

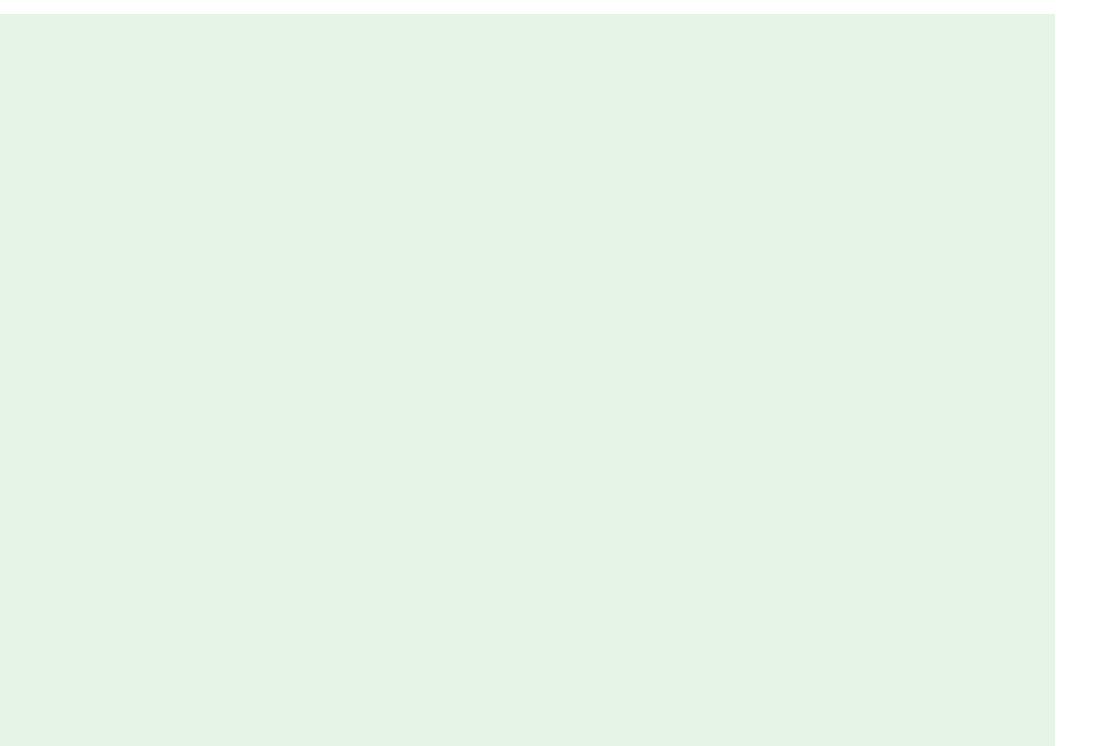
## Digital Dumpster Diving



For Further Information Visit:

[WWW.HACKERONE.COM](http://WWW.HACKERONE.COM) | [WWW.HACKER101.COM](http://WWW.HACKER101.COM)

## ADDITIONAL NOTES SECTION:



## GITHUB RECON EXAMPLES

- "company.com" "dev"
- "dev.company.com"
- "company.com" API\_key
- "company.com" password
- "api.company.com" authorization

## Tools

- gitrob
- git-all-secrets
- truffleHog
- git-secrets
- repo-supervisor
- Do it manually?

## DIGITAL DUMPSTER DIVING EXAMPLES

1

- Looked up the "umbrella" company name
- Combine "umbrella\_company" + asset\_name + "password", and found below code:  
"server": {  
"host": "dedXXXX.PATTERN.PROVIDER.com",  
"port": 21,  
"user": "some\_username",  
"password": "definitely\_ftp\_passwords"  
}
- Got access to umbrella\_company's FTP server → \$10,000 Bounty

