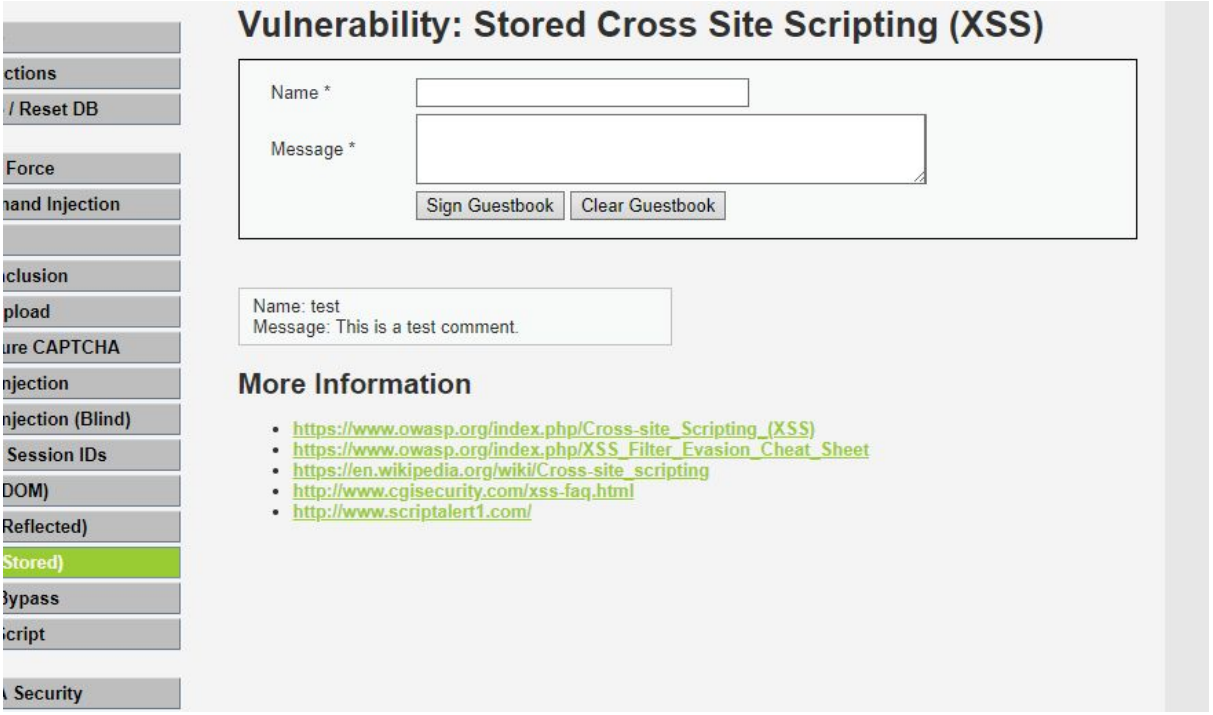
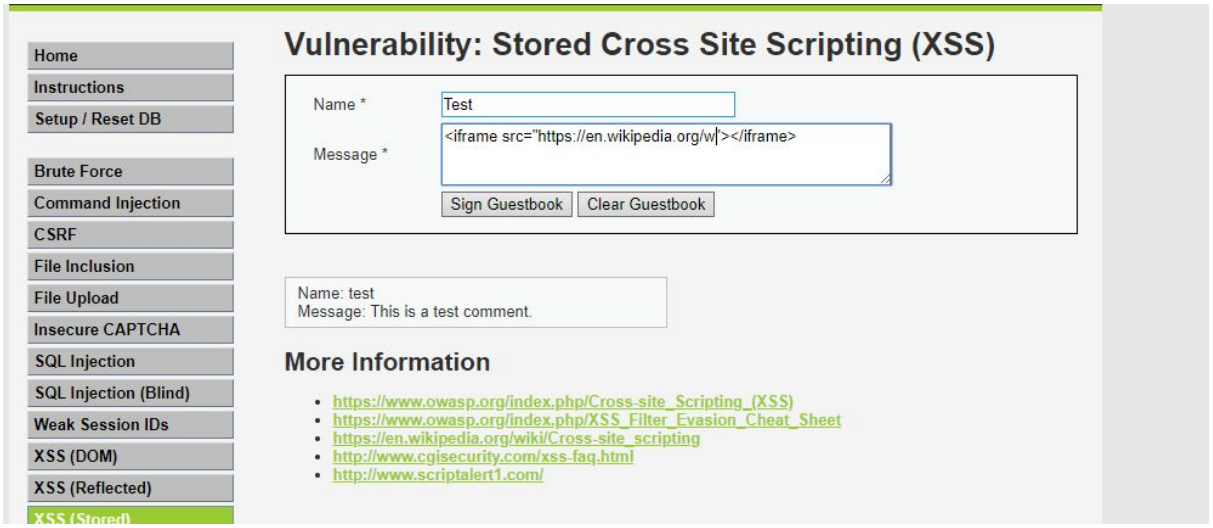
Все скрины предоставлены для уровня LOW

