EyeWitness – Hacker Tools: Hacking through screenshots □□

BY ANNA HAMMOND · JANUARY 11, 2022 · LAST UPDATED ON MARCH 6, 2025

EyeWitness is an incredible tool that allows you to quickly get a feel for what assets to target first. We all know hundreds of content discovery tools that give us vast amounts of data, but do we ever focus on efficiently parsing all that data? How do you go through hundreds of endpoints? If you're doing it manually, then be sure to read this article as EyeWitness may be of great help to you!

□□ What is EyeWitness?

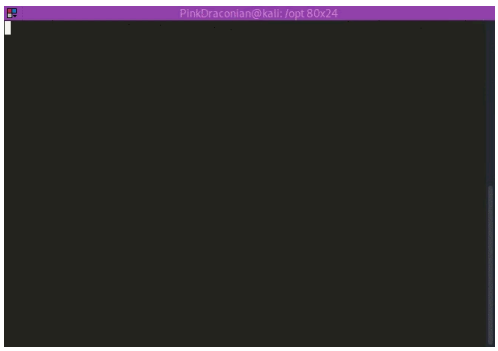
EyeWitness is a Python tool written by @CptJesus and @christruncer. It's goal is to help you efficiently assess what assets of your target to look into first.

It achieves this by taking screenshots of every assets and showing you those screenshots alongside some header information and potential default credentials if applicable.

Reading on what this tool can do is all fun and games, but let's put the tool to the test by using it!

□□ Installing EyeWitness

You can't run a tool without installing it first. Luckily, it's as easy as shown in this GIF.



Installing EyeWitness

As you can see, installing EyeWitness consists of 2 steps:

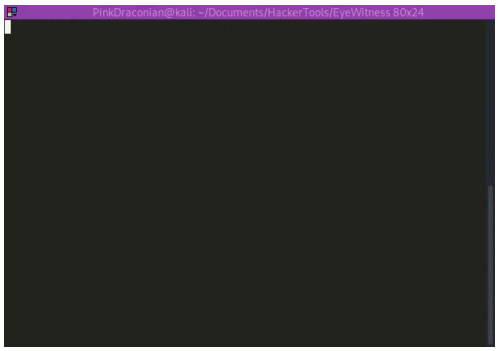
- Clone the repository: `git clone https://github.com/FortyNorthSecurity/EyeWitness.git`
- Run the setup.sh script: `sh EyeWitness/Python/setup/setup.sh`

That's all! If all goes well, you've now successfully installed EyeWitness!

□□ Our first run!

Let's get into it! There's only one obvious thing we still need: A list of domain names to target. This can easily be gotten from one of the reconnaissance tools we've already discussed in the past! Check out our Hacking Tools page in the Intigriti Hackademy!

Now we can execute **eyewitness -f domains.txt** and this will start the tool. Take a look at the gif below to see what such a run looks like.



Running EyeWitness

After executing, the tool will open the result in your browser. Here you can assess the results. Let's discuss them the screenshot below.

The result page starts off by giving us a nice overlay of all everything that it found. In this case we have Unauthorized pages, Not Found pages and Bad requests already filtered out of all the rest. Nice!

Scrolling down, we find screenshots and the headers of all these pages. We can now quickly assess which page we would like to target first!

