Axiom is sponsored by SecurityTrails

axiom

The dynamic infrastructure framework for everybody

created by

@pry0cc // Ben Bidmead - 0x00sec.org

presented by

@0xtavian // Octavian

What is axiom?

- Axiom is the dynamic infrastructure framework for everybody - it is designed to be easy to use, intuitive and simple.
- Axiom supports several cloud providers currently, DigitalOcean, Azure, Linode, and IBM Cloud
- Google Compute & AWS support is on the roadmap
- Axiom enables the average weekend warrior or pentesting professional to quickly spin up one or many disposable instances at a time, preloaded with many popular bug bounty & pentesting tools.
- Distributed scanning allows scan times 60x-100x faster than a traditional stand-alone VPS
- I wanted to create something that would enable the average person to compete with enterprise-level solutions, so it is very affordable.
- A standard axiom instance on DigitalOcean will cost you $0.007 per hour to run, and comes with 1GB of ram and a single CPU core.
- 15 instances for 2 hours = 15 * 0.007 * 2 == $0.21 / 21 cents

But why?

- Faster scanning times means you can scan more often, useful for bug bounty.
- Reduce timelines of penetration tests for large external scopes
- Faster scanning means you can throw more data at the problem - bigger wordlists, deeper coverage
- Many different instance IP's, avoid block-lists
- Basically a fully legal botnet.
- Why not?

What does axiom come with?

Tools

- Subfinder
- HTTPx
- DNSx
- Amass
- Nuclei
- Dalfox
- Ffuf
- Shuffledns
- Hakrawler
- Gau
- Meg
- fff
- gowitness
- aquatone
- Many more…

