

# Passive-ish Recon Techniques



@TomNomNom

# Me

Just someone who hunts bugs for fun.

I <3 questions

[ <https://twitter.com/tomnomnom> ]

[ <https://github.com/tomnomnom> ]

[ <https://hackerone.com/tomnomnom> ]

# Passive... Ish?

*Reconnaissance that doesn't connect to the target.*

*...Or is mostly indistinguishable from 'normal' browsing traffic.*

# Mostly It's Asset Identification

- What's the target's footprint?
- Domains?
- Subdomains?
- IP Ranges?
- 3rd Party Accounts?
  - ◆ Source Code Hosting
  - ◆ Continuous (Integration|Deployment) Systems
  - ◆ Bug Trackers
- Employees\* (:

...But It Can Be *Anything*

*“Knowledge is power”*

- Some Wise Dude

# Subdomains

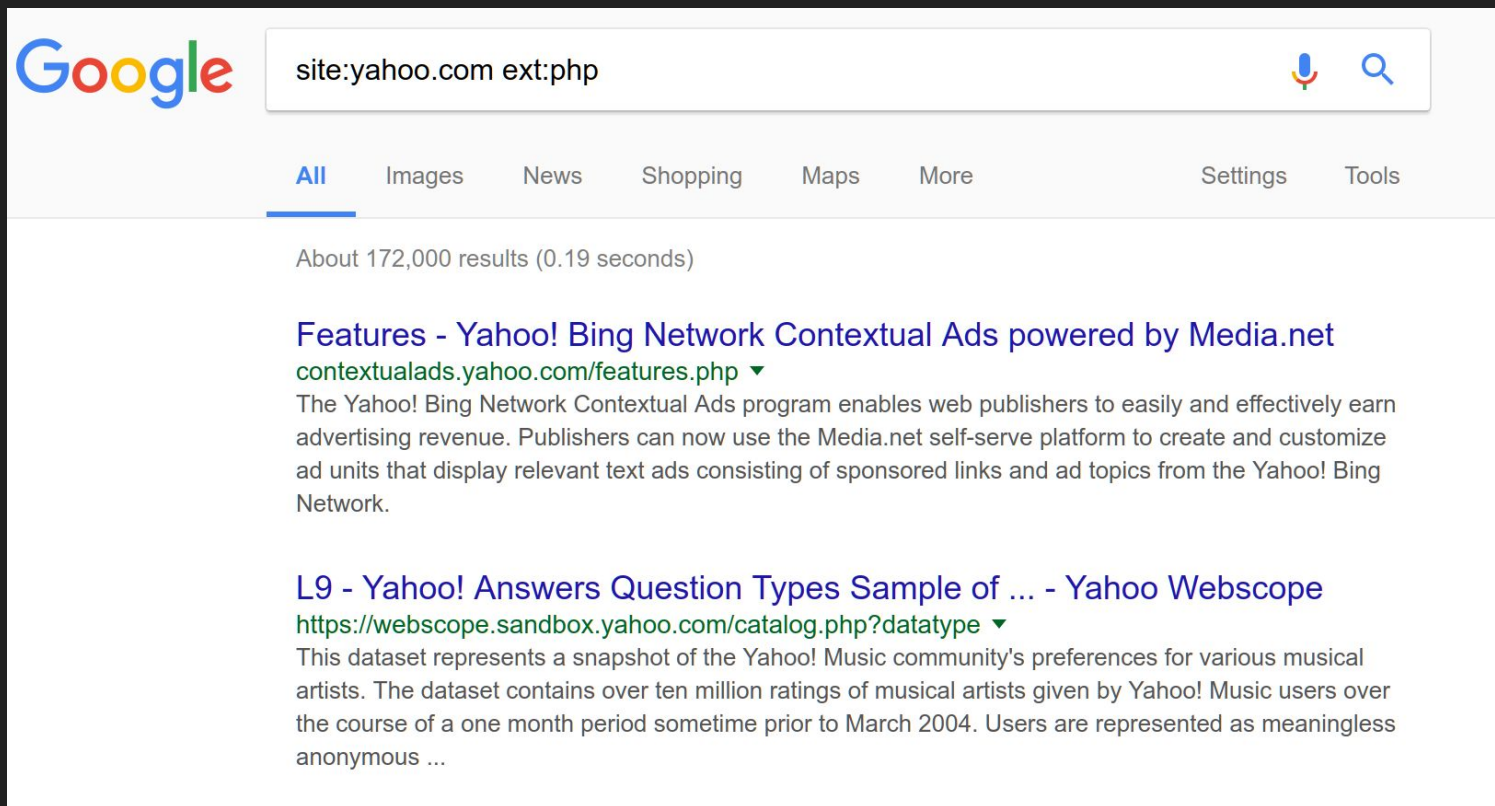
- Brute force\* (recon-ng is good)
- <https://dnsdumpster.com>
- <https://www.threatcrowd.org>
- <https://www.censys.io>
- <https://www.zoomeye.org>
- Rapid7 FDNS Logs ([https://scans.io/study/sonar.fdns\\_v2](https://scans.io/study/sonar.fdns_v2))
- Certificate Transparency (<https://crt.sh>)
- Google :)
- Bing :o
- CSP Headers?