## JAVASCRIPT FILE EXAMPLES

```
JS Parser - Home
/v1/help/submit_contact
2660: return e.save_contact_us_only = 1, t.isEmpty(e.message) && (e.message = "Created for Matchbox"), $post(t.default.get("v1/help/submit_contact"), e).then(function(e) {
/v1/help/issues
3086: var i = [v1/help/issues"] + String(e),
/v2/channel
3700: return r.default.get("v2/channel", {
/chat
3724: babeHelpers.classCallCheck(this, e), this.baseURL = t.baseURL || "chat"
/availability
3730: return r.default.getJSON(String(this.baseURL) + "availability", {
/estimatedWaitTime
3740: r.default.getJSON(String(this.baseURL) + "estimatedWaitTime", {
/reload
3750: var s = default.reloadHandler(this, this.baseURL + "reload?waitTime=" + t.waitTime)

```

## Process

## Look for:

- (hidden) endpoints
- ...and definitely more bugs
- Leaked cloud instances and their secret\_keys



## NOTES SECTION:

2

#215500 Leaked FTP credentials on github leads to RCE on amex.someothersite.com

State	Resolved (Closed)	Severity	No Rating (---)
Reported To		Participants	(Manage collaborators)
Weakness	Command Injection - Generic	Visibility	Private
Bounty	\$1,000	Collapse	

hackerone

## Recon Cheat Sheet

A Reference Guide for Our Newest Hackers

## Asset Discovery

### BRUTE FORCE



### CERTIFICATE TRANSPARENCY TOOLS

Censys	Shodan	Certspotter	Crt.sh
Look for SSL certificates: Example: 443.https. tls.certificate.parsed. extensions.subject_alt_name. dns_names:snapchat.com	Search by hostname. Filter for: Ports: 8443, 8080, etc   Title: "Dashboard [Jenkins]"   Product:Tomcat Hostname: somecorp.com   Org: evilcorp ssl: Google	Great API   Easy to automate   Make a bash alias → Automate → Win	Great API and web interface   Allows using a wild card   You may get different results from different sources

### CERTIFICATE TRANSPARENCY EXAMPLES

Vulnerabilities found with Shodan

Search Query: hostname:host.com port:15672  
[#10068 Access to RabbitMQ on stageREDACTED.REDACTED.com:15672](#)

Search Query: hostname:host.com title:Dashboard [Jenkins]  
[#220836 jenkins-REDACTED.REDACTED.REDACTED.com publicly facing without authentication leaks AWS\\_Secret\\_key + Build info](#)

Vulnerabilities found with Censys

AUGUST 22, 2017  
**"Secure your jenkins instance or hackers will force you to! (Snapchat's \$5,000 vulnerability)"**

Script Console

```

Type in an arbitrary GoScript and execute for the server. Useful for trouble-shooting and diagnostics. Use the print() command to see the output if you use sysout().out. It will print to the Jenkins log file. Jenkins has its own built-in GoScript interpreter.

print(sysout().out.println("Hello Jenkins!"))
print(sysout().out.println("Hello Jenkins!"))
  
```

All the classes from the plugin are visible: jenkins, jenkins.model,\*, Hudson,\*, and Hudson.model.\* are pre-imported.

```

def root() {
    new StringHolder();
    new StringHolder();
    print("Hello Jenkins!");
}
  
```

At the classes from the plugin are visible: jenkins, jenkins.model,\*, Hudson,\*, and Hudson.model.\* are pre-imported.

NOTES SECTION:

## OSINT

### ACQUISITIONS

- Big programs (Facebook, Google, Verizon Media, etc.)
- Acquired assets usually in scope after 6 months



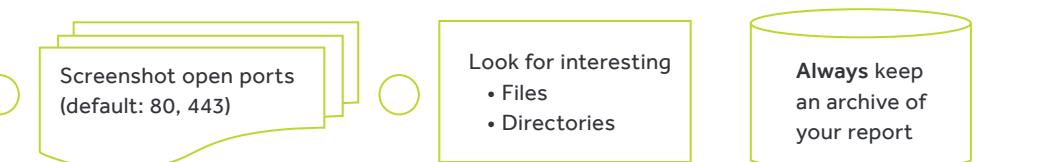
### WHOIS

- ARIN (Canada, United States, some Caribbean nations) | RIPE NCC (Europe, Russia, Middle East, Central Asia) | APNIC (Asia-Pacific region) | LACNIC (Latin America, some Caribbean nations) | AFRINIC (Africa)
- Search Yahoo, or any other large program. Shodan helps here, too

