Выполнил Мешечкин Д. Инфобез-2837 (Ранее 2345)

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

Ოχ̆ Ʒӹძχ̆Ʒӹ Ǥ dƺdʓʒԊq
Уязвимость расположена по адресу

http://localhost/xss_get.php

Наименование продукта: bWAPP an extremely buggy web app!

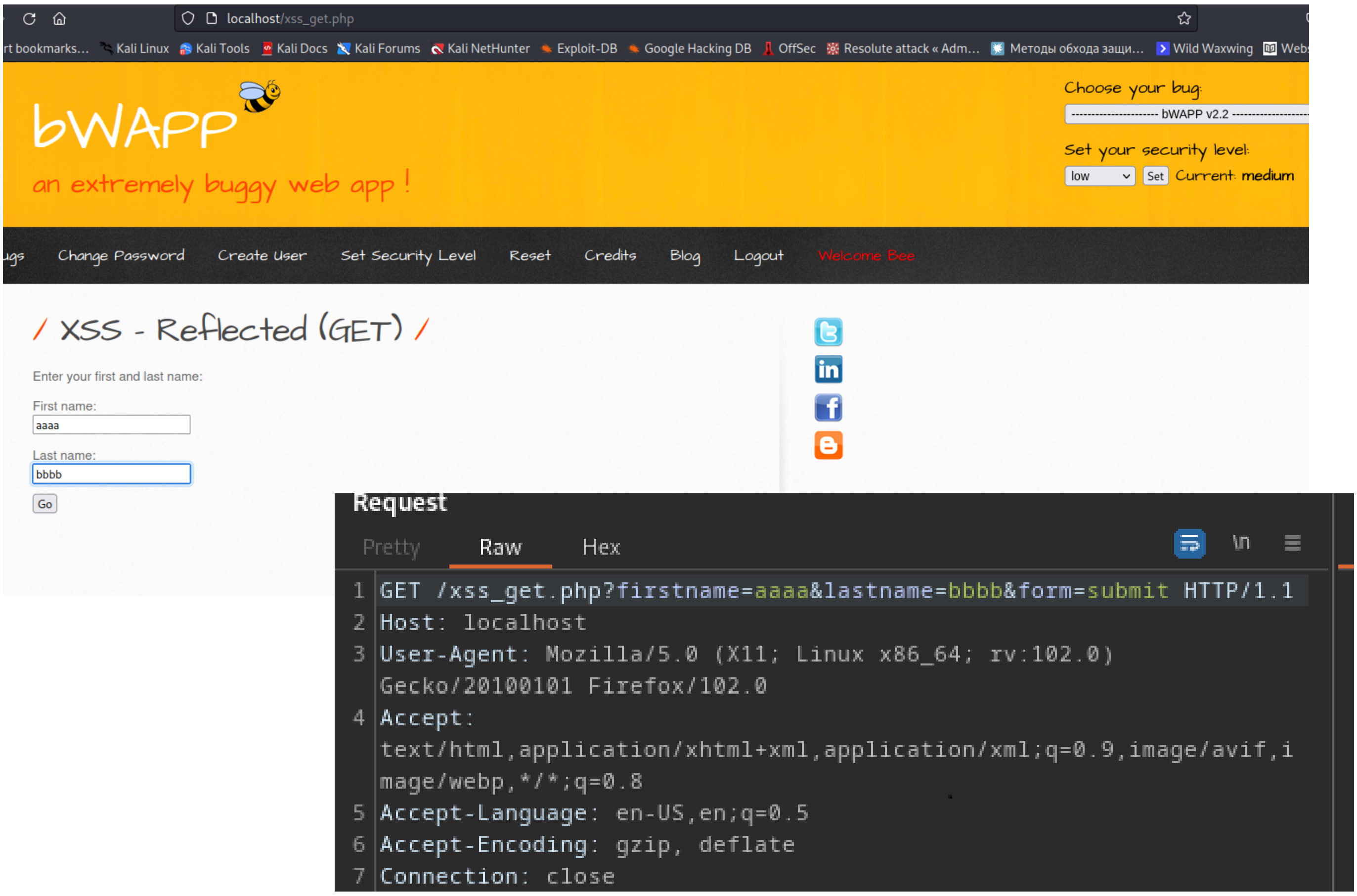
Наименование продукта: bWAPP /XSS - Reflected (GET) - medium/

ЭχʊƷdƐχԊძχ̆ χ̆χ̆ӹ̈Ʒd ʒƑƷӹԽǤϰχ̆Ʒd d ƒʒԊԽʒddƒχ̆χ̆Ʒd :

Уязвимость можно обнаружить на странице http://localhost/xss_get.php.

