



Method v.s. Madness

Developing Flexible Automation Workflows

Who Am I

@mhmdiaa on Twitter, GitHub, etc

<https://mhmdiaa.com/projects>

Trickest's Head of Workflows

<https://github.com/trickest>

<https://trickest.com/blog>



Content, content, and more content



Twitter



YouTube



Disclosed Reports



Documentation



Blogs



Conference Talks



GitHub



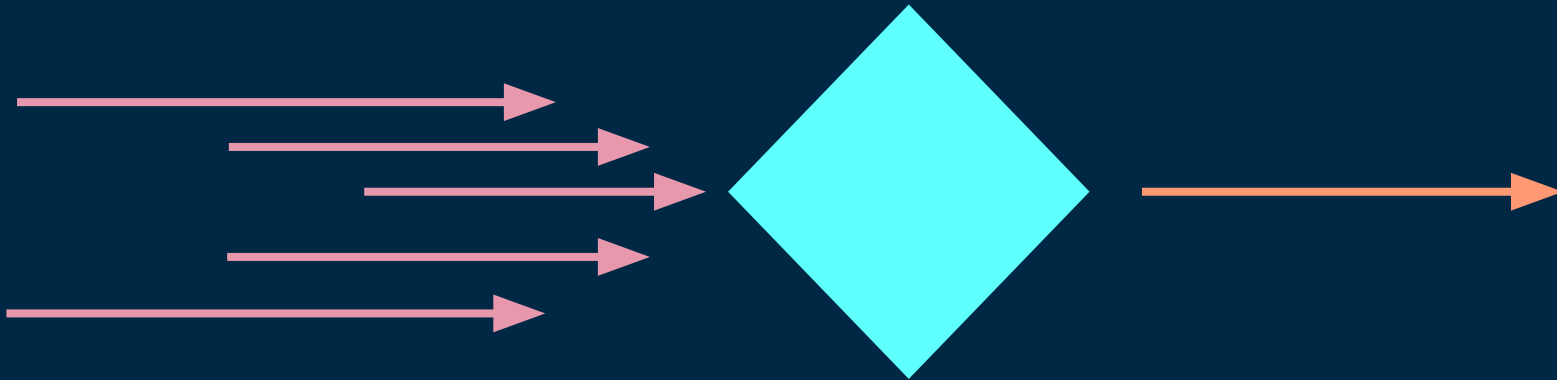
Research



■ which is awesome

BUT...

We Can't Remember Everything



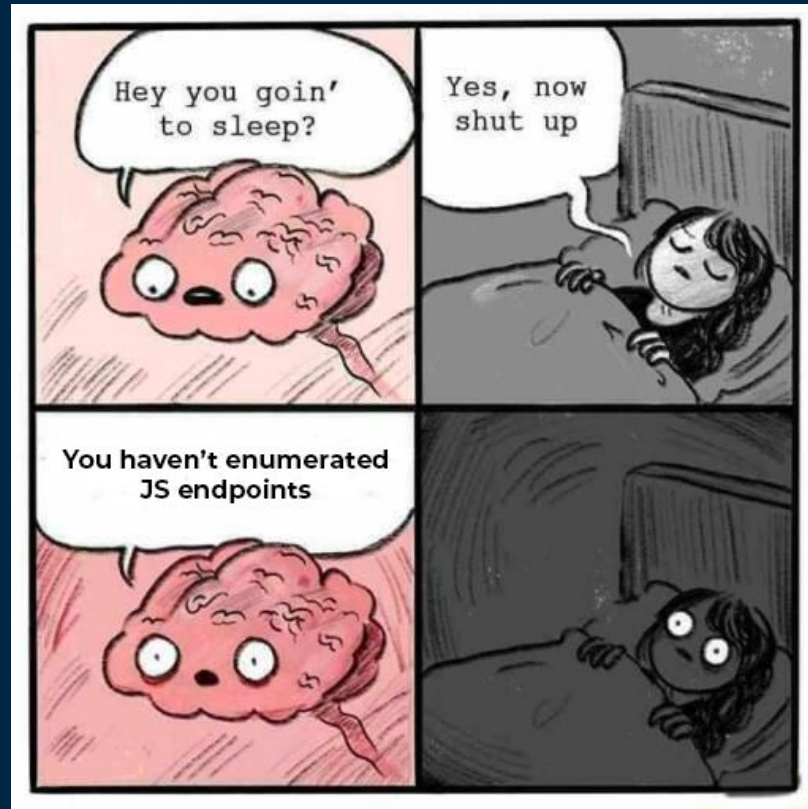


Yay, I got a new
client/BBP invite
Now what?