# CSP Headers

× Headers Preview Response Cookies Timing

```
content-security-policy: default-src 'none'; base-uri 'self'; block-all-mixed-content; child-src www.youtube-nocookie.com app-sj17.marketo.com; connect-src 'self' hackerone.com *.mktresourc.p.com checkout.stripe.com; font-src 'self'; form-action 'self' syndication.twitter.com platform.twitter.com; frame-ancestors 'self'; frame-src www.youtube.com www.youtube-nocookie.com app-sj17.marketo.com boards.greenhouse.io platform.twitter.com syndication.twitter.com checkout.stripe.com; img-src 'self' data: www.google-analytics.com syndication.twitter.com platform.twitter.com *.twimg.com q.stripe.com; media-src 'self'; script-src 'self' www.google-analytics.com app-sj17.marketo.com munchkin.marketo.net boards.greenhouse.io platform.twitter.com cdn.syndication.twimg.com checkout.stripe.com; style-src 'self' 'unsafe-inline' app-sj17.marketo.com boards.greenhouse.io boards-us1-cdn.greenhouse.io platform.twitter.com checkout.stripe.com; report-uri https://errors.hackerone.net/api/30/csp-report/?sentry_key=61c1e2f50d21487c97a071737701f598
```

# Google Dorking



The image shows a Google search interface. The search bar contains the query "site:yahoo.com ext:php". Below the search bar, there are navigation tabs for "All", "Images", "News", "Shopping", "Maps", "More", "Settings", and "Tools". The "All" tab is selected. Below the tabs, it says "About 172,000 results (0.19 seconds)". There are two search results displayed:

- Features - Yahoo! Bing Network Contextual Ads powered by Media.net**  
[contextualads.yahoo.com/features.php](https://contextualads.yahoo.com/features.php) ▼  
The Yahoo! Bing Network Contextual Ads program enables web publishers to easily and effectively earn advertising revenue. Publishers can now use the Media.net self-serve platform to create and customize ad units that display relevant text ads consisting of sponsored links and ad topics from the Yahoo! Bing Network.
- L9 - Yahoo! Answers Question Types Sample of ... - Yahoo Webscope**  
<https://webscope.sandbox.yahoo.com/catalog.php?datatype> ▼  
This dataset represents a snapshot of the Yahoo! Music community's preferences for various musical artists. The dataset contains over ten million ratings of musical artists given by Yahoo! Music users over the course of a one month period sometime prior to March 2004. Users are represented as meaningless anonymous ...



# Google Dorking++

Google

site:pastebin.com "[REDACTED]".net

All News Videos Shopping Images More Settings Tools

6 results (0.27 seconds)

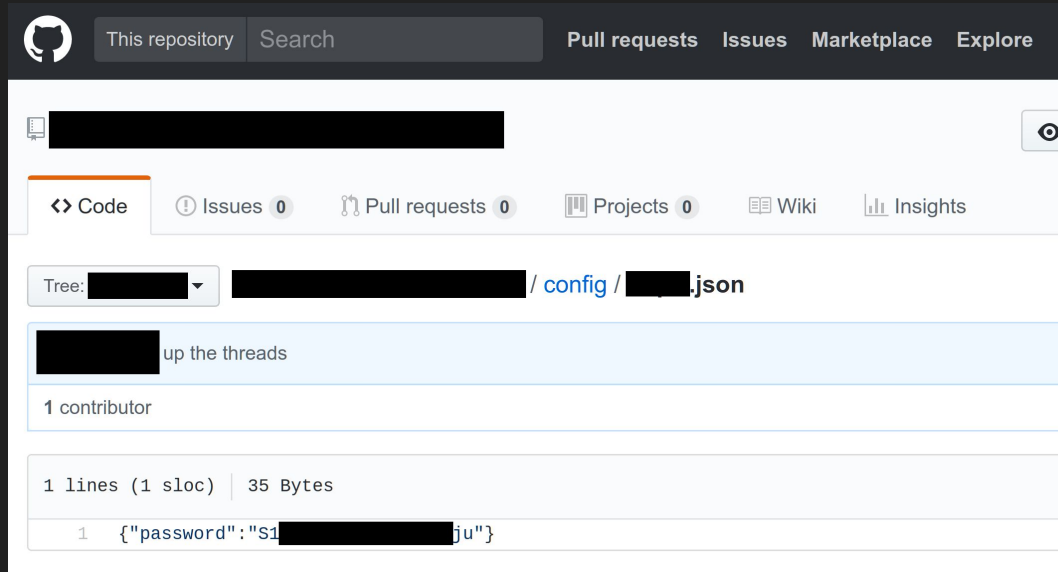
**Host £\* ForwardAgent yes ProxyCommand ssh [REDACTED].net nc**  
<https://pastebin.com/ss3CMRhi> ▾  
16 Jun 2017 - ProxyCommand ssh [REDACTED].net nc \$(echo %h | awk -F£ '{print \$2}') %p.  
RAW Paste Data. Host £\* ForwardAgent yes ProxyCommand ssh [REDACTED].net nc \$(echo %h | awk -F£ '{print \$2}') %p. create new paste / deals <sup>new!</sup> / api / trends / syntax languages / faq / tools / privacy / cookies ...  
You've visited this page 2 times. Last visit: 21/01/18

