# Описание уязвимости

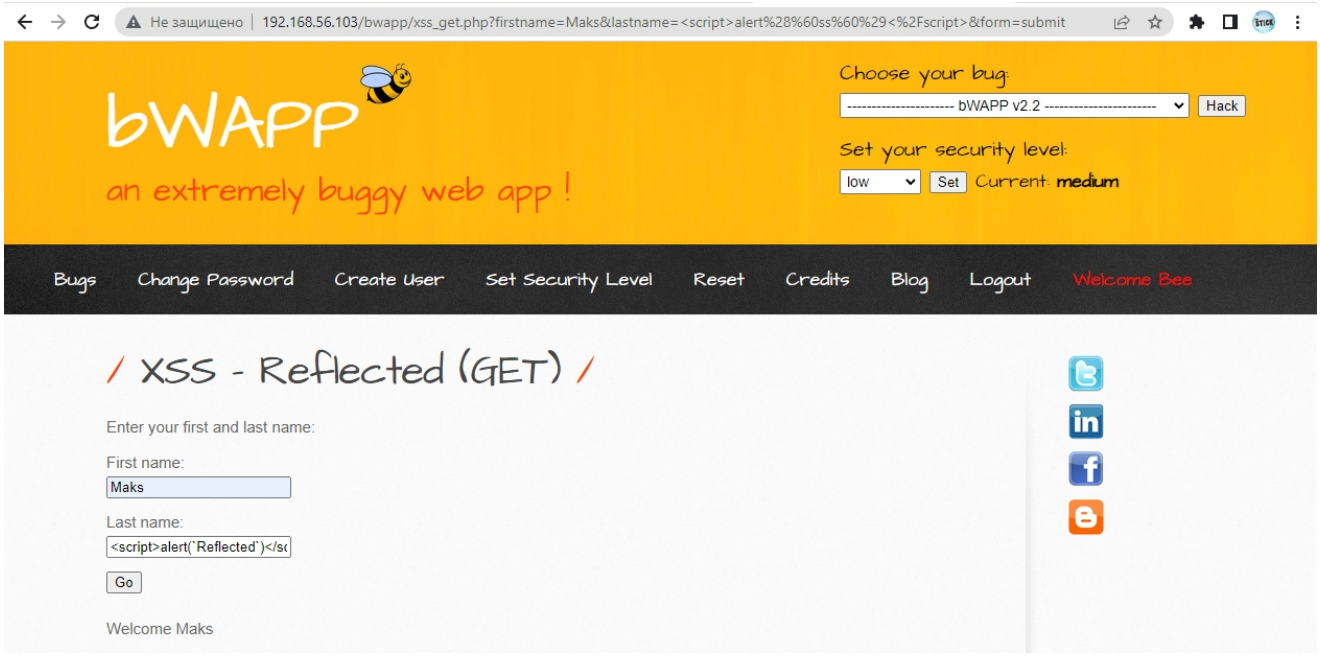
На сайте **http://192.168.56.103/bwapp/xss_get.php** обнаружена недостаточная фильтрация вводимых пользователем данных. Это позволяет выполнять JS код на странице и инжектить некоторые HTML-сущности.

# Где найдена уязвимость

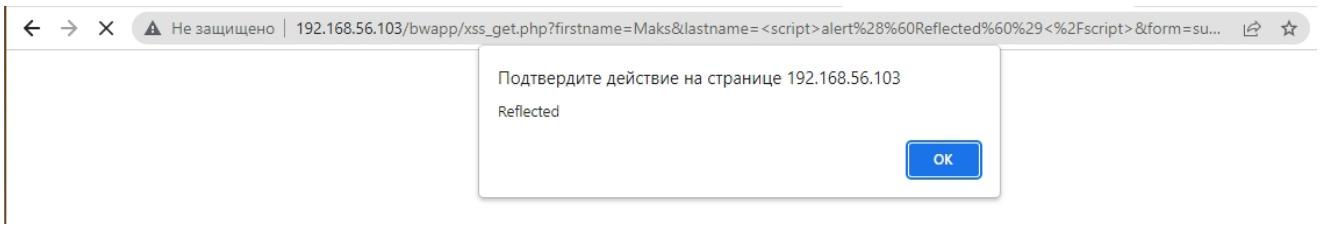
Уязвимость расположена по адресу **http://192.168.56.103/bwapp/xss_get.php**.
Наименование продукта: BWAPP.

