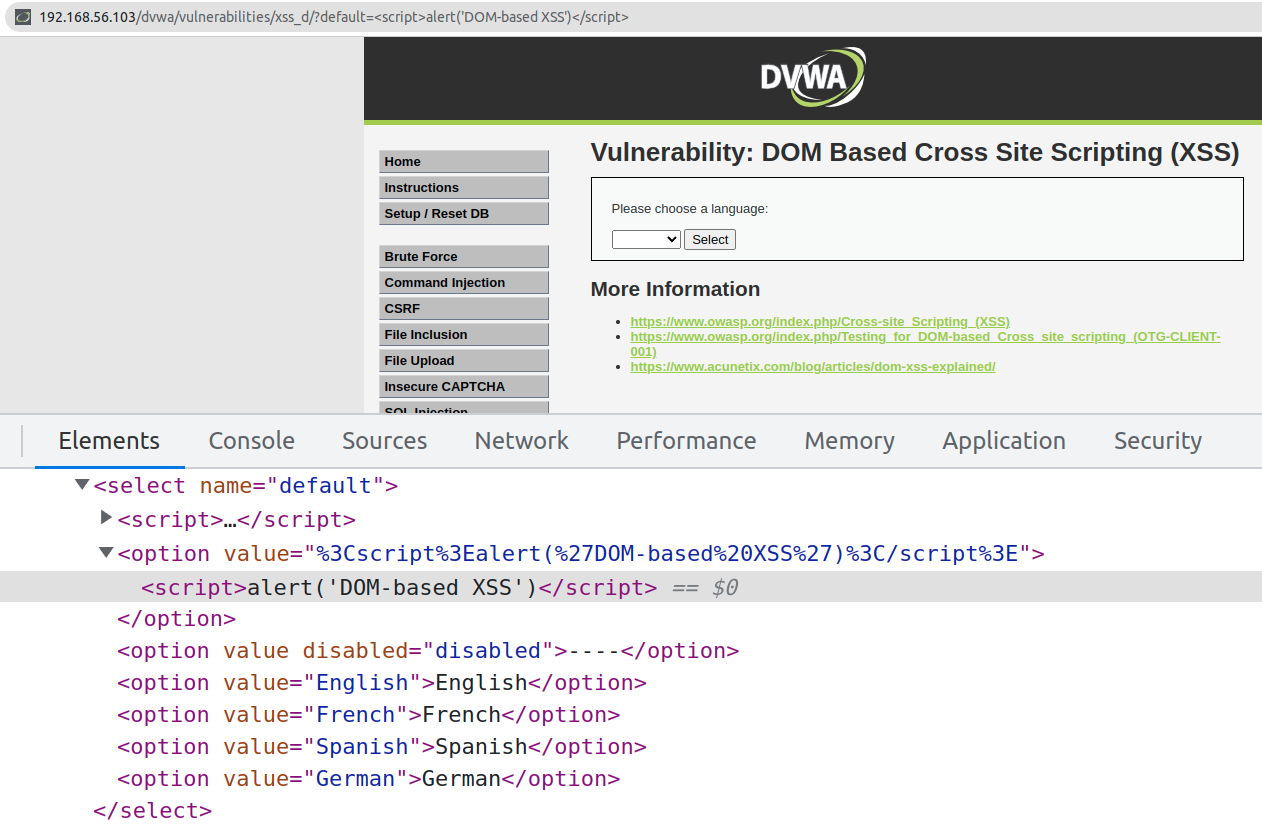
**Описание уязвимости**

На сайте **http://192.168.56.103/dvwa/vulnerabilities/xss\_d/** отсутствует фильтрация вводимых пользователем данных. Это позволяет удалённо выполнять JS код на странице и инжектить HTML-сущности.  
  
**Где найдена уязвимость**

Уязвимость расположена по адресу [**http://192.168.56.103/dvwa/vulnerabilities/xss\_d/**](http://192.168.56.103/dvwa/vulnerabilities/xss_s/).  
Наименование продукта: DVWA.  
  
**Технические детали обнаружения и воспроизведения**

Уязвимость можно обнаружить, если выбрать любой из предоставленых в списке языков, нажать кнопку «Select». После этого в адресной строке появится переменная «default» со значением того языка, который был выбран.  
Теперь в значение этой переменной можно написать любой HTML-тег, и нажать Enter.



**Выводы и рекомендации по устранению**

**Выводы**:  
Тип уязвимости: DOM-based XSS.  
Контекст уязвимости: HTML.  
Уязвимость позволяет получить доступ к конфиденциальной информации. Не требует дополнительных уязвимостей для эксплуатации.

**Рекомендации по устранению**:  
● Сделать фильтрацию вводимых пользователем данных на уровне разработки.  
  
**Используемое программное обеспечение**

● Google Chrome