Выполнил Мешечкин Д. Инфобез-2837

Задание 1: Выполните развертывание среды DVWA (или используйте готовый образ). Решите задание Command Injection на уровне сложности Low, Medium и High. Каким образом можно обойти защиту?

Low

Ввод команды localhost; ls -la/root
Получаю список директорий корня машины. Команда прошла. Защиты нет. Всё отлично.

Medium

Ввод команды localhost | cat /etc/passwd
Получаю содержимое файла passwd
Команда прошла. Защита минимальная.

High

Необходимо изучение кода, замена символов.
Ввод команды localhost|pwd
Получаю директорию расположения. Команда прошла. Защита больше.

Задание 2: Изучите страницу http://192.168.56.11/bwapp/phpi.php и определите, какие уязвимости там присутствуют. Составьте отчет о найденной уязвимости.

В адресной строке браузера выполняются команды на языке php - инъекции.
Это позволяет получить полный доступ к информации, хранящейся на сервере, а также к её обработке, без необходимости выстраивания сложной схемы проникновения и эксплуатации.

Где найдена уязвимость:
Уязвимость расположена по адресу
http://localhost/bwapp/phpi.php?message=test

Наименование продукта:
bWAPP (an extremely buggy web app!)

Технические детали обнаружения и воспроизведения:
Изначально уязвимость обнаруживает себя нахождением значений после переменной.
Уязвимость можно протестировать, подставляя различные команды в строку браузера на ресурсе после **test** на языке **php**
http://localhost/bwapp/phpi.php?message=test; system(ls -l /);

Выводы и рекомендации по устранению:

Уязвимость позволяет получить доступ к конфиденциальной информации.
Не требует дополнительных уязвимостей для эксплуатации.

Рекомендации по устранению:

- Установить фильтры всех входящих параметров
- Пересобирать файлы, присланные от пользователей
- Отключить небезопасные функции php. (Например, с помощью disable_functions в файле php.ini)
- Защитить системные файлы от чтения с любой учётной записи

Используемое программное обеспечение:
Браузер Firefox browser 102.8.0esr (64-bit)
bWAPP docker