**Описание уязвимости**

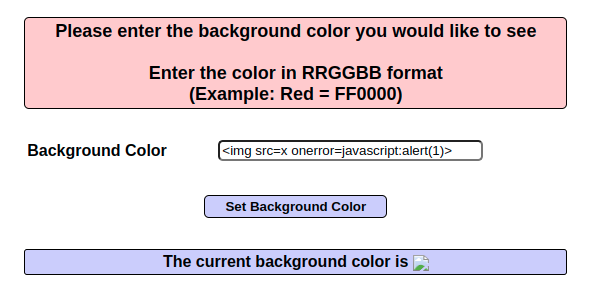
На сайте **http://192.168.56.103/mutillidae/index.php?page=set-background-color.php** обнаружена недостаточная фильтрация вводимых пользователем данных. Это позволяет выполнять JS код на странице и внедрять HTML-сущности на страницу.

**Где найдена уязвимость**

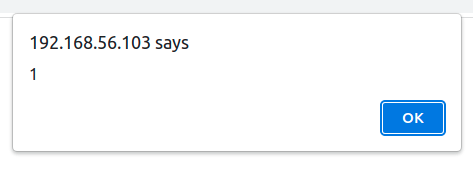
Уязвимость расположена по адресу **http://192.168.56.103/mutillidae/index.php?page=set-background-color.php**.  
Наименование продукта: Mutillidae.

**Технические детали обнаружения и воспроизведения**

Уязвимость можно обнаружить, если в поле “Background Color” ввести любую HTML-сущность и нажать на кнопку “Set Background Color”.

****

Результат эксплуатации:



**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**:  
● Добавить фильтрацию вводимых пользователем данных на уровне разработки.  
● Можно внедрить политику CSP.

**Используемое программное обеспечение**

● Google Chrome