

Authentication and Authorization Attacks

Sentry MBA



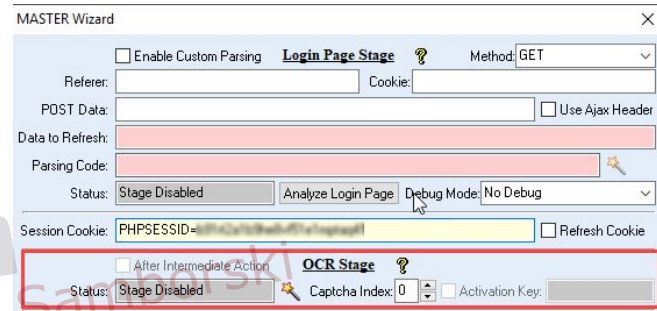
Sentry MBA

- Research about “How to Bypass Captcha using OCR” in Sentry MBA
- You can install wordpress CAPTCHA Booster plugin on wordpress and try bypassing it using OCR
- If you don't installed wordpress locally, you can also use the online lab
 - <http://lab.awh.exdemy.com/chapter1/wordpress-4.7>



Sentry MBA - Solution

- Sentry MBA has its own built-in OCR system which can solve CAPTCHAs using Image Processing techniques
- Open up **MASTER Wizard** and see the **OCR Stage** where you can setup the system to recognize the CAPTCHA
- As you see in the picture there are lots of options to use
- To start working, set the **CAPTCHA field refresh** to automatic then click on **analyze** button until Sentry MBA finds images
- Among those images select the generated CAPTCHA URL and click on **Test** button



MASTER Wizard

☐ Enable Custom Parsing **Login Page Stage** ? Method: GET

Referer: Cookie: ☐ Use Ajax Header

POST Data:

Data to Refresh:

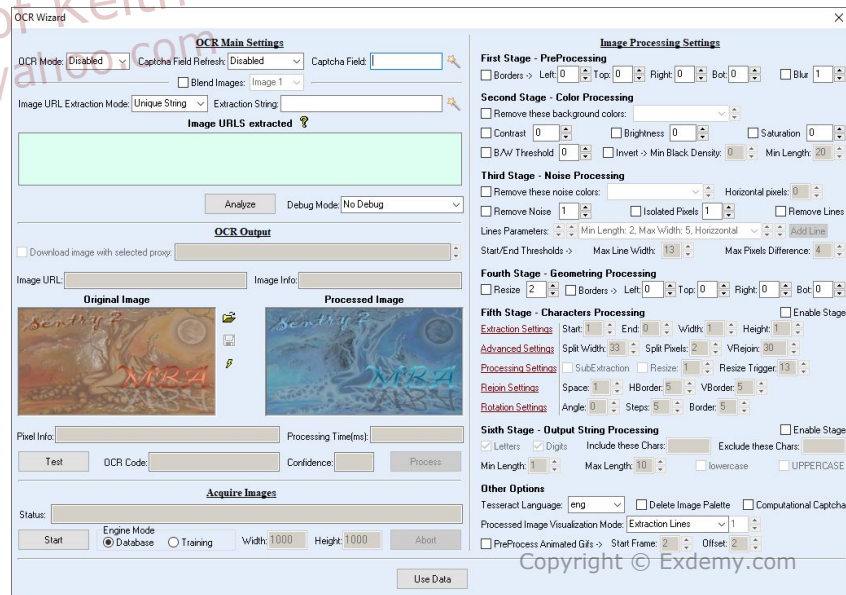
Parsing Code: ?

Status: Stage Disabled Analyze Login Page Debug Mode: No Debug

Session Cookie: PHPSESSID= ☐ Refresh Cookie

☐ After Intermediate Action **OCR Stage** ?

Status: Stage Disabled Captcha Index: 0 Activation Key:



OCR Wizard

OCR Main Settings

OCR Mode: Disabled Capcha Field Refresh: Disabled Capcha Field:

☐ Blend Images: Image 1

Image URL Extraction Mode: Unique String Extraction String:

Image URLs extracted ?