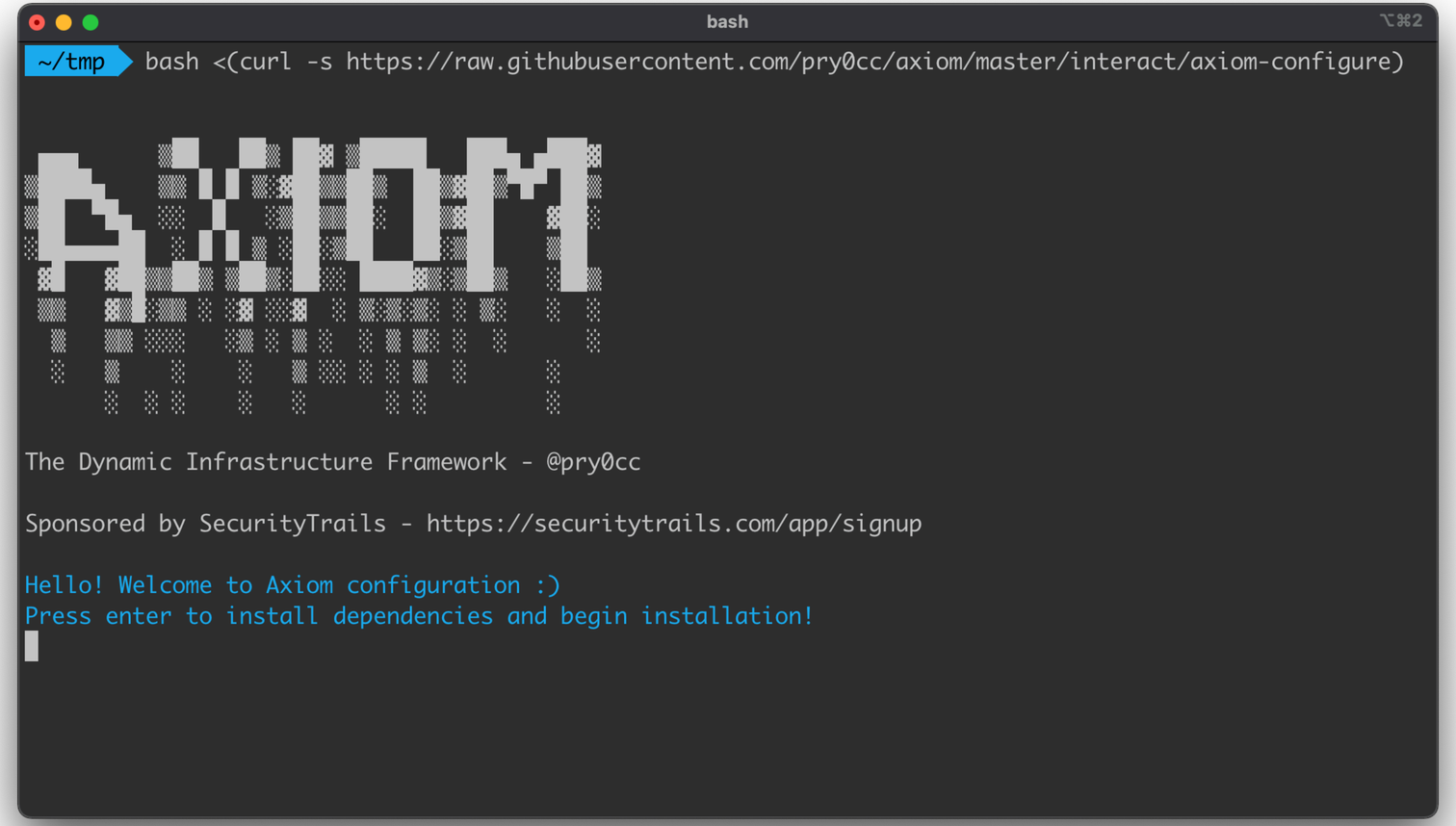
Wordlists

- Assetnote
- SecLists
- Jhaddix-all.txt

Crash Course Introduction

Installation

```
bash <(curl -s https://raw.githubusercontent.com/pry0cc/axiom/master/interact/axiom-configure)
```



https://github.com/pry0cc/axiom/wiki

axiom-init

Initialize a single instance

```
axiom-init
op@home  ~  axiom-init
Initializing 'jarvis21'
>> T-Minus 259 to full initialization...
```

```
op@home: ~
op@home  ~  axiom-init
Initializing 'jarvis21'
Initialized instance 'jarvis21' at '138.197.5.173'!
To connect, run 'axiom-ssh jarvis21' or 'axiom-connect'
✘ op@home  ~
```

axiom-ssh

SSH into an instance

```
op@hoover03: ~                                                    ⌥⌘2
~/tmp  axiom-ssh hoover03                                   12:27:46

Public IP: 159.89.45.179 - Instance: hoover03

hoover03:~:%
```

axiom-fleet -i=15

```
axiom-fleet -i=15                                                    ⌥⌘2
~ axiom-fleet -i=15                                                  11:35:08
Initializing new fleet 'hoover' with 15 instances...
INITIALIZING IN 3 SECONDS, CTRL+C to quit...
Instances: [ hoover01 hoover02 hoover03 hoover04 hoover05 hoover06 hoover07
 hoover08 hoover09 hoover10 hoover11 hoover12 hoover13 hoover14 hoover15  ]
>> T-Minus 382 to fleet hoover initialization...
```

Initialize 15 instances

```
axiom-fleet -i=15                                                    ⌥⌘2
~ axiom-fleet -i=15                                                  11:35:08
Initializing new fleet 'hoover' with 15 instances...
INITIALIZING IN 3 SECONDS, CTRL+C to quit...
Instances: [ hoover01 hoover02 hoover03 hoover04 hoover05 hoover06 hoover07
 hoover08 hoover09 hoover10 hoover11 hoover12 hoover13 hoover14 hoover15  ]
Initialized instance 'hoover15' at '104.248.1.172'!
Initialized instance 'hoover04' at '165.22.38.110'!
Initialized instance 'hoover12' at '134.122.6.54'!
Initialized instance 'hoover06' at '167.172.234.43'!
Initialized instance 'hoover07' at '165.227.216.108'!
Initialized instance 'hoover08' at '64.225.24.23'!
Initialized instance 'hoover05' at '167.71.166.17'!
Initialized instance 'hoover02' at '165.22.40.71'!
Initialized instance 'hoover11' at '134.122.12.242'!
Initialized instance 'hoover14' at '159.89.45.227'!
Initialized instance 'hoover13' at '159.89.45.209'!
Initialized instance 'hoover03' at '159.89.45.179'!
>> T-Minus 221 to fleet hoover initialization...
```

