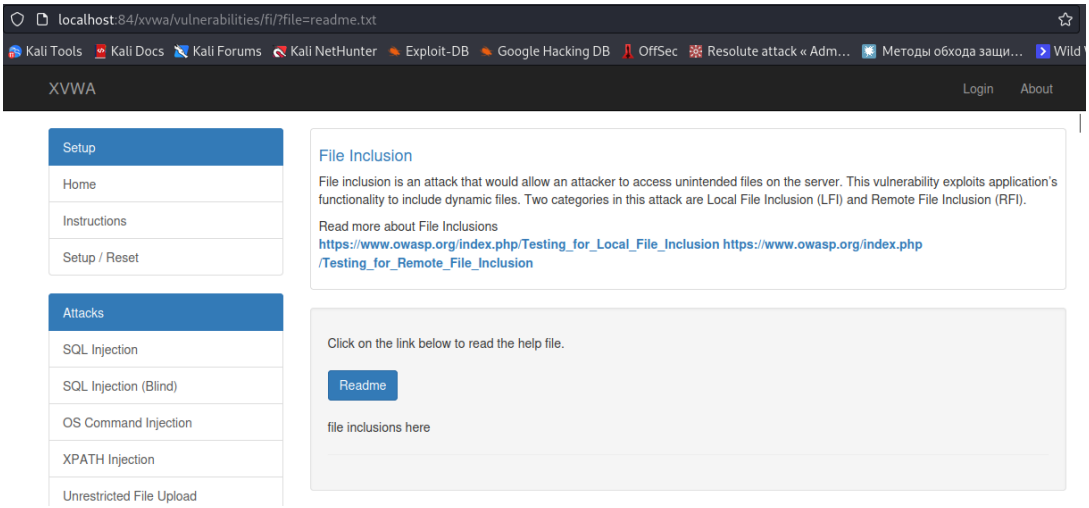
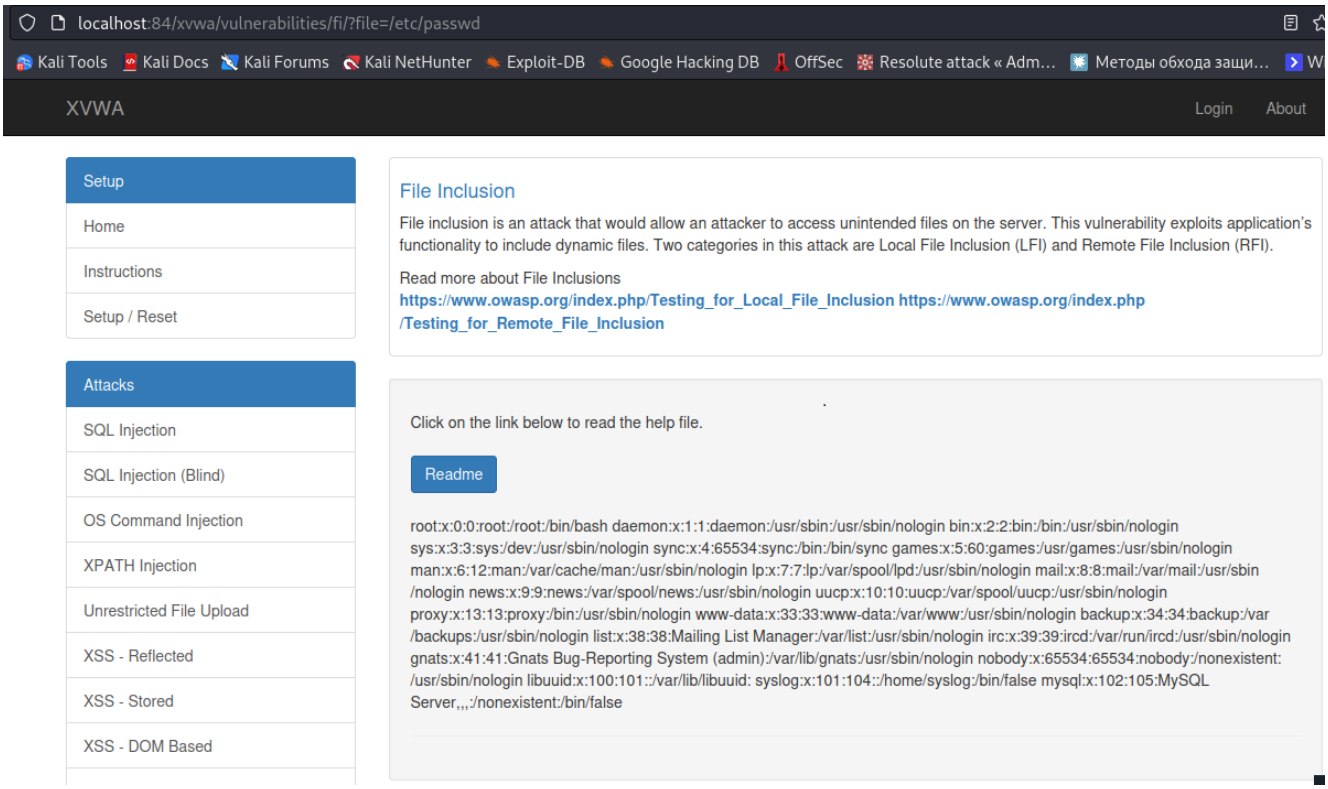
