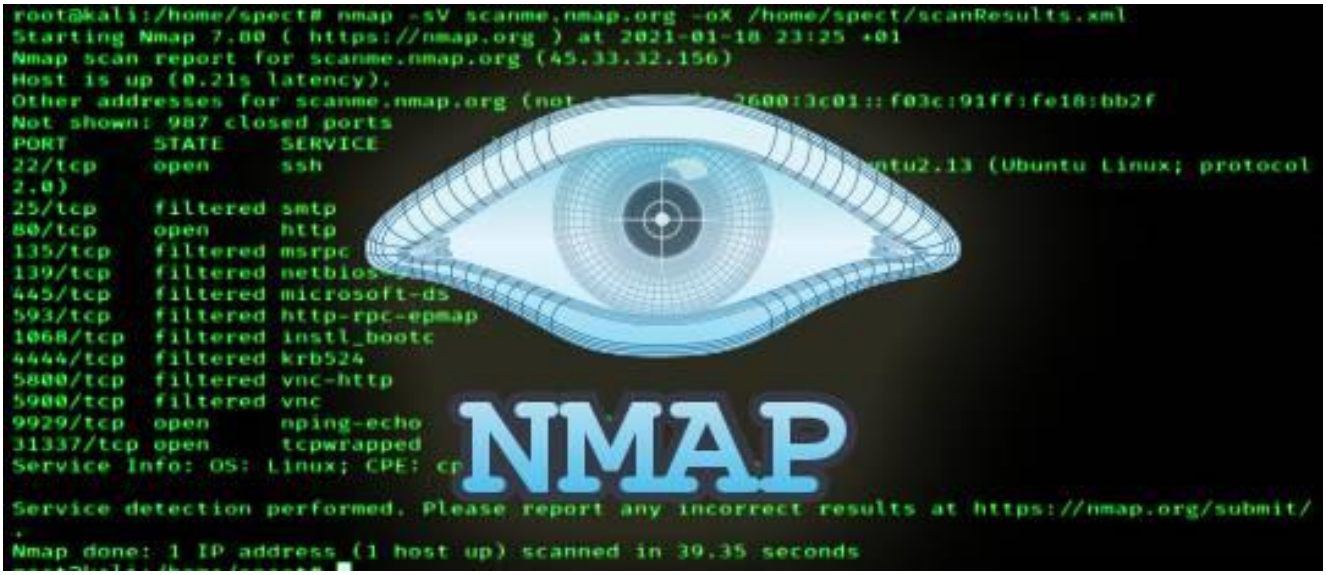
Project work

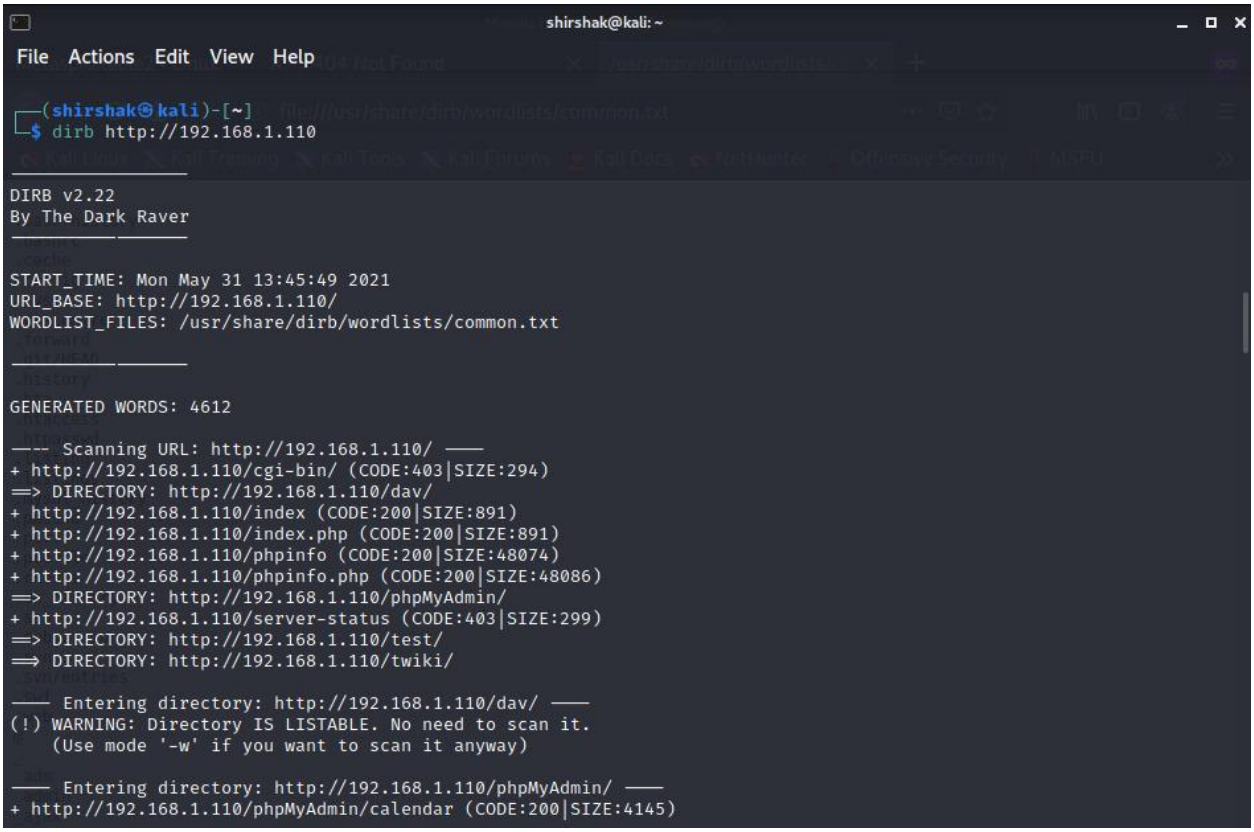
NMAP

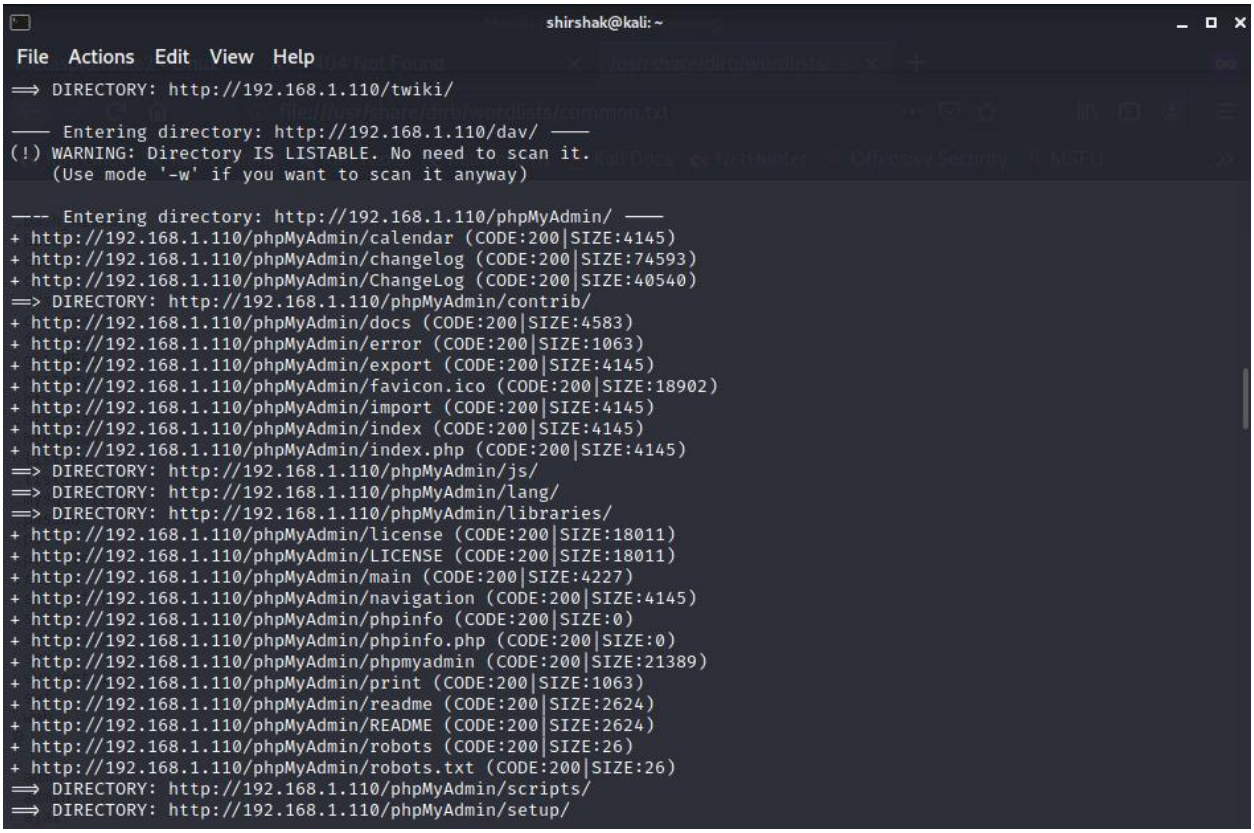


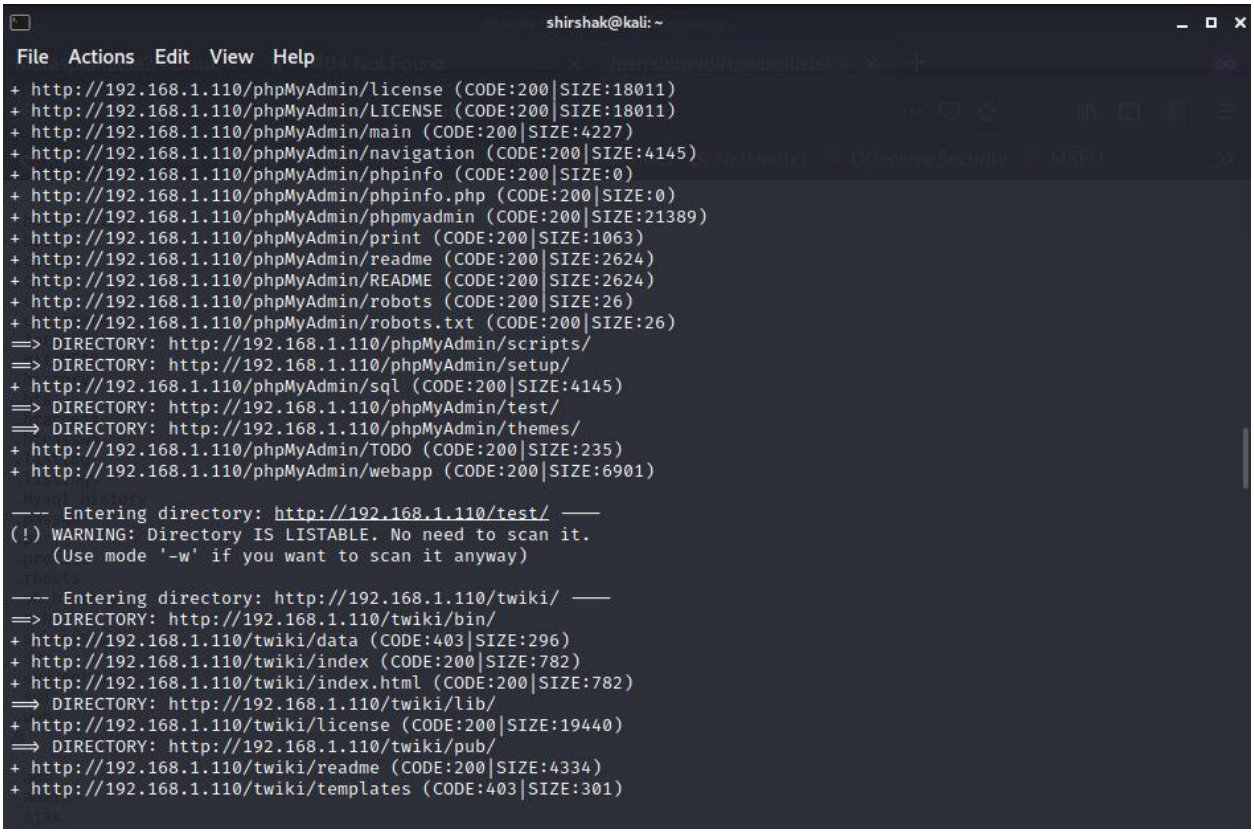
Submitted by:shirshak kumar kafle

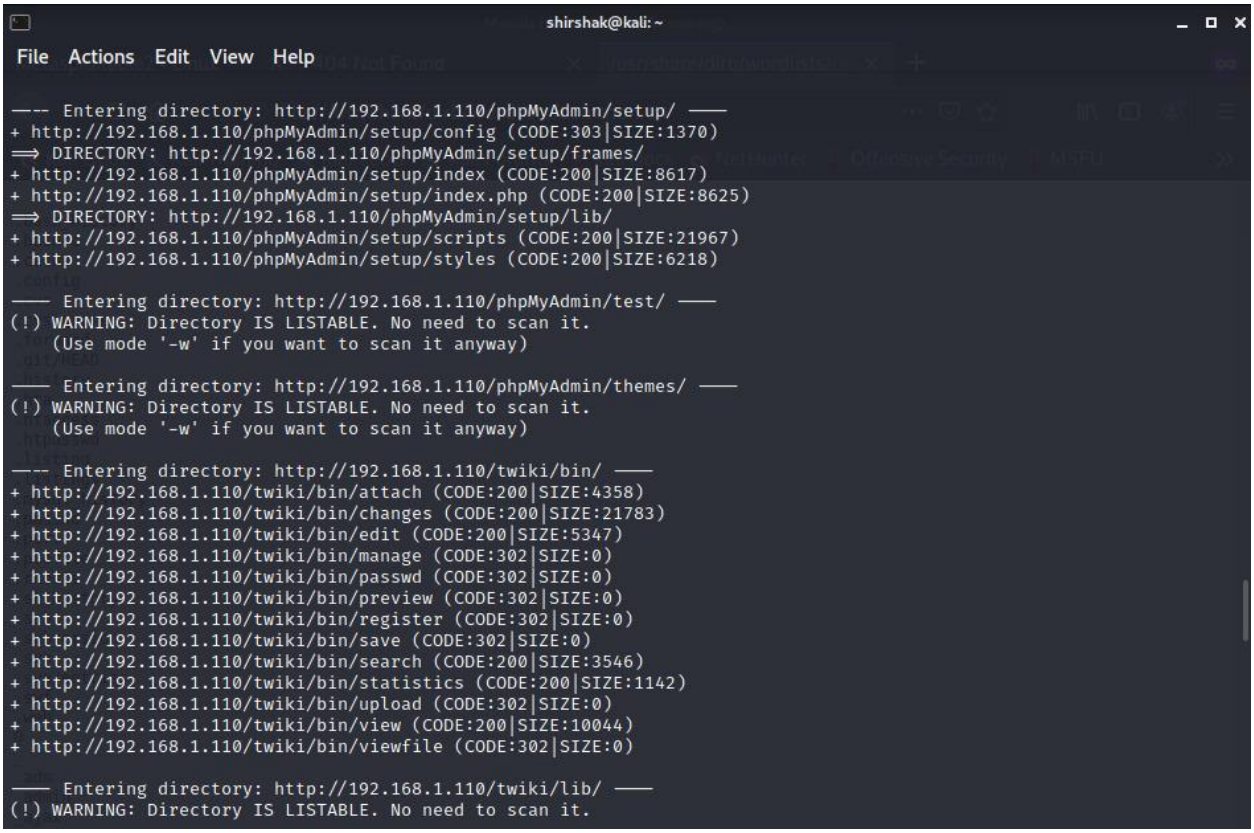
Project screenshort

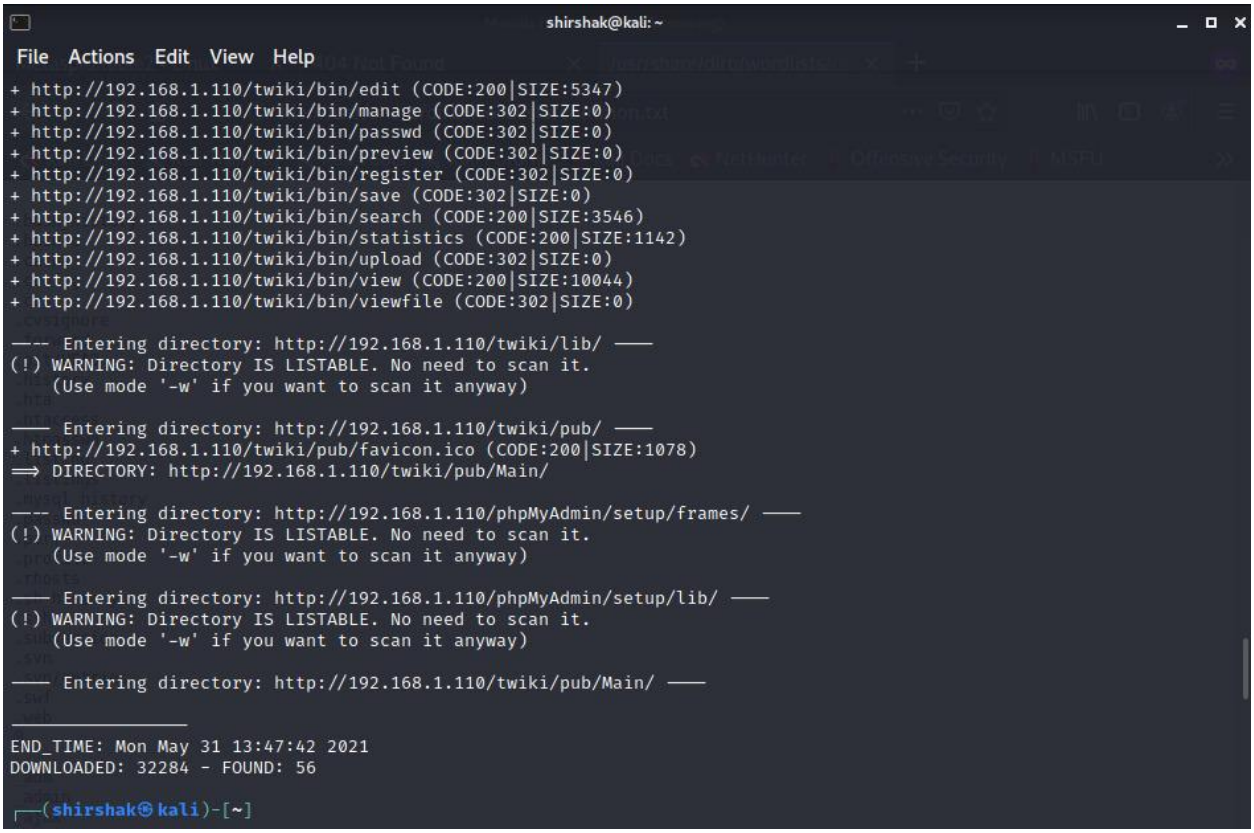
Dirb https://190.168.1.110



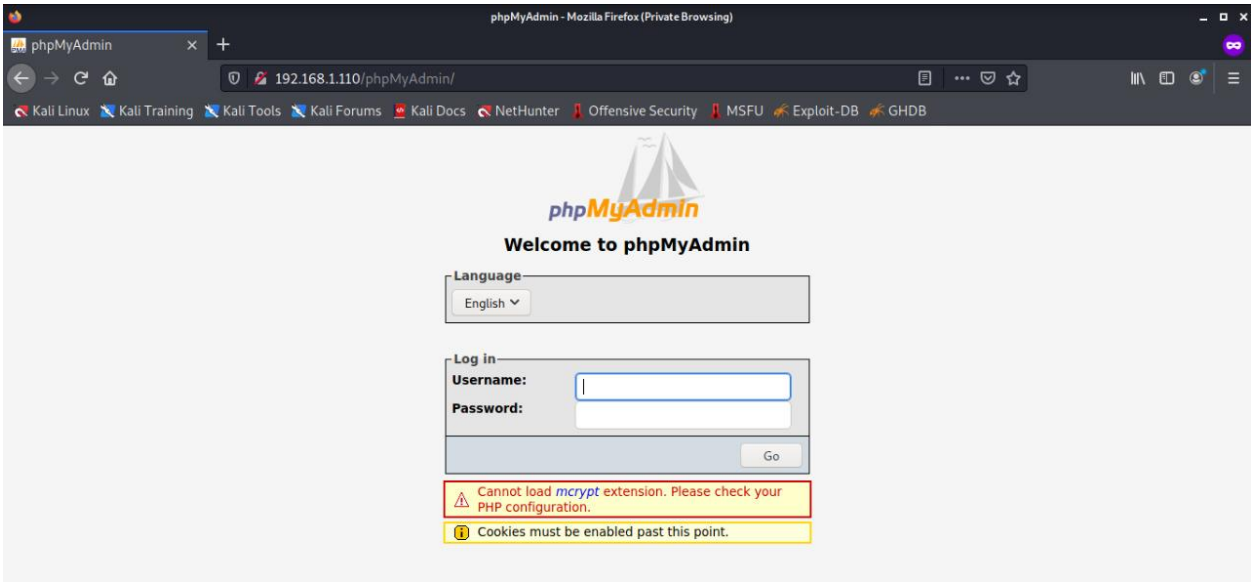

shirshak@kali: ~
File Actions Edit View Help
==> DIRECTORY: http://192.168.1.110/twiki/
---- Entering directory: http://192.168.1.110/dav/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.110/phpMyAdmin/ ----
+ http://192.168.1.110/phpMyAdmin/calendar (CODE:200|SIZE:4145)
+ http://192.168.1.110/phpMyAdmin/changelog (CODE:200|SIZE:74593)
+ http://192.168.1.110/phpMyAdmin/ChangeLog (CODE:200|SIZE:40540)
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/contrib/
+ http://192.168.1.110/phpMyAdmin/docs (CODE:200|SIZE:4583)
+ http://192.168.1.110/phpMyAdmin/error (CODE:200|SIZE:1063)
+ http://192.168.1.110/phpMyAdmin/export (CODE:200|SIZE:4145)
+ http://192.168.1.110/phpMyAdmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.1.110/phpMyAdmin/import (CODE:200|SIZE:4145)
+ http://192.168.1.110/phpMyAdmin/index (CODE:200|SIZE:4145)
+ http://192.168.1.110/phpMyAdmin/index.php (CODE:200|SIZE:4145)
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/js/
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/lang/
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/libraries/
+ http://192.168.1.110/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.1.110/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.1.110/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.1.110/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.1.110/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.1.110/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.168.1.110/phpMyAdmin/phpmyadmin (CODE:200|SIZE:21389)
+ http://192.168.1.110/phpMyAdmin/print (CODE:200|SIZE:1063)
+ http://192.168.1.110/phpMyAdmin/readme (CODE:200|SIZE:2624)
+ http://192.168.1.110/phpMyAdmin/README (CODE:200|SIZE:2624)
+ http://192.168.1.110/phpMyAdmin/robots (CODE:200|SIZE:26)
+ http://192.168.1.110/phpMyAdmin/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/scripts/
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/setup/


