Задание выполнил студент группы 2345 Романенко Кирилл

1. Найдите XSS на странице XSS – Reflected (GET) проекта bWAPP (уровень сложности Medium) и определите ее тип. Составьте отчет о найденной уязвимости.

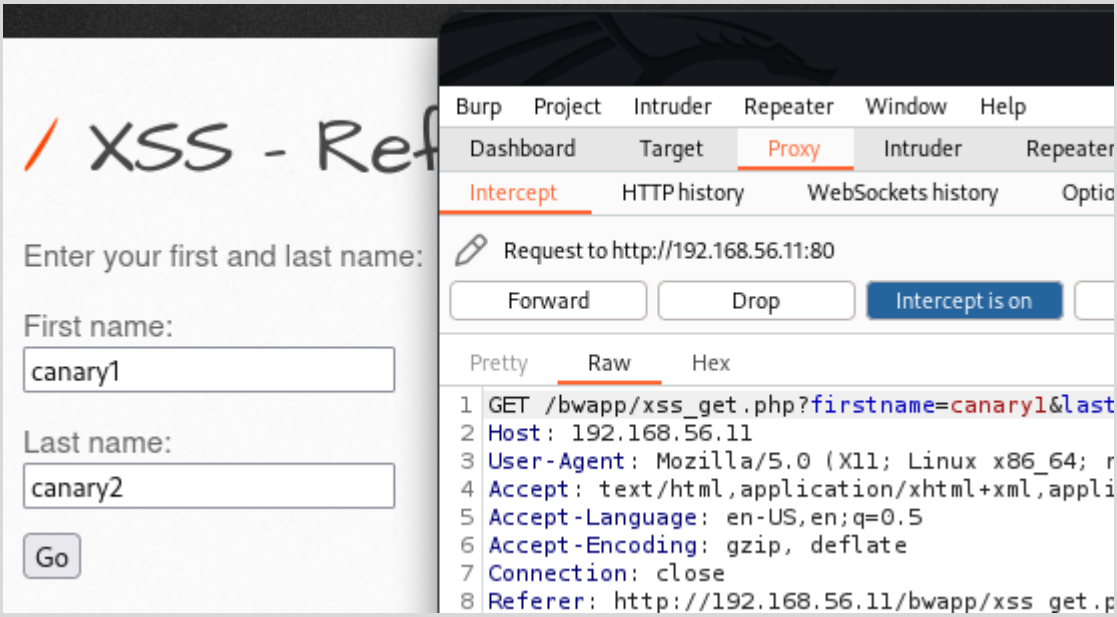
На сайте http://192.168.56.11/bwapp/xss_get.php отсутствует фильтр данных в форме для их ввода. Это позволяет выполнить XSS-инъекцию в исполняемом контексте.

Где найдена уязвимость

Уязвимость расположена по адресу
http://192.168.56.11/bwapp/xss_get.php.
Наименование продукта: Metasploitable 3 Linux virtual machine.

Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить на странице
http://192.168.56.11/bwapp/xss_get.php.
Ввел в форму ввода First name: canary1 ; Last name: canary2
и перехватил запрос в Burp Suite:

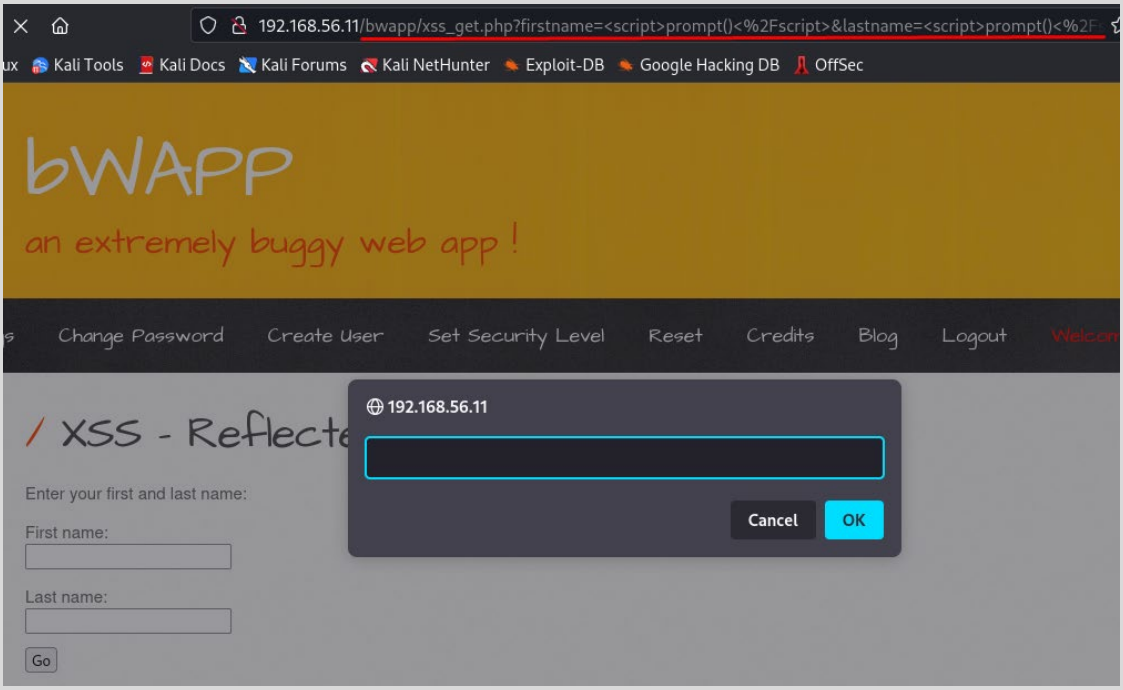


При анализе запроса-ответа обнаружил, что введенные данные падают в параметр p

```
        <p><label for="firstname">First name:</label><
br />
        <input type="text" id="firstname" name="
firstname"></p>

        <p><label for="lastname">Last name:</label><br
/>
        <input type="text" id="lastname" name="lastname
"></p>

        <button type="submit" name="form" value="submit
">Go</button>

    </form>

    <br />
    Welcome canary1 canary2
```

Ввёл конструкцию JavaScript <script>prompt()</script> в обе строки

Итог:



Выводы и рекомендации по устранению

Уязвимость позволяет вывести на экран окно с полем ввода конфиденциальной информации. Не требует дополнительных уязвимостей для эксплуатации. Рекомендации по устранению:

- Запретить теги в пользовательском виде,
- Запретить спец.символы,
- Настроить CSP

Используемое программное обеспечение

- BurpSuite.

- FireFox Extended Support Release 102.5.0esr (64-bit).