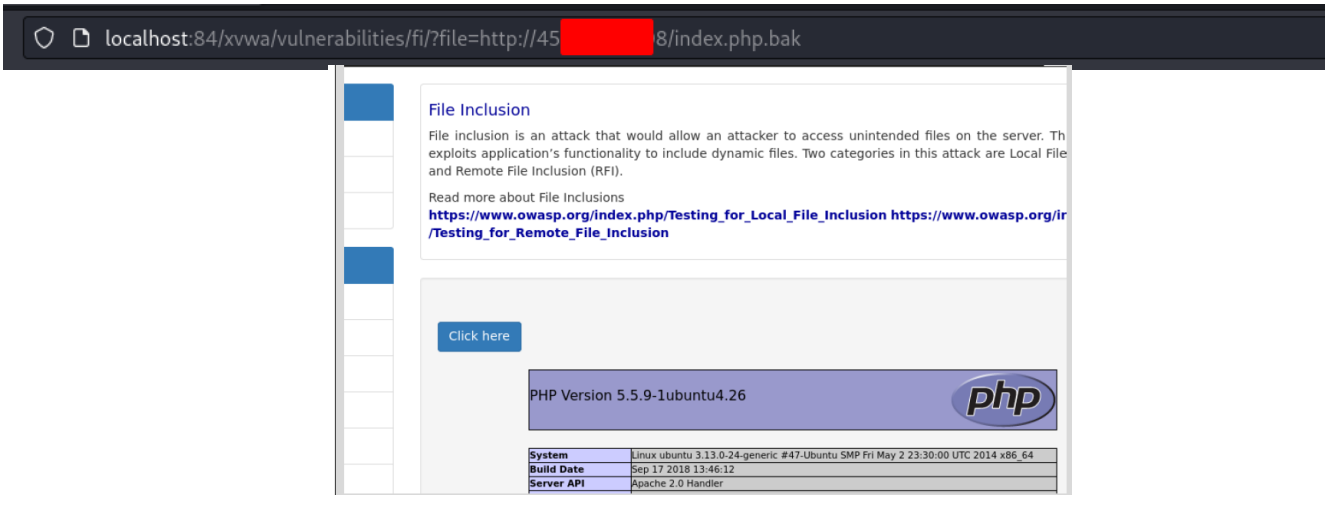
Выполнил Мешечкин Д. Инфобез-2837

