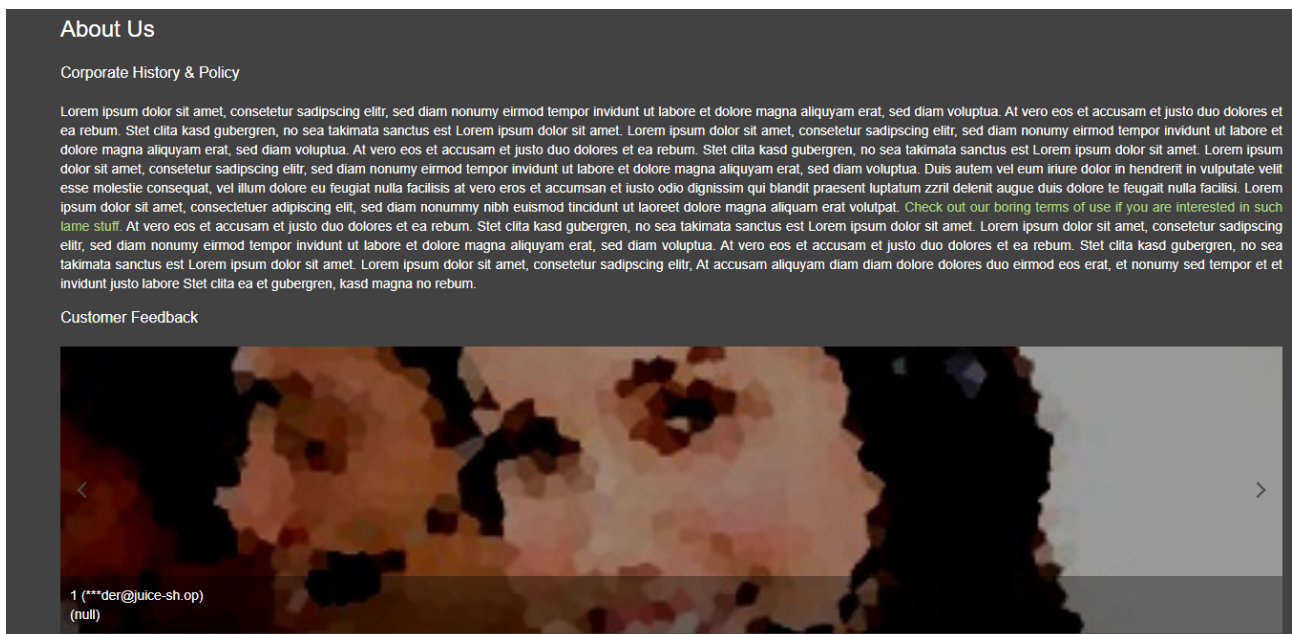
Обратить внимание на переменную кнопки `<button ... disabled=...>`.

Подсказка 3

Нужно избавиться от ненужного класса CSS для кнопки.



Около элемента button, тут я поменял опцию в enabled= с «false» на «true». После этого я нажал на кнопку отправить. До этого я пытался менять минимальное количество звёзд, но так не срабатывало — всё равно была одна звезда.



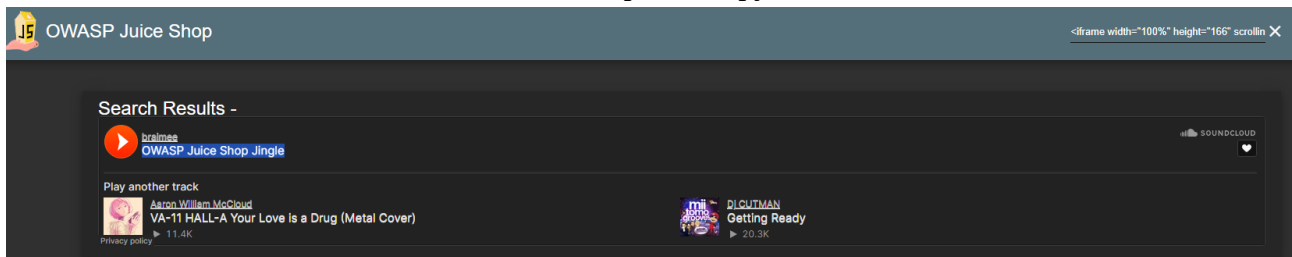
Это готовый результат (количество звёзд: Null).

Task 8: Поищем что-то повеселей [~5 мин]

Закрепить ранее пройденный материал (задача 7, урок 4) по XSS. Теперь вместо обычного сообщения нужно подгрузить медиаконтент, например видео. Для этого в адресную строку необходимо просто ввести код:

<iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="https://w.soundcloud.com/player/?url=https://api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true"></iframe>

Ответ на это задание — название песни, которая подгрузилась.



Название данной песни: OWASP Juice Shop Jingle.

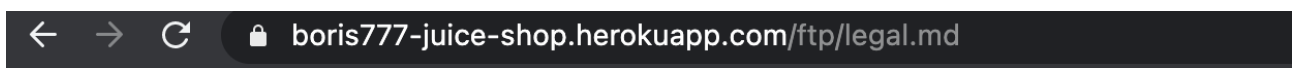
Task 9: Поиск секретного документа [~5 мин]

Есть информация, что в магазине соков прячется секретный документ. Тут нужно проверить эту теорию. Рекомендуется сначала прочитать информацию о самой компании.

В меню магазина слева выбрать About Us.

Ответ на это задание — название файла секретного документа.

Подсказка 1



Legal Information

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy
 eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam
 voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet
 clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit
 amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam
 nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat,
 sed diam voluptua. At vero eos et accusam et justo duo dolores et ea
 rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem
 ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing
 elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna

Заметили странную ссылку в соглашении о пользовании (Terms of Use)?

About Us

Corporate History & Policy

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. Duis autem vel eum inire dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et justo odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consetetur adipiscing elit, sed diam nonumy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. [Check out our boring terms of use if you are interested in such lame stuff.](#) At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, At accusam aliquyam diam diam dolore dolores duo eirmod eos erat, et nonumy sed tempor et et invidunt justo labore Stet clita ea et gubergren, kasd magna no rebum.

Customer Feedback

На данной части домена <ftp/legal.md> есть странные буквы: [ftp](#). А это является протоколом передачи файлов.



Убрав от ftp «/legal.md» - вылезет данная страница, где активен FTP сервер.

В моём случае это: <https://demo.owasp-juice.shop/ftp>

P.S. У меня даже есть шутка: Что общего между составом продуктов и политикой конфиденциальности - её(его) никто не читает.

Критерии оценки

Зачёт: выполнены хотя бы три из пяти задач ДЗ и дан верный ответ.

На доработку: верно выполнено менее трёх задач ДЗ.