shirshak@kali: ~
File Actions Edit View Help
+ http://192.168.1.110/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.1.110/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.1.110/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.1.110/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.1.110/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.1.110/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.168.1.110/phpMyAdmin/phpmyadmin (CODE:200|SIZE:21389)
+ http://192.168.1.110/phpMyAdmin/print (CODE:200|SIZE:1063)
+ http://192.168.1.110/phpMyAdmin/readme (CODE:200|SIZE:2624)
+ http://192.168.1.110/phpMyAdmin/README (CODE:200|SIZE:2624)
+ http://192.168.1.110/phpMyAdmin/robots (CODE:200|SIZE:26)
+ http://192.168.1.110/phpMyAdmin/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/scripts/
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/setup/
+ http://192.168.1.110/phpMyAdmin/sql (CODE:200|SIZE:4145)
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/test/
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/themes/
+ http://192.168.1.110/phpMyAdmin/TODO (CODE:200|SIZE:235)
+ http://192.168.1.110/phpMyAdmin/webapp (CODE:200|SIZE:6901)
---- Entering directory: http://192.168.1.110/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.1.110/twiki/ ----
==> DIRECTORY: http://192.168.1.110/twiki/bin/
+ http://192.168.1.110/twiki/data (CODE:403|SIZE:296)
+ http://192.168.1.110/twiki/index (CODE:200|SIZE:782)
+ http://192.168.1.110/twiki/index.html (CODE:200|SIZE:782)
==> DIRECTORY: http://192.168.1.110/twiki/lib/
+ http://192.168.1.110/twiki/license (CODE:200|SIZE:19440)
==> DIRECTORY: http://192.168.1.110/twiki/pub/
+ http://192.168.1.110/twiki/readme (CODE:200|SIZE:4334)
+ http://192.168.1.110/twiki/templates (CODE:403|SIZE:301)

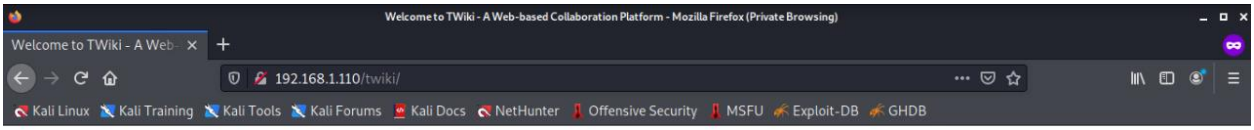

shirshak@kali: ~
File Actions Edit View Help
—-- Entering directory: http://192.168.1.110/phpMyAdmin/setup/ ——
+ http://192.168.1.110/phpMyAdmin/setup/config (CODE:303|SIZE:1370)
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/setup/frames/
+ http://192.168.1.110/phpMyAdmin/setup/index (CODE:200|SIZE:8617)
+ http://192.168.1.110/phpMyAdmin/setup/index.php (CODE:200|SIZE:8625)
==> DIRECTORY: http://192.168.1.110/phpMyAdmin/setup/lib/
+ http://192.168.1.110/phpMyAdmin/setup/scripts (CODE:200|SIZE:21967)
+ http://192.168.1.110/phpMyAdmin/setup/styles (CODE:200|SIZE:6218)
—— Entering directory: http://192.168.1.110/phpMyAdmin/test/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.1.110/phpMyAdmin/themes/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—-- Entering directory: http://192.168.1.110/twiki/bin/ ——
+ http://192.168.1.110/twiki/bin/attach (CODE:200|SIZE:4358)
+ http://192.168.1.110/twiki/bin/changes (CODE:200|SIZE:21783)
+ http://192.168.1.110/twiki/bin/edit (CODE:200|SIZE:5347)
+ http://192.168.1.110/twiki/bin/manage (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/passwd (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/preview (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/register (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/save (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/search (CODE:200|SIZE:3546)
+ http://192.168.1.110/twiki/bin/statistics (CODE:200|SIZE:1142)
+ http://192.168.1.110/twiki/bin/upload (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/view (CODE:200|SIZE:10044)
+ http://192.168.1.110/twiki/bin/viewfile (CODE:302|SIZE:0)
—— Entering directory: http://192.168.1.110/twiki/lib/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.


shirshak@kali: ~
File Actions Edit View Help
+ http://192.168.1.110/twiki/bin/edit (CODE:200|SIZE:5347)
+ http://192.168.1.110/twiki/bin/manage (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/passwd (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/preview (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/register (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/save (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/search (CODE:200|SIZE:3546)
+ http://192.168.1.110/twiki/bin/statistics (CODE:200|SIZE:1142)
+ http://192.168.1.110/twiki/bin/upload (CODE:302|SIZE:0)
+ http://192.168.1.110/twiki/bin/view (CODE:200|SIZE:10044)
+ http://192.168.1.110/twiki/bin/viewfile (CODE:302|SIZE:0)
—-- Entering directory: http://192.168.1.110/twiki/lib/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.1.110/twiki/pub/ ——
+ http://192.168.1.110/twiki/pub/favicon.ico (CODE:200|SIZE:1078)
==> DIRECTORY: http://192.168.1.110/twiki/pub/Main/
—-- Entering directory: http://192.168.1.110/phpMyAdmin/setup/frames/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.1.110/phpMyAdmin/setup/lib/ ——
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
—— Entering directory: http://192.168.1.110/twiki/pub/Main/ ——
END_TIME: Mon May 31 13:47:42 2021
DOWNLOADED: 32284 - FOUND: 56
(shirshak㉿kali)-[~]

Php my admin

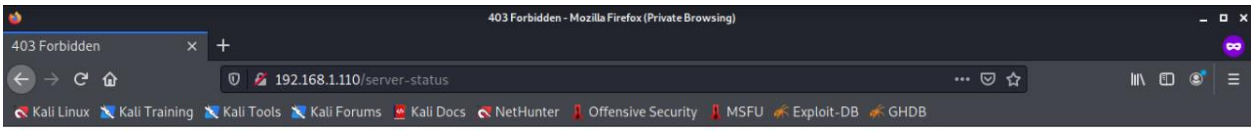

phpMyAdmin - Mozilla Firefox (Private Browsing)
phpMyAdmin
192.168.1.110/phpMyAdmin/
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
phpMyAdmin
Welcome to phpMyAdmin
Language
English
Log in
Username:
Password:
Go
Cannot load mcrypt extension. Please check your PHP configuration.
Cookies must be enabled past this point.

Twiki



Welcome to TWiki

- readme.txt
- license.txt
- TWikiDocumentation.html
- TWikiHistory.html
- Lets get started with this web based collaboration platform

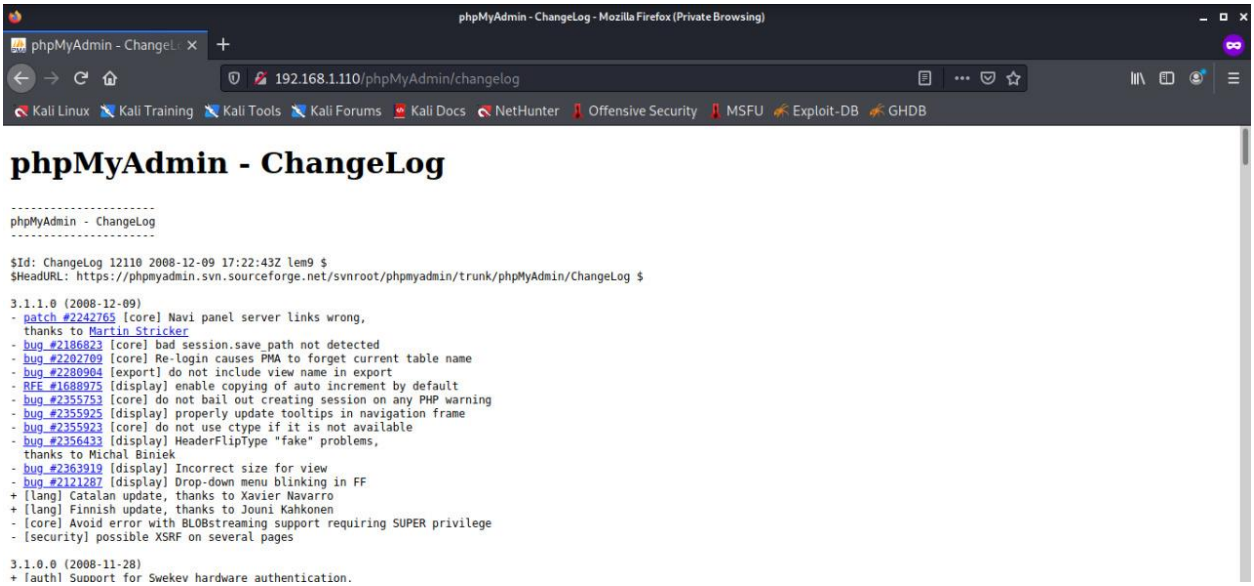


Forbidden

You don't have permission to access /server-status on this server.