XSS_Stored

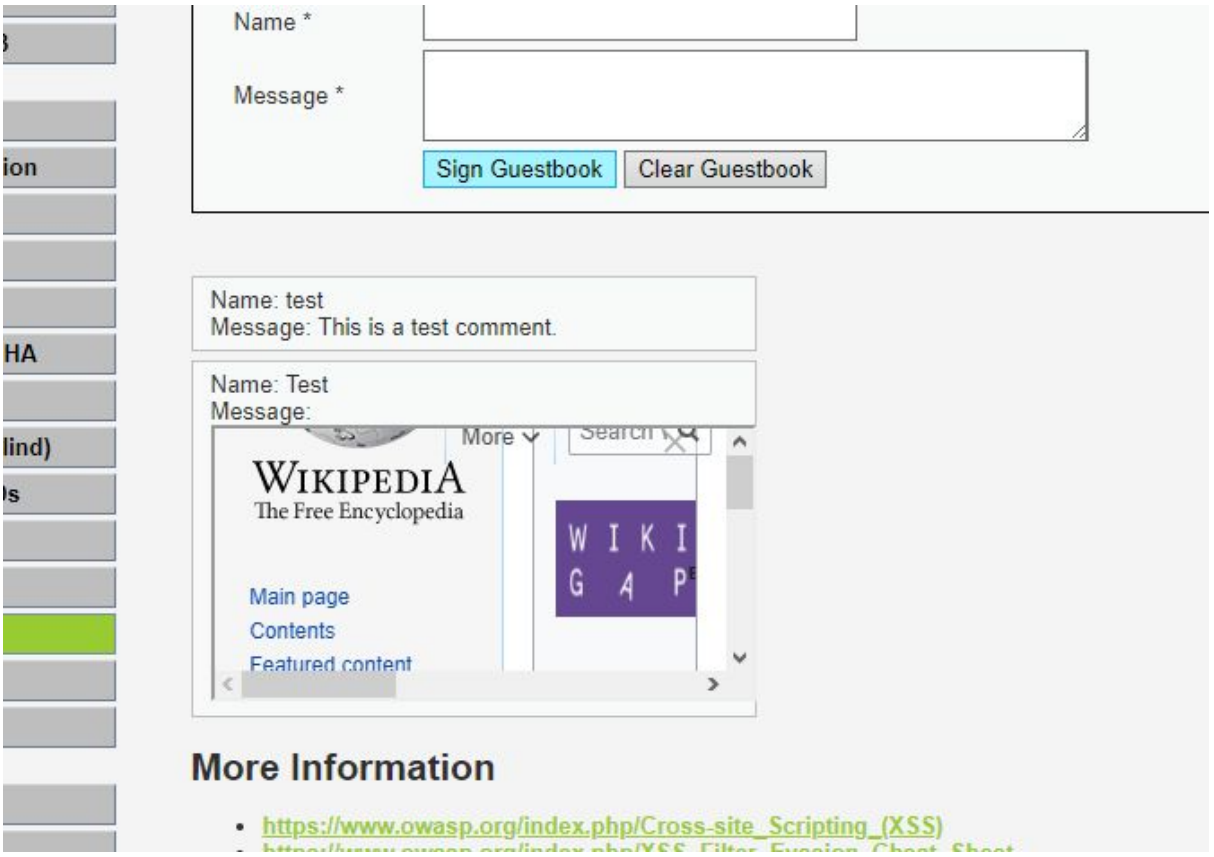
Нормальное состояние -



Уязвимость со вставкой frame- прописывает скрипт



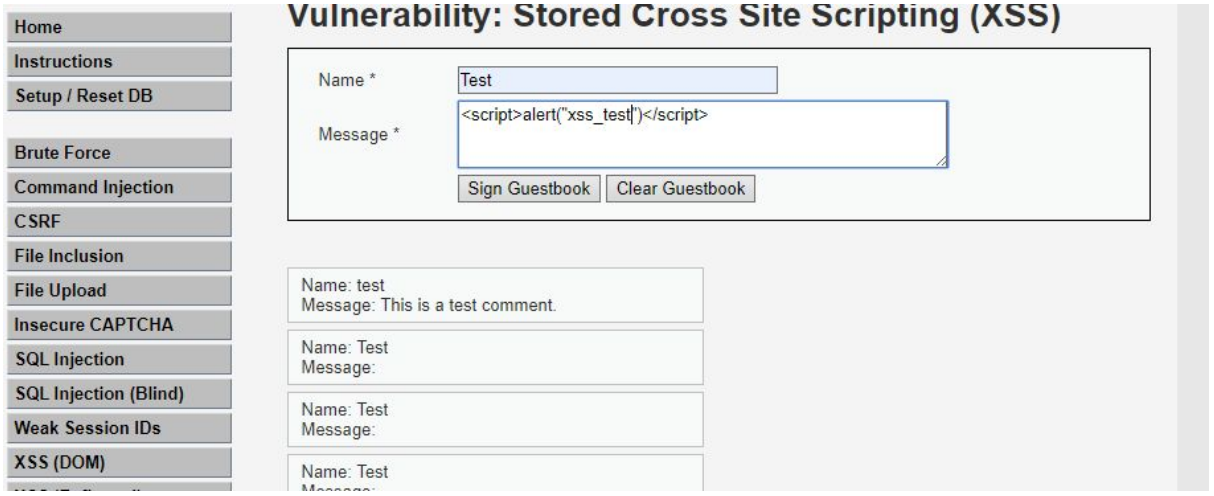
На выходе получаем



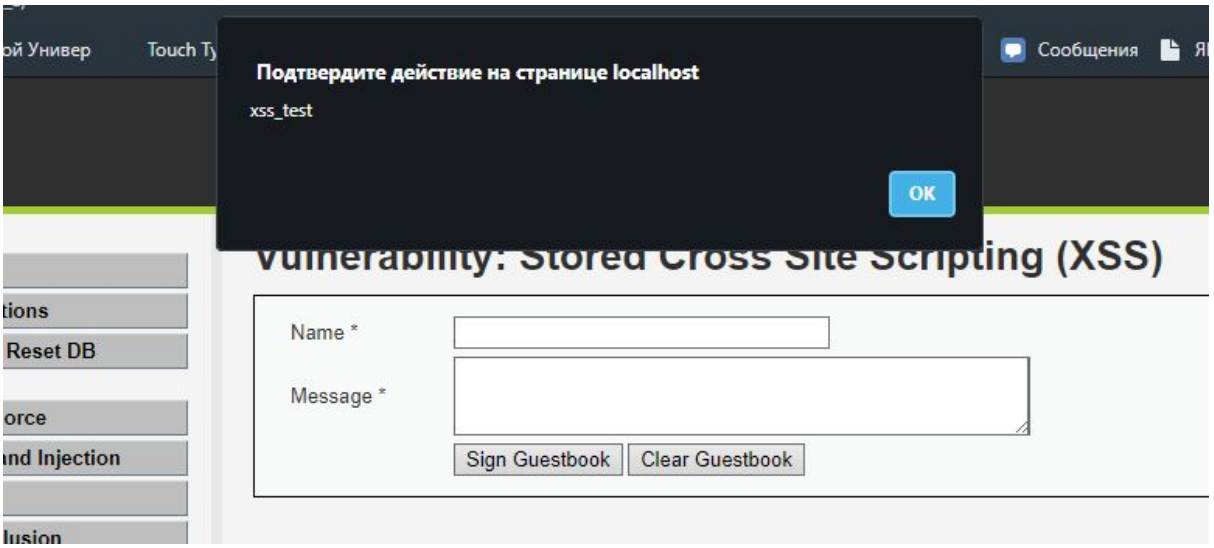
