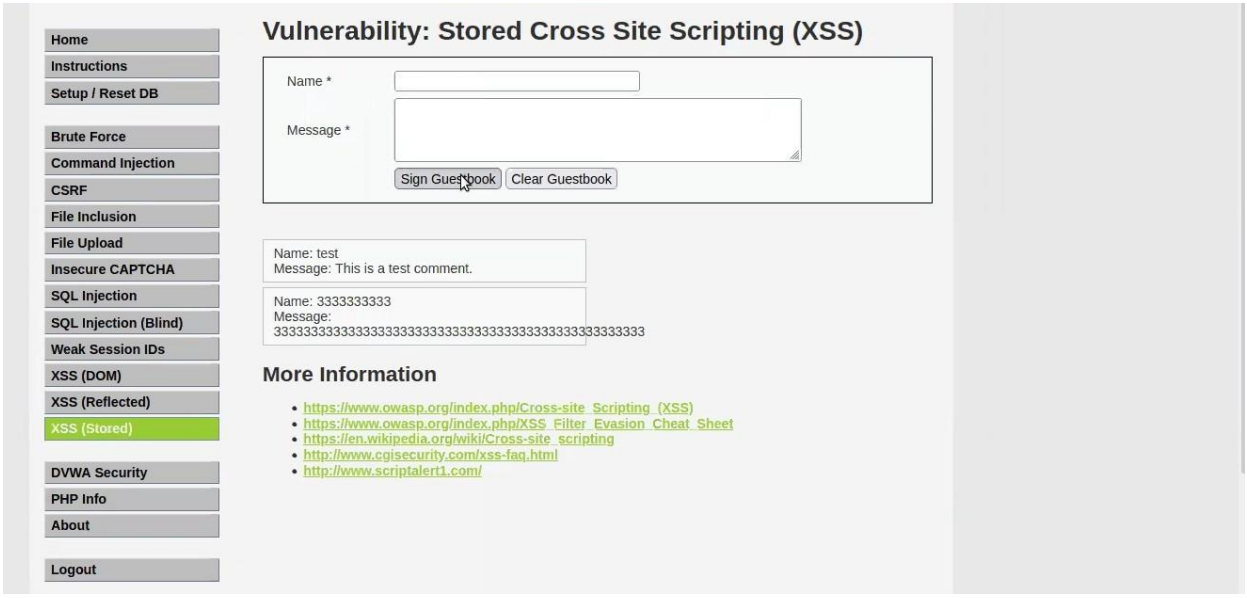
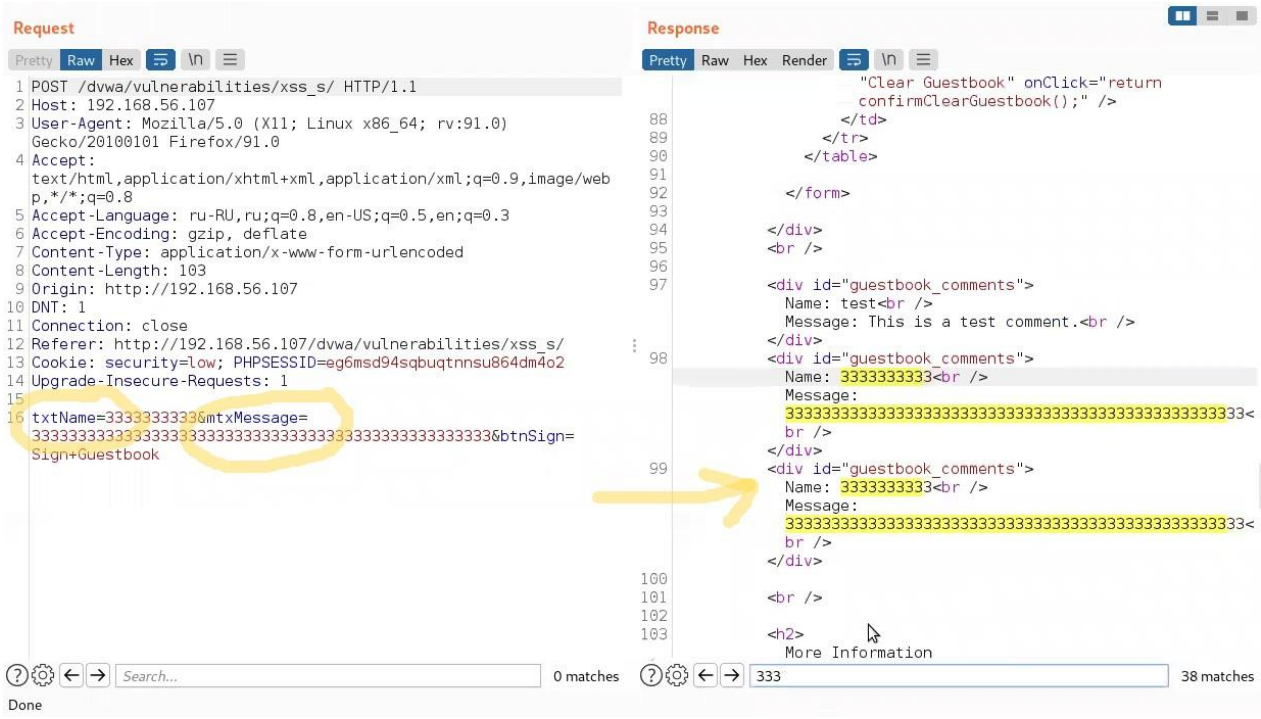
1. Страница XSS(Stored) проекта DVWA на простом (Low) уровне сложности

