Описание уязвимости

На сайте http://192.168.56.11/mutillidae/index.php?page=dns-lookup.php отсутствует фильтрация вводимых пользователем данных. Это позволяет удалённо выполнять команды на сервере.

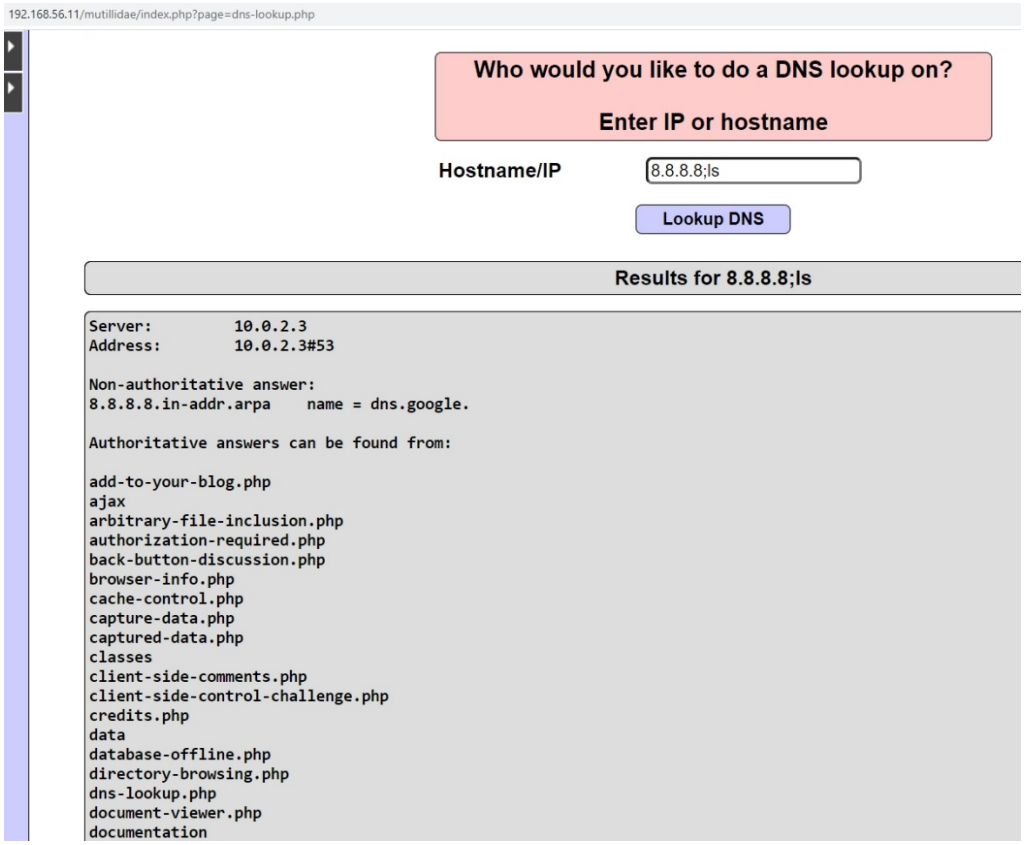
Где найдена уязвимость

Уязвимость расположена по адресу http://192.168.56.11/mutillidae/index.php?page=dns-lookup.php.

Наименование продукта: Metasploitable 3 Linux virtual machine.

Технические детали обнаружения и воспроизведения

Уязвимость можно обнаружить, если в поле, предназначенном для ввода DNS адреса, ввести адресс и после него, через точку с запятой “ ; ” ввести любую команду терминала Linux (payload - полезную нагрузку). Например ls или pwd.



Выводы и рекомендации по устранению

Уязвимость позволяет получить доступ к конфиденциальной информации. Не требует дополнительных уязвимостей для эксплуатации. Рекомендации по устранению:

- Сделать фильтрацию вводимых пользователем данных на уровне разработки.

Используемое программное обеспечение

- Google Chrome