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.1.110 Port 80

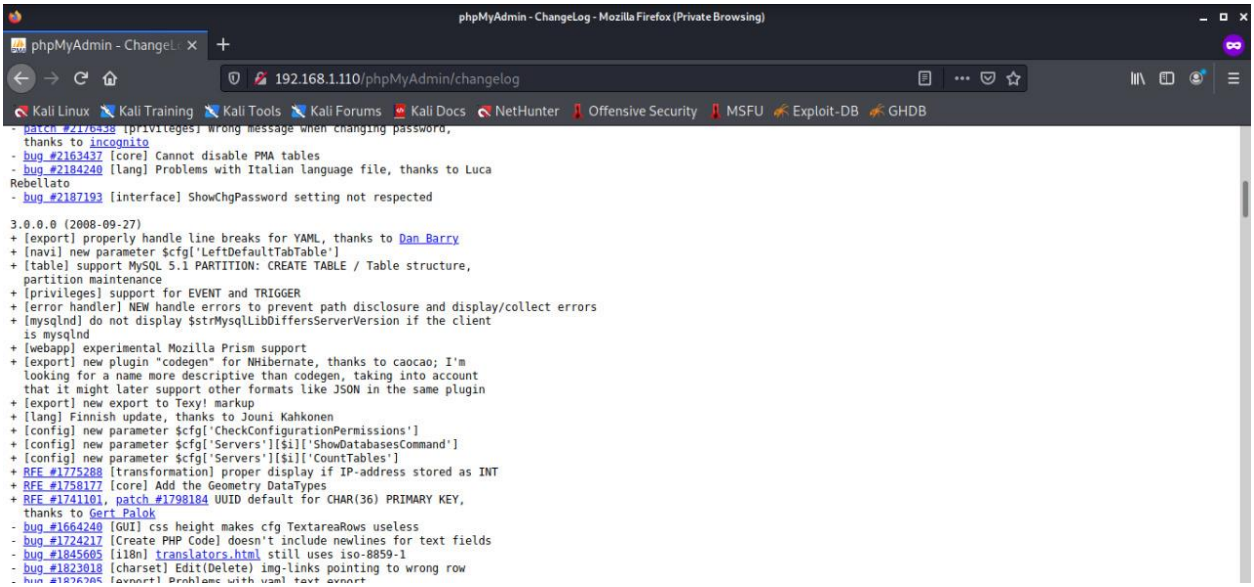
Php my admin: Change log



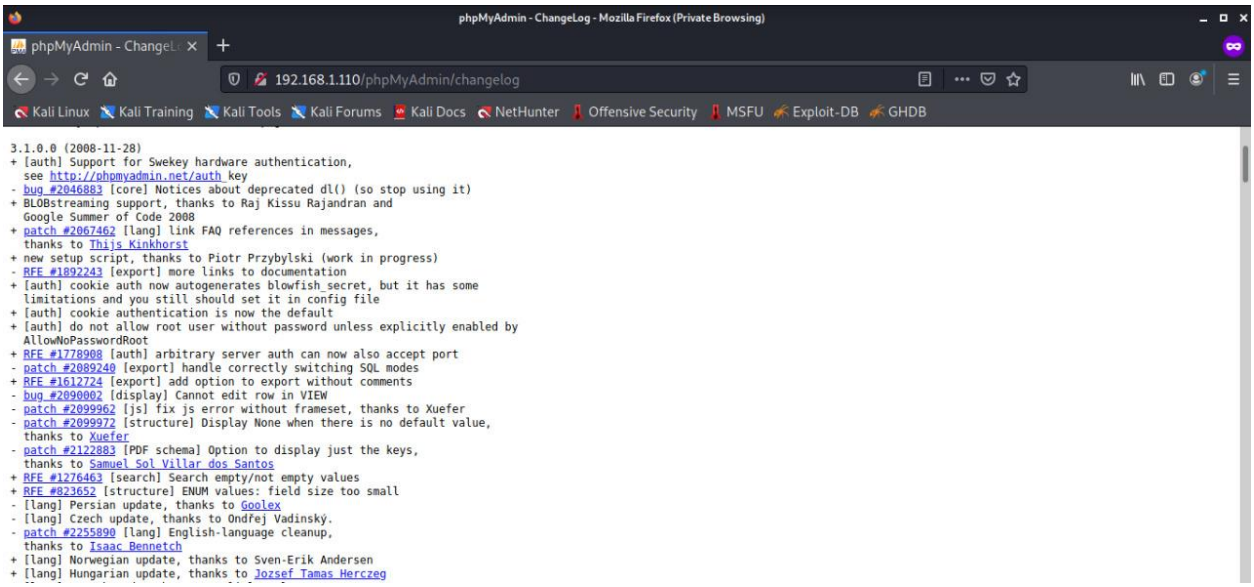
phpMyAdmin - ChangeLog

```
---------------------
phpMyAdmin - ChangeLog
---------------------

$Id: ChangeLog 12110 2008-12-09 17:22:43Z lem9 $
$HeadURL: https://phpmyadmin.svn.sourceforge.net/svnroot/phpmyadmin/trunk/phpMyAdmin/ChangeLog $

3.1.1.0 (2008-12-09)
- patch #2242765 [core] Navi panel server links wrong,
  thanks to Martin Stricker
- bug #2186823 [core] bad session.save_path not detected
- bug #2202709 [core] Re-login causes PMA to forget current table name
- bug #2280904 [export] do not include view name in export
- RFE #1688975 [display] enable copying of auto increment by default
- bug #2355753 [core] do not bail out creating session on any PHP warning
- bug #2355925 [display] properly update tooltips in navigation frame
- bug #2355923 [core] do not use ctype if it is not available
- bug #2356433 [display] HeaderFlipType "fake" problems,
  thanks to Michal Biniek
- bug #2363919 [display] Incorrect size for view
- bug #2121287 [display] Drop-down menu blinking in FF
+ [lang] Catalan update, thanks to Xavier Navarro
+ [lang] Finnish update, thanks to Jouni Kahkonen
- [core] Avoid error with BLOBstreaming support requiring SUPER privilege
- [security] possible XSRF on several pages

3.1.0.0 (2008-11-28)
+ [auth] Support for Swekey hardware authentication.
```

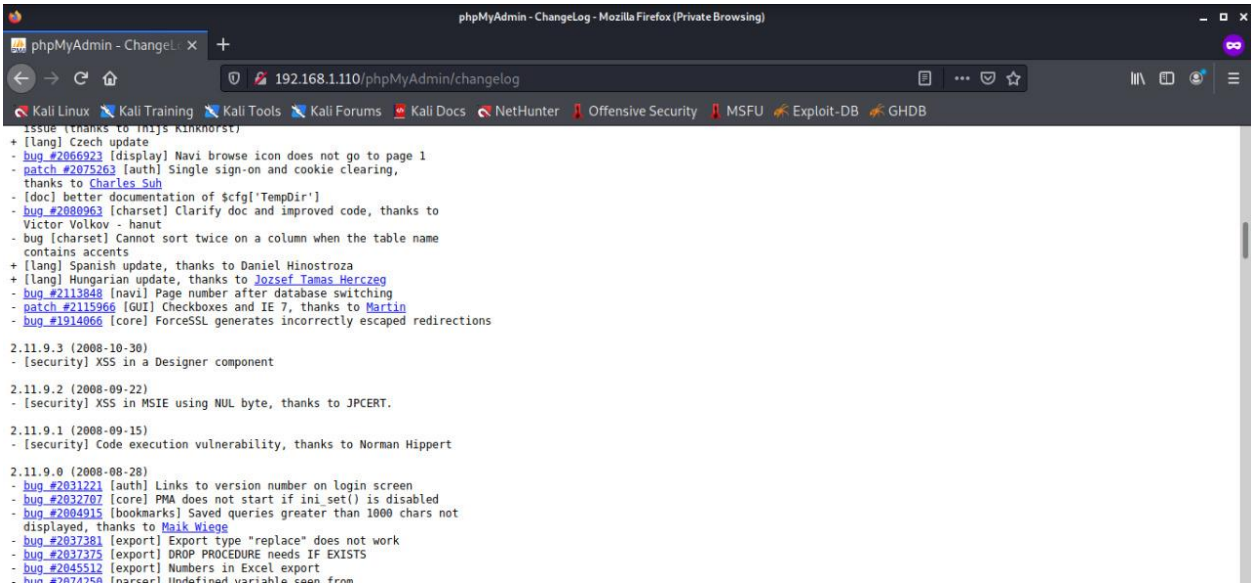

```
+ [engines] Maria support
+ [engines] MyISAM and InnoDB: support ROW_FORMAT table option
+ prevent search indexes from indexing phpMyAdmin installations
+ [engines] PBXT: table options, foreign key (relation view, designer)
+ [lang] New Bangla, thanks to Raquibul Islam and Joy Kumar Nag
+ [interface] Display options; thanks to Dave Grijalva
  for the idea about showing the display field while browsing
- bug #1910621 [display] part 2: do not display a BINARY content as text
+ RFE #1962383 [designer] Option to create a PDF page
- patch #2007196, Typos in comments, thanks to knittl
- bug #1982315 [GUI] Comma and quote in ENUM, thanks to Joshua Hogendorn
+ [GUI] Color picker
- bug #1970836 [parser] SQL parser is slow, thanks to Christian Schmidt
+ RFE #1692928 [transformation] Option to disable browser transformations
+ [import] Speed optimization to be able to import the sakila database
+ [doc] Documentation for distributing phpMyAdmin in README.VENDOR.
+ [display] headwords for sorted column
- bug #2033962 [import] Cannot import zip file
+ [lang] Swedish update, thanks to Björn T. Hallberg
- bug #2050068 [gui] "Check tables having overhead" selects wrong tables
+ [lang] Belarusian update, thanks to Jaska Zedlik
+ [lang] Norwegian update, thanks to Sven-Erik Andersen
+ [lang] Italian update, thanks to Luca Rebellato
- [core] safer handling of temporary files with open_basedir (thanks to Thijs
  Kinkhorst)
- [core] do not automatically set and create TempDir, it might lead to security
  issue (thanks to Thijs Kinkhorst)
+ [lang] Czech update
- bug #2066923 [display] Navi browse icon does not go to page 1
- patch #2075263 [auth] Single sign-on and cookie clearing,
  thanks to Charles Suh
- [doc] better documentation of $cfg['TempDir']
- bug #2080963 [charset] Clarify doc and improved code, thanks to
```

