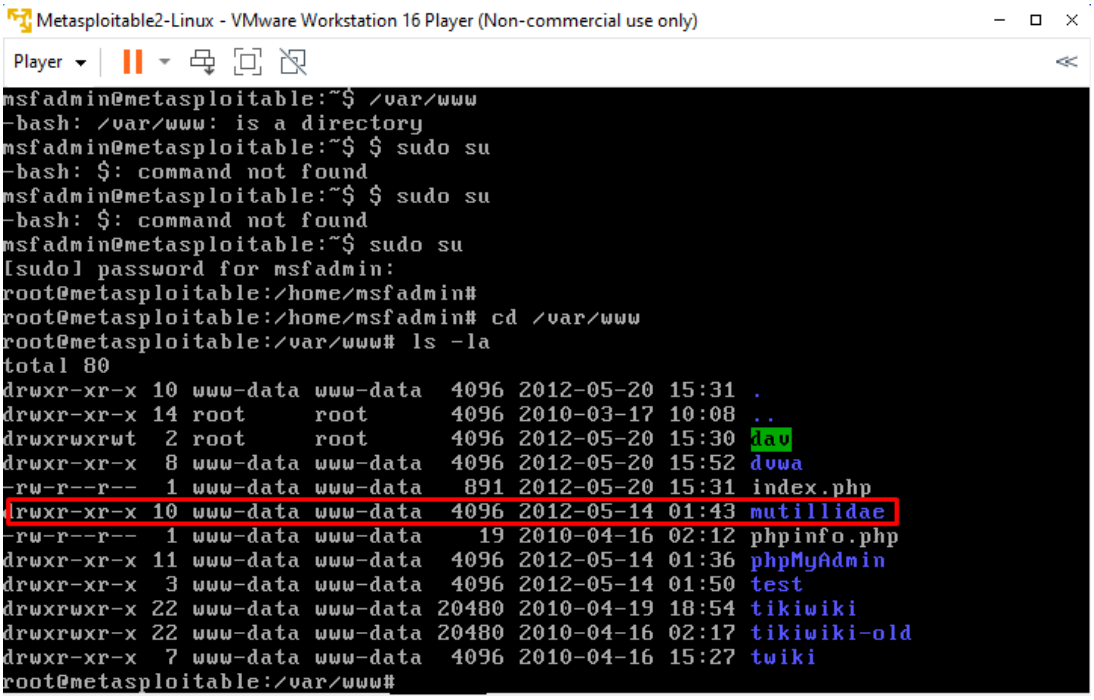
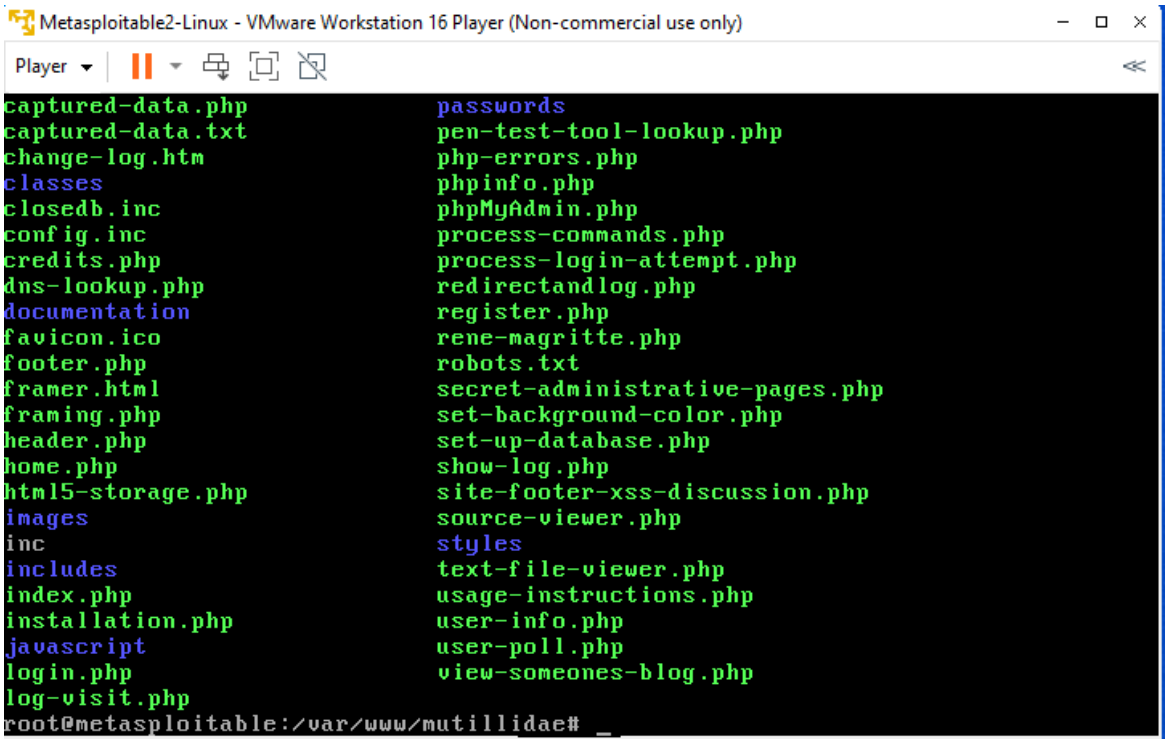
Задание 4.



