Authentication and Authorization Attacks

Sentry MBA

ZDResearch
www.zdresearch.com
ZDResearch Advanced Web Hacking

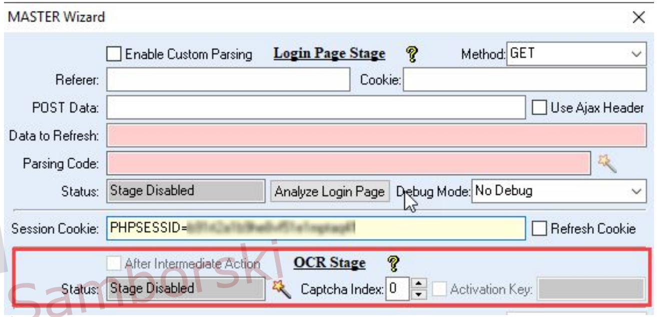
Sentry MBA

- 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

ZDResearch

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:

POST Data: □ Use Ajax Header

Data to Refresh:

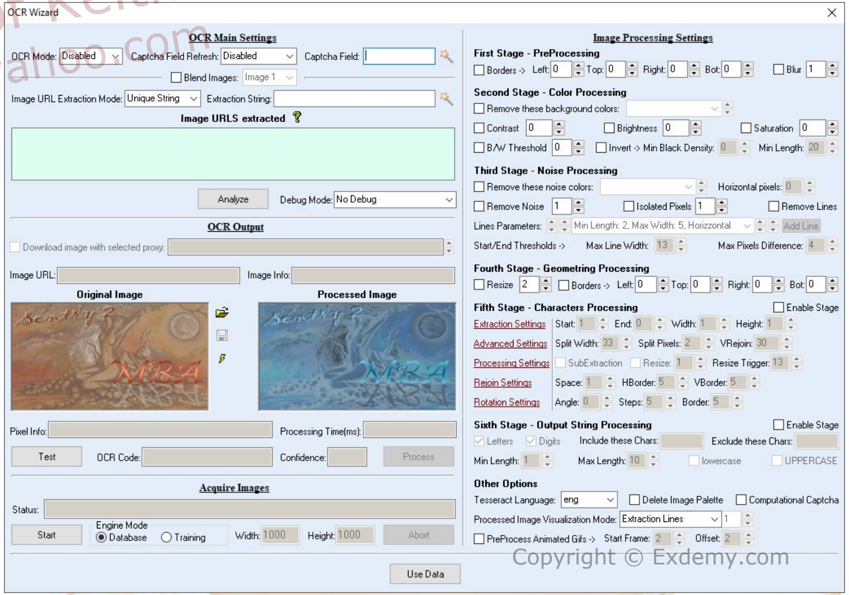
Parsing Code:

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

Session Cookie: PHPSESSID=[redacted] □ Refresh Cookie

□ After Intermediate Action **OCR Stage**

Status: Stage Disabled Captcha Index: 0 □ Activation Key:



OCR Wizard

OCR Main Settings

OCR Mode: Disabled Captcha Field Refresh: Disabled Captcha Field:

□ Blend Images: Image 1

Image URL Extraction Mode: Unique String Extraction String:

Image URLS extracted

Analyze Debug Mode: No Debug

OCR Output

□ 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 Abort

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, Horizzontal Add Line

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

Fourth Stage - Geometring Processing

□ Resize 2 □ Borders -> Left: 0 Top: 0 Right: 0 Bot: 0

Fifth Stage - Characters Processing □ Enable Stage

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

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

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

Rejoin Settings Space: 1 HBorder: 5 VBorder: 5

Rotation Settings Angle: 0 Steps: 5 Border: 5

Sixth Stage - Output String Processing □ Enable Stage

☑ 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 Captcha

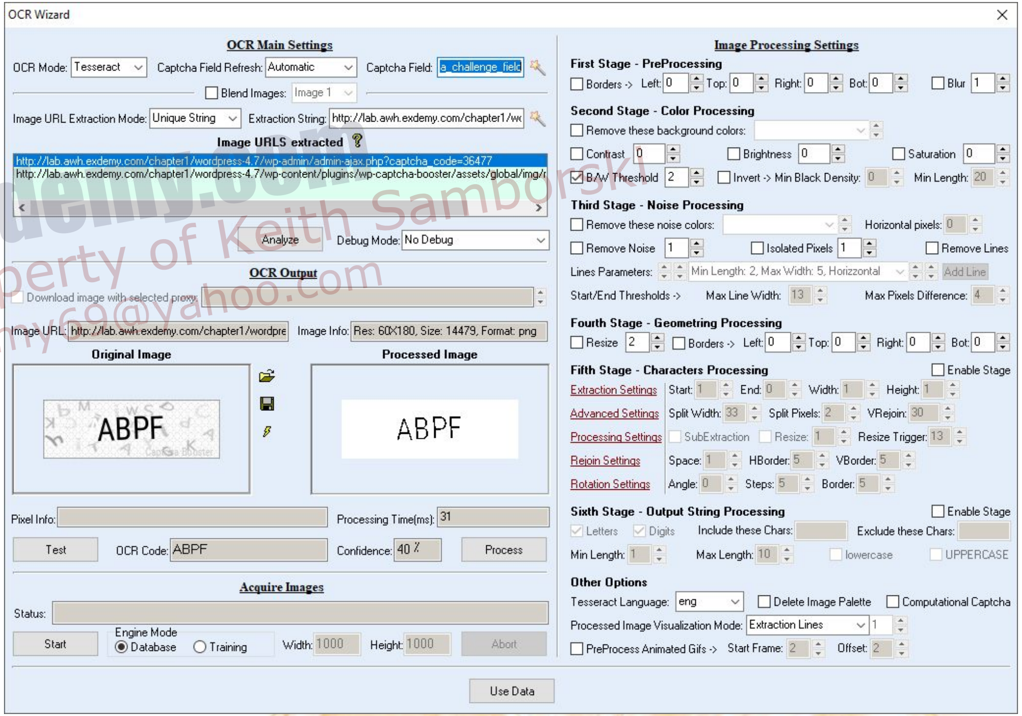
Processed Image Visualization Mode: Extraction Lines 1

□ PreProcess Animated Gifs -> Start Frame: 2 Offset: 2

ZDResearch

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 optimizing 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)



OCR Wizard

OCR Main Settings

OCR Mode: Tesseract Captcha Field Refresh: Automatic Captcha Field: a_challenge_field

□ Blend Images: Image 1

Image URL Extraction Mode: Unique String Extraction String: http://lab.awh.exdemy.com/chapter1/w

Image URLS extracted

http://lab.awh.exdemy.com/chapter1/wordpress-4.7/wp-admin/admin-ajax.php?captcha_code=36477
http://lab.awh.exdemy.com/chapter1/wordpress-4.7/wp-content/plugins/wp-captcha-booster/assets/global/img/r

Debug Mode: No Debug

OCR Output

□ Download image with selected proxy:

Image URL: http://lab.awh.exdemy.com/chapter1/wordpre Image Info: Res: 60X180, Size: 14479, Format: png

Pixel Info: Processing Time(ms): 31

OCR Code: ABPF Confidence: 40 %

Acquire Images

Status:

Engine Mode ● Database ○ Training Width: 1000 Height: 1000

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 2 □ 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, Horizzontal
Start/End Thresholds -> Max Line Width: 13 Max Pixels Difference: 4

Fourth Stage - Geometring Processing
□ Resize 2 □ Borders -> Left: 0 Top: 0 Right: 0 Bot: 0

Fifth Stage - Characters Processing □ Enable Stage
Extraction Settings Start: 1 End: 0 Width: 1 Height: 1
Advanced Settings Split Width: 33 Split Pixels: 2 VRejoin: 30
Processing Settings □ SubExtraction □ Resize: 1 Resize Trigger: 13
Rejoin Settings Space: 1 HBorder: 5 VBorder: 5
Rotation Settings Angle: 0 Steps: 5 Border: 5

Sixth Stage - Output String Processing □ Enable Stage
☑ 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 Captcha
Processed Image Visualization Mode: Extraction Lines 1
□ PreProcess Animated Gifs -> Start Frame: 2 Offset: 2

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com