Задание 1: Исследуйте страницу File Inclusion проекта XVWA (xvwa/vulnerabilities/fi/) и составьте отчет об обнаруженных уязвимостях.



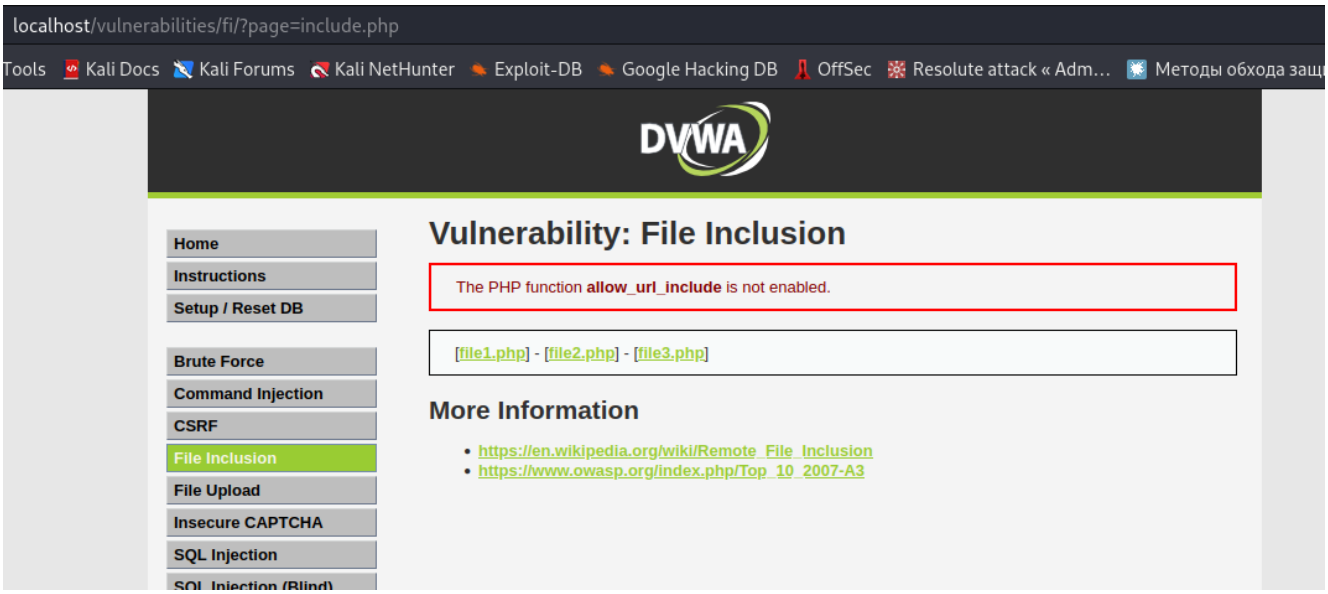
Опять же, все лабораторные машины будут запущены в докере. Сайт для нагрузки используется свой арендованый VPS.

