**Описание уязвимости**

В каталоге vulnerabilities/fi/ [проекта](http://192.168.56.11/) XVWA найдены следующие уязвимости: Local File Inclusion (LFI), Remote File Inclusion (RFI).  
Данные уязвимости позволяют запускать на сервере несанкционированные файлы, которые могут повлиять на конфиденциальность и целостность информационной системы, а также читать произвольные файлы на сервере.

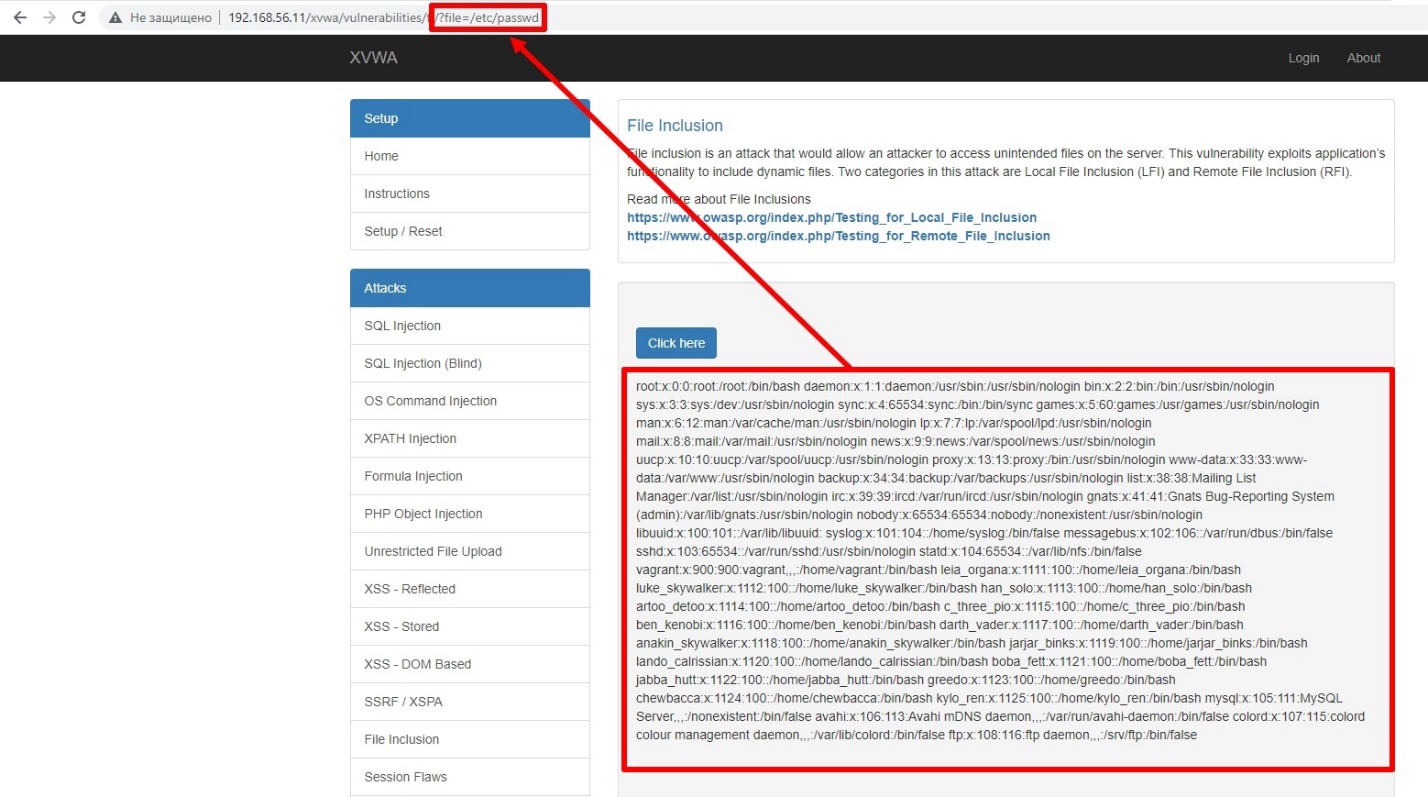
**Где найдена уязвимость**

Уязвимость расположена по адресу http://192.168.56.11/xvwa/vulnerabilities/fi/.

Наименование продукта: XVWA.