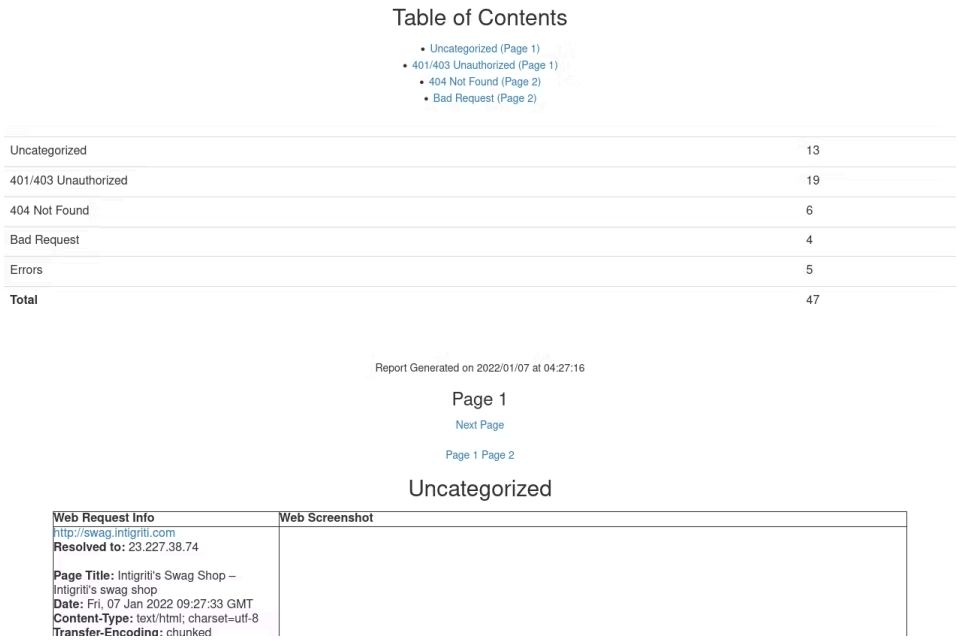


Table of Contents

- Uncategorized (Page 1)
- 401/403 Unauthorized (Page 1)
- 404 Not Found (Page 2)
- Bad Request (Page 2)

Uncategorized	13
401/403 Unauthorized	19
404 Not Found	6
Bad Request	4
Errors	5
Total	47

Report Generated on 2022/01/07 at 04:27:16

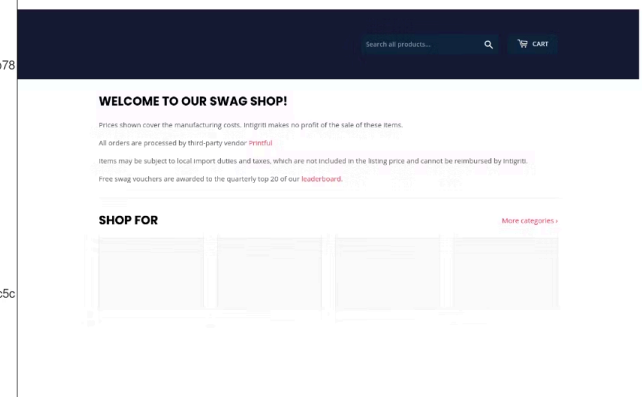
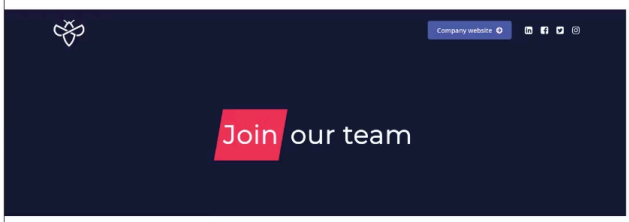
Page 1