т.е. отображается страничка

Уязвимость с выводом через alert

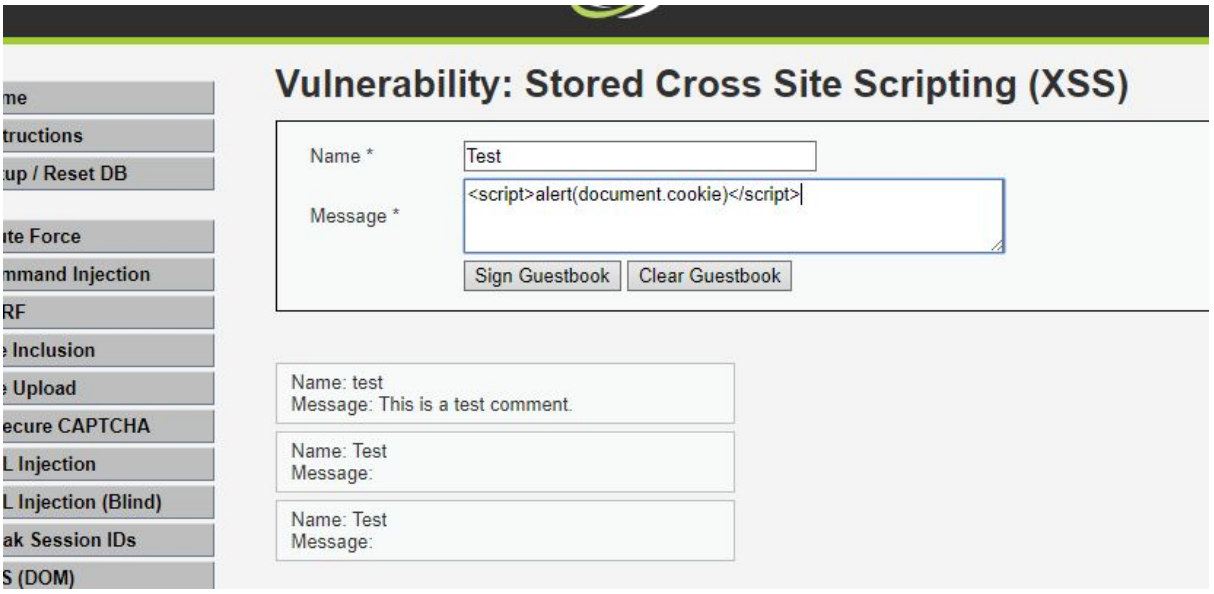
Вводим скрипт



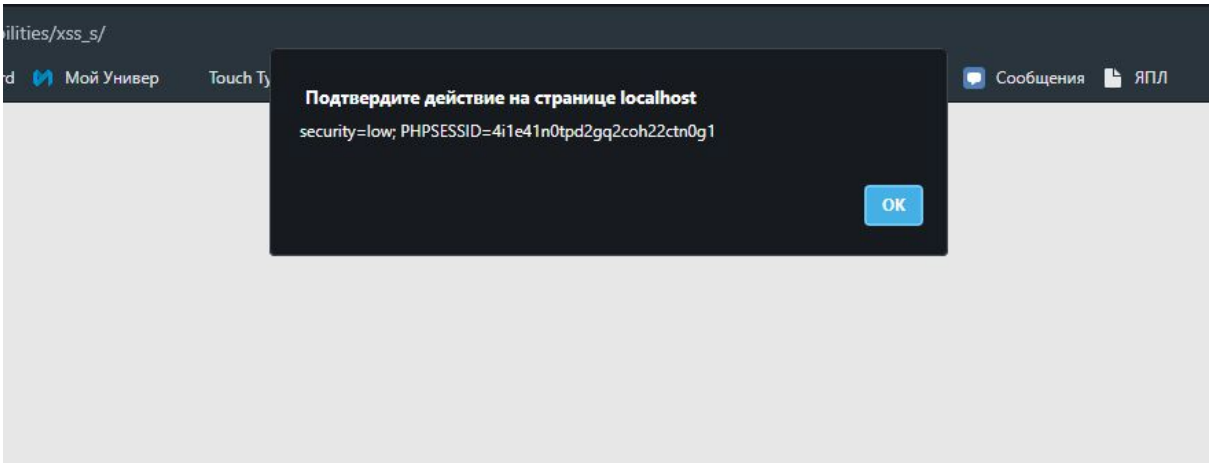
Получаем



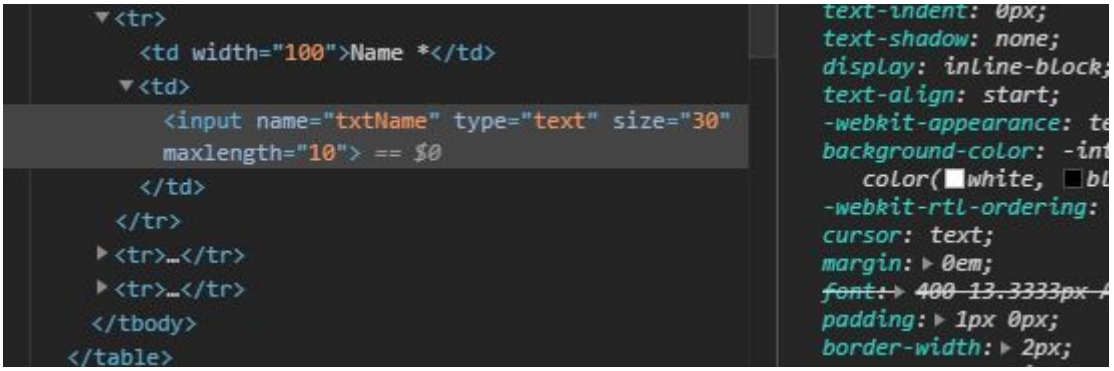
Уязвимость с получением cookie
Вводим скрипт



