

## Задание 4.

```
Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | [Icons]
msfadmin@metasploitable:~$ /var/www
-bash: /var/www: is a directory
msfadmin@metasploitable:~$ $ sudo su
-bash: $: command not found
msfadmin@metasploitable:~$ $ sudo su
-bash: $: command not found
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd /var/www
root@metasploitable:/var/www# ls -la
total 80
drwxr-xr-x 10 www-data www-data 4096 2012-05-20 15:31 .
drwxr-xr-x 14 root root 4096 2010-03-17 10:08 ..
drwxrwxrwt 2 root root 4096 2012-05-20 15:30 tau
drwxr-xr-x 8 www-data www-data 4096 2012-05-20 15:52 duwa
-rw-r--r-- 1 www-data www-data 891 2012-05-20 15:31 index.php
-rwxr-xr-x 10 www-data www-data 4096 2012-05-14 01:43 mutillidae
-rw-r--r-- 1 www-data www-data 19 2010-04-16 02:12 phpinfo.php
drwxr-xr-x 11 www-data www-data 4096 2012-05-14 01:36 phpMyAdmin
drwxr-xr-x 3 www-data www-data 4096 2012-05-14 01:50 test
drwxrwxr-x 22 www-data www-data 20480 2010-04-19 18:54 tikiwiki
drwxrwxr-x 22 www-data www-data 20480 2010-04-16 02:17 tikiwiki-old
drwxr-xr-x 7 www-data www-data 4096 2010-04-16 15:27 twiki
root@metasploitable:/var/www#
```

Смотрим список папок metasploitable и переходим в папку mutillidae

```
Metasploitable2-Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | [Icons]
captured-data.php passwords
captured-data.txt pen-test-tool-lookup.php
change-log.htm php-errors.php
classes phpinfo.php
closedb.inc phpMyAdmin.php
config.inc process-commands.php
credits.php process-login-attempt.php
dns-lookup.php redirectandlog.php
documentation register.php
favicon.ico rene-magritte.php
footer.php robots.txt
framer.html secret-administrative-pages.php
framing.php set-background-color.php
header.php set-up-database.php
home.php show-log.php
html5-storage.php site-footer-xss-discussion.php
images source-viewer.php
inc styles
includes text-file-viewer.php
index.php usage-instructions.php
installation.php user-info.php
javascript user-poll.php
login.php view-someones-blog.php
log-visit.php
root@metasploitable:/var/www/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/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:

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

수호신

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



## Информация о php

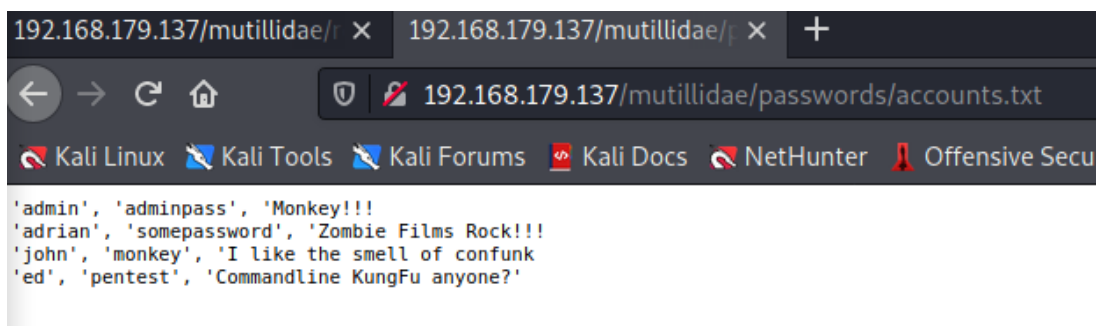
192.168.179.137/mutillidae/r
+

← → ↻ 🏠
192.168.179.137/mutillidae/robots.txt

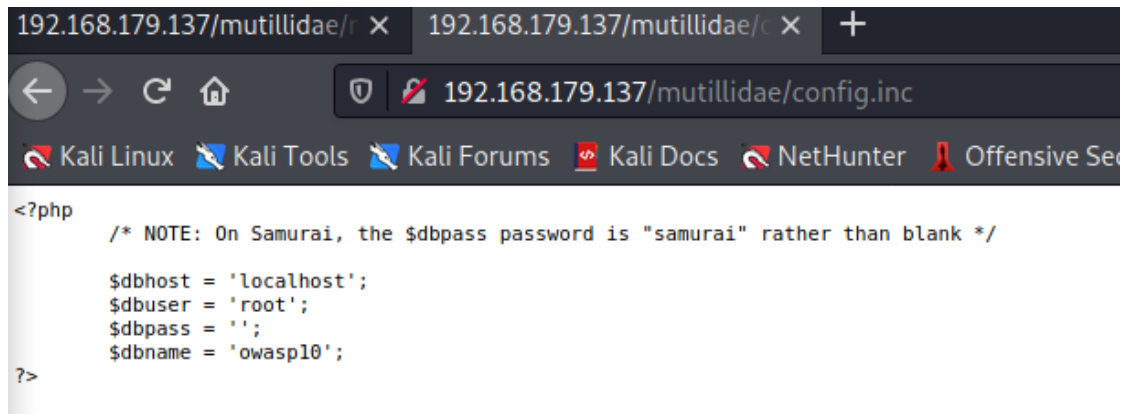
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensi

User-agent: \*  
Disallow: ./passwords/  
Disallow: ./config.inc  
Disallow: ./classes/  
Disallow: ./javascript/  
Disallow: ./owasp-esapi-php/  
Disallow: ./documentation/

В файле robots находи еще больше скрытых файлов:



## Аккаунты пользователей



## Подключение к БД