


HW5. Web Security

L091025 清大資工所 熊詩旻

Task1. takes a screenshot of your phpinfo page with the following information.

PHP Version 7.3.28-2+ubuntu18.04.1+deb.sury.org+1	
	
System	Linux xiung-VirtualBox 5.4.0-74-generic #83~18.04.1-Ubuntu SMP Tue May 11 16:01:00 UTC 2021 x86_64
Build Date	Jun 4 2021 21:23:19
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-bcmath.ini, /etc/php/7.3/apache2/conf.d/20-bz2.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-imagick.ini, /etc/php/7.3/apache2/conf.d/20-intl.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini, /etc/php/7.3/apache2/conf.d/20-wddx.ini, /etc/php/7.3/apache2/conf.d/20-xmlreader.ini, /etc/php/7.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.3/apache2/conf.d/20-xsl.ini, /etc/php/7.3/apache2/conf.d/20-zip.ini

imagick

imagick module	enabled
imagick module version	3.4.4
imagick classes	Imagick, ImagickDraw, ImagickPixel, ImagickPixelIterator, ImagickKernel
Imagick compiled with ImageMagick version	ImageMagick 6.9.7-4 Q16 x86_64 20170114 http://www.imagemagick.org
Imagick using ImageMagick library version	ImageMagick 6.9.7-4 Q16 x86_64 20170114 http://www.imagemagick.org
ImageMagick copyright	© 1999-2017 ImageMagick Studio LLC
ImageMagick release date	20170114
ImageMagick number of supported formats:	230
ImageMagick supported formats	3FR, AAI, AI, ART, ARW, AVI, AVS, BGR, BGRA, BGRO, BIE, BMP, BMP2, BMP3, BRF, CAL, CALS, CANVAS, CAPTION, CIN, CIP, CLIP, CMYK, CMYKA, CR2, CRW, CUR, CUT, DATA, DCM, DCR, DCX, DDS, DFONT, DJVU, DNG, DOT, DPX, DXT1, DXT5, EPDF, EPI, EPS, EPS2, EPS3, EPSF, EPSI, EPT, EPT2, EPT3, ERF, EXR, FAX, FILE, FITS, FRACTAL, FTP, FTS, G3, G4, GIF, GIF87, GRADIENT, GRAY, GROUP4, GV, H, HALD, HDR, HISTOGRAM, HRZ, HTM, HTML, HTTP, HTTPS, ICB, ICO, ICON, IIQ, INFO, INLINE, IPL, ISOBRL, ISOBRL6, JBG, JBIG, JNG, JNX, JPE, JPEG, JPG, JPS, JSON, K25, KDC, LABEL, M2V, M4V, MAC, MAGICK, MAP, MASK, MAT, MATTE, MEF, MIFF, MKV, MNG, MONO, MOV, MP4, MPC, MPEG, MPG, MRW, MSL, MSVG, MTV, MVG, NEF, NRW, NULL, ORF, OTB, OTF, PAL, PALM, PAM, PANGO, PATTERN, PBM, PCD, PCDS, PCL, PCT, PCX, PDB, PDF, PDFA, PEF, PES, PFA, PFB, PFM, PGM, PICON, PICT, PIX, PJPEG, PLASMA, PNG, PNG00, PNG24, PNG32, PNG48, PNG64, PNG8, PNM, PPM, PREVIEW, PS, PS2, PS3, PSB, PSD, PTIF, PWP, RADIAL-GRADIENT, RAF, RAS, RAW, RGB, RGBA, RGBO, RGF, RLA, RLE, RMF, RW2, SCR, SCT, SFW, SGI, SHTML, SIX, SIXEL, SPARSE-COLOR, SR2, SRF, STEGANO, SUN, SVG, SVZ, TEXT, TGA, THUMBNAIL, TIFF, TIFF64, TILE, TIM, TTC, TTF, TXT, UBRL, UBRL6, UIL, UYVY, VDA, VICAR, VID, VIFF, VIPS, VST, WBMP, WMF, WMV, WMZ, WPG, X, X3F, XBM, XC, XCF, XPM, XPS, XV, XWD, YCbCr, YCbCrA, YUV

gd

GD Support	enabled
GD headers Version	2.3.0
GD library Version	2.3.0
FreeType Support	enabled
FreeType Linkage	with freetype
FreeType Version	2.8.1
GIF Read Support	enabled
GIF Create Support	enabled
JPEG Support	enabled
libJPEG Version	8
PNG Support	enabled
libPNG Version	1.6.34
WBMP Support	enabled
XPM Support	enabled
libXpm Version	30411
XBM Support	enabled
WebP Support	enabled

Directive	Local Value	Master Value
gd.jpeg_ignore_warning	1	1

Task2. use the SQL statement via MySQL-CLI interface to list the tables and paste the list in your report.

```
MariaDB [(none)]> USE wordpress_l091025; SHOW TABLES;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
+-----+
| Tables_in_wordpress_l091025 |
+-----+
| wp_commentmeta |
| wp_comments    |
| wp_links       |
| wp_options     |
| wp_postmeta    |
| wp_posts       |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta    |
| wp_terms       |
| wp_usermeta    |
| wp_users       |
+-----+

12 rows in set (0.000 sec)

MariaDB [wordpress_l091025]>
```

Task3. Show the results from running the shell command 'ip addr' on the WordPress server.

[illegible]

[illegible]

Print "A" 、 "B" 、 "C" 、 "E"

Wordpress 提供兩種方式來處理圖片，分別是 Imagick 和 GD，而 Imagick 的 priority 較高，GD 次之，所以這個順序會影響到最終環境的應用。

- Imagick 不會去除掉圖片中 exif 的部分，因為他認為那是圖片的一部分，所以我們可以將 php payload 加到 exif 的部分。
- GD 會去除圖片的 exif 部分，所以我們的 payload 很難存活，應該會被移除掉。

Wordpress 的主題位於 `wp-content/themes` 目錄中並為不同的案例提供模板文件。正常情況下，是無法透過 `web` 方式訪問寫入此目錄。但是此時我們已經將我們的 `evil.jpg` 插入此目錄，接著就可以透過加載這個 `themes`，執行我們的惡意圖片 `payload`。