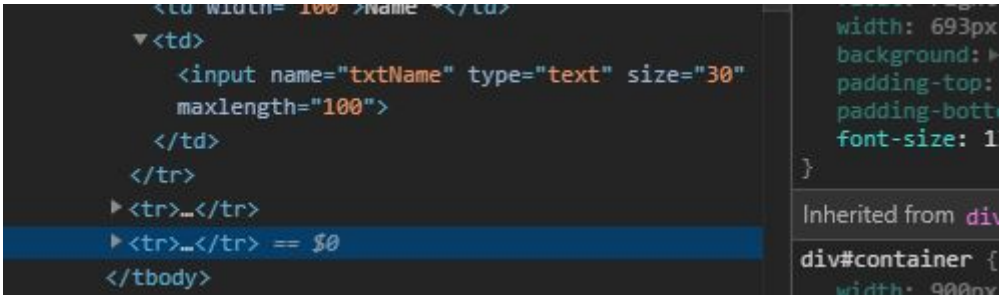
Получаем



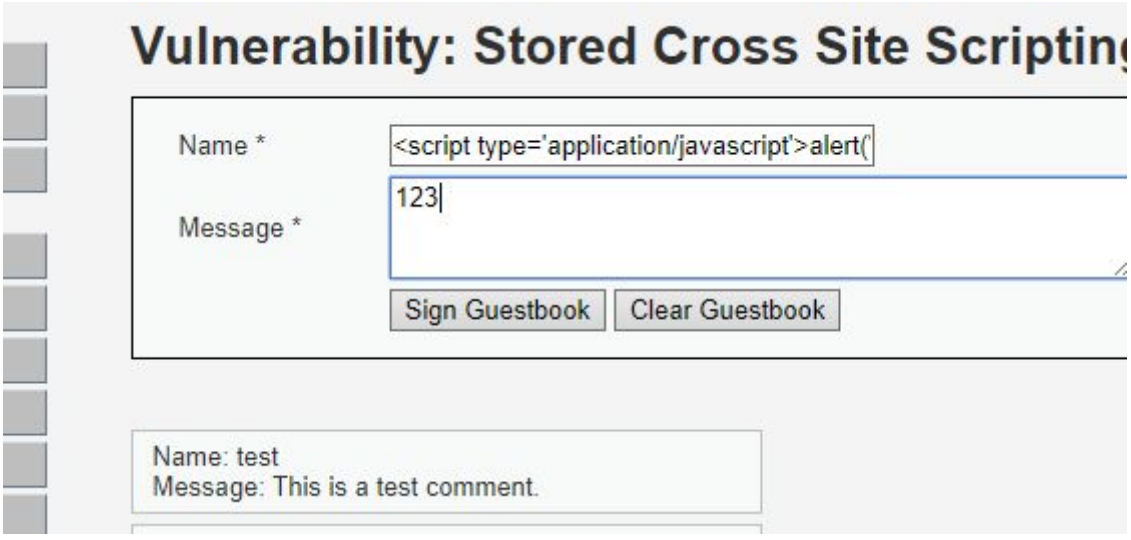
Также данные скрипты возможно ввести в поле Name, но там стоит ограничение длины сообщения