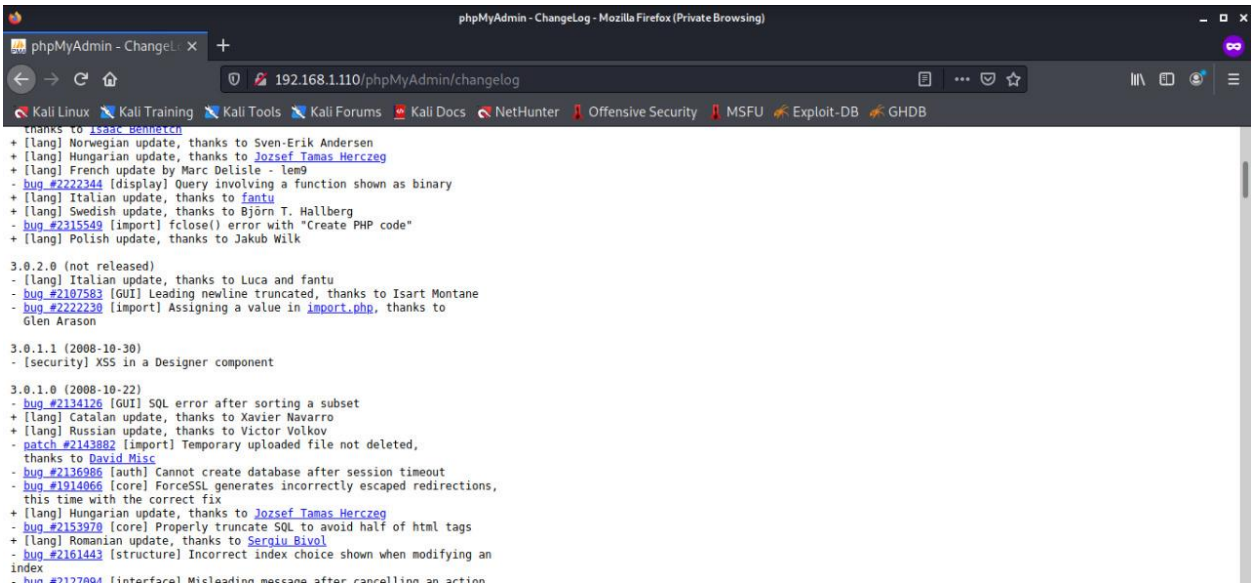



```
  patch #2176438 [privileges] Wrong message when changing password,
  thanks to incognito
- bug #2163437 [core] Cannot disable PMA tables
- bug #2184240 [lang] Problems with Italian language file, thanks to Luca
Rebellato
- bug #2187193 [interface] ShowChgPassword setting not respected

3.0.0.0 (2008-09-27)
+ [export] properly handle line breaks for YAML, thanks to Dan Barry
+ [navi] new parameter $cfg['LeftDefaultTabTable']
+ [table] support MySQL 5.1 PARTITION: CREATE TABLE / Table structure,
  partition maintenance
+ [privileges] support for EVENT and TRIGGER
+ [error handler] NEW handle errors to prevent path disclosure and display/collect errors
+ [mysqlnd] do not display $strMysqlLibDiffersServerVersion if the client
  is mysqlnd
+ [webapp] experimental Mozilla Prism support
+ [export] new plugin "codegen" for NHibernate, thanks to caocao; I'm
  looking for a name more descriptive than codegen, taking into account
  that it might later support other formats like JSON in the same plugin
+ [export] new export to Texy! markup
+ [lang] Finnish update, thanks to Jouni Kahkonen
+ [config] new parameter $cfg['CheckConfigurationPermissions']
+ [config] new parameter $cfg['Servers'][$i]['ShowDatabasesCommand']
+ [config] new parameter $cfg['Servers'][$i]['CountTables']
+ RFE #1775288 [transformation] proper display if IP-address stored as INT
+ RFE #1758177 [core] Add the Geometry DataTypes
+ RFE #1741101, patch #1798184 UUID default for CHAR(36) PRIMARY KEY,
  thanks to Gert Palok
- bug #1664240 [GUI] css height makes cfg TextareaRows useless
- bug #1724217 [Create PHP Code] doesn't include newlines for text fields
- bug #1845605 [i18n] translators.html still uses iso-8859-1
- bug #1823018 [charset] Edit(Delete) img-links pointing to wrong row
- bug #1826905 [export] Problems with yaml text export
```

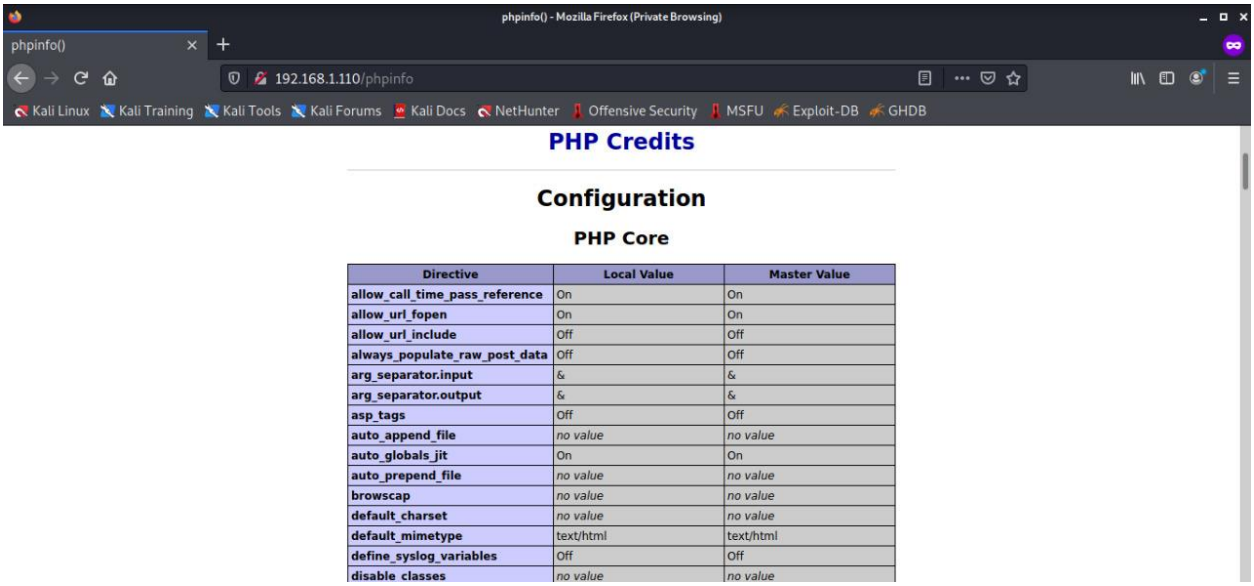



```
3.1.0.0 (2008-11-28)
+ [auth] Support for Swekey hardware authentication,
  see http://phpmyadmin.net/auth key
- bug #2046883 [core] Notices about deprecated dl() (so stop using it)
+ BLOBstreaming support, thanks to Raj Kissu Rajandran and
  Google Summer of Code 2008
+ patch #2067462 [lang] link FAQ references in messages,
  thanks to Thijs Kinkhorst
+ new setup script, thanks to Piotr Przybylski (work in progress)
- RFE #1892243 [export] more links to documentation
+ [auth] cookie auth now autogenerates blowfish_secret, but it has some
  limitations and you still should set it in config file
+ [auth] cookie authentication is now the default
+ [auth] do not allow root user without password unless explicitly enabled by
  AllowNoPasswordRoot
+ RFE #1778908 [auth] arbitrary server auth can now also accept port
- patch #2089240 [export] handle correctly switching SQL modes
+ RFE #1612724 [export] add option to export without comments
- bug #2090002 [display] Cannot edit row in VIEW
- patch #2099962 [js] fix js error without frameset, thanks to Xuefer
- patch #2099972 [structure] Display None when there is no default value,
  thanks to Xuefer
- patch #2122883 [PDF schema] Option to display just the keys,
  thanks to Samuel Sol Villar dos Santos
+ RFE #1276463 [search] Search empty/not empty values
+ RFE #823652 [structure] ENUM values: field size too small
- [lang] Persian update, thanks to Goolex
- [lang] Czech update, thanks to Ondřej Vadinský.
- patch #2255890 [lang] English-language cleanup,
  thanks to Isaac Bennetch
+ [lang] Norwegian update, thanks to Sven-Erik Andersen
+ [lang] Hungarian update, thanks to Jozsef Tamas Herczeg
```


phpMyAdmin - ChangeLog - Mozilla Firefox (Private Browsing)
phpMyAdmin - ChangeLo
192.168.1.110/phpMyAdmin/changelog
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
issue (thanks to Thijs Kinkhorst)
+ [lang] Czech update
- bug #2066923 [display] Navi browse icon does not go to page 1
- patch #2075263 [auth] Single sign-on and cookie clearing,
thanks to Charles Suh
- [doc] better documentation of $cfg['TempDir']
- bug #2080963 [charset] Clarify doc and improved code, thanks to
Victor Volkov - hanut
- bug [charset] Cannot sort twice on a column when the table name
contains accents
+ [lang] Spanish update, thanks to Daniel Hinostroza
+ [lang] Hungarian update, thanks to Jozsef Tamas Herczeg
- bug #2113848 [navi] Page number after database switching
- patch #2115966 [GUI] Checkboxes and IE 7, thanks to Martin
- bug #1914066 [core] ForceSSL generates incorrectly escaped redirections
2.11.9.3 (2008-10-30)
- [security] XSS in a Designer component
2.11.9.2 (2008-09-22)
- [security] XSS in MSIE using NUL byte, thanks to JPCERT.
2.11.9.1 (2008-09-15)
- [security] Code execution vulnerability, thanks to Norman Hippert
2.11.9.0 (2008-08-28)
- bug #2031221 [auth] Links to version number on login screen
- bug #2032707 [core] PMA does not start if ini_set() is disabled
- bug #2004915 [bookmarks] Saved queries greater than 1000 chars not
displayed, thanks to Maik Wiege
- bug #2037381 [export] Export type "replace" does not work
- bug #2037375 [export] DROP PROCEDURE needs IF EXISTS
- bug #2045512 [export] Numbers in Excel export


phpMyAdmin - ChangeLog - Mozilla Firefox (Private Browsing)
phpMyAdmin - ChangeLo
192.168.1.110/phpMyAdmin/changelog
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
thanks to Isaac Bennetch
+ [lang] Norwegian update, thanks to Sven-Erik Andersen
+ [lang] Hungarian update, thanks to Jozsef Tamas Herczeg
+ [lang] French update by Marc Delisle - lem9
- bug #2222344 [display] Query involving a function shown as binary
+ [lang] Italian update, thanks to fantu
+ [lang] Swedish update, thanks to Björn T. Hallberg
- bug #2315549 [import] fclose() error with "Create PHP code"
+ [lang] Polish update, thanks to Jakub Wilk
3.0.2.0 (not released)
- [lang] Italian update, thanks to Luca and fantu
- bug #2107583 [GUI] Leading newline truncated, thanks to Isart Montane
- bug #2222230 [import] Assigning a value in import.php, thanks to
Glen Arason
3.0.1.1 (2008-10-30)
- [security] XSS in a Designer component
3.0.1.0 (2008-10-22)
- bug #2134126 [GUI] SQL error after sorting a subset
+ [lang] Catalan update, thanks to Xavier Navarro
+ [lang] Russian update, thanks to Victor Volkov
- patch #2143882 [import] Temporary uploaded file not deleted,
thanks to David Misc
- bug #2136986 [auth] Cannot create database after session timeout
- bug #1914066 [core] ForceSSL generates incorrectly escaped redirections,
this time with the correct fix
+ [lang] Hungarian update, thanks to Jozsef Tamas Herczeg
- bug #2153970 [core] Properly truncate SQL to avoid half of html tags
+ [lang] Romanian update, thanks to Sergiu Bivol
- bug #2161443 [structure] Incorrect index choice shown when modifying an
index

