Задание выполнил студент группы 2345 Романенко Кирилл

1. Решите задачу по эксплуатации CSRF из проекта DVWA (уровень сложности Medium).

На сайте http://192.168.56.11/dvwa/vulnerabilities/csrf/ отсутствует проверка соответствия Host - Referer

Где найдена уязвимость

Уязвимость расположена по адресу

http://192.168.56.11/dvwa/vulnerabilities/csrf/

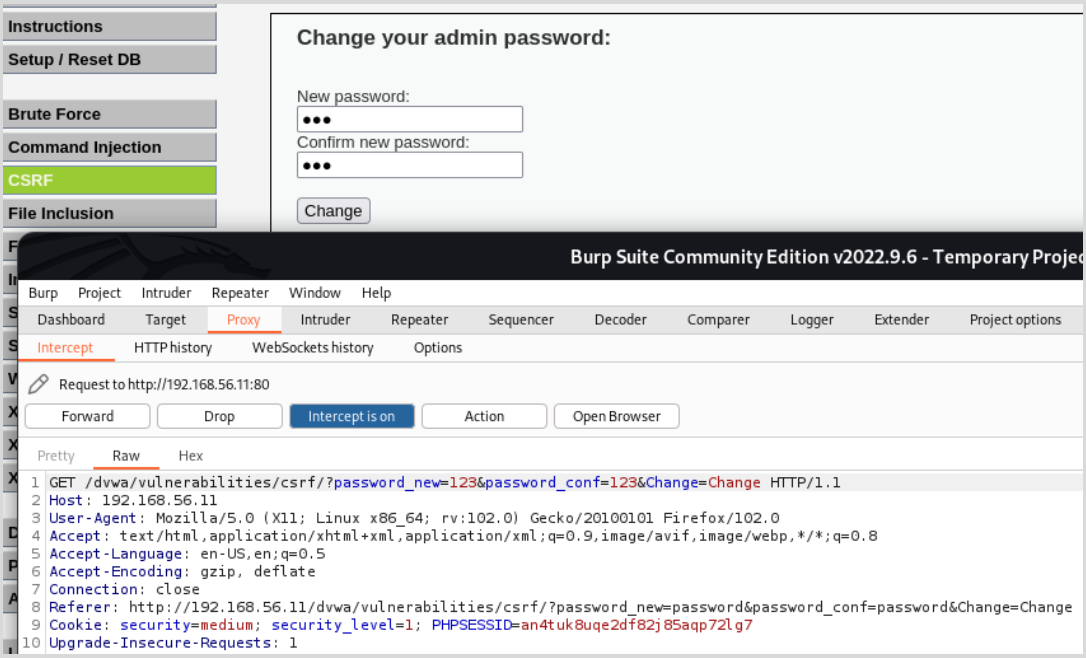
Наименование продукта: Metasploitable 3 Linux virtual machine.

Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить на странице

http://192.168.56.11/dvwa/vulnerabilities/csrf/

Ввел в форму ввода 123 и перехватил запрос в Burp Suite:

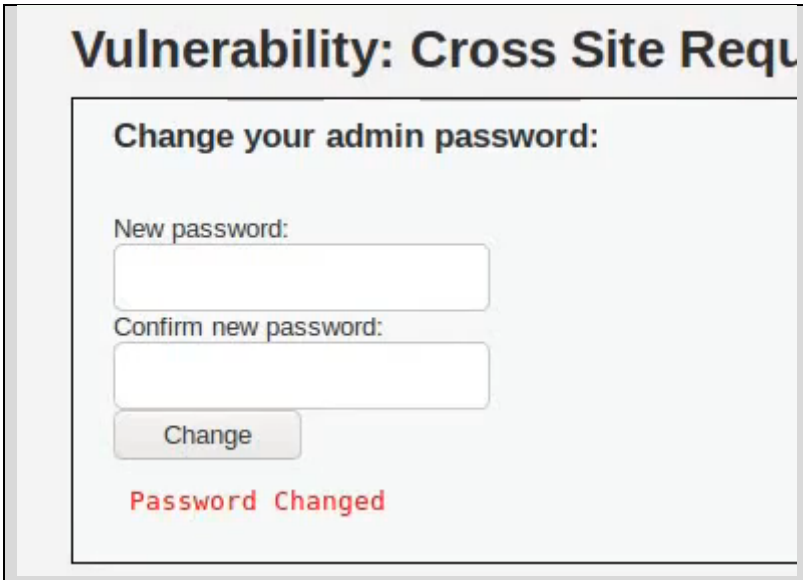


Заменил Referer

ДО: http://192.168.56.11/dvwa/vulnerabilities/csrf/

ПОСЛЕ: 127.0.0.1

Forward



Выводы и рекомендации по устранению

Уязвимость позволяет изменить пароль от любой учётной записи. Не требует дополнительных уязвимостей для эксплуатации. Рекомендации по устранению:

- Использовать CSRF-токены
- SameSite Cookie

Используемое программное обеспечение

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