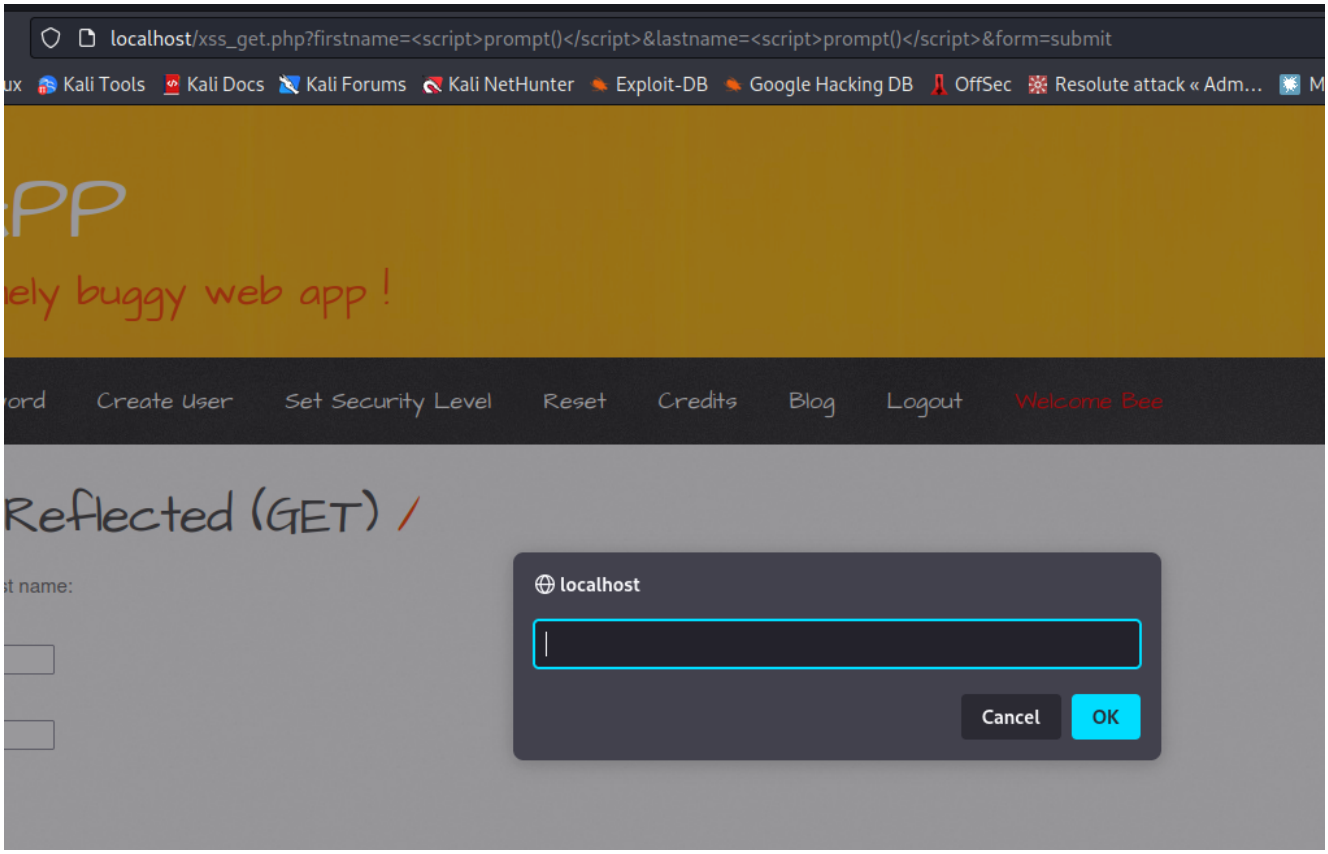
Ввел в форму ввода First name: aaaa ; Last name: bbbb

и перехватил запрос в Burp Suite:



При анализе запроса-ответа обнаружил, что введенные данные падают в переменные
- firstname=
- lastname=

Пробую уязвимость конструкцией JavaScript *<script>prompt()</script>* в обе переменные



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:

- Необходима настройка валидации входных данных.
- Экранирование вывода.
- Настройка CSP.

Используемое программное обеспечение

- BurpSuite
- Браузер Firefox browser 102.8.0esr (64-bit)