чтобы это исправить меняем максимальную длину сообщения

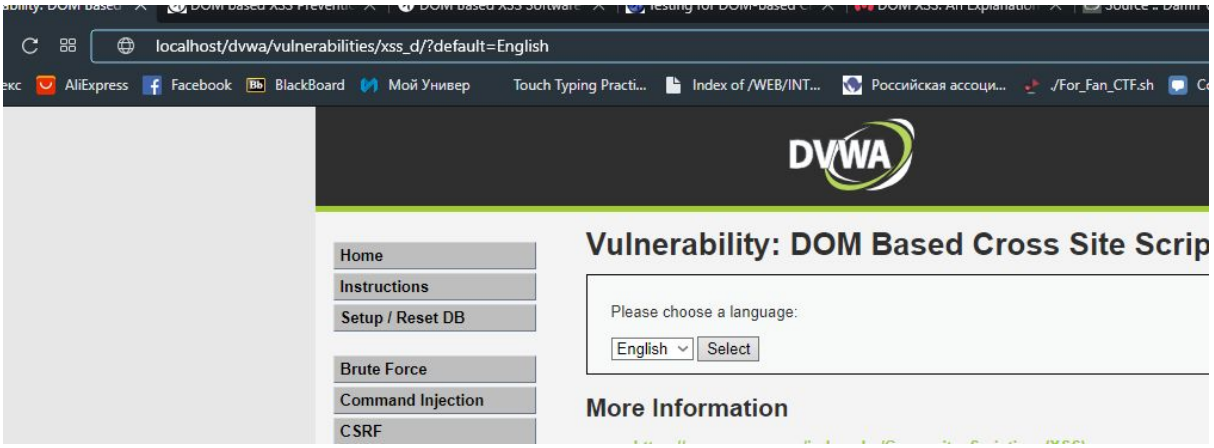


И вводим нужный нам скрипт



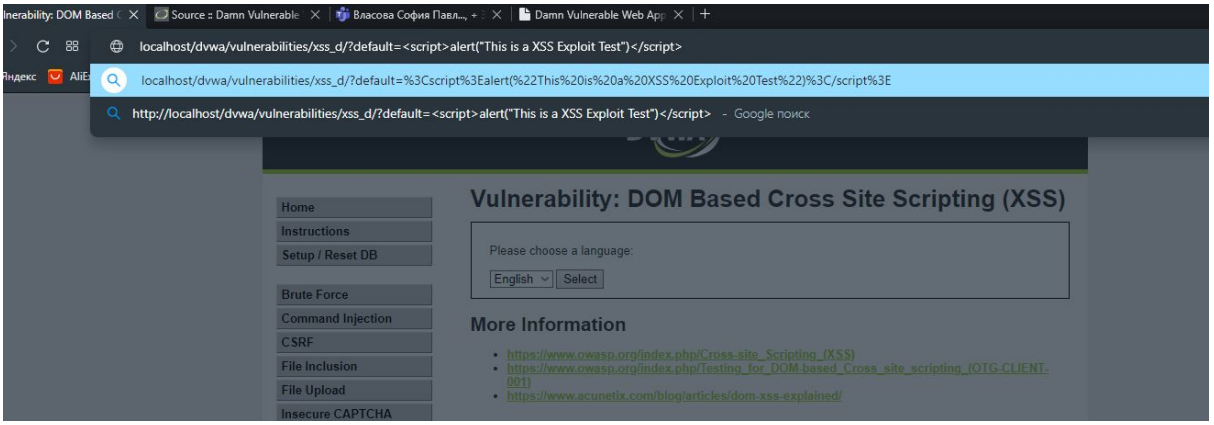
Разница различных уровней защиты:
LOW - нет проверки на спецсимволы
MEDIUM - проверка на спецсимволы для сообщений, для name ограничение на <script>
HIGH - проверка на спецсимволы для сообщений, для name ограничение на <script> через регулярки
IMPOSSIBLE - проверка на спецсимволы для имени и сообщений