# Технические детали обнаружения и воспроизведения

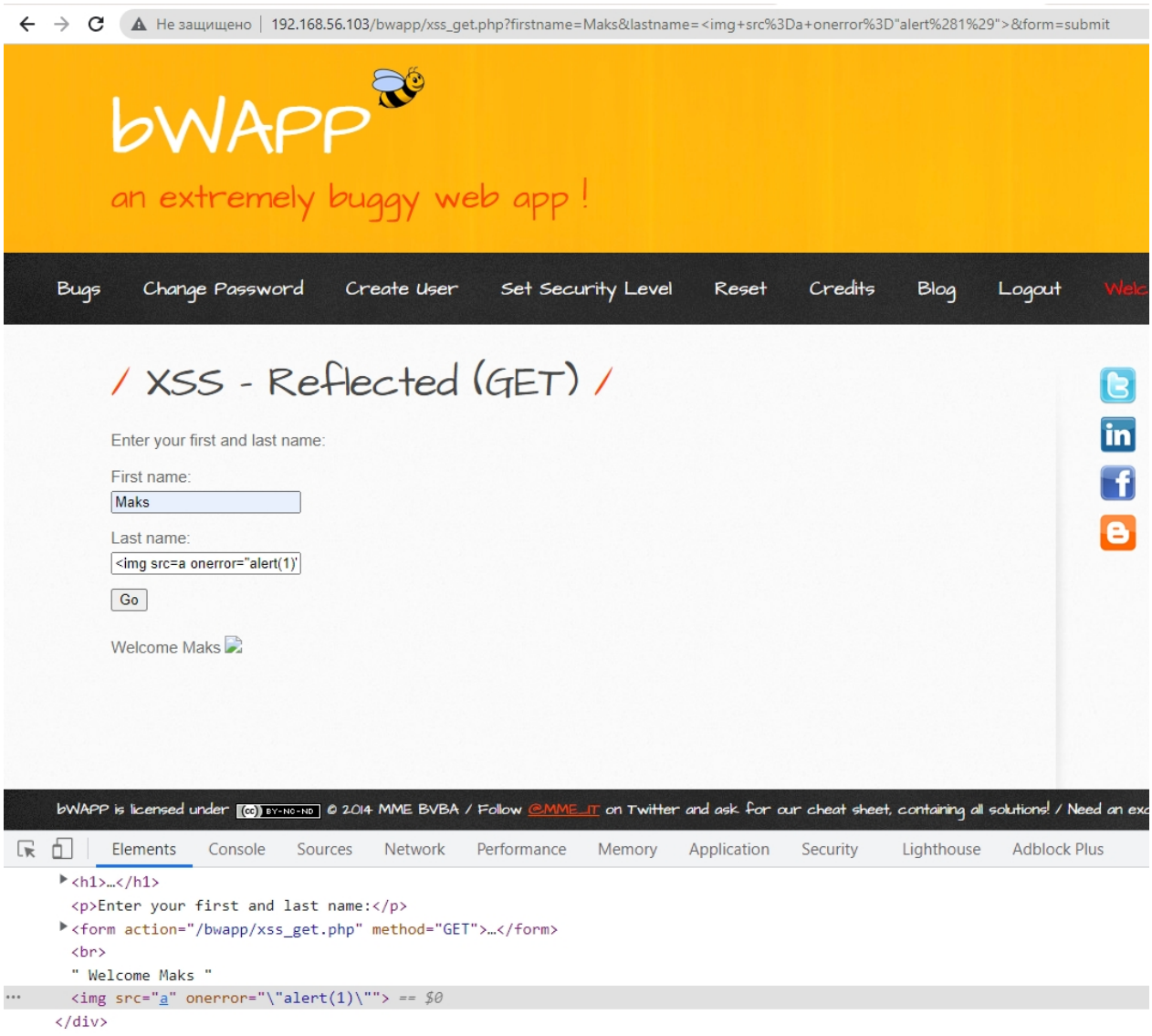
Уязвимость можно обнаружить, если в поле “First name” или в поле “Last name” ввести такой HTML-объект, который не содержит двойные и одинарные ковычки. Однако, это не касается косых ковычек ``.




Результат эксплуатации



Вот результат вектора **onerror:**




# 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**:
- Дополнить фильтрацию вводимых пользователем данных на уровне разработки.
- Можно внедрить политику CSP.

# Используемое программное обеспечение

- Google Chrome