

Описание уязвимости

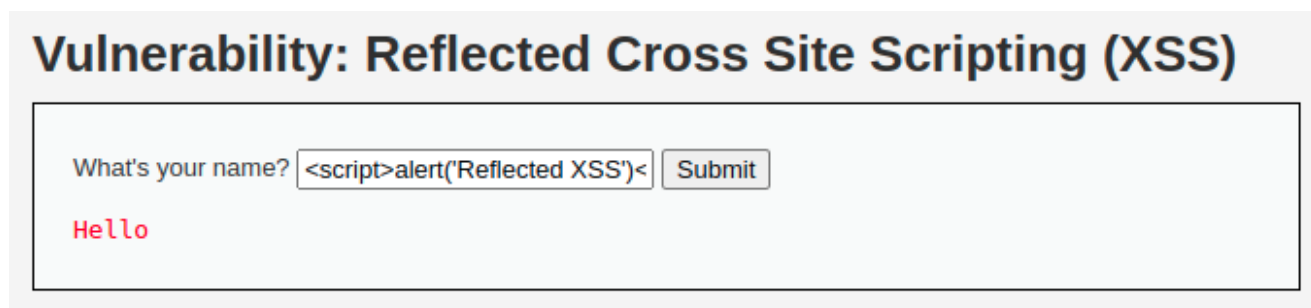
На сайте http://192.168.56.103/dvwa/vulnerabilities/xss_r/ отсутствует фильтрация вводимых пользователем данных. Это позволяет удалённо выполнять JS код на странице и инжектировать HTML-сущности.

Где найдена уязвимость

Уязвимость расположена по адресу http://192.168.56.103/dvwa/vulnerabilities/xss_r/.
Наименование продукта: DVWA.

Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить, если в поле "What's your name?" ввести любой HTML-тег и нажать кнопку "Submit".



Выводы и рекомендации по устранению

Выводы:

Тип уязвимости: Reflected 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