axiom-ls

List your instances

pry@Ghostbook-Air: ~

```
~ axiom-ls                                                                  11:41:08
Instance   IP               Region   Memory       $/M
home       165.227.100.19   nyc3     s-2vcpu-4gb  20
ctf        104.131.0.82     nyc3     s-1vcpu-1gb  5
kevin      134.122.9.34     nyc3     s-1vcpu-1gb  5
jarvis21   138.197.5.173    nyc3     s-1vcpu-1gb  5
hoover01   174.138.58.74    nyc3     s-1vcpu-1gb  5
hoover02   165.22.40.71     nyc3     s-1vcpu-1gb  5
hoover03   159.89.45.179    nyc3     s-1vcpu-1gb  5
hoover04   165.22.38.110    nyc3     s-1vcpu-1gb  5
hoover05   167.71.166.17    nyc3     s-1vcpu-1gb  5
hoover06   167.172.234.43   nyc3     s-1vcpu-1gb  5
hoover08   64.225.24.23     nyc3     s-1vcpu-1gb  5
hoover07   165.227.216.108  nyc3     s-1vcpu-1gb  5
hoover09   159.89.45.186    nyc3     s-1vcpu-1gb  5
hoover10   159.89.45.200    nyc3     s-1vcpu-1gb  5
hoover11   134.122.12.242   nyc3     s-1vcpu-1gb  5
hoover12   134.122.6.54     nyc3     s-1vcpu-1gb  5
hoover13   159.89.45.209    nyc3     s-1vcpu-1gb  5
hoover14   159.89.45.227    nyc3     s-1vcpu-1gb  5
hoover15   104.248.1.172    nyc3     s-1vcpu-1gb  5
_          _                _        Total        $110
~                                                                           ✘ 11:41:09
```