Next Page

Page 1 Page 2

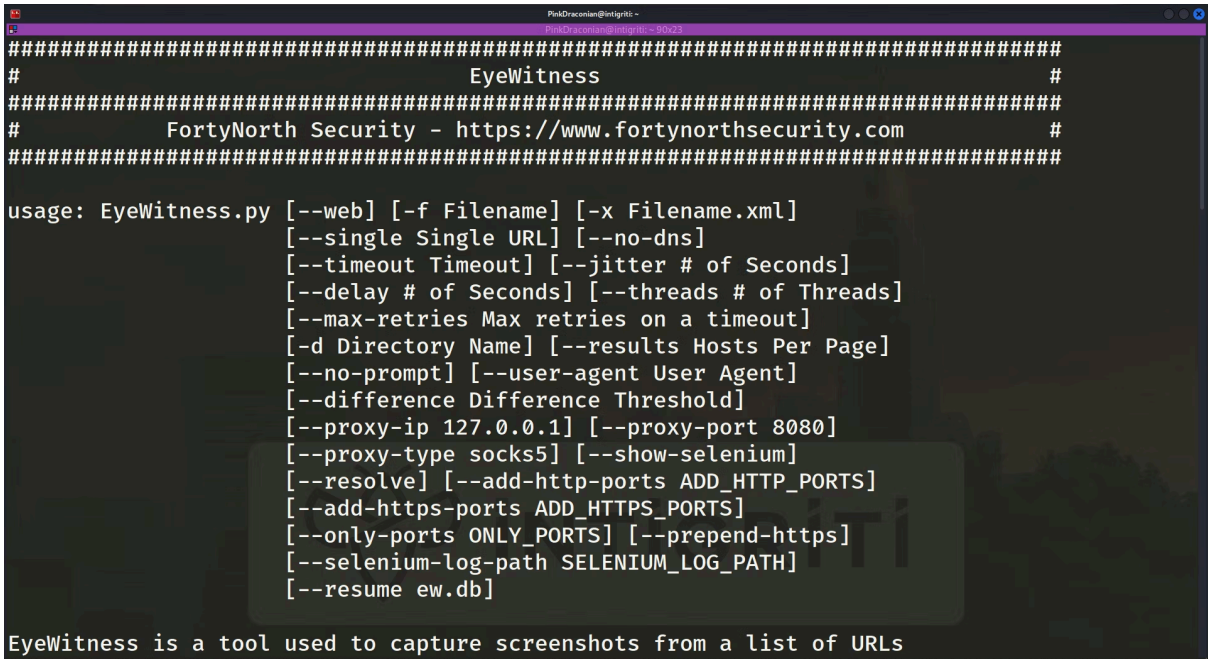
Uncategorized

Web Request Info	Web Screenshot
http://swag.intigriti.com **Resolved to:** 23.227.38.74 **Page Title:** Intigriti's Swag Shop – Intigriti's swag shop **Date:** Fri, 07 Jan 2022 09:27:33 GMT **Content-Type:** text/html; charset=utf-8 **Transfer-Encoding:** chunked	

Web Request Info	Web Screenshot
http://swag.intigriti.com **Resolved to:** 23.227.38.74 **Page Title:** Intigriti's Swag Shop – Intigriti's swag shop **Date:** Fri, 07 Jan 2022 09:27:33 GMT **Content-Type:** text/html; charset=utf-8 **Transfer-Encoding:** chunked **Connection:** close **X-Sorting-Hat-PodId:** 216 **X-Sorting-Hat-ShopId:** 43125932198 **X-Storefront-Renderer-Rendered:** 1 **Set-Cookie:** secure_customer_sig=; path=/; expires=Sat, 07 Jan 2023 09:27:33 GMT; secure; HttpOnly **Link:** <https://cdn.shopify.com>; rel=preconnect, <https://cdn.shopify.com>; rel=preconnect; crossorigin **X-Alternate-Cache-Key:** cacheable:bce6416a7ffb695a64ce881b78eaa6e6 **X-Cache:** hit, server **X-Frame-Options:** DENY **Content-Security-Policy:** block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests; **Strict-Transport-Security:** max-age=7889238 **X-ShopId:** 43125932198 **X-ShardId:** 216 **Content-Language:** en **X-Shopify-Stage:** canary **X-Dc:** gcp-europe-west1,gcp-us-east1,gcp-us-east1 **X-Request-ID:** f981ac14-5d35-4e05-8db5-144c209b9c5c **X-Content-Type-Options:** nosniff **X-Permitted-Cross-Domain-Policies:** none **X-XSS-Protection:** 1; mode=block **X-Download-Options:** noopen **CF-Cache-Status:** DYNAMIC **Expect-CT:** max-age=604800, report-	
Source Code http://careers.intigriti.com **Resolved to:** 35.242.209.60 **Page Title:** Careers - Intigriti **Access-Control-Allow-Methods:** GET, POST, PATCH, DELETE, OPTIONS, HEAD **Access-Control-Allow-Origin:** * **Access-Control-Expose-Headers:** ETag, Content-Length **Access-Control-Max-Age:** 1728000 **Cache-Control:** max-age=0, private, must-revalidate **Content-Type:** text/html; charset=utf-8 **Date:** Fri, 07 Jan 2022 09:27:35 GMT **Etag:** W/"3d2ae0361f7686f223f7669fa7f9b134" **Referrer-Policy:** strict-origin-when-cross-origin **Server:** Caddy **Strict-Transport-Security:** max-age=31536000; **Vary:** Origin **X-Content-Type-Options:** nosniff **X-Download-Options:** noopen **X-Frame-Options:** ALLOWALL **X-Permitted-Cross-Domain-Policies:** none **X-Request-Id:** 62888c09-5885-4bfb-b365-8086cc4e7dbf **X-Runtime:** 0.011275 **X-Xss-Protection:** 1; mode=block **Connection:** close **Transfer-Encoding:** chunked **Response Code:** 200 Source Code	
http://www.careers.intigriti.com **Resolved to:** 35.242.209.60 **Page Title:** Careers - Intigriti **Access-Control-Allow-Methods:** GET, POST, PATCH, DELETE, OPTIONS, HEAD	

Features

Let's take a closer look at some more features that EyeWitness has in store for us!