Prioritize What Matters

We've all been there...



The background features a dark blue field with scattered geometric elements. These include thin white vertical lines of varying lengths, and small squares in teal, orange, and pink. Some squares are solid, while others are hollow outlines. The overall aesthetic is clean and modern.

Help
Others

The background is a dark teal color. It features several vertical white lines of varying lengths. Scattered throughout are small squares in teal, orange, and light blue. Some squares are solid, while others are hollow. The text is centered and consists of three lines: 'Accelerate learning' in orange, 'and be a' in white, and 'better researcher.' in orange.

Accelerate learning
and be a
better researcher.

Solution

The background is a dark blue gradient. It features several vertical white lines of varying lengths. Scattered throughout are small squares in teal, pink, and orange. Some squares are solid, while others are hollow outlines. The word "Solution" is centered in a large, bold, teal font.



■ Build a System
■ around the knowledge

- Not all systems are created equal

Memory

Consume content, **hope** to recall it

01



■ “I’ll just remember it!”

■ —Someone who didn’t remember it, probably

Archive

- Keep track of valuable insights
- By source (Twitter, YouTube, etc)

02

Archive

- Keep track of valuable insights
- By source (Twitter, YouTube, etc)

02

Archive

- Keep track of valuable insights
- ~~By source (Twitter, YouTube, etc)~~

02

Methodology

Structure by *actionability*

03

Automation

- Remove the need for triggers
- Scale, monitor, etc

04

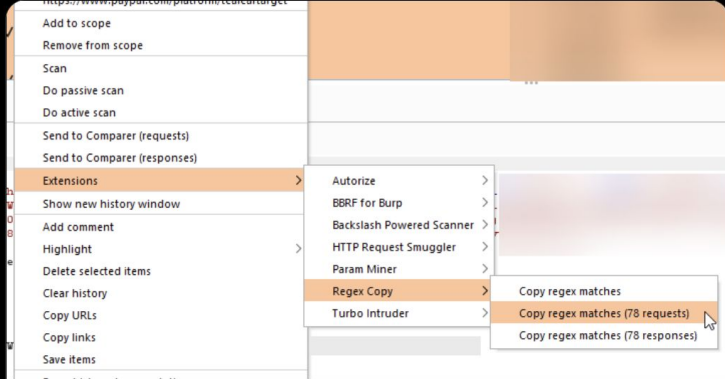
The background is a dark blue field filled with a pattern of small, scattered squares and thin vertical lines. The squares are in three colors: teal, orange, and pink. Some squares are solid, while others are hollow. The lines are thin and white, extending vertically across the frame. The overall aesthetic is modern and minimalist.

Have a bias
for action

Adrien
@adrien_jeanneau

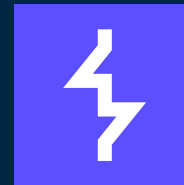
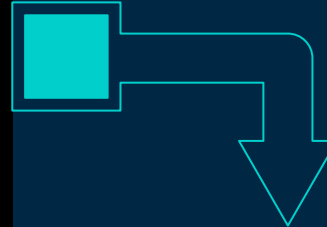
My favorite plugin of the current time for Burp Suite:
Copy Regex Matches (from @honoki)

Very useful to build a custom wordlist for example



The screenshot shows the Burp Suite interface with a context menu open. The 'Extensions' menu item is selected, and a sub-menu is displayed. In this sub-menu, the 'Regex Copy' option is highlighted, which has opened a further sub-menu. This final sub-menu contains three items: 'Copy regex matches', 'Copy regex matches (78 requests)', and 'Copy regex matches (78 responses)'. The first item, 'Copy regex matches', is the one being pointed to by a red arrow from the right.

github.com
GitHub - honoki/burp-copy-regex-matches: Burp Suite plugin to copy regex ma...
Burp Suite plugin to copy regex matches from selected requests and/or responses to the clipboard. - GitHub - honoki/burp-copy-regex-matches: Burp ...

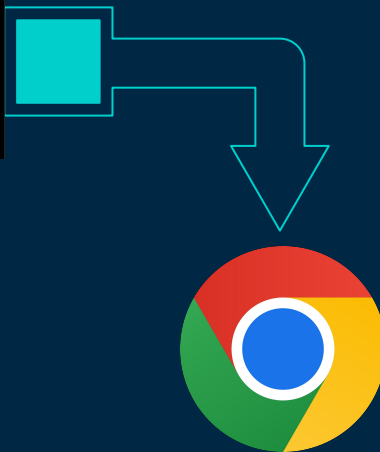




pry0cc.eth // Ben Bidmead

@pry0cc

“Copy URLs” extension for Chrome is one of my favourite all time tools for pentesting





ProjectDiscovery.io

@pdiscoveryio

[NEW-PROJECT] 🥳🥳

Katana — A next-generation crawling and spidering framework.