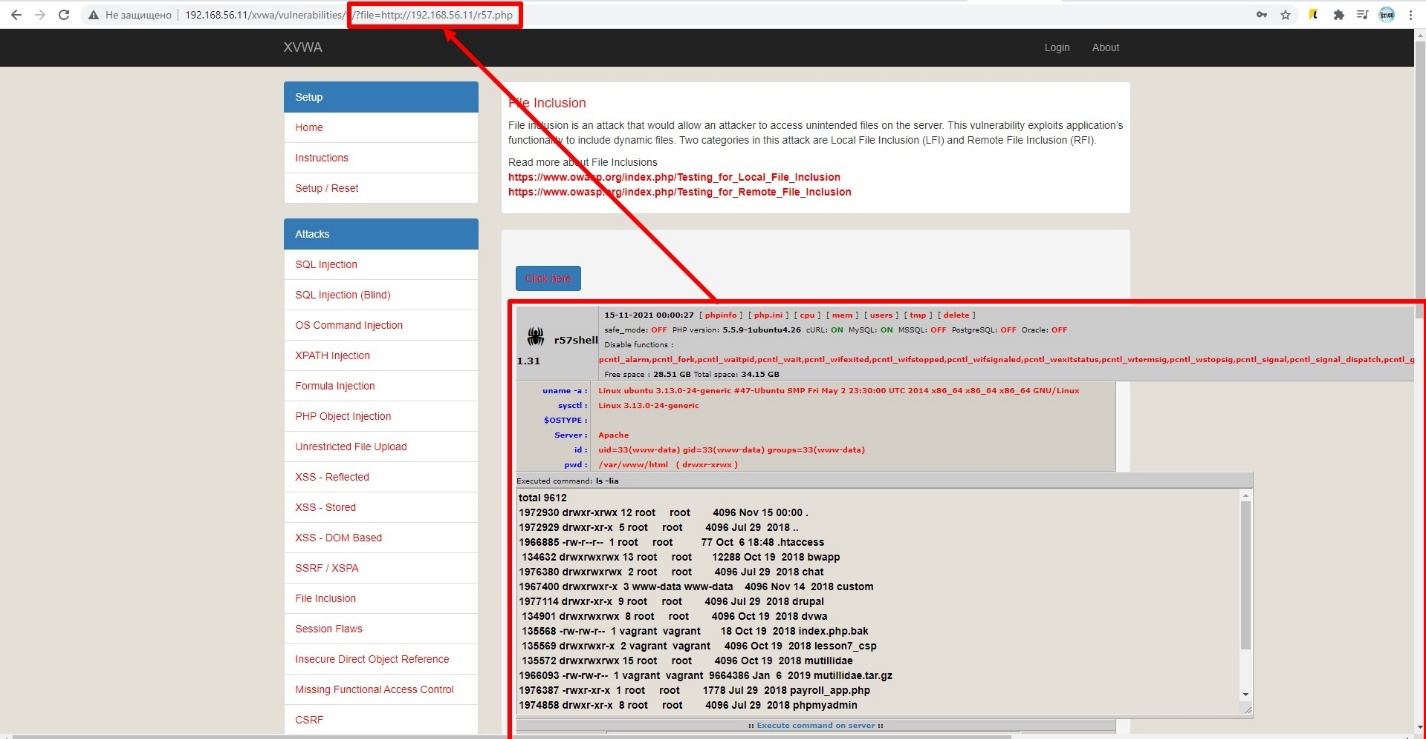
**Технические детали обнаружения и воспроизведения**

Обнаружить уязвимость LFI удалось, изменив параметр file в URI, следующим образом:



Здесь мы указали локальный файл “passwd”. Содержимое файла вывелось ниже кнопки “Click here” (в красном прямоугольнике).

Обнаружить уязвимость RFI удалось, изменив параметр file в URI, следующим образом:



Здесь мы указали ссылку на php файл, находящийся на удалённом сервере. Файл выполнился на уязвимой странице. Результат исполнения можно увидеть так же ниже кнопки “Click here” (в красном прямоугольнике).

**Выводы и рекомендации по устранению**

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

* Фильтровать протоколы в параметрах URI.
* Можно отключить настройки инклуда (НЕ для всех).
* Можно отключить небезопасные функции на уровне php. Делается это при помощи опции disable\_functions в файле php.ini.
* Необходимо фильтровать введенные пользователем данные, а также задавать пользователю ограничение на доступ к различным сущностям.
* Обновление уязвимых компонентов. Если уязвимость присутствует, например, в плагине для Wordpress, то необходимо обновить уязвимый компонент.
* Можно установить Web application firewall. В этом случае необходимо будет активировать набор правил для защиты от атаки LFI.

**Используемое программное обеспечение**

● Google Chrome