**[Java] # Configuration for cowbell in production mode # Over-all ...**  
<https://pastebin.com/LnRFXfh> ▾  
6 Jun 2017 - DO NOT set apollo.domain, it will be populated by Helios in production! # Set it in cowbell-user.conf for development. logIncomingRequests: true. logOutgoingRequests: true. } # Hermes client settings. # https://ghe [REDACTED]/apollo/apollo-modules/blob/master/modules/hermes/README.md#hermes-client.  
You've visited this page 2 times. Last visit: 21/01/18

# Read The Source, Luke

- Open source projects
  - ◆ Don't forget GitLab et al!
- Forked repos
- Client-side JavaScript
  - ◆ DOM XSS and its ilk
  - ◆ Endpoints. Endpoints everywhere
- `grep` is your friend :)
  - ◆ `passw(d|ord)`
  - ◆ `api[_-]?key`
  - ◆ `authorization`

# Truffle Hunting



The screenshot shows a GitHub repository page for a repository named [REDACTED]. The repository is public and has 0 pull requests, 0 issues, 0 projects, and 0 wiki pages. The file being viewed is `config/[REDACTED].json`. The file content is as follows:

```
1 {"password": "S1[REDACTED]ju"}
```

The file is 35 bytes and contains 1 line of code (1 sloc). The repository has 1 contributor.

[ <https://github.com/dxa4481/truffleHog> ]

# Android Apps

```
tom@girru:~/src/github.com/skylot/jadx/build/jadx (master)▶ ./bin/jadx -d output ~/recon/target/classes.dex
20:15:07 INFO - loading ...
20:15:07 WARN - Unknown 'R' class, create references to 'R'
20:15:07 INFO - processing ...
20:15:08 WARN - Several 'all' handlers in try/catch block in com.a.a.a.d.b(java.net.Socket):boolean
20:15:08 WARN - Several 'all' handlers in try/catch block in com.a.a.a.d.b(java.net.Socket):boolean
20:15:08 WARN - No exception handlers in catch block, method: com.flurry.android.f.a(com.flurry.android.f, a
20:15:08 WARN - No exception handlers in catch block, method: com.flurry.android.f.d(com.flurry.android.f):v
```

```
tom@girru:~/src/github.com/skylot/jadx/build/jadx/output (master)▶ grep -Hnri authorization
/d/di.java:61:         r0 = "Authorization";         Catch:{ all -> 0x00c8, ab -> 0x00cd, UnknownHostE:
/d/dd.java:113:         httpPost.setHeader("Authorization", "Basic am          NO");
/d/df.java:41:         httpGet.setHeader("Authorization", "Basic am          NO");
```

[ <https://github.com/skylot/jadx> ]

# Androids Dream Of Basic Auth

```
HttpRequest httpGet = new HttpGet(k.a("https://jira.██████████.com/rest/api/2/user/search?username=%s", this.b));  
httpGet.setHeader("Accept", "application/json");  
httpGet.setHeader("Content-Type", "application/json");  
httpGet.setHeader("Authorization", "Basic am██████████NO");
```

The screenshot shows a web browser window displaying the JIRA user profile for 'JIRA Bot'. The browser's address bar shows the URL: `https://jira.██████████.com/secure/ViewProfile.jspa`. The page has a navigation bar with 'Dashboards', 'Projects', 'Issues', 'Boards', 'Portfolio', 'TestRail', and a 'Create' button. The main content area is titled 'Profile: JIRA Bot' and includes a 'Tools' dropdown. Below the title is a 'Summary' section with a 'Filters' dropdown. The 'Details' section on the left shows the user's avatar (a robot), username 'jirabot', administration role 'Administer User', full name 'JIRA Bot', email 'jirabot@██████████', and groups 'jira-administrators', 'jira-developers', and 'jira-users'. The 'Preferences' section on the left lists settings such as Page Size (500), Email Type (Text), Language (██████████), Time Zone (██████████), My Changes (Notify me), Filter and Dashboard (Unshared), Sharing, Keyboard shortcuts (Enabled), and Autowatch (Inherit from global settings). The 'Activity Stream' section on the right shows a list of activities from 'Yesterday', including 'JIRA Bot attached 9 files to ██████████' and 'JIRA Bot created ██████████'. The file list includes 'history.json', 'selectedirection.json', 'sem.json', 'userState.json', 'favorites.json', 'apiRequests.json', 'experiments.txt', and 'networkinfo.json'. Another activity shows 'JIRA Bot attached 13 files to ██████████' with files like 'selectedFeed.json', 'ads.json', and 'notificationFeed.json'.