- Standard / Headless
- Customizable Config
- Scope control
- Output Filters

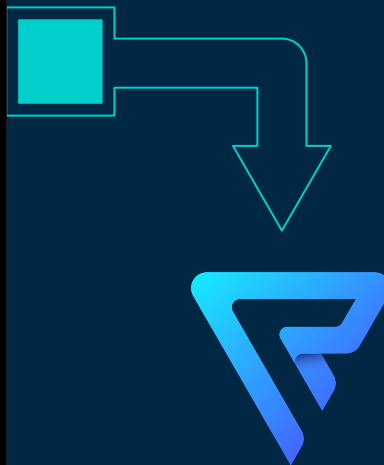
GitHub Project — github.com/projectdiscovery

#hackwithautomation #cybersecurity #crawler
#opensource #bugbounty

```
katana -u https://tesla.com

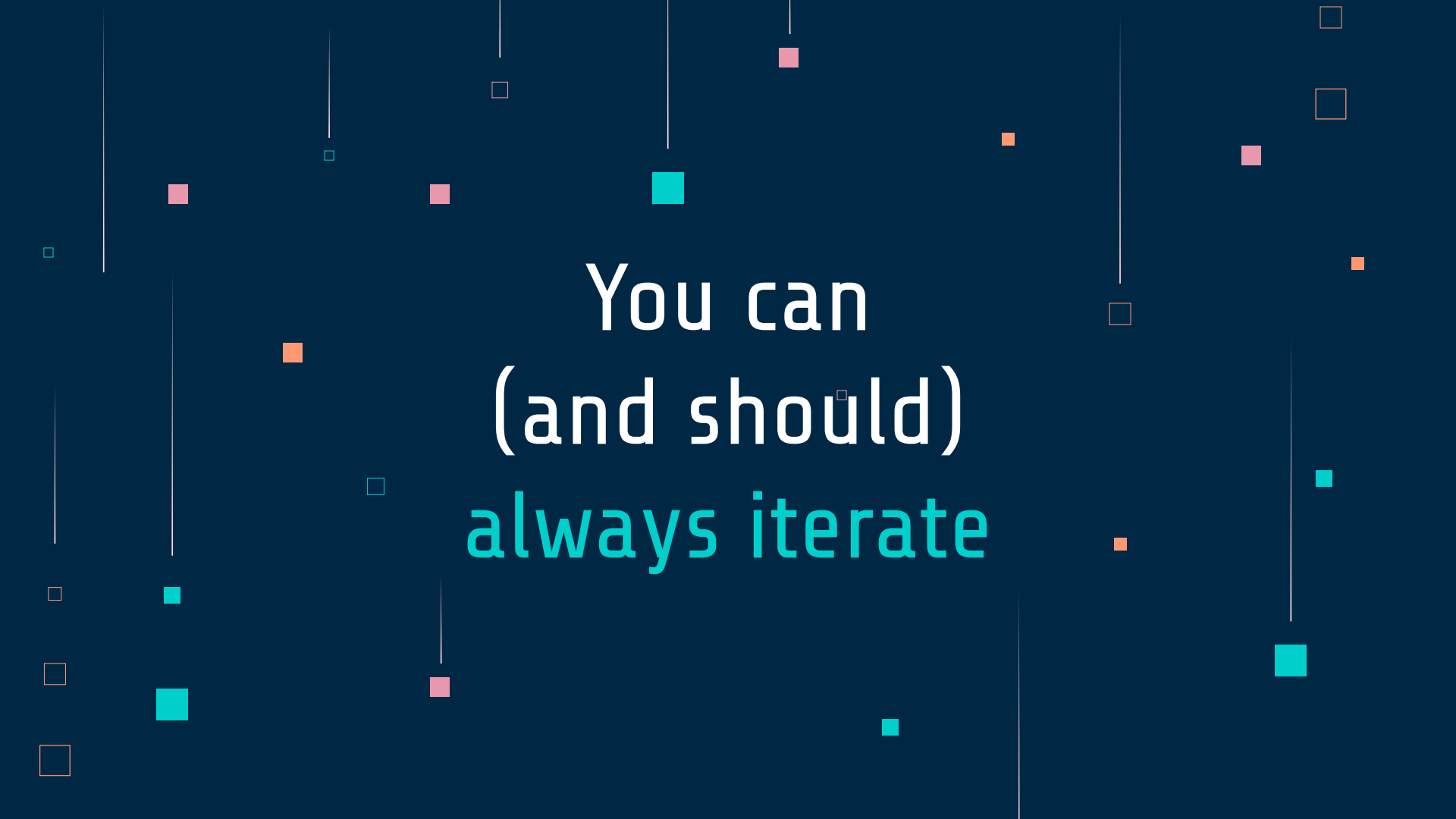
  _____
 /_ _ _ _ _ \
/_ _ _ _ _ \ v0.0.1
  _____
  projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions.
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
https://www.tesla.com/support/taking-delivery?redirect=no
https://www.tesla.com/shop?tesref=true
https://www.tesla.com/modules/custom/tesla_banners/js/index.js?v=1.x
https://www.tesla.com/sv_se/request-virtual-consultation?redirect=no
https://www.tesla.com/pt_PT/event/schedule-virtual-sales-consultation?redirect=no
https://shop.tesla.com/en_ae?redirect=no
https://www.tesla.com/ja_jp/shop?tesref=true
https://www.tesla.com/en_NZ/inventory/used/m3?redirect=no
https://www.tesla.com/en_nz/shop?tesref=true
https://www.tesla.com/zh_hk/event/modely-wmhotel-zhkh?redirect=no
https://www.tesla.com/en_au/shop?tesref=true
https://shop.tesla.com?tesref=true
https://www.tesla.com/de_DE/event/schedule-virtual-sales-consultation?redirect=no
https://www.tesla.com/energy/design?poi=solarroof
https://www.tesla.com/?redirect=no
```