Phpinfo

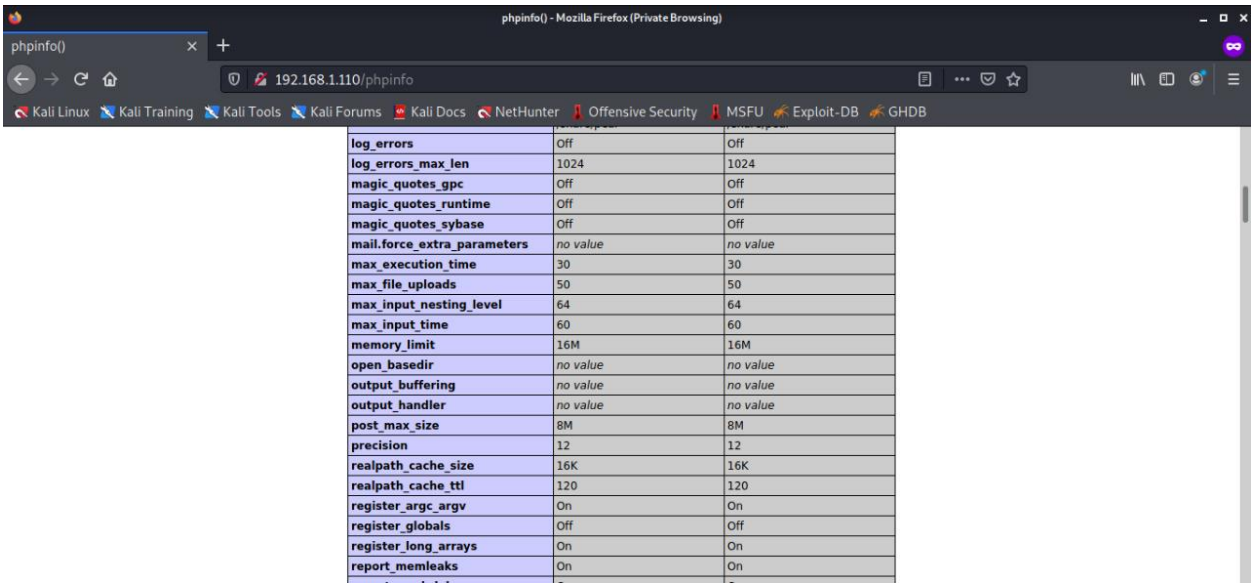


PHP Credits

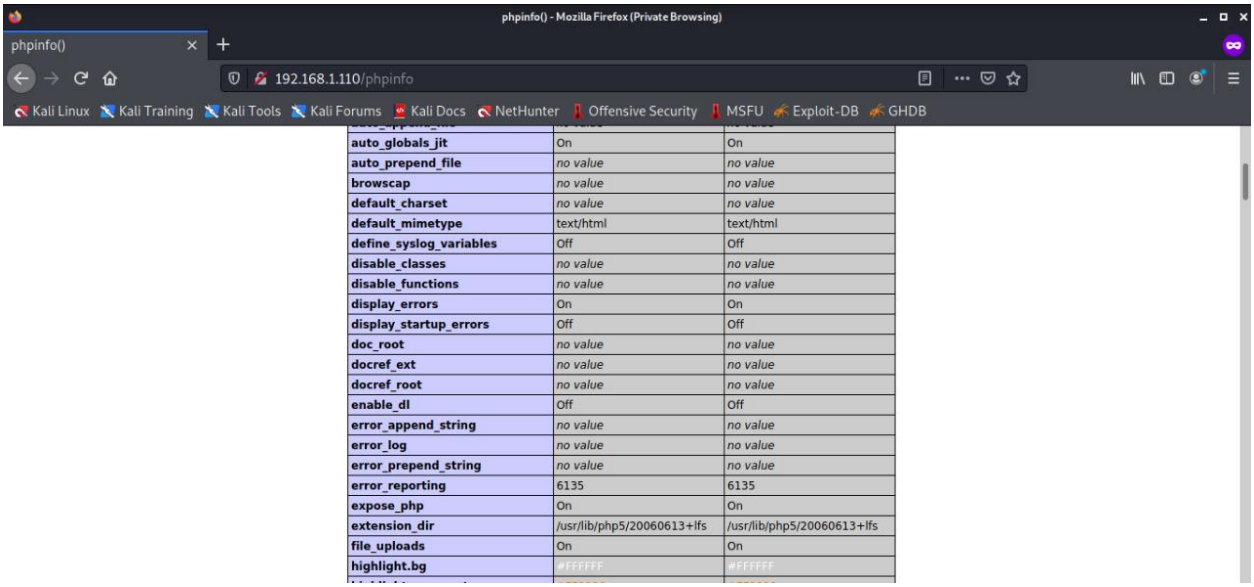
Configuration

PHP Core

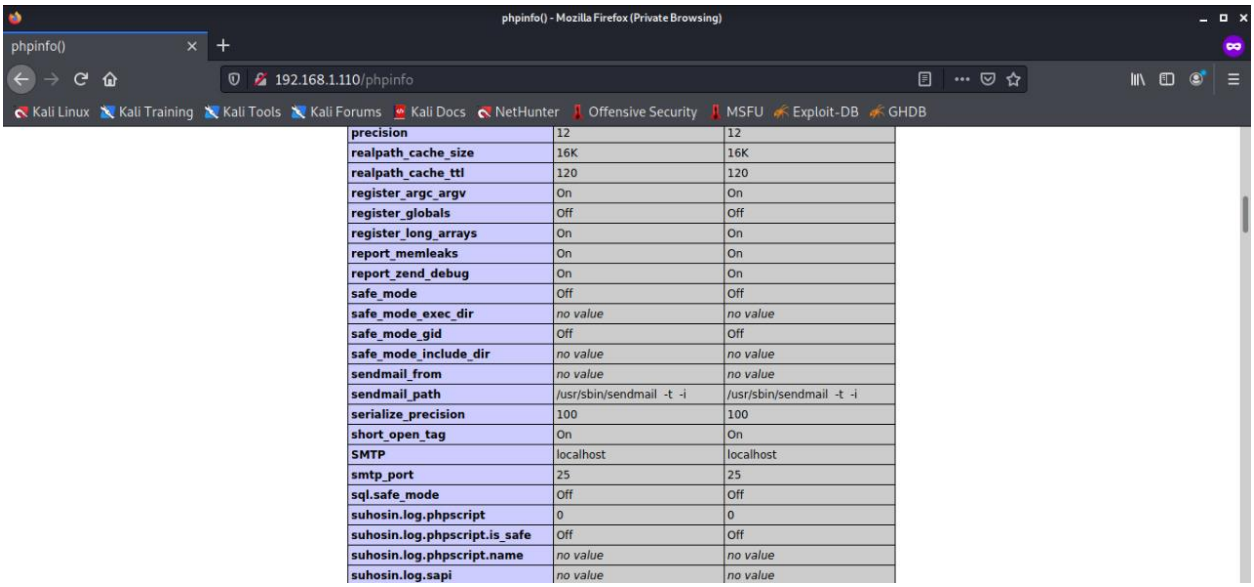
Directive	Local Value	Master Value
allow_call_time_pass_reference	On	On
allow_url_fopen	On	On
allow_url_include	Off	Off
always_populate_raw_post_data	Off	Off
arg_separator.input	&	&
arg_separator.output	&	&
asp_tags	Off	Off
auto_append_file	*no value*	*no value*
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	*no value*	*no value*
default_mimetype	text/html	text/html
define_syslog_variables	Off	Off
disable_classes	*no value*	*no value*



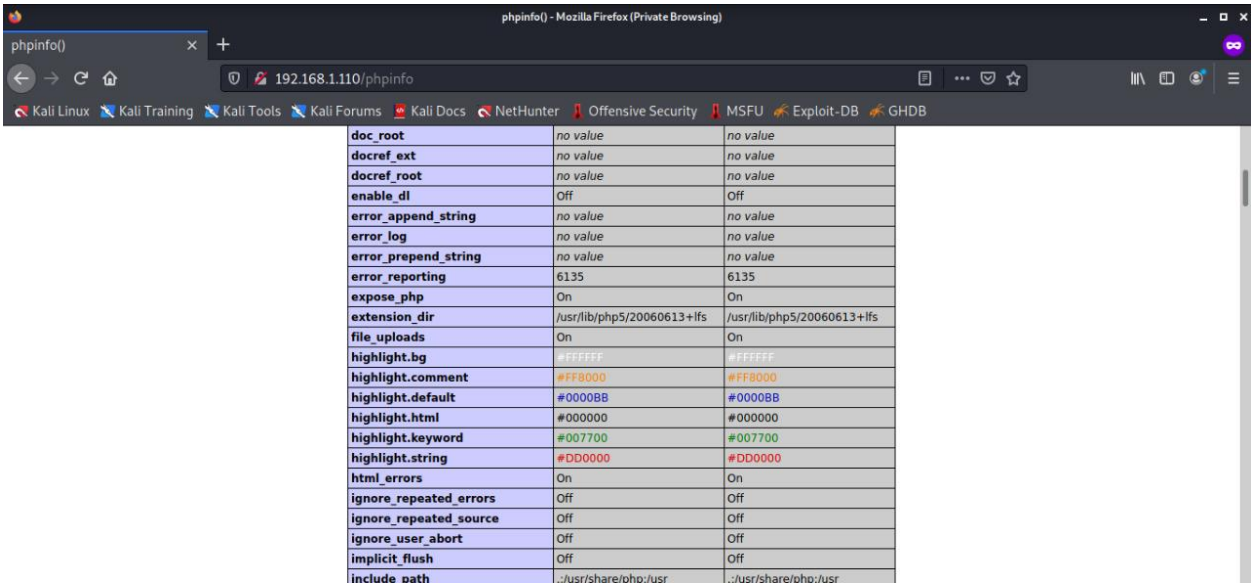
log_errors	Off	Off
log_errors_max_len	1024	1024
magic_quotes_gpc	Off	Off
magic_quotes_runtime	Off	Off
magic_quotes_sybase	Off	Off
mail.force_extra_parameters	*no value*	*no value*
max_execution_time	30	30
max_file_uploads	50	50
max_input_nesting_level	64	64
max_input_time	60	60
memory_limit	16M	16M
open_basedir	*no value*	*no value*
output_buffering	*no value*	*no value*
output_handler	*no value*	*no value*
post_max_size	8M	8M
precision	12	12
realpath_cache_size	16K	16K
realpath_cache_ttl	120	120
register_argc_argv	On	On
register_globals	Off	Off
register_long_arrays	On	On
report_memleaks	On	On



