

## Описание уязвимости

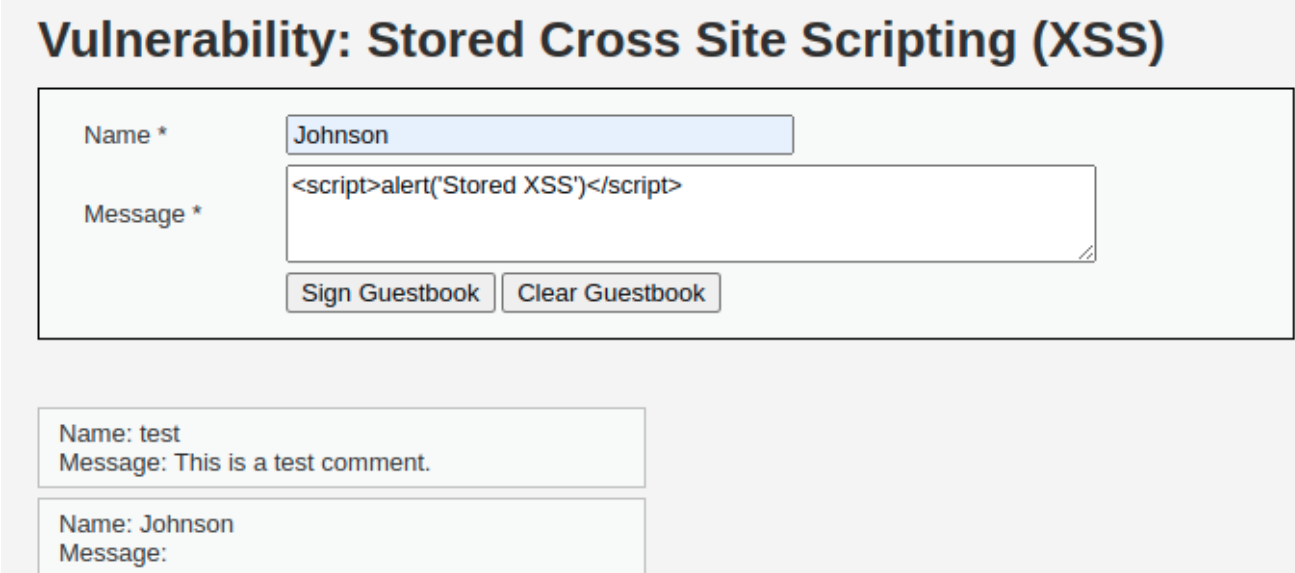
На сайте [http://192.168.56.103/dvwa/vulnerabilities/xss\\_s/](http://192.168.56.103/dvwa/vulnerabilities/xss_s/) отсутствует фильтрация вводимых пользователем данных. Это позволяет удалённо выполнять JS код на странице и инжектировать HTML-сущности.

## Где найдена уязвимость

Уязвимость расположена по адресу [http://192.168.56.103/dvwa/vulnerabilities/xss\\_s/](http://192.168.56.103/dvwa/vulnerabilities/xss_s/).  
Наименование продукта: DVWA.

## Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить, если в поле "Message" ввести любой HTML-тег и нажать кнопку "Sign Guestbook".



The screenshot shows the 'Vulnerability: Stored Cross Site Scripting (XSS)' page. The 'Name' field contains 'Johnson' and the 'Message' field contains the JavaScript payload `<script>alert('Stored XSS')</script>`. Below the input fields are two buttons: 'Sign Guestbook' and 'Clear Guestbook'. At the bottom, there are two boxes showing the state of the guestbook. The first box shows a previous entry: 'Name: test' and 'Message: This is a test comment.' The second box shows the current entry after the exploit: 'Name: Johnson' and 'Message:' (which will display the alert).

## Выводы и рекомендации по устранению

### Выводы:

Тип уязвимости: Stored 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