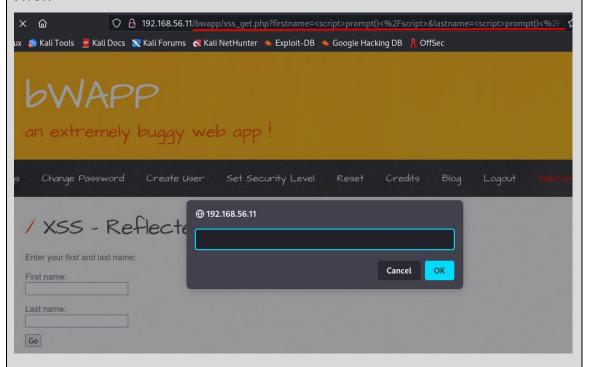
Задание выполнил студент группы 2345 Романенко Кирилл

параметр р

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

Ha 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: Burp Project Intruder Window Repeater Help / XSS - Re-Dashboard Target Proxy Intruder Repeater Intercept HTTP history WebSockets history Optic Request to http://192.168.56.11:80 Enter your first and last name: Forward Drop Intercept is on First name: Pretty Raw Hex canary1 1 GET /bwapp/xss_get.php?firstname=canaryl&last 2 Host: 192.168.56.11 Last name: 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; r canary2 4 Accept: text/html,application/xhtml+xml,appli 5 Accept-Language: en-US, en; q=0.5 6 Accept-Encoding: gzip, deflate Go 7 Connection: close 8 Referer: http://192.168.56.11/bwapp/xss get.p При анализе запроса-ответа обнаружил, что введенные данные падают в

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).