XSS_Dom
Нормальное состояние

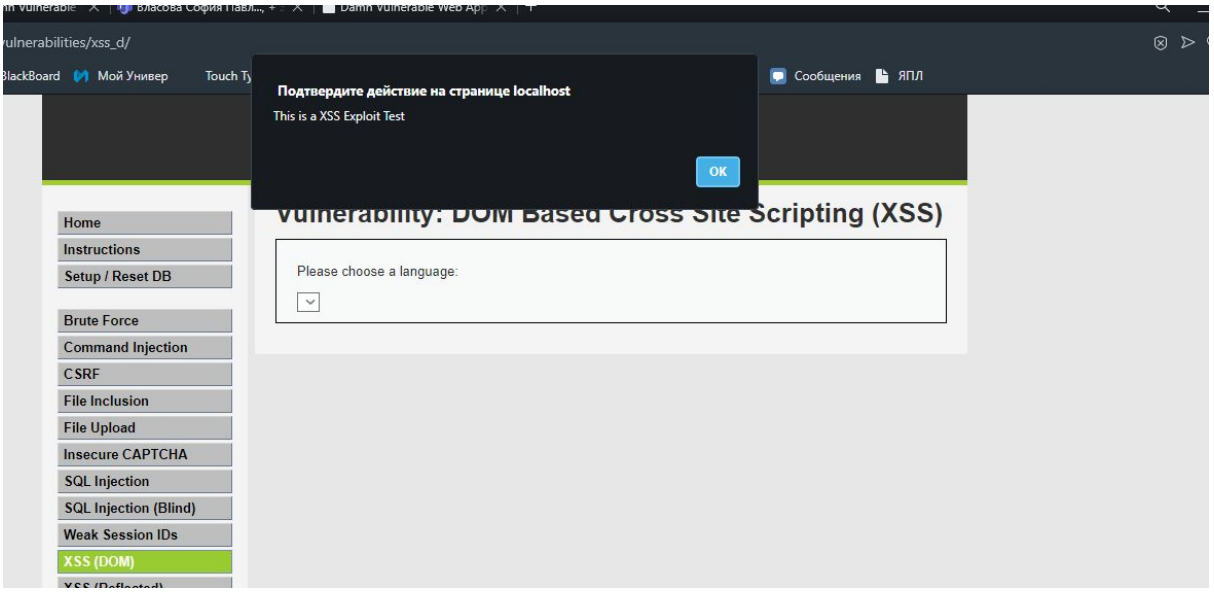


Уязвимость через alert

Вводим скрипт после *?default=

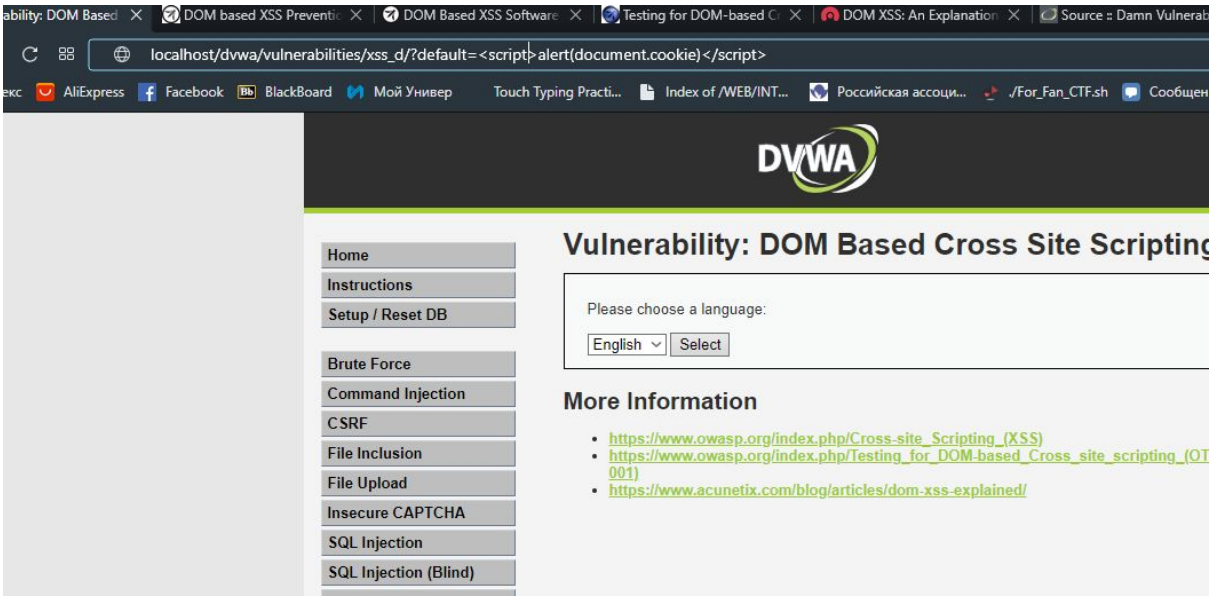


Получаем

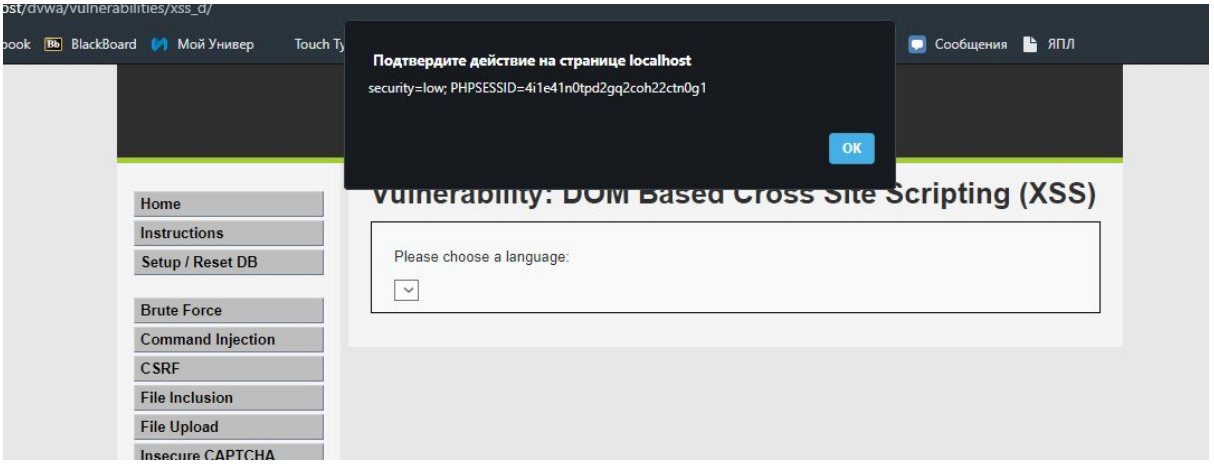


Уязвимость с cookie

Вводим скрипт



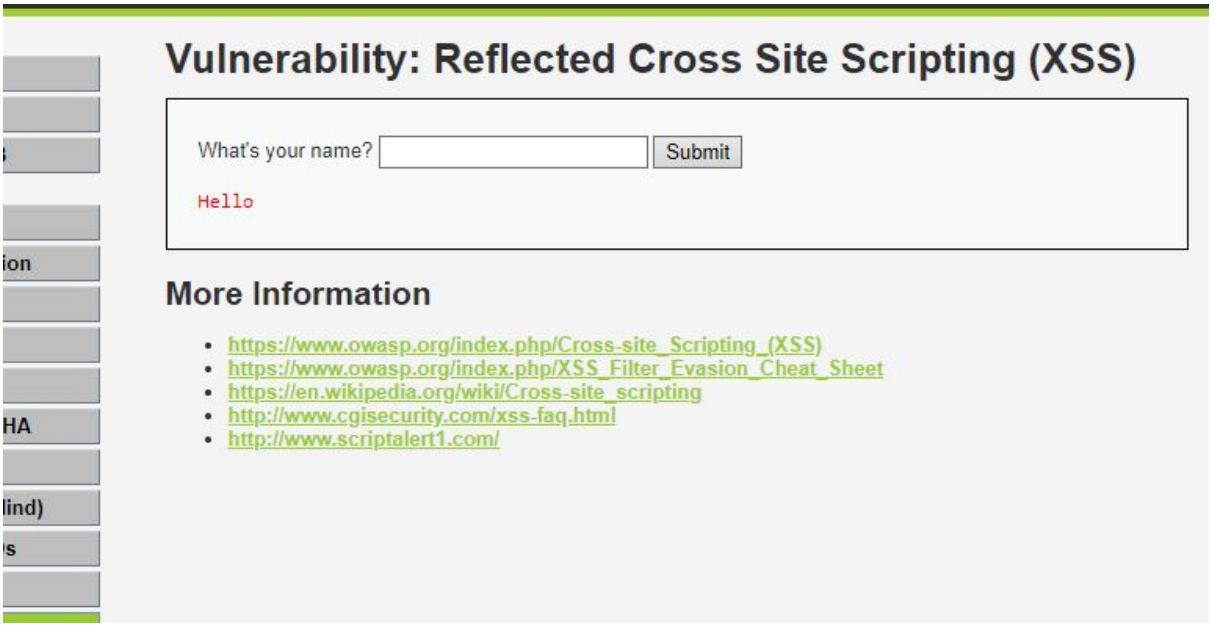
Получаем



Различия уровней защиты:
LOW - нет защиты
MEDIUM - проверка на <script, поэтому необходимы другие способы, например onload=alert(“XSS”)
HIGH - возможны только предопределенные значения, поэтому нужно запустить скрипт не заходя на сервер, тут помогает #, т.е. пишем, после *default=English#скрипт
IMPOSSIBLE - описания нет, но судя по всему ничего не сделать