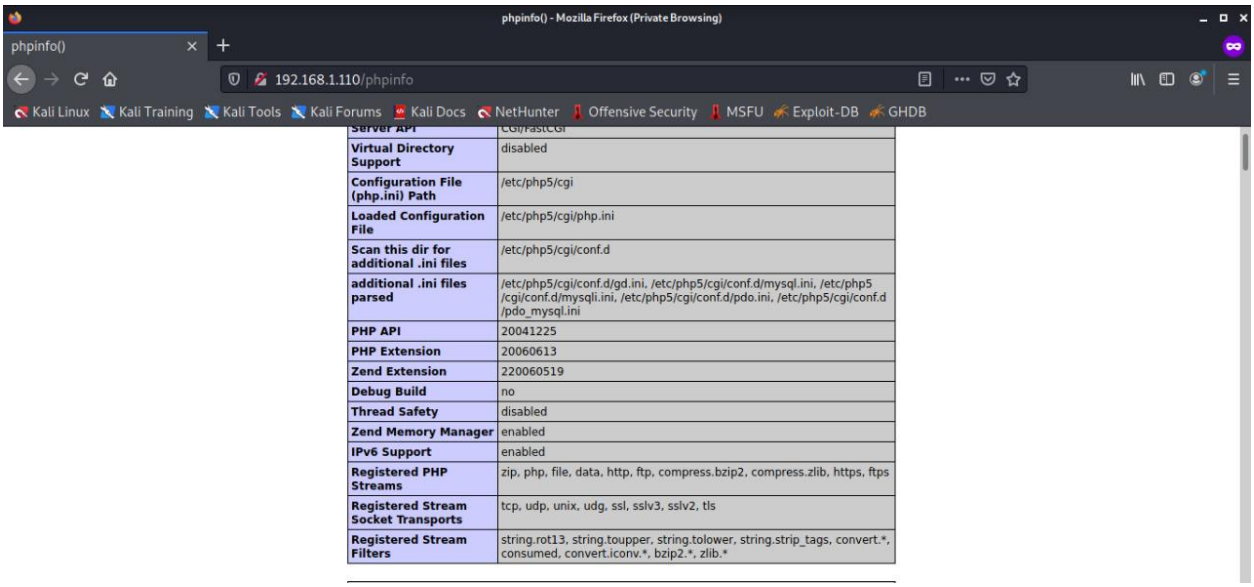
auto_globals_jit	On	On
auto_prepend_file	*no value*	*no value*
browscap	*no value*	*no value*
default_charset	*no value*	*no value*
default_mimetype	text/html	text/html
define_syslog_variables	Off	Off
disable_classes	*no value*	*no value*
disable_functions	*no value*	*no value*
display_errors	On	On
display_startup_errors	Off	Off
doc_root	*no value*	*no value*
docref_ext	*no value*	*no value*
docref_root	*no value*	*no value*
enable_dl	Off	Off
error_append_string	*no value*	*no value*
error_log	*no value*	*no value*
error_prepend_string	*no value*	*no value*
error_reporting	6135	6135
expose_php	On	On
extension_dir	/usr/lib/php5/20060613+lfs	/usr/lib/php5/20060613+lfs
file_uploads	On	On
highlight.bg	#FFFFFF	#FFFFFF



precision	12	12
realpath_cache_size	16K	16K
realpath_cache_ttl	120	120
register_argc_argv	On	On
register_globals	Off	Off
register_long_arrays	On	On
report_memleaks	On	On
report_zend_debug	On	On
safe_mode	Off	Off
safe_mode_exec_dir	*no value*	*no value*
safe_mode_gid	Off	Off
safe_mode_include_dir	*no value*	*no value*
sendmail_from	*no value*	*no value*
sendmail_path	/usr/sbin/sendmail -t -i	/usr/sbin/sendmail -t -i
serialize_precision	100	100
short_open_tag	On	On
SMTP	localhost	localhost
smtp_port	25	25
sql.safe_mode	Off	Off
suhosin.log.phpscript	0	0
suhosin.log.phpscript.is_safe	Off	Off
suhosin.log.phpscript.name	*no value*	*no value*
suhosin.log.sapi	*no value*	*no value*



doc_root	*no value*	*no value*
docref_ext	*no value*	*no value*
docref_root	*no value*	*no value*
enable_dl	Off	Off
error_append_string	*no value*	*no value*
error_log	*no value*	*no value*
error_prepend_string	*no value*	*no value*
error_reporting	6135	6135
expose_php	On	On
extension_dir	/usr/lib/php5/20060613+lfs	/usr/lib/php5/20060613+lfs
file_uploads	On	On
highlight.bg	#FFFFFF	#FFFFFF
highlight.comment	#FF8000	#FF8000
highlight.default	#0000BB	#0000BB
highlight.html	#000000	#000000
highlight.keyword	#007700	#007700
highlight.string	#DD0000	#DD0000
html_errors	On	On
ignore_repeated_errors	Off	Off
ignore_repeated_source	Off	Off
ignore_user_abort	Off	Off
implicit_flush	Off	Off
include_path	.:/usr/share/php:/usr	.:/usr/share/php:/usr



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.*

GetText Support	enabled

hash

hash support	enabled
Hashing Engines	md2 md4 md5 sha1 sha256 sha384 sha512 ripemd128 ripemd160 ripemd256 ripemd320 whirlpool tiger128,3 tiger160,3 tiger192,3 tiger128,4 tiger160,4 tiger192,4 snefru gost adler32 crc32 crc32b haval128,3 haval160,3 haval192,3 haval224,3 haval256,3 haval128,4 haval160,4 haval192,4 haval224,4 haval256,4 haval128,5 haval160,5 haval192,5 haval224,5 haval256,5

iconv

iconv support	enabled
iconv implementation	glibc
iconv library version	2.7

Directive	Local Value	Master Value
iconv.input_encoding	ISO-8859-1	ISO-8859-1
iconv.internal_encoding	ISO-8859-1	ISO-8859-1
iconv.output_encoding	ISO-8859-1	ISO-8859-1

ftp

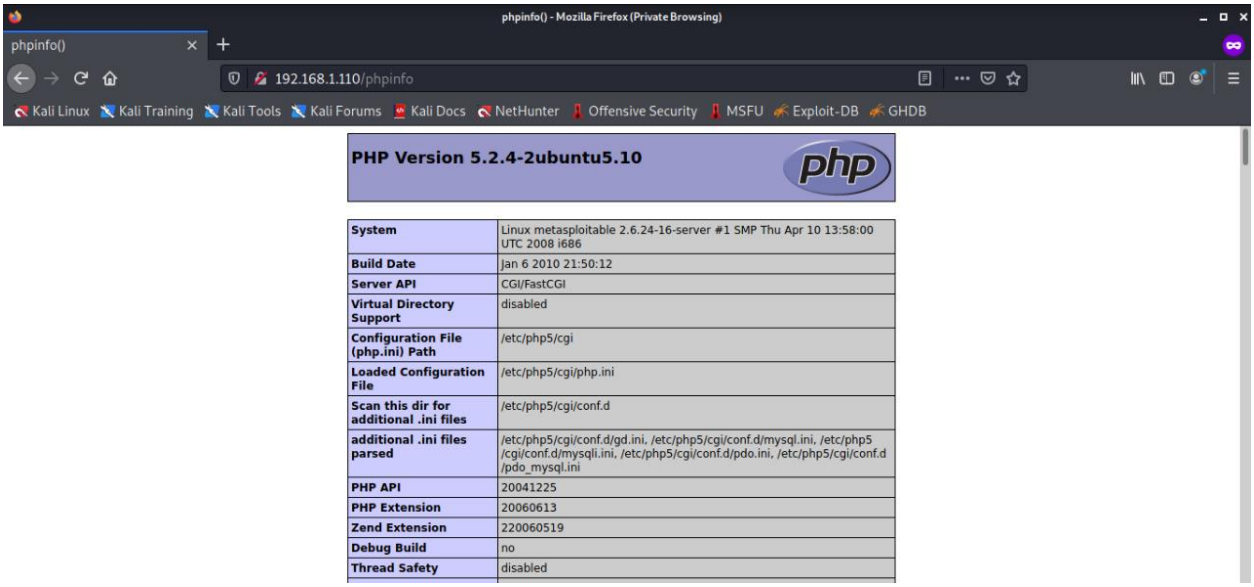
FTP support	enabled

gd

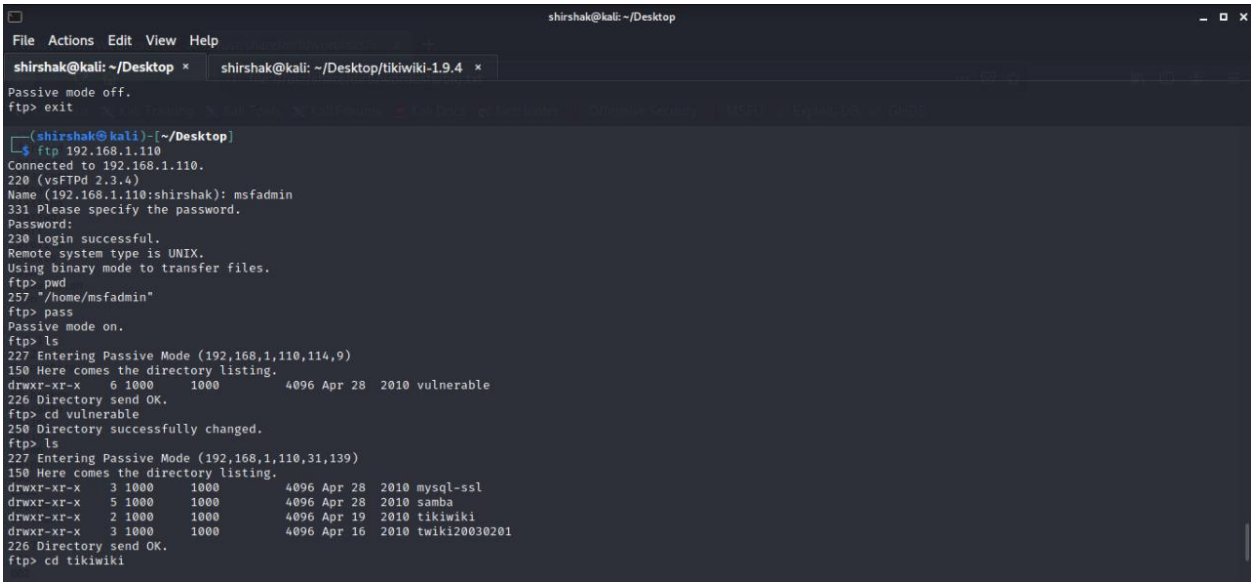
GD Support	enabled
GD Version	2.0 or higher
FreeType Support	enabled
FreeType Linkage	with freetype
FreeType Version	2.3.5
T1Lib Support	enabled
GIF Read Support	enabled
GIF Create Support	enabled
JPG Support	enabled
PNG Support	enabled
WBMP Support	enabled