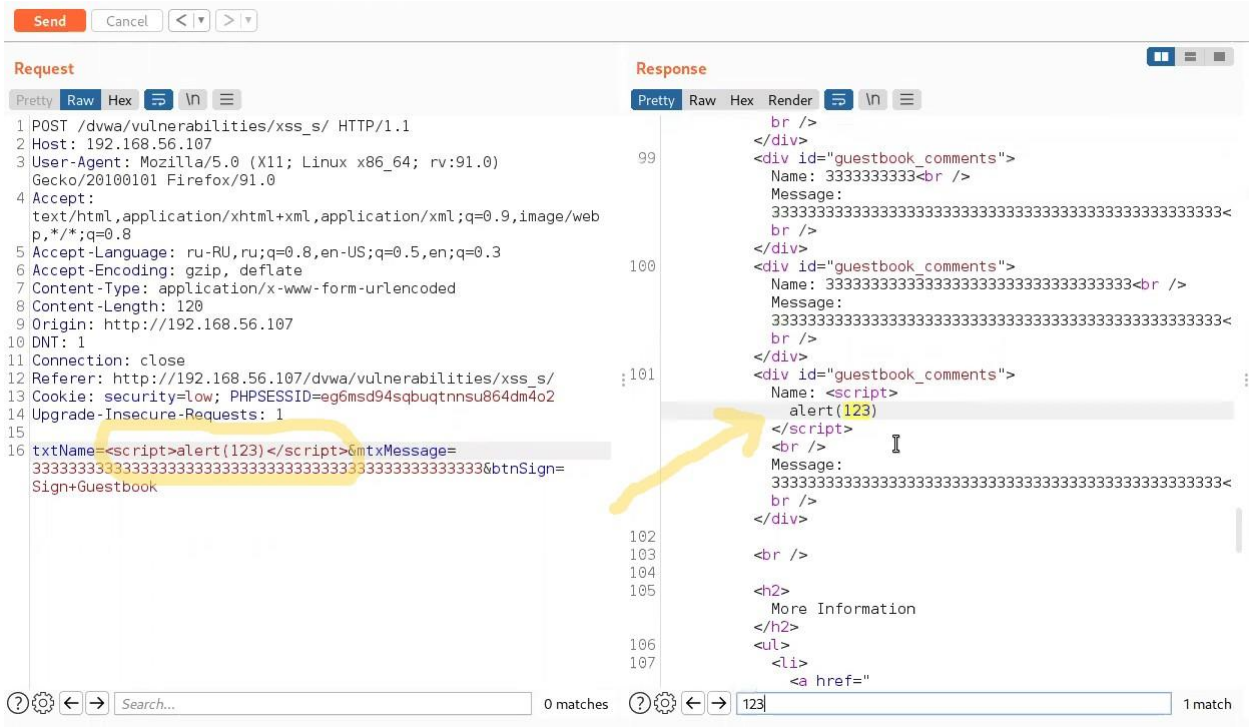
Оба параметра на странице Stored – уязвимы к XSS.

