

Задание выполнил студент группы 2345 Романенко Кирилл Д.

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

Ввёл команду 192.168.56.11|cp var/www/html/phpinfo.php
var/www/html/goodluck.php

Команда прошла. Защиты 0

Medium

Ввёл команду 192.168.56.11|cp var/www/html/phpinfo.php
var/www/html/goodluck.php

Команда прошла. Защита не сработала

High

Происходит замена символов на другие. С помощью замены обычных символов на специальные на языке php изменил запрос.

Заменял | и / с помощью команды htmlspecialchars
(<https://www.php.net/manual/ru/function htmlspecialchars>)

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

В 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://192.168.56.11/bwapp/phpi.php?message=test>

Наименование продукта: Metasploitable 3 Linux virtual machine.

Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить, подставляя различные команды в строку браузера на сайте после test на языке php
<http://192.168.56.11/bwapp/phpi.php?message=test>

