**Описание уязвимости**

В на старнице http://192.168.56.11/mutillidae/index.php?page=text-file-viewer.php [проекта](http://192.168.56.11/) Mutillidae найдены следующие уязвимости: Remote File Inclution (RFI).  
Данная уязвимость позволяетисполнять как на сервере так и на клиенте несанкционированные файлы, которые могут повлиять на конфиденциальность и целостность информационной системы.

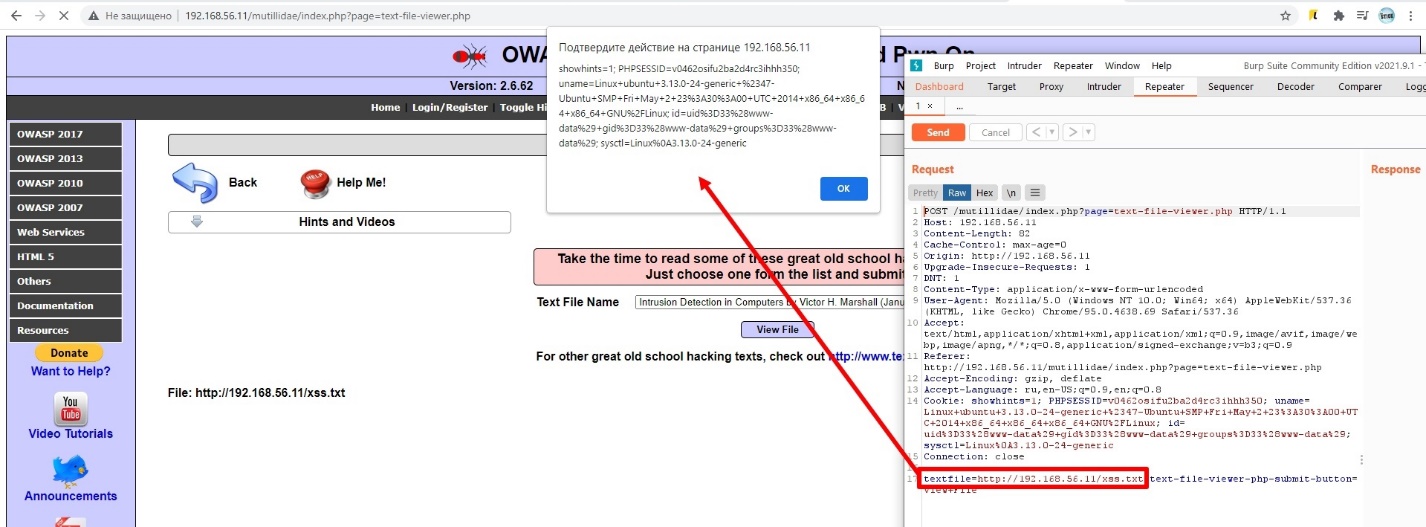
**Где найдена уязвимость**

Уязвимость расположена по адресу http://192.168.56.11/mutillidae/index.php?page=text-file-viewer.php.

Наименование продукта: Mutillidae.

**Технические детали обнаружения и воспроизведения**

Обнаружить уязвимость LFI удалось, перехватив запрос на чтение файла из списка в Burp Suite CE и изменив параметр textfile на файл, находящийся на удалённом сервере.



Здесь мы указали txt файл с кодом javascript внутри, который выводит в alert куки пользователя. Содержимое файла вывелось в pop-up.

**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 GET и POST параметров.
* 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.
* Обновление уязвимых компонентов. Если уязвимость присутствует, например, в плагине для Wordpress, то необходимо обновить уязвимый компонент.

**Используемое программное обеспечение**

● Google Chrome