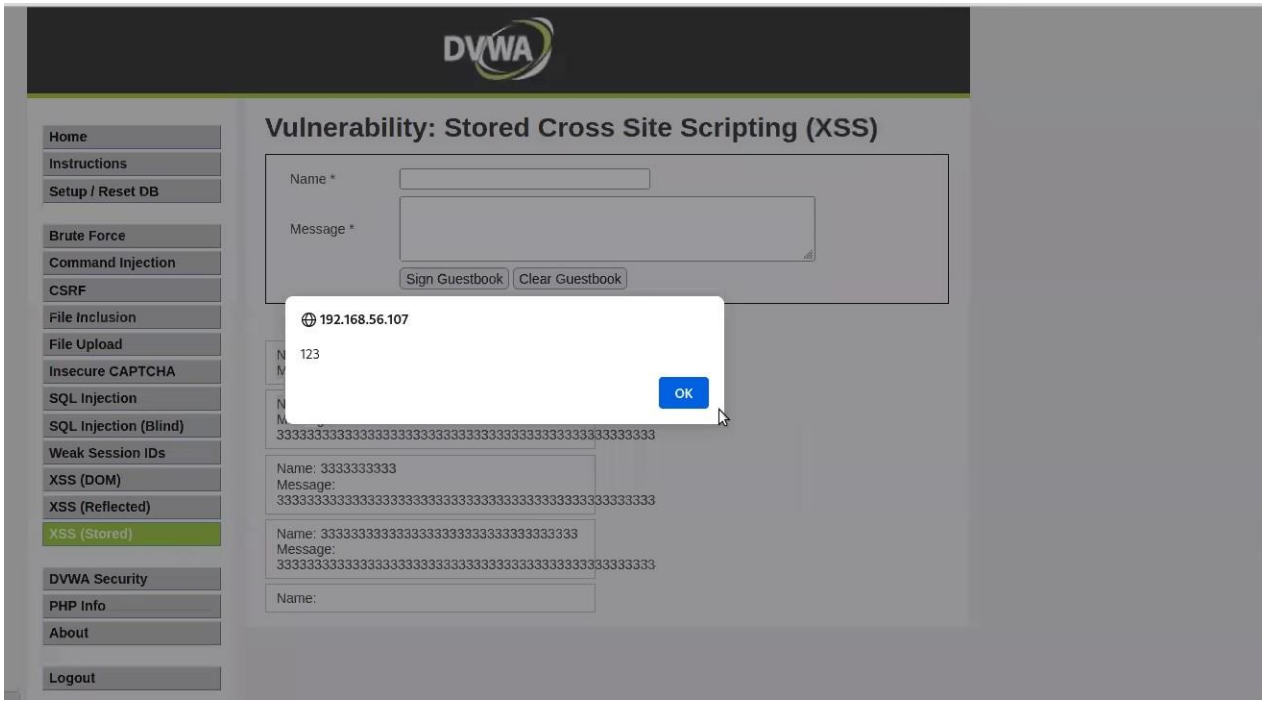




Данные падают в html контекст. Подбираем вектор под html контекст.

Например:

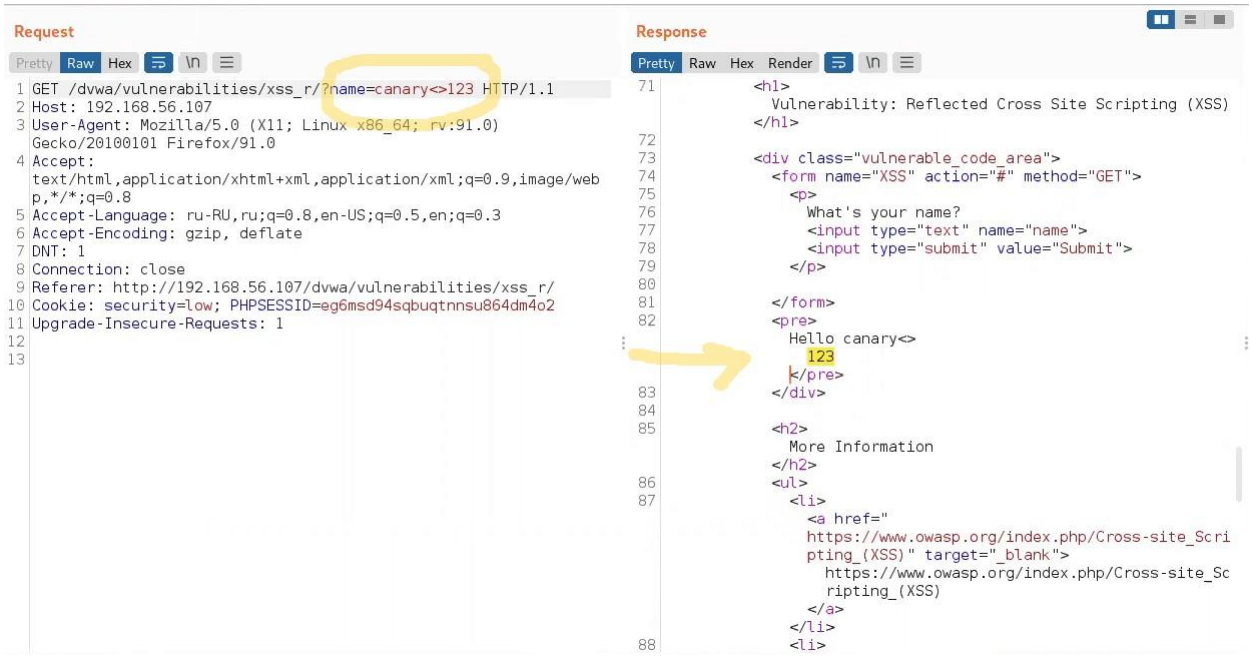




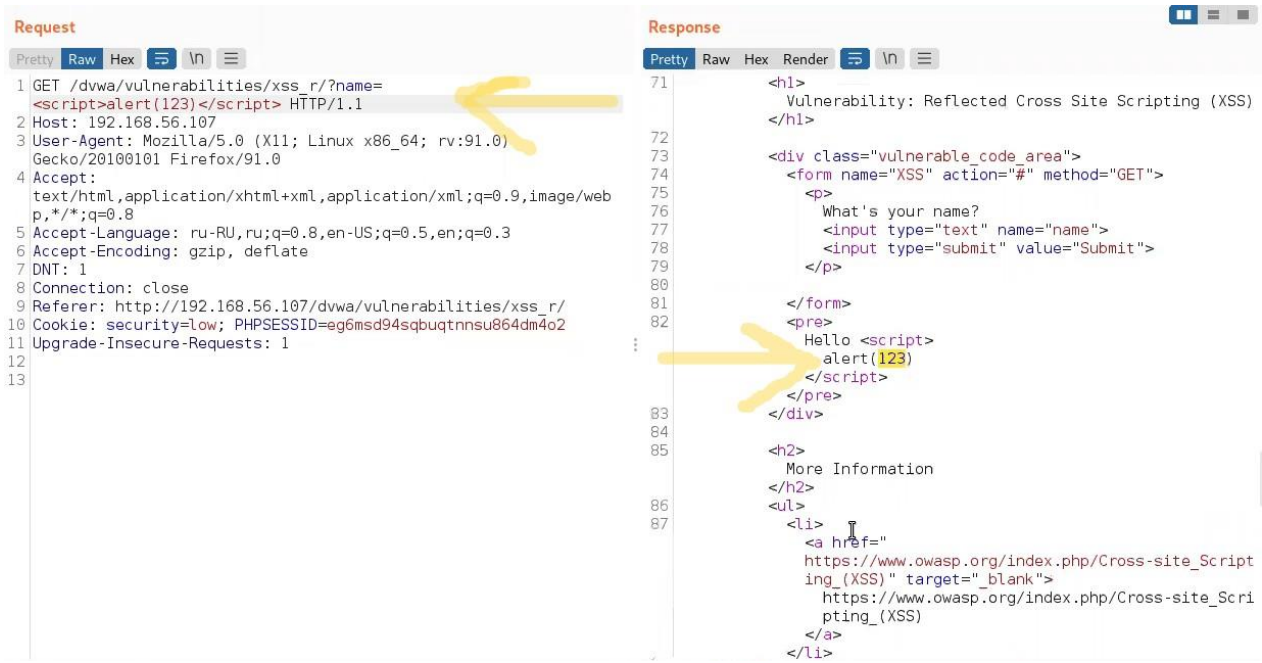
Alert box сработал, т.е. мы имеем дело с XXS.