EyeWitness Usage

Input options

These are the options that can help you input the targets to take screenshots of.

- **-f Filename**
  Line-separated file containing URLs to capture. As seen in the example above.
- **-x Filename.xml**
  Nmap XML or .Nessus file because yes, this tool can parse that output!
- **--single Single URL**
  Single URL/Host to capture. If for some reason you'd only want to scan a single target.
- **--no-dns**
  Skip DNS resolution when connecting to websites. Can be useful in specific cases if you're going through a VPN for example.

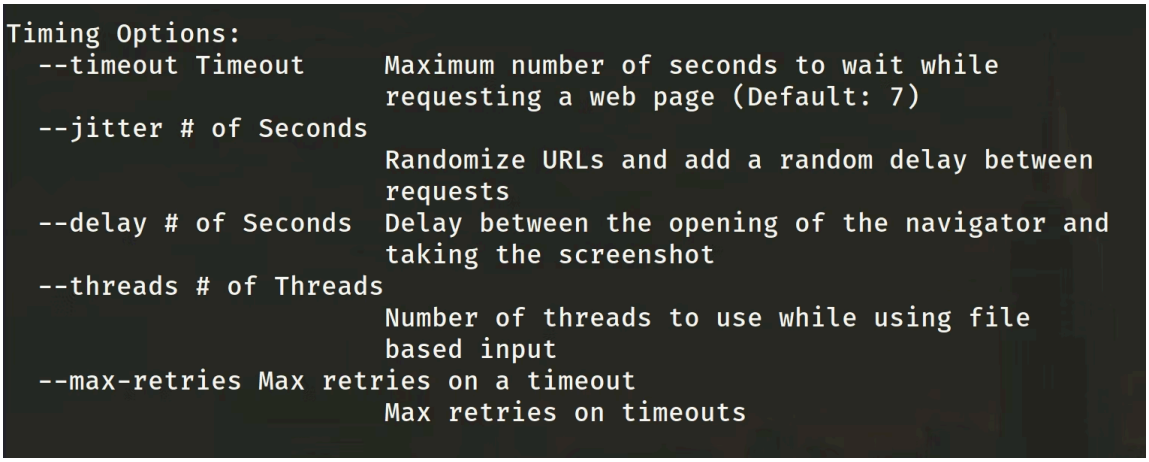
```
Input Options:
  -f Filename           Line-separated file containing URLs to capture
  -x Filename.xml       Nmap XML or .Nessus file
  --single Single URL   Single URL/Host to capture
  --no-dns              Skip DNS resolution when connecting to
                        websites
```

Input Options

Timing Options

Need to go fast, need to slow down? These options help you go to town! Please take a close look at these options as they can help you stay within the required limits of bug bounty programs!

- **--timeout**
  Timeout Maximum number of seconds to wait while requesting a web page (Default: 7).
- **--jitter # of Seconds**
  Randomize URLs and add a random delay between requests.
- **--delay # of Seconds**
  Delay between the opening of the navigator and taking the screenshot.
- **--threads # of Threads**
  Number of threads to use while using file based input.
- **--max-retries Max retries on a timeout**
  Max retries on timeouts.



Timing Options

Report Output Options

Couple of minor options to change the output file.

- **-d Directory Name**
  Directory name for report output
- **--results Hosts Per Page**
  Number of Hosts per page of report
- **--no-prompt**
  Don't prompt to open the report