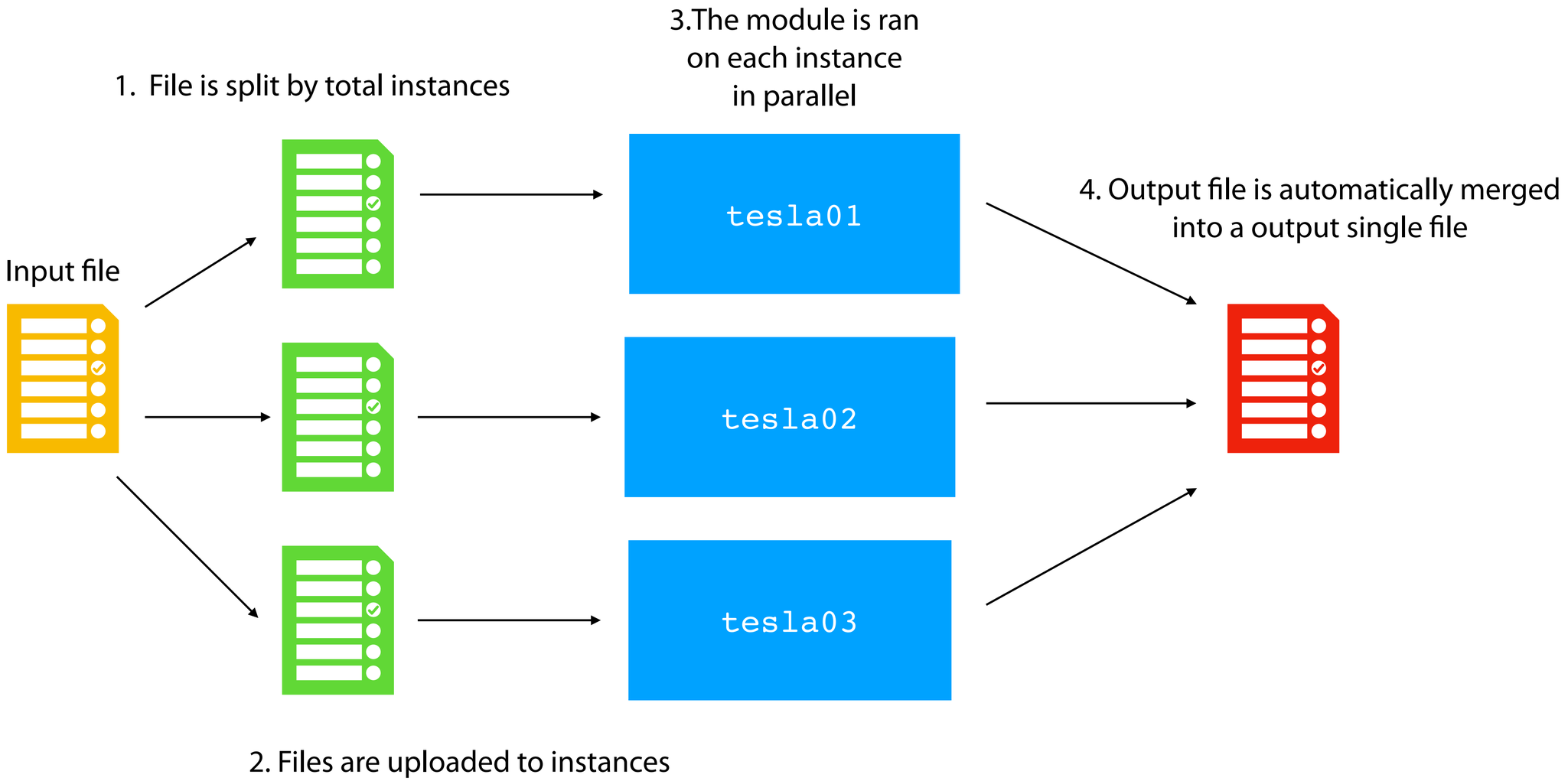
axiom-fleet fire -i=10 --regions=ap-west,ca-central,ap-southeast,us-central,us-west,us-east,eu-west,ap-south,eu-central,ap-northeast

```
user@localhost: ~ — zsh
user@localhost:~$ axiom-fleet fire -i=10 --regions=ap-west,ca-central,ap-southeast,us-c
entral,us-west,us-east,eu-west,ap-south,eu-central,ap-northeast
Cycling through following regions:ap-west,ca-central,ap-southeast,us-central,us-west,us
-east,eu-west,ap-south,eu-central,ap-northeast...
Initializing new fleet 'fire' with 10 instances...
INITIALIZING IN 3 SECONDS, CTRL+C to quit...
Instances: [ fire01 fire02 fire03 fire04 fire05 fire06 fire07 fire08 fire09 fire10  ]
Initialized instance 'fire01' at '192.46.215.212'!
Initialized instance 'fire02' at '172.105.111.169'!
Initialized instance 'fire03' at '172.105.174.217'!
Initialized instance 'fire04' at '172.104.199.119'!
Initialized instance 'fire05' at '192.81.129.150'!
Initialized instance 'fire06' at '45.33.68.46'!
Initialized instance 'fire07' at '178.79.138.17'!
Initialized instance 'fire08' at '192.53.116.56'!
Initialized instance 'fire01' at '192.46.215.212'!
Initialized instance 'fire02' at '172.105.111.169'!
Initialized instance 'fire03' at '172.105.174.217'!
Initialized instance 'fire04' at '172.104.199.119'!
Initialized instance 'fire05' at '192.81.129.150'!
Initialized instance 'fire06' at '45.33.68.46'!
Initialized instance 'fire07' at '178.79.138.17'!
Initialized instance 'fire09' at '45.79.249.103'!
Initialized instance 'fire10' at '139.162.104.25'!
Initialized instance 'fire08' at '192.53.116.56'!
Selected: [ fire01 fire02 fire03 fire04 fire05 fire06 fire07 fire08 fire09 fire10 ]
Fleet started succesfully!
To delete your fleet, just run 'axiom-rm "fire*" -f'
user@localhost:~$
```

```
user@localhost: ~ — zsh
user@localhost:~$ axiom-ls
Instance                IP               Region        Memory  $/M
ubuntu-us-central-001   50.116.26.150    us-central    2048
fire01                  192.46.215.212   ap-west       2048
fire02                  172.105.111.169  ca-central    2048
fire03                  172.105.174.217  ap-southeast  2048
fire04                  172.104.199.119  us-central    2048
fire05                  192.81.129.150   us-west       2048
fire06                  45.33.68.46      us-east       2048
fire07                  178.79.138.17    eu-west       2048
fire09                  45.79.249.103    eu-central    2048
fire10                  139.162.104.25   ap-northeast  2048
fire08                  192.53.116.56    ap-south      2048
-                       -                -             Total   $0
user@localhost:~$
```