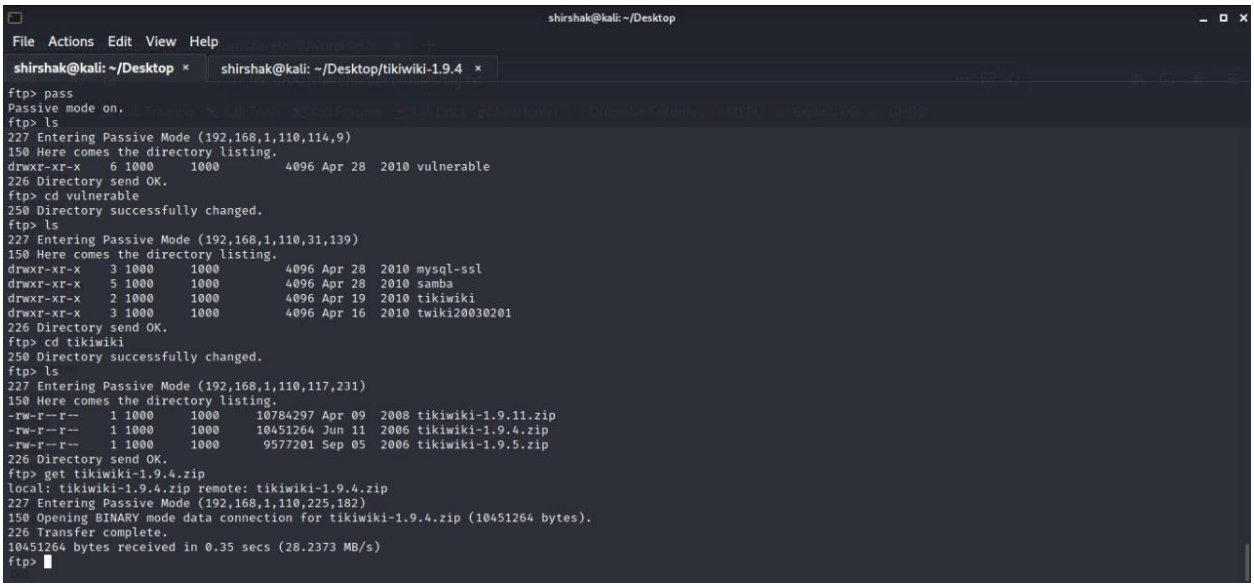
gettext

GetText Support	enabled

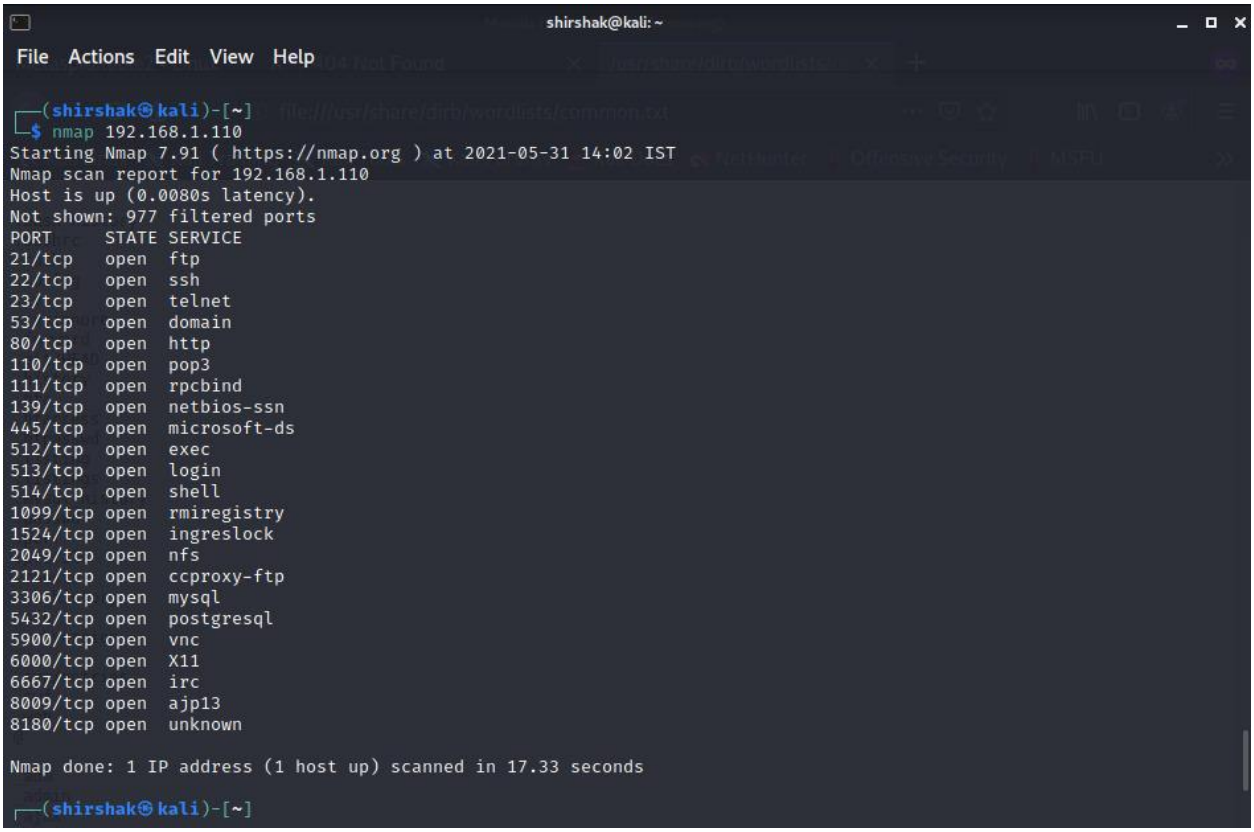

phpinfo() - Mozilla Firefox (Private Browsing)
phpinfo()
192.168.1.110/phpinfo
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
PHP Version 5.2.4-2ubuntu5.10
php
System
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 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

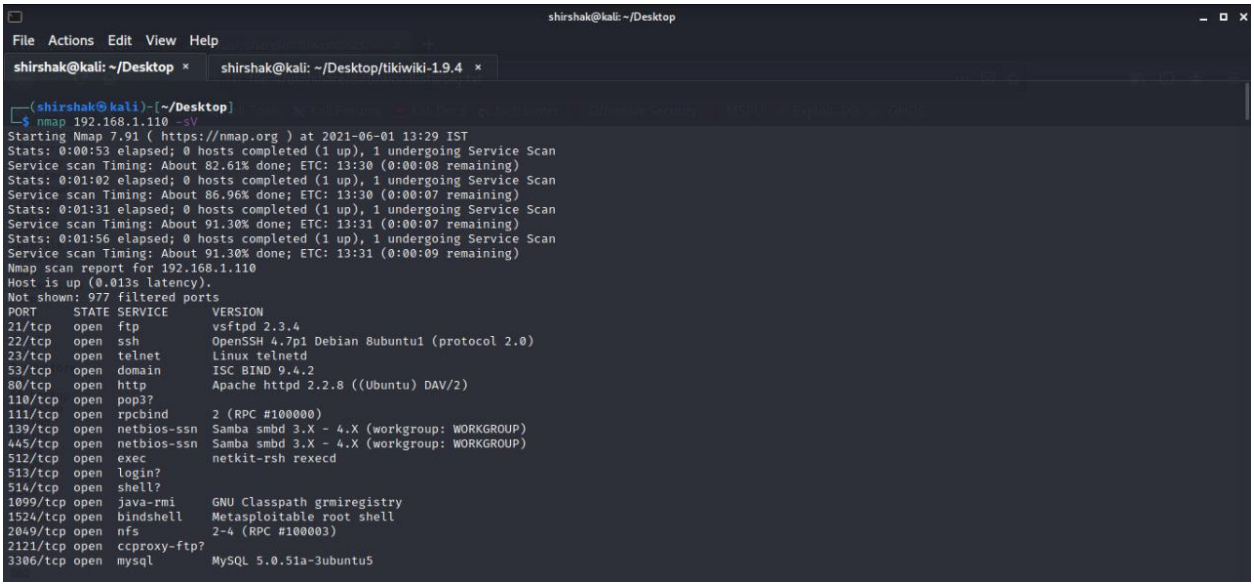
Ftp ports


shirshak@kali: ~/Desktop
File Actions Edit View Help
shirshak@kali: ~/Desktop
shirshak@kali: ~/Desktop/tikiwiki-1.9.4
Passive mode off.
ftp> exit
(shirshak㉿kali)-[~/Desktop]
$ ftp 192.168.1.110
Connected to 192.168.1.110.
220 (vsFTPd 2.3.4)
Name (192.168.1.110:shirshak): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/msfadmin"
ftp> pass
Passive mode on.
ftp> ls
227 Entering Passive Mode (192,168,1,110,114,9)
150 Here comes the directory listing.
drwxr-xr-x 6 1000 1000 4096 Apr 28 2010 vulnerable
226 Directory send OK.
ftp> cd vulnerable
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (192,168,1,110,31,139)
150 Here comes the directory listing.
drwxr-xr-x 3 1000 1000 4096 Apr 28 2010 mysql-ssl
drwxr-xr-x 5 1000 1000 4096 Apr 28 2010 samba
drwxr-xr-x 2 1000 1000 4096 Apr 19 2010 tikiwiki
drwxr-xr-x 3 1000 1000 4096 Apr 16 2010 twiki20030201
226 Directory send OK.
ftp> cd tikiwiki


shirshak@kali: ~/Desktop
File Actions Edit View Help
shirshak@kali: ~/Desktop
shirshak@kali: ~/Desktop/tikiwiki-1.9.4
ftp> pass
Passive mode on.
ftp> ls
227 Entering Passive Mode (192,168,1,110,114,9)
150 Here comes the directory listing.
drwxr-xr-x 6 1000 1000 4096 Apr 28 2010 vulnerable
226 Directory send OK.
ftp> cd vulnerable
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (192,168,1,110,31,139)
150 Here comes the directory listing.
drwxr-xr-x 3 1000 1000 4096 Apr 28 2010 mysql-ssl
drwxr-xr-x 5 1000 1000 4096 Apr 28 2010 samba
drwxr-xr-x 2 1000 1000 4096 Apr 19 2010 tikiwiki
drwxr-xr-x 3 1000 1000 4096 Apr 16 2010 twiki20030201
226 Directory send OK.
ftp> cd tikiwiki
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (192,168,1,110,117,231)
150 Here comes the directory listing.
-rw-r--r-- 1 1000 1000 10784297 Apr 09 2008 tikiwiki-1.9.11.zip
-rw-r--r-- 1 1000 1000 10451264 Jun 11 2006 tikiwiki-1.9.4.zip
-rw-r--r-- 1 1000 1000 9577201 Sep 05 2006 tikiwiki-1.9.5.zip
226 Directory send OK.
ftp> get tikiwiki-1.9.4.zip
local: tikiwiki-1.9.4.zip remote: tikiwiki-1.9.4.zip
227 Entering Passive Mode (192,168,1,110,225,182)
150 Opening BINARY mode data connection for tikiwiki-1.9.4.zip (10451264 bytes).
226 Transfer complete.
10451264 bytes received in 0.35 secs (28.2373 MB/s)
ftp>

Nmap for open ports





THANK YOU…….