Demo Time!





You can
(and should)
always iterate



Jason Haddix
@Jhaddix

#BountyProTip: found a 401/403, basic auth, or domain that seems interesting but is somehow locked down? Look at its archive.org/web/ entries. Sometimes you win instantly with API keys or URL structure that you can forcefully browse to unprotected content still there.





Jason Haddix
@Jhaddix

#BountyProTip: found a 401/403, basic auth, or domain that seems interesting but is somehow locked down? Look at its archive.org/web/ entries. Sometimes you win instantly with API keys or URL structure that you can forcefully browse to unprotected content still there.

5:00 PM · May 9, 2018

150 Retweets · 1 Quote Tweet · 389 Likes



Tweet your reply

Reply



Mohammed Diaa @mhmdiaa · May 11, 2018

Replying to @Jhaddix

If there are so many entries that you can't go through all of them manually, you can use waybackunifier to get the unique parts out of each snapshot and save them together in a unified file.

mhmdiaa/chronos

Extract pieces of info from a web page's Wayback Machine history



0

Contributors

1

Issue

116

Stars

29

Forks



github.com

GitHub - mhmdiaa/chronos: Extract pieces of info from a web page's ...

Extract pieces of info from a web page's Wayback Machine history -

GitHub - mhmdiaa/chronos: Extract pieces of info from a web page's ...



Mohammed Diaa @mhmdiaa · May 11, 2018

Replying to @Jhaddix

If there are so many entries that you can't go through all of them manually, you can use waybackunifier to get the unique parts out of each snapshot and save them together in a unified file.

mhmdiaa/chronos

Extract pieces of info from a web page's Wayback Machine history



0

Contributors

1

Issue

116

Stars

29

Forks



github.com

GitHub - mhmdiaa/chronos: Extract pieces of info from a web page's ...

Extract pieces of info from a web page's Wayback Machine history -

GitHub - mhmdiaa/chronos: Extract pieces of info from a web page's ...



Jason Haddix
@Jhaddix

#BountyProTip: found a 401/403, basic auth, or domain that seems interesting but is somehow locked down? Look at its archive.org/web/ entries. Sometimes you win instantly with API keys or URL structure that you can forcefully browse to unprotected content still there.





Jason Haddix

@Jhaddix

#BountyProTip: found a 401/403, basic auth, or domain that seems interesting but is somehow locked down? Look at its archive.org/web/ entries. Sometimes you win instantly with API keys or URL structure that you can forcefully browse to unprotected content still there.



Takeaways

- Have a bias for action
- Start with the biggest time sinks
- Don't 100% rely on automation and cancel out your creativity
- It's a journey, not a sprint
- Develop your skills
- Frequently review your methodology and approach with objectivity
- Help others



Thanks!

Questions?