Initialize 10 Linode instances, round robin warning - caveats

How distributed scanning works



aHR0cHM6Ly9zZWN1cml0eXRyYWlscy5jb20vYXBwL2FjY291bnQvcHJvbW90aW9ucz9wcm9tb2NvZGU9NjdaQzVSSTVXRAo=

Scan modules

The anatomy of an axiom-scan module

pry@Ghostbook-Air: ~/tmp ⌥⌘2

```
~/tmp  cat ~/.axiom/modules/httpx.json | jq                    12:14:11
[
  {
    "command": "cat input | /home/op/go/bin/httpx -o output",
    "ext": "txt"
  }
]
~/tmp                                                          12:14:11
```

Oneshot modules

For tools that take a single target as input

pry@Ghostbook-Air: ~/tmp

```
~/tmp  cat ~/.axiom/modules/nmapx.json | jq                    12:16:13
[
  {
    "command": "sudo nmap -v _target_ -oG _output_/_target_.txt",
    "ext": "txt",
    "threads": 15
  },
  {
    "command": "sudo nmap -v _target_ -oX _output_/_target_.xml",
    "ext": "xml",
    "threads": 15
  },
  {
    "command": "sudo nmap -v _target_ -oN _output_/_target_.nmap",
    "ext": "dir",
    "threads": 15
  }
]
~/tmp                                                          12:16:16
```