Смотрим список папок metasploitable и переходим в папку mutillidae



Видим список всех файлов внутри нее

```
┌──(root💀kali)-[~]
└─# dirb http://192.168.179.137/mutillidae/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Dec  9 03:14:28 2021
URL_BASE: http://192.168.179.137/mutillidae/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.179.137/mutillidae/ ----
==> DIRECTORY: http://192.168.179.137/mutillidae/classes/
+ http://192.168.179.137/mutillidae/credits (CODE:200|SIZE:509)
==> DIRECTORY: http://192.168.179.137/mutillidae/documentation/
+ http://192.168.179.137/mutillidae/favicon.ico (CODE:200|SIZE:1150)
+ http://192.168.179.137/mutillidae/footer (CODE:200|SIZE:450)
+ http://192.168.179.137/mutillidae/header (CODE:200|SIZE:19879)
+ http://192.168.179.137/mutillidae/home (CODE:200|SIZE:2930)
==> DIRECTORY: http://192.168.179.137/mutillidae/images/
+ http://192.168.179.137/mutillidae/inc (CODE:200|SIZE:386260)
==> DIRECTORY: http://192.168.179.137/mutillidae/includes/
+ http://192.168.179.137/mutillidae/index (CODE:200|SIZE:24237)
+ http://192.168.179.137/mutillidae/index.php (CODE:200|SIZE:24237)
+ http://192.168.179.137/mutillidae/installation (CODE:200|SIZE:8138)
==> DIRECTORY: http://192.168.179.137/mutillidae/javascript/
+ http://192.168.179.137/mutillidae/login (CODE:200|SIZE:4102)
+ http://192.168.179.137/mutillidae/notes (CODE:200|SIZE:1721)
+ http://192.168.179.137/mutillidae/page-not-found (CODE:200|SIZE:705)
==> DIRECTORY: http://192.168.179.137/mutillidae/passwords/
+ http://192.168.179.137/mutillidae/phpinfo (CODE:200|SIZE:48918)
+ http://192.168.179.137/mutillidae/phpinfo.php (CODE:200|SIZE:48930)
+ http://192.168.179.137/mutillidae/phpMyAdmin (CODE:200|SIZE:174)
+ http://192.168.179.137/mutillidae/register (CODE:200|SIZE:1823)
+ http://192.168.179.137/mutillidae/robots (CODE:200|SIZE:160)
+ http://192.168.179.137/mutillidae/robots.txt (CODE:200|SIZE:160)
==> DIRECTORY: http://192.168.179.137/mutillidae/styles/

---- Entering directory: http://192.168.179.137/mutillidae/classes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.179.137/mutillidae/documentation/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.179.137/mutillidae/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.179.137/mutillidae/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.179.137/mutillidae/javascript/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.179.137/mutillidae/passwords/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.179.137/mutillidae/styles/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Thu Dec  9 03:14:34 2021
DOWNLOADED: 4612 - FOUND: 18
```

Произведем сканирование этого пути в kali linux. Тут мы видим скрытые файлы:

PHP Version 5.2.4-2ubuntu5.10

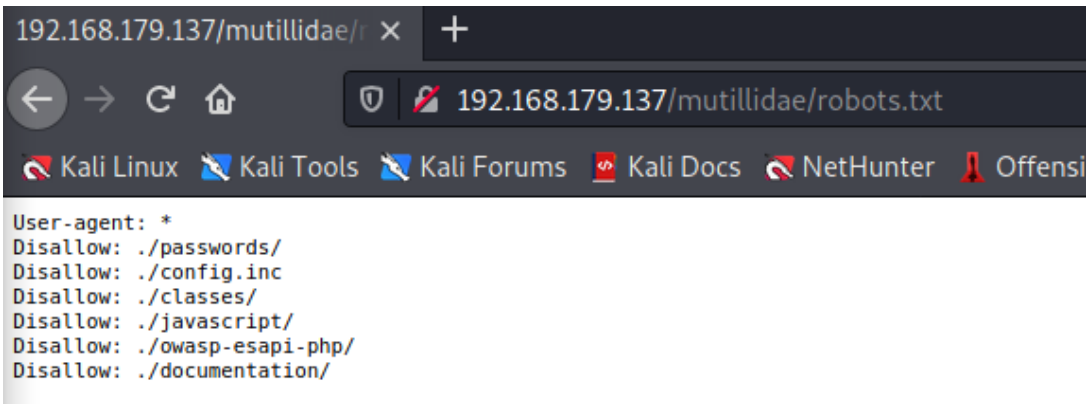
System	Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Build Date	Jan 6 2010 21:50:12
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
additional .ini files parsed	/etc/php5/cgi/conf.d/gd.ini, /etc/php5/cgi/conf.d/mysql.ini, /etc/php5/cgi/conf.d/mysqli.ini, /etc/php5/cgi/conf.d/pdo.ini, /etc/php5/cgi/conf.d/pdo_mysql.ini
PHP API	20041225
PHP Extension	20060613
Zend Extension	220060519
Debug Build	no
Thread Safety	disabled
Zend Memory Manager	enabled
IPv6 Support	enabled
Registered PHP Streams	zip, php, file, data, http, ftp, compress.bzip2, compress.zlib, https, ftps
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, sslv2, tls
Registered Stream Filters	string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, convert.iconv.*, bzip2.*, zlib.*

This server is protected with the Suhosin Patch 0.9.6.2
Copyright (c) 2006 Hardened-PHP Project

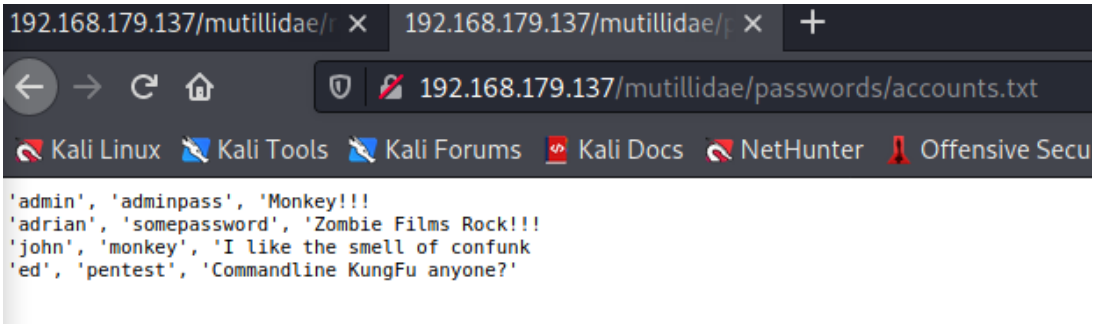
This program makes use of the Zend Scripting Language Engine:
Zend Engine v2.2.0, Copyright (c) 1998-2007 Zend Technologies

Powered By Zend Engine 2

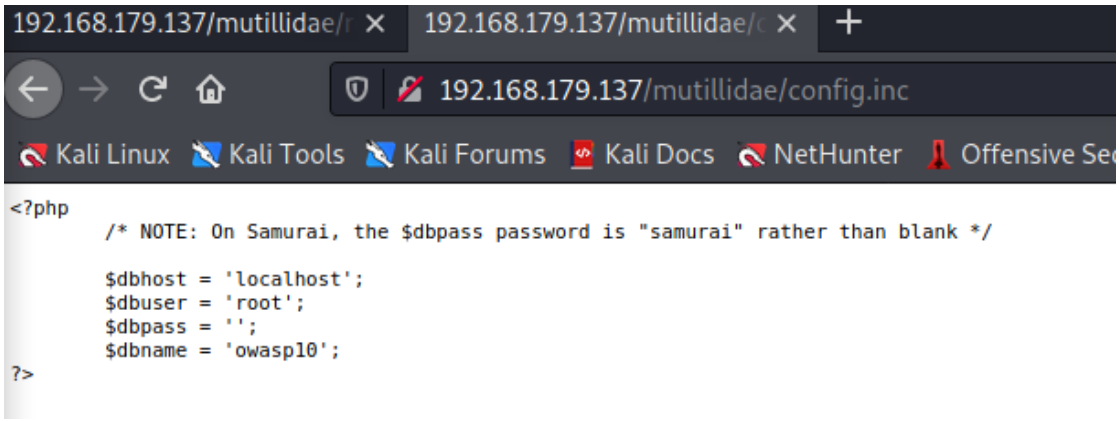
Информация о php



В файле robots находи еще больше скрытых файлов:



Аккаунты пользователей



Подключение к БД