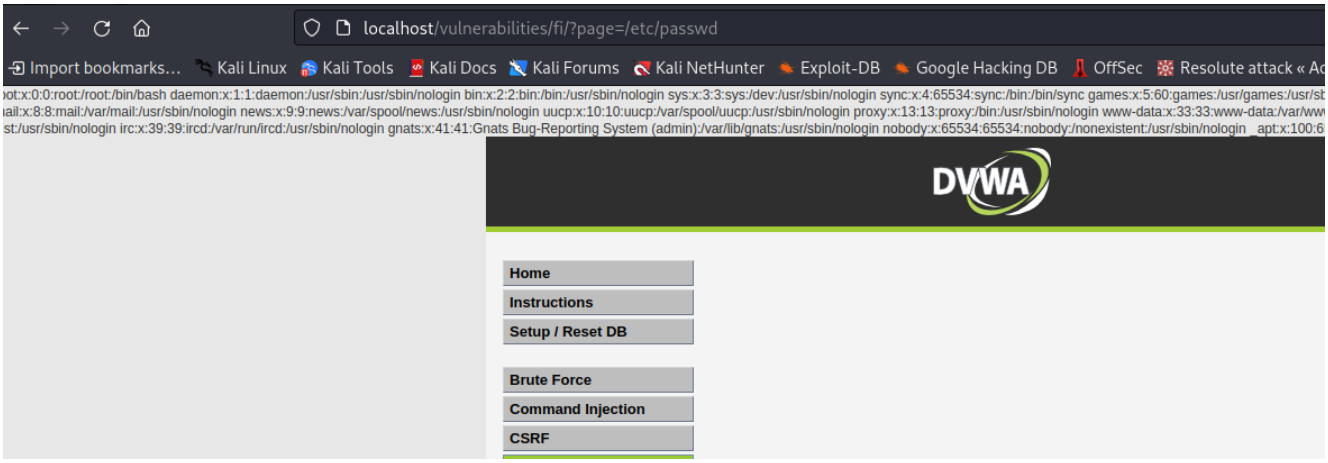


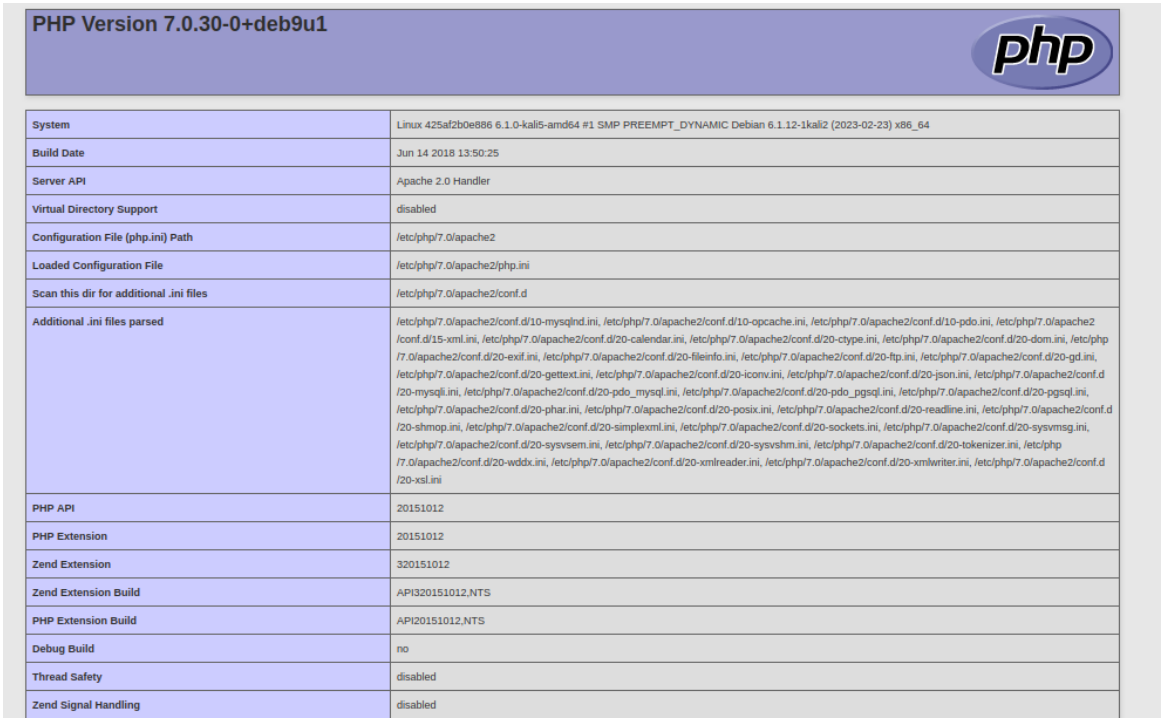


Обе уязвимости LFI и RFI отлично отрабатывают, уровень "защиты" оставляет желать лучшего, больше времени уходит на запуск докера, чем на "раскручивание" уязвимости.

Задание 2: *Исследуйте страницу File Inclusion проекта DVWA (dvwa/vulnerabilities/fi/) и составьте отчет об обнаруженных уязвимостях*





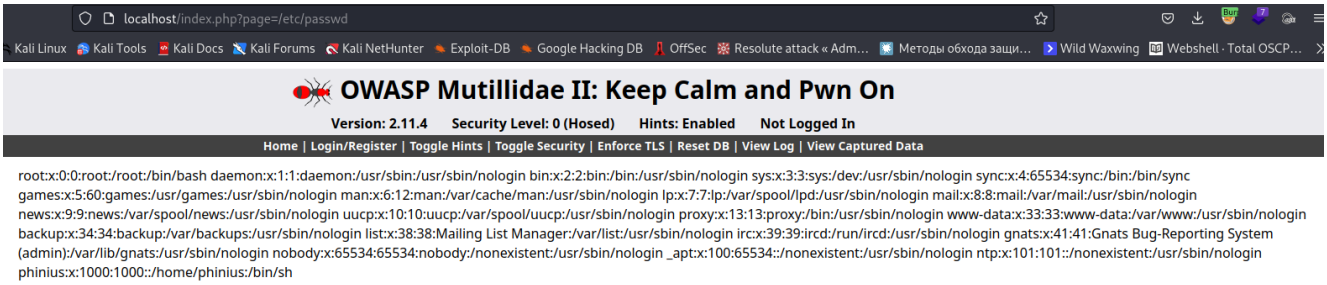


PHP Version 7.0.30-0+deb9u1

System	Linux 425af2b0e886 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23) x86_64
Build Date	Jun 14 2018 13:50:25
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_pgsql.ini, /etc/php/7.0/apache2/conf.d/20-pgsql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-simplexml.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20-wddx.ini, /etc/php/7.0/apache2/conf.d/20-xmlreader.ini, /etc/php/7.0/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.0/apache2/conf.d/20-xsl.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled

Абсолютно та же картина представляется в DVWA. LFI RFI выполняются простой подстановкой самых "прямых" нагрузок.

Задание 3: На странице text-file-viewer.php проекта mutillidae (/mutillidae/index.php?page=text-file-viewer.php) присутствует уязвимость класса Inclusion. Ваша задача — составить сценарий атаки, направленной на клиента (а не на сервер) и реализовать его. Составить отчет о проделанной работе.



Да, в задании нет того, что требуется, но ведь задание идёт по LFI RFI. Аналогичная ситуация и в mutillidae. На минимальных уровнях - слишком всё просто.

В любом случае на данный момент проходит более интересное и жёсткое обучение в сфере пентеста, по этому на данный курс уделяется минимум времени.