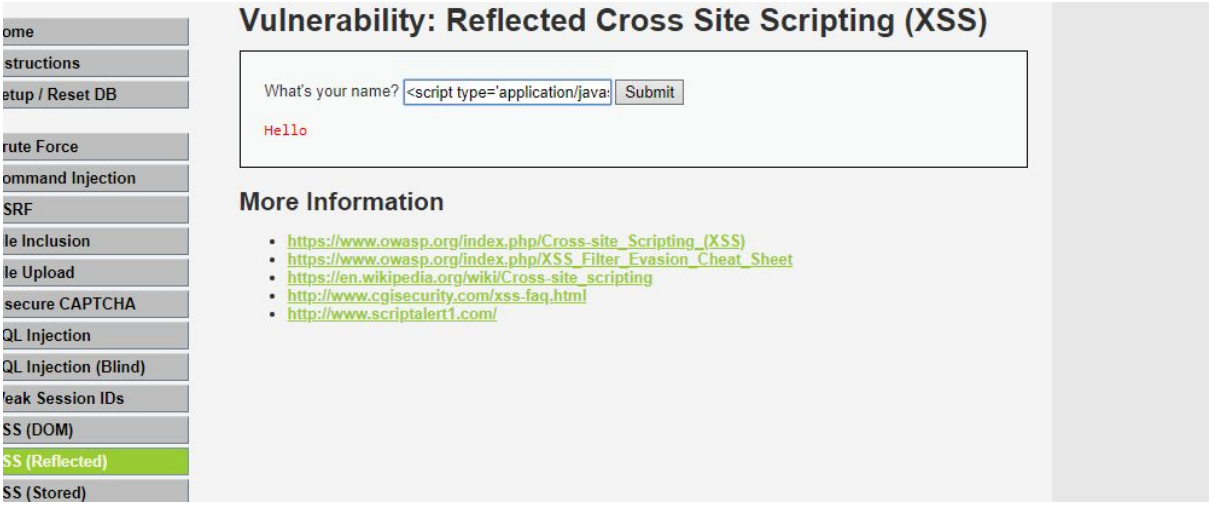
XSS_Reflected

Нормальное состояниее

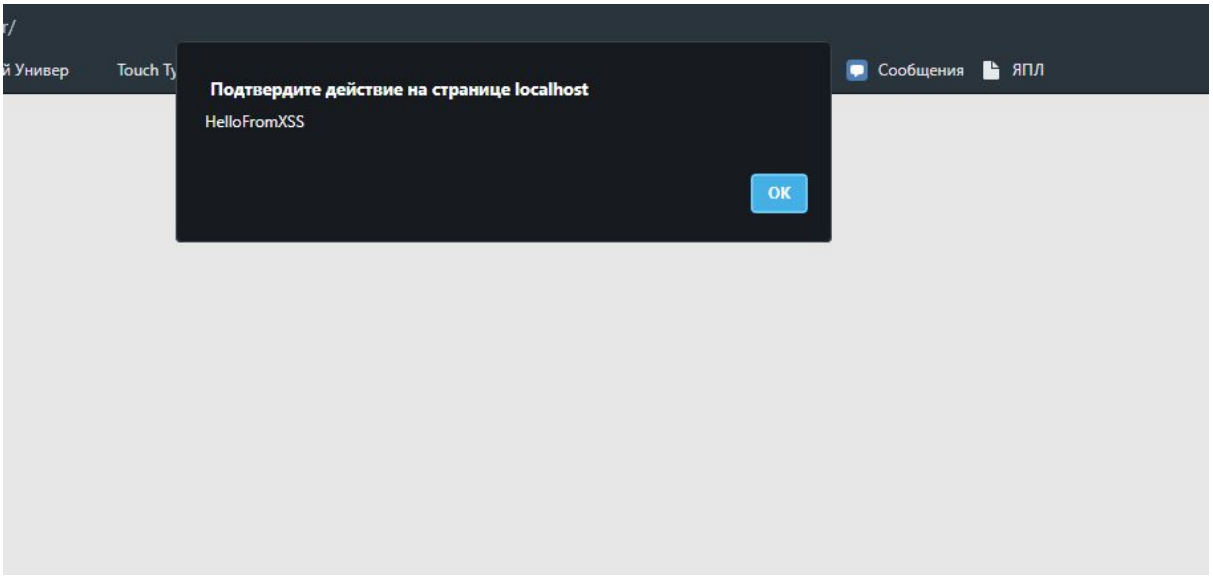


Уязвимость через alert

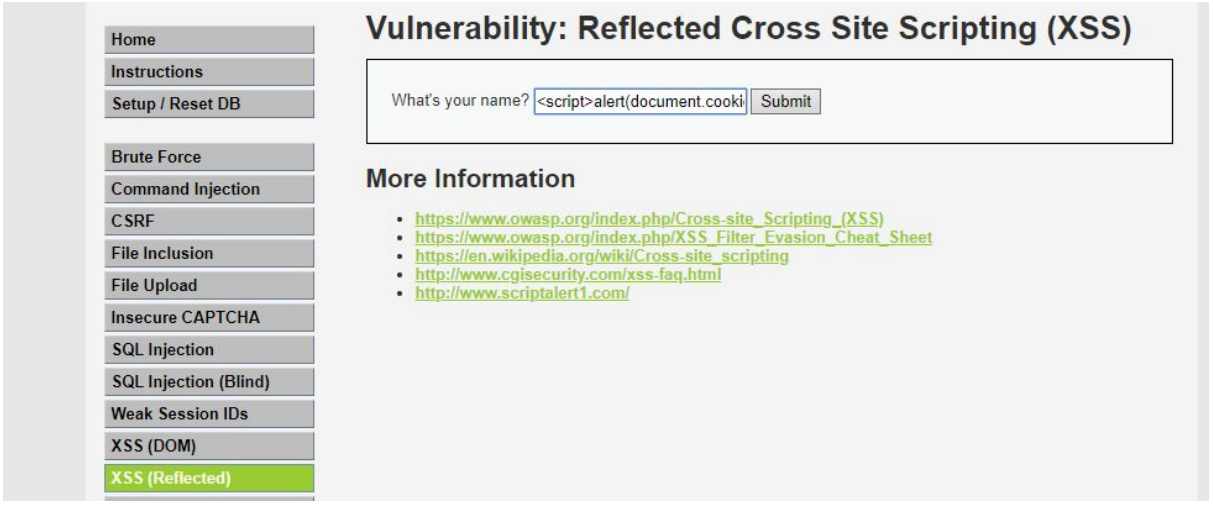
Вводим скрипт



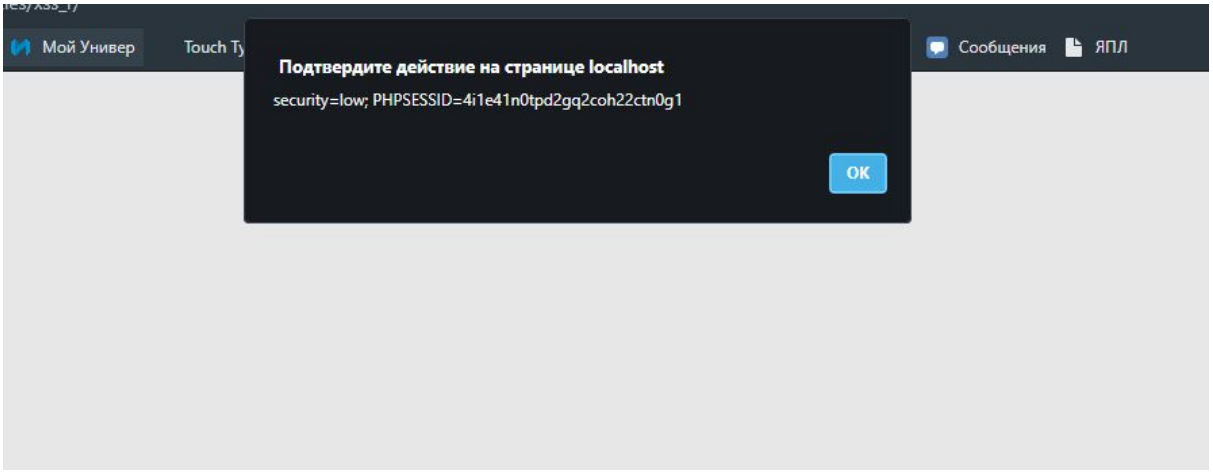
Результат



Уязвимость с cookie
Вводим скрипт



Получаем

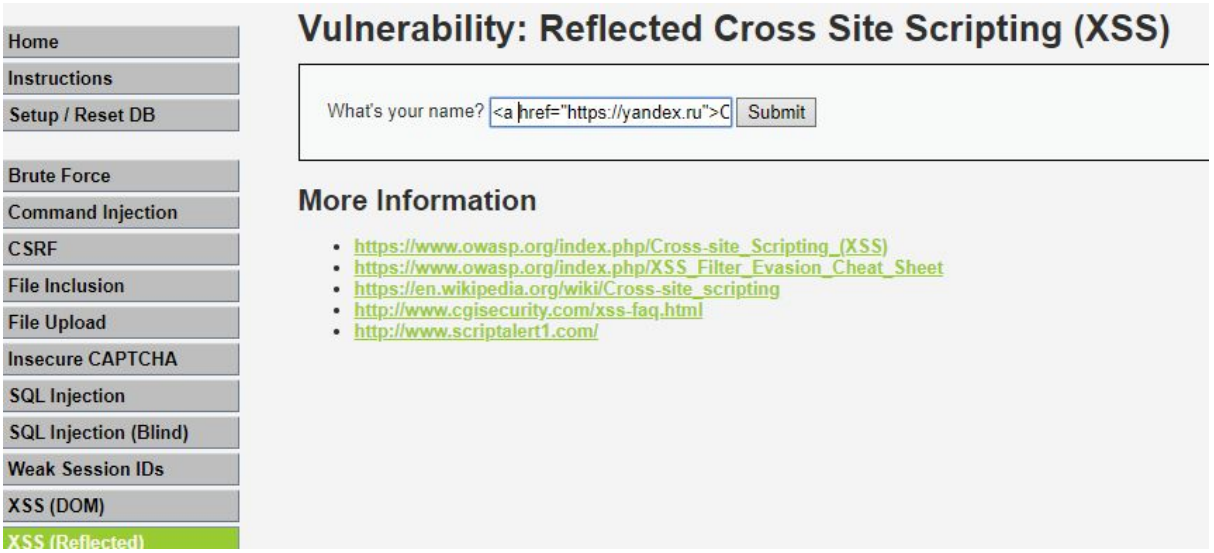