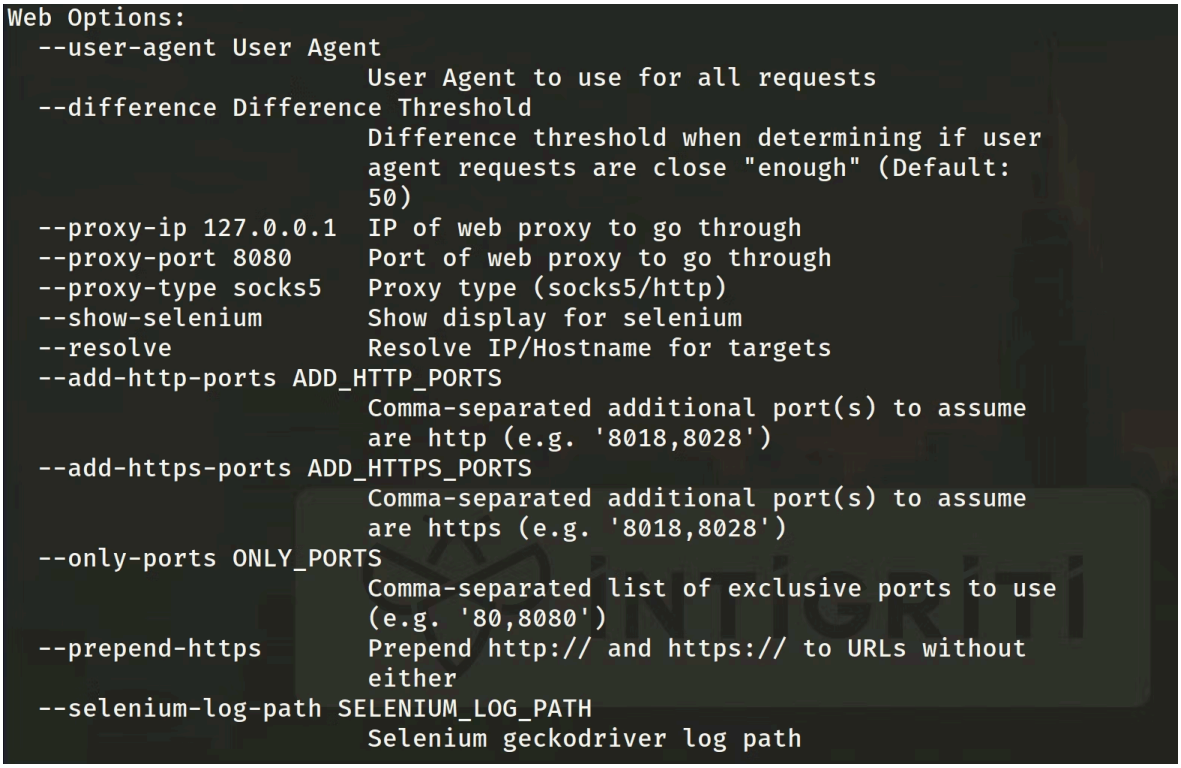
```
Report Output Options:
  -d Directory Name     Directory name for report output
  --results Hosts Per Page
                        Number of Hosts per page of report
  --no-prompt           Don't prompt to open the report
```

Report Output Options

Web Options

These options deal with the way that EyeWitness takes screenshots of the resulting pages. All of this can be configured to handle that HTTP(S) traffic in just the way you want it! Note that some of these options are also required to adhere to some bug bounty program's rules.

- **`--user-agent User Agent`**
  User Agent to use for all requests.
- **`--difference Difference Threshold`**
  Difference threshold when determining if user agent requests are close "enough" (Default: 50).
- **`--proxy-ip 127.0.0.1`**
  IP of web proxy to go through.
- **`--proxy-port 8080`**
  Port of web proxy to go through.
- **`--proxy-type socks5`**
  Proxy type (socks5/http).
- **`--show-selenium`**
  Show display for selenium.
- **`--resolve`**
  Resolve IP/Hostname for targets.
- **`--add-http-ports ADD_HTTP_PORTS`**
  Comma-separated additional port(s) to assume are http (e.g. '8018,8028').
- **`--add-https-ports ADD_HTTPS_PORTS`**
  Comma-separated additional port(s) to assume are https (e.g. '8018,8028')
- **`--only-ports ONLY_PORTS`**
  Comma-separated list of exclusive ports to use (e.g. '80,8080').
- **`--prepend-https`**
  Prepend http:// and https:// to URLs without either
- **`--selenium-log-path SELENIUM_LOG_PATH`**
  Selenium geckodriver log path.



Web Options

Resume Options

This option is a really, really nice one that allows you to resume scanning if your previous scan crashed. When we're dealing with potentially thousands of endpoints, crashes can occur, so this options is a real lifesaver!

- **`--resume ew.db`**
  Path to db file if you want to resume. You can find the database file in the directory (named the current date and time) that EyeWitness automatically creates when running.

Resume Options

Conclusion

EyeWitness is a simple, yet helpful tool designed to help you get more efficient in your post reconnaissance phase! Start using it today to hack even faster!

If you would like to recommend a tool for us to cover next week, then be sure to let us know down below. Also be sure to check out all the previous Hacker Tools articles, such as the last one on GoSpider.

Did you know that there is a video accompanying this article? Check out the playlist!

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com