Network Resources	
LVLT-YAHOO-1-8-3-34 (NET-8-3-34-0-1)	8.3.34.0 - 8.3.35.255
NET-216-34-77-0 (NET-216-34-77-0-1)	216.34.77.0 - 216.34.77.127
COLOC-1-YAHOO-1-8-8-178 (NET-8-8-178-0-1)	8.8.178.0 - 8.8.178.255
SAVY-64-209-232-0-0 (NET-64-209-232-0-1)	64.209.232.0 - 64.209.232.255
SAVY-S235114-9 (NET-64-39-38-208-1)	64.39.38.208 - 64.39.38.223

## Content Discovery

### CONTENT DISCOVERY PROCESS



### CONTENT DISCOVERY EXAMPLES

- You see an open port on 8443
  - Directory brute force
  - /admin/ returns 403
  - You brute force for more files/dirs on /admin/
  - /admin/users.php returns 200
  - Repeat on other domains, ports, folders, etc.
- Nmap common ports (3868, 3366, 8443, 8080, 9443, 9091, 3000, 8000, 5900, 8081, 6000, 10000, 8181, 3306, 5000, 4000, 8888, 5432, 15672, 9999, 161, 4044, 7077, 4040, 9000, 8089, 443, 7447, 7080, 8880, 8983, 5673, 7443)
  - Take screenshots (webscreenshot.py)
  - Directory/File brute force
  - Robots.txt sometimes does this for you ^\\_(ツ)\_/^-

NOTES SECTION:

### AWS RECON PROCESS

- Look for S3 buckets on Google (site:s3.amazonaws.com +inurl:company\_name) | AWS instances (site:amazonaws.com -s3)
- Repeat on Github!

Google search results for "site:s3.amazonaws.com inurl:uber". The search shows 14,361 available code results. A terminal window shows the command: ./root@ubt:~/tools/lazy3d/ruby lazy3d.rb test. The output indicates it found several buckets: test-admin-staging, test-admin-production, and test-admin-dev.

Create aliases to cut down your work

```

certspotter() {
  curl -s https://certspotter.com/api/v0/certs?domain=$1 | jq '.[].dns_names[]' | sed 's/\^\//g' | sed 's/\^\.\//g' | sort -u | grep $1 > -/$1$1.txt
}

dirbruteforce() {
  cd / tools / dirsearch
  cat -/$1$1.txt |
  while read line;
  do python3 dirsearch.py -e. -u "https://$line"; done
}

screenshots() {
  python -/tools/webscreenshot / webscreenshot.py -o. / $1 / screenshots / -i-/$1$1.txt--timeout = 10 -m
}

recon() {
  certspotter $1
  dirbruteforce $1
  screenshot $1
}
  
```

Automate the tasks you perform for each target

73886 URLs to be screenshot

### AWS RECON EXAMPLES

Danil Gribkov (dpgrbikov)	Pete (yaworski)
Reputation: 350   Rank: 63rd   Signal: 2.90   Percentile: 78th   Impact: 22.50   95th Percentile: 95th	Reputation: 5623   Rank: 63rd   Signal: 5.79   Percentile: 93rd   Impact: 17.89   89th Percentile: 89th
Subdomain takeover on happymondays.starbucks.com due to non-used AWS S3 DNS record	AWS S3 bucket writeable for authenticated aws users
State: Resolved (Closed)	State: No Rating (-)
Disclosed publicly: December 19, 2016 2:59pm -0800	Disclosed publicly: April 5, 2016 6:06am -0700
Reported To: Starbucks	Reported To: HackerOne
Weakness: Privilege Escalation	Weakness: Improper Authentication - Generic
Bounty: \$2,500	Bounty: \$2,500

NOTES SECTION: