**Урок 7. Remote Code Execution**

Задание 1:

Есть сценарий (dig.PHP), его следует проверить на наличие уязвимостей, которые приводят к RCE. Установите сценарий, протестируйте его и дайте рекомендации, как повысить безопасность его использования.

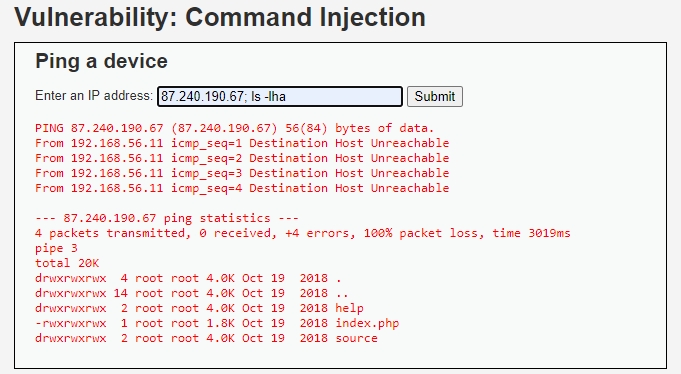
Решение:

Задание 2:

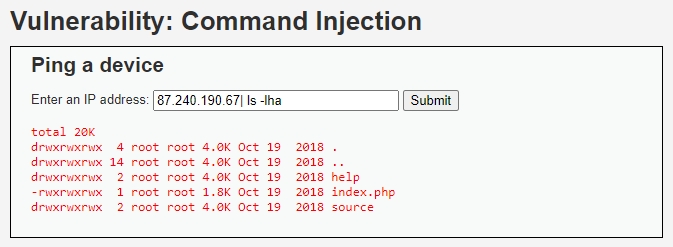
Выполните развертывание среды DVWA (или используйте готовый образ). Решите задание Command Injection на уровне сложности Low, Medium и High. Каким образом можно обойти защиту?

Решение:

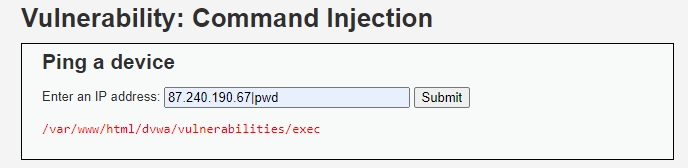
На уровне сложности low:



На уровне сложности medium:



И на high:



Задание 3:

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

Решение:

Если обратить внимание на адресную строку, то можно заметить, что страница сервиса bwapp уязвима к RCE, а именно code injection.



Задание 4:

\*Решите задание <https://www.root-me.org/en/Challenges/Web-Server/Backup-file>.

Решение:

Просто