2. Страница XSS(Reflected) проекта DVWA на простом (Low) уровне сложности

Проверяем есть ли фильтрация данных и видим, что данные не фильтруются, они упали в html контекст.



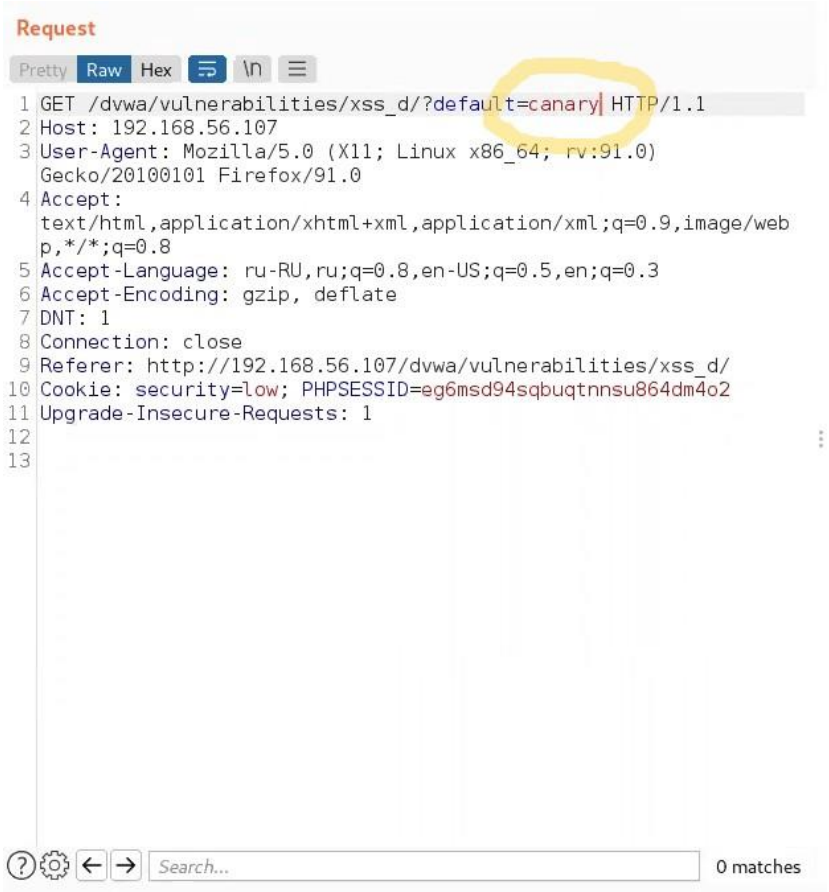
Соответственно, можно подобрать вектор под этот html контекст. Например:



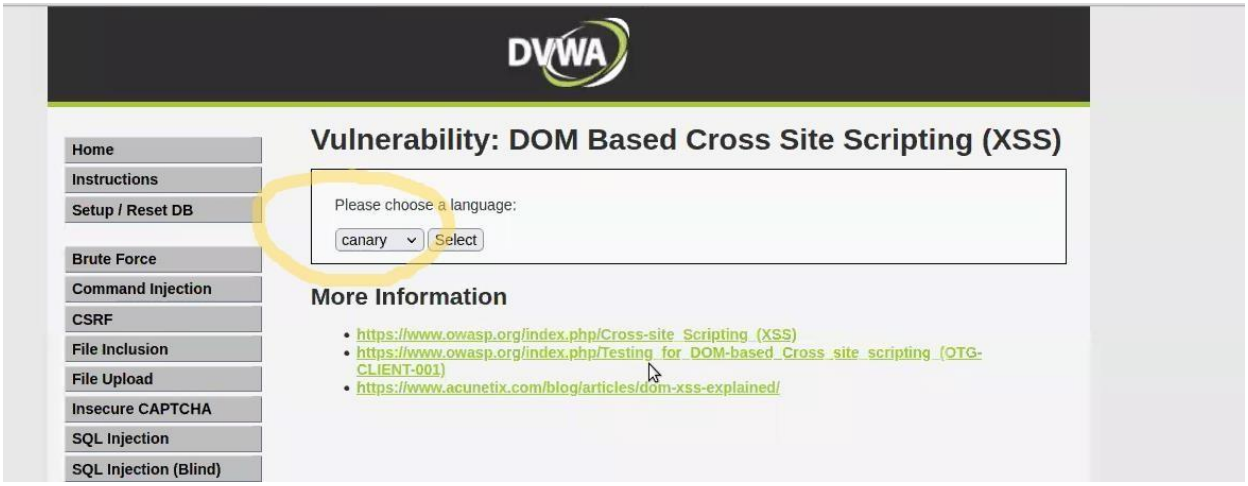
Alert box сработал, т.е. мы имеем дело с XXS. Вектор на странице не остается, поэтому мы имеем дело с отраженной XXS.

3. Страница XSS(DOM) проекта DVWA на простом (Low) уровне сложности

Здесь мы имеем дело с GET запросом, данные добавляются в список. Раз мы имеем дело с запросом – значит его можно увидеть. Здесь важно передать такой текст, который на странице не встречается.

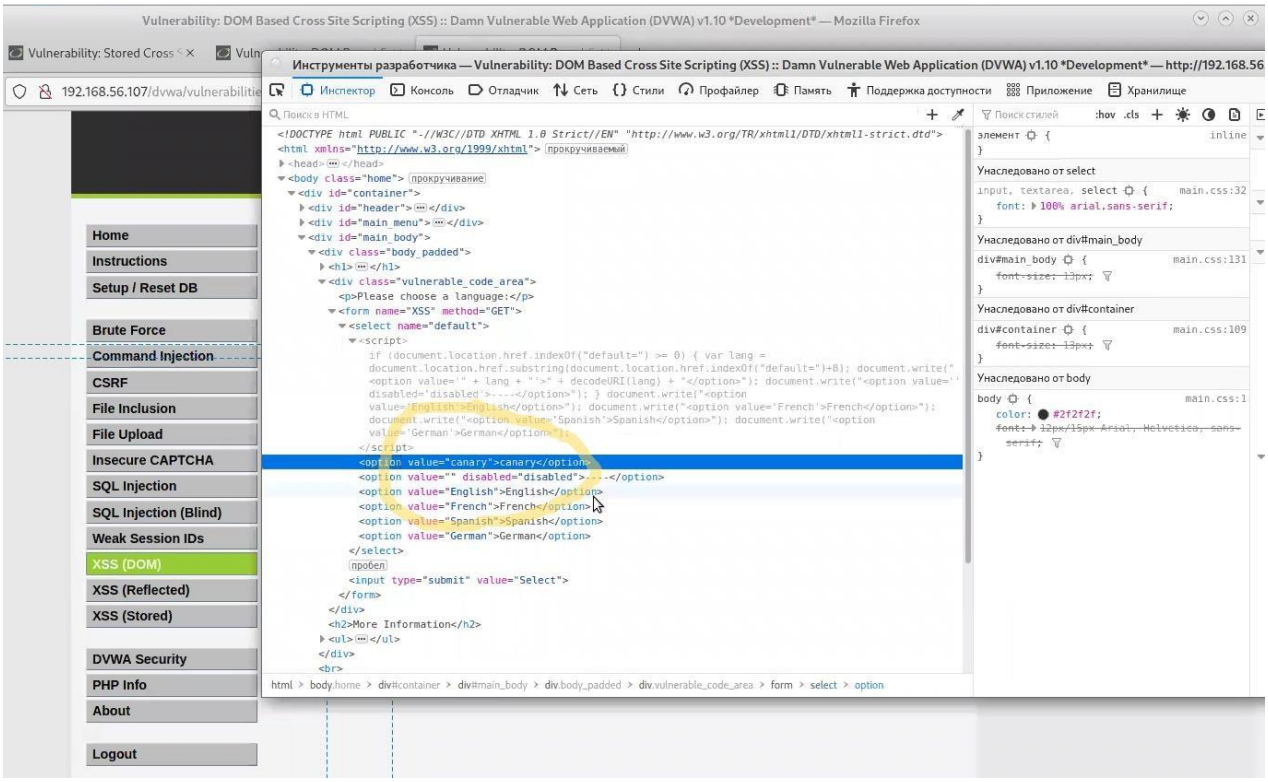


Открываем в браузере:

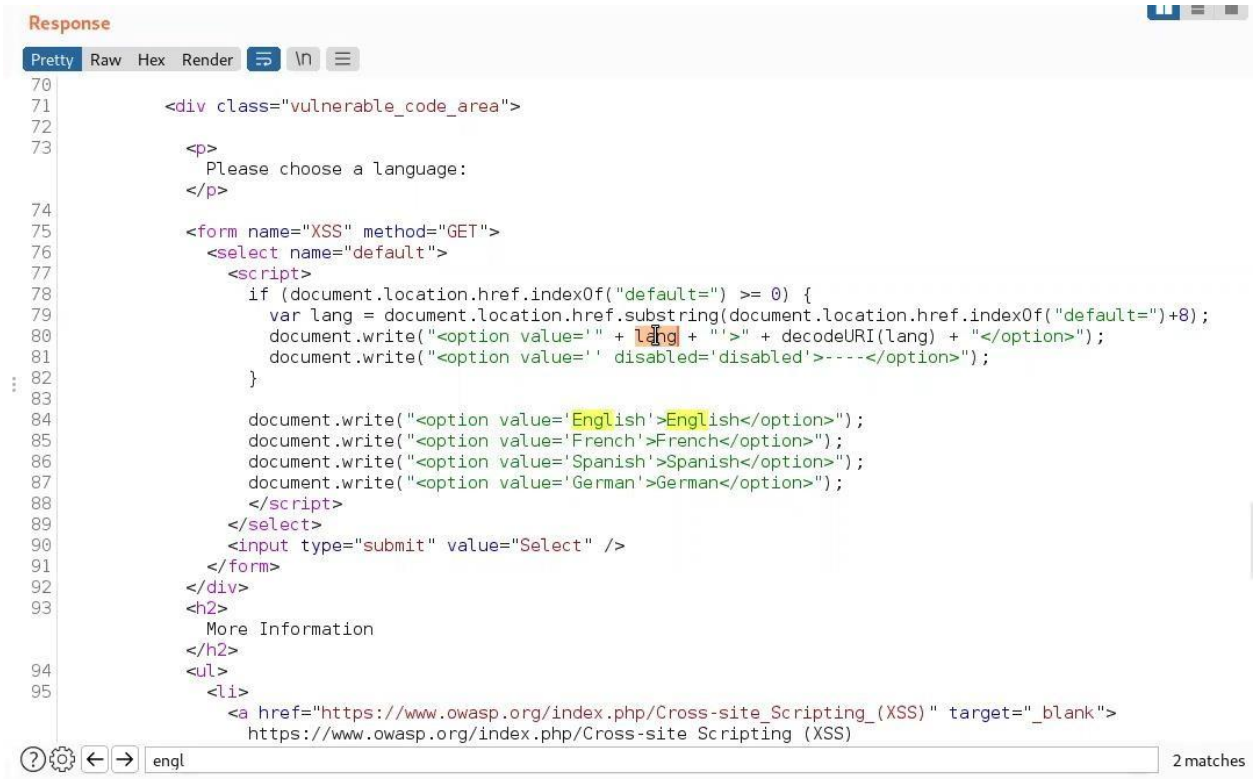


И видим, что текст добавился в список - с помощью кода DOM based он дописывается уже после того как response целиком загрузился в браузер.

Открываем инструмент разработчика, где мы сможем увидеть полностью отрисованную страницу:



Чуть выше тега с текстом canary, мы видим скрипт (светло-серым шрифтом) с DOM XXS.



В данном случае мы имеем дело с уязвимым параметром default, который падает в переменную lang. Контекст в данном случае - DOM based, хоть мы и видим зависимость от Java Script, но конструкция здесь document.write, которая зависит от document tree. Дерево построено не будет и ничего не выполнится.