Уязвимость с frame
Вводим скрипт

Получаем

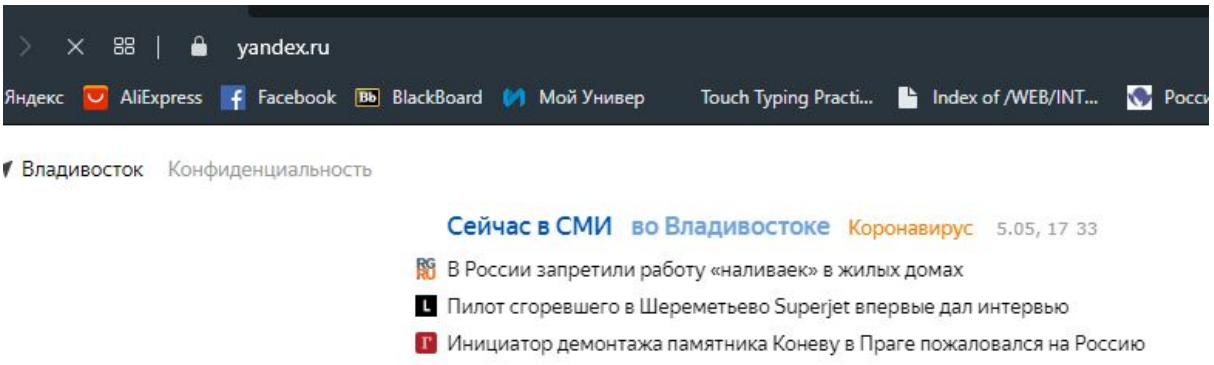
Уязвимость с ссылкой на другой сайт(href)

Вводим скрипт



Получаем

Кликаем по ссылке, нас перекидывает на другой сайт



Уровни безопасности:
LOW - нет защиты
MEDIUM - проверка на <script
HIGH - проверка на <script через регулярки
IMPOSSIBLE - проверка на спецсимволы