Analyze Debug Mode: No Debug

Download image with selected proxy:

Image URL: Image Info:

Original Image Processed Image

Pixel Info: Processing Time(ms):

Test OCR Code: Confidence: Process

Acquire Images

Status:

Start Engine Mode: ☒ Database ☐ Training Width: 1000 Height: 1000 About

Use Data

Image Processing Settings

First Stage - PreProcessing

☐ Borders > Left: 0 Top: 0 Right: 0 Bot: 0 ☐ Blur 1

Second Stage - Color Processing

☐ Remove these background colors:

Contrast 0 Brightness 0 Saturation 0

B/W Threshold 0 Invert > Min Black Density: 0 Min Length: 20

Third Stage - Noise Processing

☐ Remove these noise colors: Horizontal pixels: 0

☐ Remove Noise 1 ☐ Isolated Pixels 1 ☐ Remove Lines

Lines Parameters: Min Length: 2 Max Width: 5 Horizontal Add Line

Start/End Thresholds > Max Line Width: 13 Max Pixels Difference: 4

Fourth Stage - Geomerting Processing

☐ Resize 2 ☐ Borders > Left: 0 Top: 0 Right: 0 Bot: 0

Fifth Stage - Characters Processing

Extraction Settings Start: 1 End: 0 Width: 1 Height: 1

Advanced Settings Split Width: 33 Split Pixels: 2 VRegion: 30

Processing Settings ☐ SubExtraction ☐ Resize 1 ☐ Resize Trigger: 13

Region Settings Space: 1 HBorder: 5 VBorder: 5

Rotation Settings Angle: 0 Steps: 5 Border: 5

Sixth Stage - Output String Processing

☒ Letters ☒ Digits Include these Chars: Exclude these Chars:

Min Length: 1 Max Length: 10 ☐ lowercase ☐ UPPERCASE

Other Options

Tesseract Language: eng ☐ Delete Image Palette ☐ Computational Capcha

Processed Image Visualization Mode: Extraction Lines 1

☐ PreProcess Animated Gifs > Start Frame: 2 Offset: 2

Copyright © Exdemy.com

Sentry MBA - Solution - Contd.

- Clicking on **Test** button makes the OCR system try to recognize the code from the CAPTCHA
- If you encountered **Image not recognized** message in **OCR Code** section
 - You have to optimize the settings based on the CAPTCHA parameters until the detected **OCR Code** becomes accurate
- In the image, see a sample configuration for the **OCR Wizard**
- We used Wordpress **Captcha Booster** plugin with customized settings (to make captchas simpler)

The screenshot displays the OCR Wizard application interface, which is divided into several sections for configuring OCR settings.

- OCR Main Settings:** Includes fields for OCR Mode (Tesseract), Captcha Field Refresh (Automatic), Captcha Field (challenge.html), Blend Images (Image 1), Image URL Extraction Mode (Unique String), and Extraction String (http://lab.awh.exdemy.com/chapter1/ww).
- Image URLs extracted:** Shows a list of extracted URLs, including http://lab.awh.exdemy.com/chapter1/wordpress-4.7/wp-admin/admin-ajax.php?captcha-code=36477 and http://lab.awh.exdemy.com/chapter1/wordpress-4.7/wp-content/plugins/wp-captcha-booster/assets/global/img/.
- OCR Output:** Includes a download button and a text box for the image URL (http://lab.awh.exdemy.com/chapter1/wordpress).
- Image Processing Settings:** A detailed section with multiple stages:
 - First Stage - PreProcessing:** Includes Borders, Top, Bottom, Right, Left, and Blur settings.
 - Second Stage - Color Processing:** Includes Remove these background colors, Contrast, Brightness, Saturation, BAW Threshold, Invert, Min Black Density, and Min Length settings.
 - Third Stage - Noise Processing:** Includes Remove these noise colors, Horizontal pixels, Remove Noise, Isolated Pixels, Remove Lines, Lines Parameters, Start/End Thresholds, Max Line Width, and Max Pixels Difference settings.
 - Fourth Stage - Geomting Processing:** Includes Resize, Borders, Top, Bottom, Right, Left, and Bot settings.
 - Fifth Stage - Characters Processing:** Includes Enable Stage, Extraction Settings (Start, End, Width, Height), Advanced Settings (Split Width, Split Pixels, VRejoin), Processing Settings (SubExtraction, Resize, Resize Trigger), Rejoin Settings (Space, HBorder, VBorder), and Rotation Settings (Angle, Steps, Border).
 - Sixth Stage - Output String Processing:** Includes Enable Stage, Letters, Digits, Include these Chars, Exclude these Chars, Min Length, Max Length, lowercase, and UPPERCASE settings.
- Other Options:** Includes Tesseract Language (eng), Delete Image Palette, Computational Captcha, Processed Image Visualization Mode (Extraction Lines), and PreProcess Animated Gifs settings.

The interface also shows a preview of the original image (ABPF) and the processed image (ABPF), along with a Pixel Info section and a Processing Time (ms) of 31. A Test button is visible, and the OCR Code is displayed as ABPF with a Confidence of 40%.



Exdemy.com
Personal property of Keith Samborski
L_my69@yahoo.com

ZDRResearch Advanced Web Hacking

ZDRResearch

www.zdresearch.com

Copyright © Exdemy.com