Enhance!

Groups: `jira-administrators`  
`jira-developers`  
`jira-users`

# Wayback When

```
tom@bash:~▶ echo "[REDACTED].com" | waybackurls > urls
```

```
tom@bash:~▶ grep -iE '=[^&]+/' urls
```

```
http://www.[REDACTED].com/story_get.cgi?STORY_NAME=s[REDACTED]/06/02/01/m[REDACTED].html
```

```
http://www.[REDACTED].com/story_get.cgi?STORY_NAME=s[REDACTED]/06/07/26/S0[REDACTED]n.html
```

```
http://www.[REDACTED].com/story_get.cgi?STORY_NAME=s[REDACTED]/10/09/29/S0[REDACTED]A.html
```

[ <https://github.com/tomnomnom/waybackurls> ]

# Link Shorteners

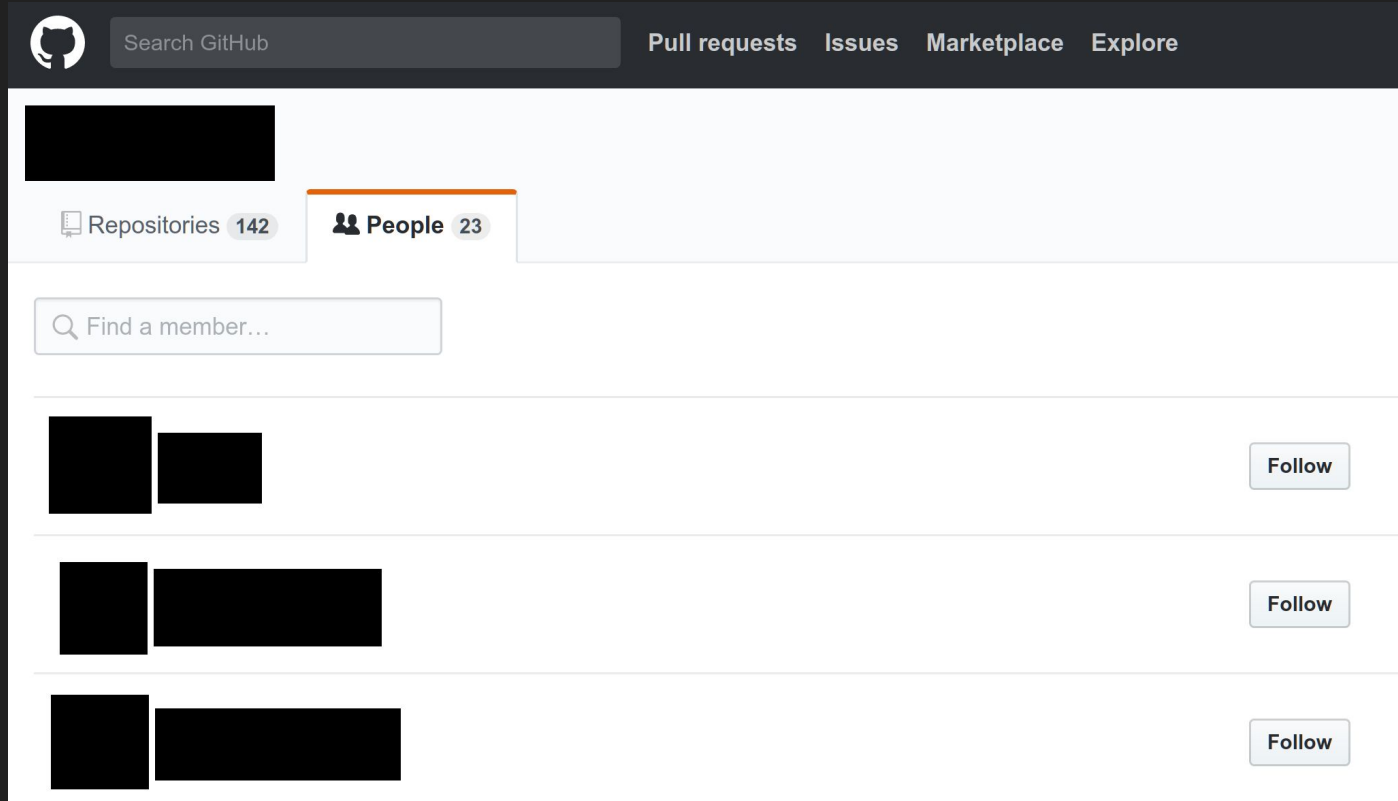
```
tom@girru:~► grep -aiE '\|https?://[a-z0-9\.-]+\.\mil/' tinyurls.txt | grep -i =http
0zt0axp|https://medsharevm.ermc.amedd.army.mil/sites/LRMC/DCCS/surg/Telehealth/Lists/Additional%
es%2FLRMC%2FDCCS%2Fsurg%2FTelehealth%2FLists%2FAdditional%2520Documents%2FAllItems%2Easp
717fv3m|http://www.marines.mil/Pages/PhotoDetails.aspx?ItemUrl=http://www.marines.mil/unit/2ndml
```

```
tom@girru:~► grep -aiE 'passw(d|ord)=[^&]+' tinyurls.txt | tail
password=200603318
password=hugoandres2483
password=Funky1123
password=AllyNa20
password=chenyong
passwd=grupp
password=Skopje13
password=Rhubarb4
password=z840248291
passwd=grupp
```

[ <https://archive.org/search.php?query=subject:urlteam> ]



# The GitHub Goldmine



The screenshot displays the GitHub interface for an organization. At the top, there is a dark navigation bar with the GitHub logo on the left, a search bar labeled "Search GitHub", and navigation links for "Pull requests", "Issues", "Marketplace", and "Explore". Below the navigation bar, the organization's profile is shown with a large blacked-out header image. Two tabs are visible: "Repositories 142" and "People 23", with the "People" tab selected and highlighted in orange. A search bar with the placeholder text "Find a member..." is positioned below the tabs. The main content area lists three members, each with a profile picture (blacked out), a name (blacked out), and a "Follow" button.

Search GitHub

Pull requests Issues Marketplace Explore

Repositories 142 **People 23**

Find a member...

Follow

Follow

Follow

# Dotfiles

The screenshot shows a GitHub profile page with a search bar at the top containing the text 'dotfile'. The navigation menu includes 'Pull requests', 'Issues', 'Marketplace', and 'Explore'. The profile section on the left is mostly obscured by black redaction boxes, but the text 'Front End Developer. Working with' is visible. A 'Follow' button is located at the bottom of the profile section. The main content area shows search results for 'dotfile' under the 'Repositories' tab. The search results indicate '1 result for repositories matching dotfile'. The result is a repository named 'dotfiles' by user 'My .files', which is categorized as 'Shell' and was updated on '13 Oct 2015'. Filter buttons for 'Type: All' and 'Language: All' are visible above the results. A 'Clear filter' button is located to the right of the search results.

Search GitHub

Pull requests Issues Marketplace Explore

Overview **Repositories** 1.1k Stars Followers Following

dotfile

Type: All Language: All

1 result for repositories matching **dotfile** Clear filter

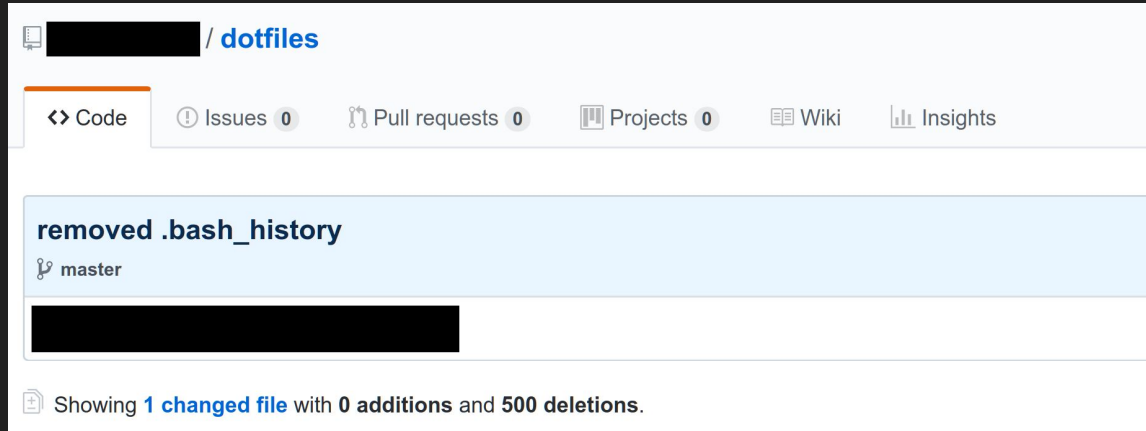
**dotfiles**

My .files

Shell Updated on 13 Oct 2015

Follow

# Ancient History



The screenshot shows a GitHub repository page for a user's 'dotfiles' repository. The repository name is redacted with a black box. The navigation bar includes 'Code', 'Issues 0', 'Pull requests 0', 'Projects 0', 'Wiki', and 'Insights'. The main content area shows a commit on the 'master' branch that removed the file '.bash\_history'. A summary at the bottom indicates 'Showing 1 changed file with 0 additions and 500 deletions.'

```
449 -brew install vagrant
450 -bsr vagrant
451 -export HOMEBREW_GITHUB_API_TOKEN="3[REDACTED]7"
452 -bsr vagrant
453 -brew cask install vagrant
454 -brew cask reinstall vagrant
```

# Clutching At Straws?

**As a Software Engineer you will:**

- Turn concepts and requirements into highly available web applications and systems using industry standard languages and technologies such as Node.JS, React, PHP, Mongo, MySQL, RabbitMQ, Chef and Docker.

# Hacking Breadth First

OWASP DirBuster 1.0-RC1 – Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

Work Method  Use GET requests only  Auto Switch (HEAD and GET)

Number Of Threads  10 Threads  Go Faster

Select scanning type:  List based brute force  Pure Brute Force

File with list of dirs/files

Char set  Min length  Max Length

Select starting options:  Standard start point  URL Fuzz

Brute Force Dirs  Be Recursive Dir to start with

Brute Force Files  Use Blank Extension File extension

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details



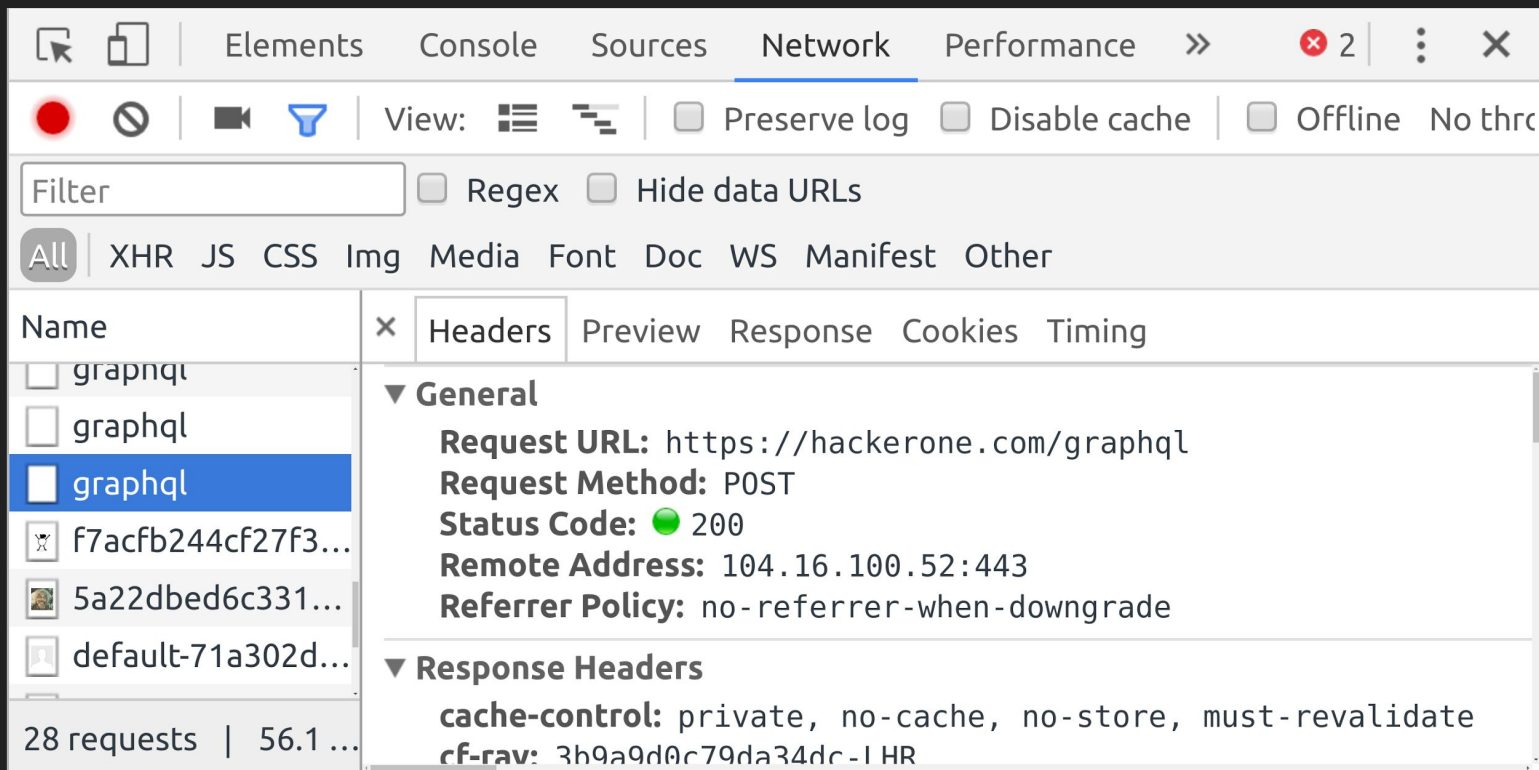
# Testing The Theory



The Mission:

- Use only breadth-first techniques
- Place in the top thirty

# Target Acquisition!



The image shows a screenshot of the Chrome DevTools Network tab. The top navigation bar includes 'Elements', 'Console', 'Sources', 'Network' (selected), and 'Performance'. Below the navigation bar, there are icons for a red dot, a no-interaction icon, a video camera, and a funnel. The 'View' section shows icons for list, tree, and table views, along with checkboxes for 'Preserve log', 'Disable cache', and 'Offline'. A search filter is present with a 'Filter' input field and checkboxes for 'Regex' and 'Hide data URLs'. The request type filter is set to 'All', with other options like 'XHR', 'JS', 'CSS', 'Img', 'Media', 'Font', 'Doc', 'WS', 'Manifest', and 'Other'. The main area shows a list of requests, with 'graphql' selected. The right-hand pane shows the details for the selected request, including 'Headers', 'Preview', 'Response', 'Cookies', and 'Timing' tabs. The 'General' section displays: 'Request URL: https://hackerone.com/graphql', 'Request Method: POST', 'Status Code: 200', 'Remote Address: 104.16.100.52:443', and 'Referrer Policy: no-referrer-when-downgrade'. The 'Response Headers' section shows: 'cache-control: private, no-cache, no-store, must-revalidate' and 'cf-ray: 3b9a9d0c79da34dc-I HR'. The bottom status bar indicates '28 requests | 56.1 ...'.

Elements Console Sources **Network** Performance >> 2

View:  Preserve log  Disable cache  Offline No thro

Filter  Regex  Hide data URLs

All XHR JS CSS Img Media Font Doc WS Manifest Other

Name  graphql  graphql  f7acfb244cf27f3...  5a22dbed6c331...  default-71a302d...

28 requests | 56.1 ...

× Headers Preview Response Cookies Timing

▼ **General**

**Request URL:** https://hackerone.com/graphql  
**Request Method:** POST  
**Status Code:** 200  
**Remote Address:** 104.16.100.52:443  
**Referrer Policy:** no-referrer-when-downgrade

▼ **Response Headers**

**cache-control:** private, no-cache, no-store, must-revalidate  
**cf-ray:** 3b9a9d0c79da34dc-I HR

# GraphQL

```
query Settings { query {
  id, teams(first: 50 after: "NQ==") {
    pageInfo { hasNextPage, hasPreviousPage },
    edges {
      cursor, node {
        _id, handle, structured_scopes {
          edges {
            node {
              id, asset_type, asset_identifier, eligible_for_submission,
              eligible_for_bounty, max_severity, archived_at, instruction
            }
          }
        }
      }
    }
  }
}
```



# Shut Up, Meg

```
tom@bash:~/recon/example (master)► meg -concurrency 80 /package.json
out/footle.com/70b038c333df500748afe8e77d3f2c746a4a8677 http://footle.com:80/package.json (HTTP/1.1 404 Not Found)
out/example.net/3a3207b353dbbe8804ee9952d5406510eb68e776 http://example.net:80/package.json (HTTP/1.1 404 Not Found)
out/example.com/76554307dfade72fcdbff52855ba32b644eb26ae http://example.com:80/package.json (HTTP/1.1 404 Not Found)
out/example.edu/e36325ff951ec70181efb8e10f6c0a80d09b4d3a http://example.edu:80/package.json (HTTP/1.1 404 Not Found)
out/footle.com/9d3be73770030c850aa40b5f5eb5e5037ba83826 https://footle.com:443/package.json (HTTP/1.1 404 Not Found)
out/example.net/feda230a5cf2b4306c0256676cffdc4873775d80 https://example.net:443/package.json (HTTP/1.1 404 Not Found)
```

```
tom@bash:~/recon/example (master)► grep prev -A3 ~/.vimrc
if $VIMENV == 'prev'
    noremap <Space> :n<CR>
    noremap <Backspace> :N<CR>
endif
tom@bash:~/recon/example (master)► cat $(which vimprev)
#!/bin/bash
VIMENV=prev vim $@
tom@bash:~/recon/example (master)► vimprev $(grep -Hnril '200 ok')
```

[ <https://github.com/tomnomnom/meg> ]



# Use Your Eyes

```
56adec2ac663c880f653dbe802bebf6eb782b742 (/recon/master/out/...) (51 of 63) - VIM 131x58
<f96a4defeb5d9043f73b515> c/56adec2ac663c880f653dbe802bebf6eb782b742 t/a2402bc660afc8d2de07d5014227f054a5573e26 ... buffers
1 | https://v:443/package.json
2
3 > GET /package.json HTTP/1.1
4 > Connection: close
5 > Host: v
6
7 < HTTP/1.1 200 OK
8 < Date: Mon, 06 Nov 2017 21:02:44 GMT
9 < Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
10 < X-OneAgent-JS-Injection: true
11 < ETags: "15081919922"
12 < Last-Modified: Mon, 16 Oct 2017 22:13:10 GMT
13 < Content-Type: application/json
14 < Content-Length: 930
15 < Accept-Ranges: bytes
16 < Set-Cookie: LK
17 < Set-Cookie: dtCookie=1$13C v; secure
18 < Connection: close
19
20
21 {
22   "name": "App",
23   "version": "0.1.0",
24   "scripts": {
25     "start": "concurrently \"grunt\" \"http-server\""
26   },
27   "devDependencies": {
28     "concurrently": "^3.4.0",
29     "dts": "0.0.1",
30     "grunt": "^0.4.5",
31     "grunt-contrib-concat": "^0.5.1",
32     "grunt-contrib-copy": "^0.8.0",
33     "grunt-contrib-sass": "^0.9.2",
34     "grunt-contrib-watch": "^0.6.1",
35     "grunt-convert": "^0.1.12",
36     "grunt-html2json": "^0.1.2",
37     "grunt-karma": "^0.11.0",
38     "http-server": "^0.10.0",
39     "jasmine-core": "^2.4.1",
40     "karma": "^0.13.19",
41     "karma-chrome-launcher": "^0.2.2",
42     "karma-html-reporter": "^0.2.7",
43     "karma-jasmine": "^0.3.6",
44     "karma-phantomjs-launcher": "^0.2.3",
45     "karma-spec-reporter": "0.0.23",
46     "karma-super-dots-reporter": "^0.1.0",
47     "lite-server": "^2.3.0",
48     "phantomjs": "^1.9.19"
49   }
50 }
51
~
~
~
NORMAL master v/56adec2ac663c880f653dbe802bebf6eb782b742 utf-8[unix] 1% 1/51 1
```

# Stats


0.151%	/package.json
0.084%	/gulpfile.js
0.051%	/Gruntfile.js
0.042%	/.git/config
0.017%	/.travis.yml
0.013%	/phpinfo.php
0.004%	/.ssh/id_rsa

# /.travis.yml

  **Plaintext storage of Slack API token in .travis.yml on**  
**████████████████████.com**


---



State ● Resolved (Closed)

Reported To 

Weakness **Insecure Storage of Sensitive Information**

Bounty **\$700**

Severity  **High (7 ~ 8.9)**

Participants  

Visibility **Private**

[Collapse](#)

# /.git/config



**GitHub API key on origin host for [REDACTED].com allows clone of github.com/[REDACTED]**

State ● Resolved (Closed)

Reported To [REDACTED]

Weakness Insecure Storage of Sensitive Information

Bounty \$1,200

Severity ■■■ High (7 ~ 8.9)

Participants  

Visibility Private

Collapse



/ (?!)



## [REDACTED].com subdomain takeover due to unregistered S3 bucket

State ● Triaged (Open)

Reported To [REDACTED]

Weakness Improper Access Control - Generic

Bounty \$250

Severity ▢ High (7 ~ 8.9)

Participants  [REDACTED]

Visibility Private

Collapse

# grep <3

```
tom@bash:~► cat $(which findtakeovers)
#!/bin/bash
searches=(
    "There is no app configured at that hostname"
    "NoSuchBucket"
    "No Such Account"
    "You're Almost There"
    "a GitHub Pages site here"
    "this shop is currently unavailable"
    "There's nothing here"
    "The site you were looking for couldn't be found"
    "The request could not be satisfied"
    "Please check that this domain has been added to a service"
)

for str in "${searches[@]}"; do
    grep -Hnri "$str" *
done
```



# ‘/’ Strikes Again!

# [REDACTED] [REDACTED] subdomain takeover

---


State ● Triaged (Open)

Reported To [REDACTED]

Weakness None

Bounty \$600

Severity ■■■■ Critical (9 ~ 10)

Participants  [REDACTED]

Visibility Private

[Collapse](#)

# Path-Based XSS

```
tom@bash:~/recon/example (master) ► meg -concurrency 80 /footle%3c%22bootle > index
tom@bash:~/recon/example (master) ► grep -hriE '(footle<|"bootle)'
      <p>Action 'footle<"bootle' was not found on handler 'premium'</p>
```

# CRLF Injection

```
tom@bash:~/recon/example (master) ► meg -concurrency 80 /%0aSet-Cookie:%20crlf=injection > index
tom@bash:~/recon/example (master) ► grep -hri '< Set-Cookie: crlf'
< Set-Cookie: crlf=injection&
```




# Open Redirects

```
tom@bash:~/recon/example (master) ► meg -concurrency 80 ///example.com/%2f.. > index
tom@bash:~/recon/example (master) ► grep -hri 'Location: //example'
< Location: //example.com/%2f../
```

# CORS Config Errors

```
tom@bash:~/recon/example (master)▶ meg -concurrency 80 -header "Origin: https://evil.com" / > index
tom@bash:~/recon/example (master)▶ grep -hri 'Access-Control-Allow-Origin: https://evil.com'
< Access-Control-Allow-Origin: https://evil.com
```

# The Results Are In

16.		<b>Daniel Bakker (jackds)</b> Independent security researcher (a.o. AOL, Micros...	<b>642</b>	<b>38</b>	<b>17</b>
17.		<b>TomH (tomnomnom)</b> I hunt for fun	<b>625</b>	<b>22</b>	<b>19</b>
18.		<b>learner (securitybreaker)</b> <	<b>597</b>	<b>46</b>	<b>21</b>

Ideas? Questions?