axiom-scan --list

List your available axiom-scan modules

pry@Ghostbook-Air: ~

```
~ axiom-scan --list                                                                                                                    11:50:33
Available Modules:
MODULE                                COMMAND
/Users/pry/.axiom/modules//soxy       cat input | /home/op/bin/soxy | tee output
/Users/pry/.axiom/modules//amass      /usr/bin/amass enum -df input -o output
/Users/pry/.axiom/modules//meg        /home/op/go/bin/meg -v / input output
/Users/pry/.axiom/modules//nuclei     /home/op/go/bin/nuclei -silent -update-templates ; cat input | /home/op/go/bin/nuclei -t _wordlist_ -o output
/Users/pry/.axiom/modules//gau        cat input | /home/op/go/bin/gau | tee output
/Users/pry/.axiom/modules//ffuf       /home/op/go/bin/ffuf -t 150 -w _wordlist_ -u '_target_/FUZZ' -of csv -o _output_/_cleantarget_ -ac
/Users/pry/.axiom/modules//gowitness  gowitness file -f input -P output
/Users/pry/.axiom/modules//findomain  /usr/bin/findomain -f input -u output
/Users/pry/.axiom/modules//arjun      /usr/local/bin/arjun -i input -oT output
/Users/pry/.axiom/modules//masscan    sudo masscan -iL input -oG output
/Users/pry/.axiom/modules//dnsx       cat input | /home/op/go/bin/dnsx -silent -r /home/op/lists/resolvers.txt -o output
/Users/pry/.axiom/modules//gospider   cat input | /home/op/go/bin/gospider -S - --depth 3 -v -t 50 -c 3 -o output
/Users/pry/.axiom/modules//hakrawler  cat input | /home/op/go/bin/hakrawler | tee output
/Users/pry/.axiom/modules//feroxbuster /usr/bin/feroxbuster -u _target_ -w _wordlist_ -o _output_/_cleantarget_
/Users/pry/.axiom/modules//subfinder  /home/op/go/bin/subfinder -silent -d _target_ -o _output_/_target_
/Users/pry/.axiom/modules//rustscan   /usr/bin/rustscan -a input -g | tee output
/Users/pry/.axiom/modules//shuffledns echo _target_ | /home/op/go/bin/shuffledns -v -d _target_ -r /home/op/lists/resolvers.txt -w _wordlist_ -o _output_/_target_
/Users/pry/.axiom/modules//ffuz       cat input | /home/op/bin/ffuz -s -o output
/Users/pry/.axiom/modules//fff        cat input | /home/op/go/bin/fff | tee output
/Users/pry/.axiom/modules//httprobe   cat input | /home/op/go/bin/httprobe | tee output
/Users/pry/.axiom/modules//cngo       /home/op/go/bin/cngo -f input | tee output
/Users/pry/.axiom/modules//naabu      cat input | /home/op/go/bin/naabu -o output
/Users/pry/.axiom/modules//nmap       sudo nmap -iL input -oG output
/Users/pry/.axiom/modules//massdns    sudo /usr/bin/massdns -r /home/op/lists/resolvers.txt -t A -o F input -w output
/Users/pry/.axiom/modules//gorgo      /home/op/bin/gorgo.py -i input -o output
/Users/pry/.axiom/modules//dnsgen     cat input | dnsgen - | tee output
/Users/pry/.axiom/modules//httpx      cat input | /home/op/go/bin/httpx -o output
/Users/pry/.axiom/modules//dalfox     /home/op/go/bin/dalfox file input -o output
/Users/pry/.axiom/modules//tlscout    cat input | /home/op/go/bin/tlscout -o output
/Users/pry/.axiom/modules//nmapx      sudo nmap -v _target_ -oG _output_/_target_.txt
~                                                                                                                                      11:50:40
```

axiom-scan input.txt -m module -o output.txt

Scan your input using selected module

axiom-scan subdomains.txt -m httpx -o http

```
                _
  ____ __  __(_)___  ____ ___       _____________ _____
 / __ `/ |/_/ / __ \/ __ `__ \_____/ ___/ ___/ __ `/ __ \
/ /_/ />  </ / /_/ / / / / / /_____(__  ) /__/ /_/ / / / /
\__,_/_/|_/_/\____/_/ /_/ /_/     /____/\___/\__,_/_/ /_/

                                  @pry0cc

Module: [ httpx  ] | Input: [ 28968 targets ] | Instances: 15 [ hoover01 hoover02 hoover03 hoover04 hoover05 hoover06 hoo
ver07 hoover08 hoover09 hoover10 hoover11 hoover12 hoover13 hoover14 hoover15 ]
Command: [ cat input | /home/op/go/bin/httpx -o output ] | Ext: [txt]
Building file structure...[ OK ]
Uploading input files...
 80%|                                                                                | 12/15 [00:00<00:00, 106.72it/s]
```

axiom-rm ‘query*’

Delete your instances

```
pry@Ghostbook-Air: ~/tmp                                    ⌥⌘2
~/tmp  axiom-rm 'knox*' -f                          ✘  12:41:31
Deleting 'knox01'...
Deleting 'knox02'...
Deleting 'knox03'...
Deleting 'knox04'...
Deleting 'knox05'...
Deleting 'knox06'...
Deleting 'knox07'...
Deleting 'knox08'...
Deleting 'knox09'...
Deleting 'knox10'...
~/tmp                                               12:41:45
```

Live Demo

Q & A

aHR0cHM6Ly9zZWN1cml0eXRyYWlscy5jb20vYXBwL2FjY291bnQvcHJvbW90aW9ucz9wcm9tb2NvZGU9NjdaQzVSSTVXRAo=

Thank you!

twitter.com/0xtavian
github.com/pry0cc/axiom
github.com/0xtavian

AXIOM IS SPONSORED BY

SecurityTrails