bugcrowd

Michael Skelton
Global Head of Security Ops

WEBINAR

SECURITY RECONNAISSANCE
How New Tricks Let Hackers See More

with Codingo *aka Michael Skelton*

Michael Skelton
Global Head of Security Ops

bugcrowd

The pay-for-results security platform that plugs your team into on-demand skills, indexed by trust and specialization

Opinions

not facts

Notable Changes *since 2019*

A number of improvements in directory brute forcing from multiple authors.

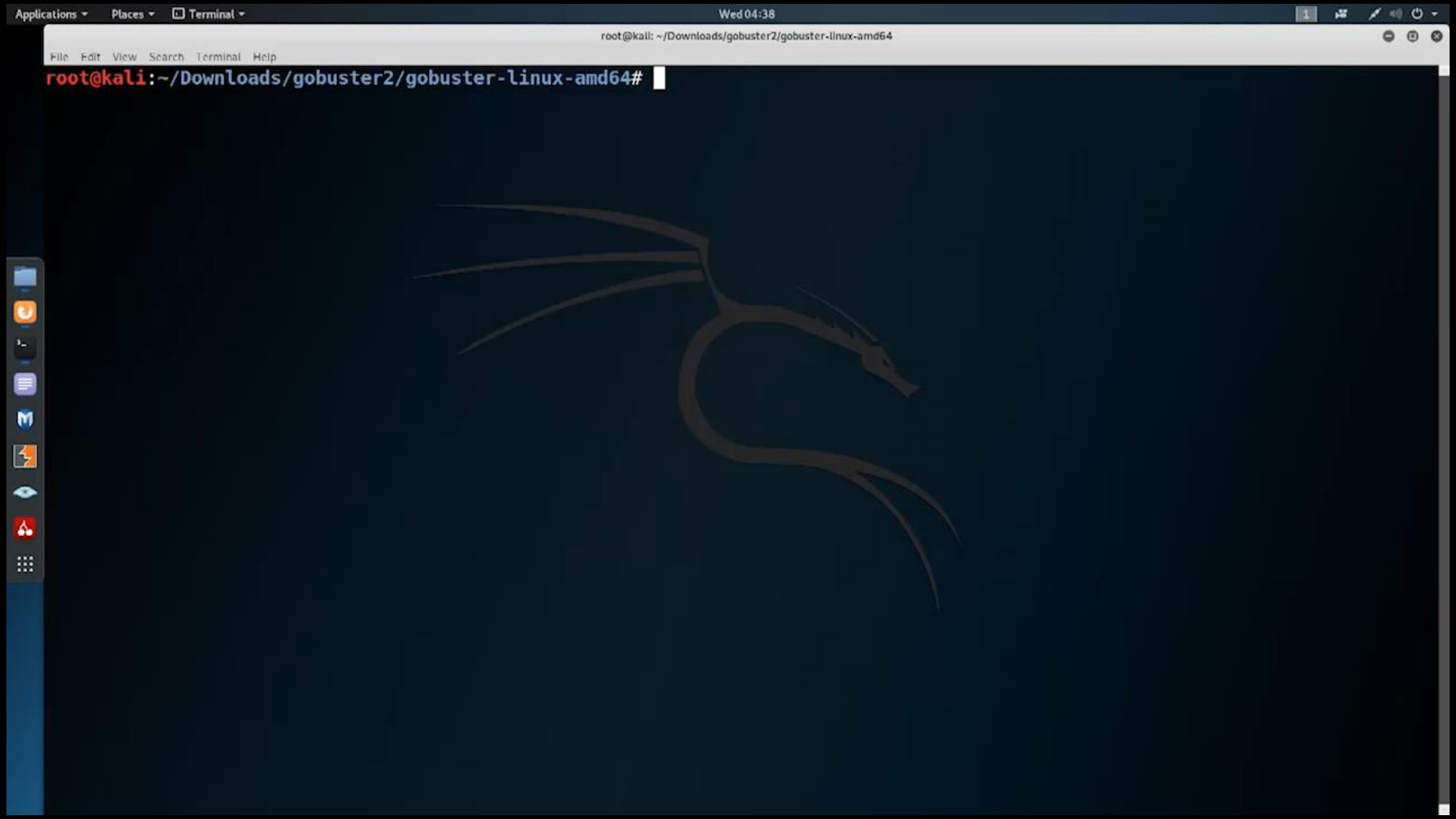
Tooling for working at scale continues to rise with the popularity of Bug Bounty programs and the increase in open scope programs for researchers to work on.

More focus on the weaknesses of the cloud, and tools that allow for exploration and exploitation beyond the traditional cloud providers. API keys in these services, and testing them have been a strong focus.

Directory

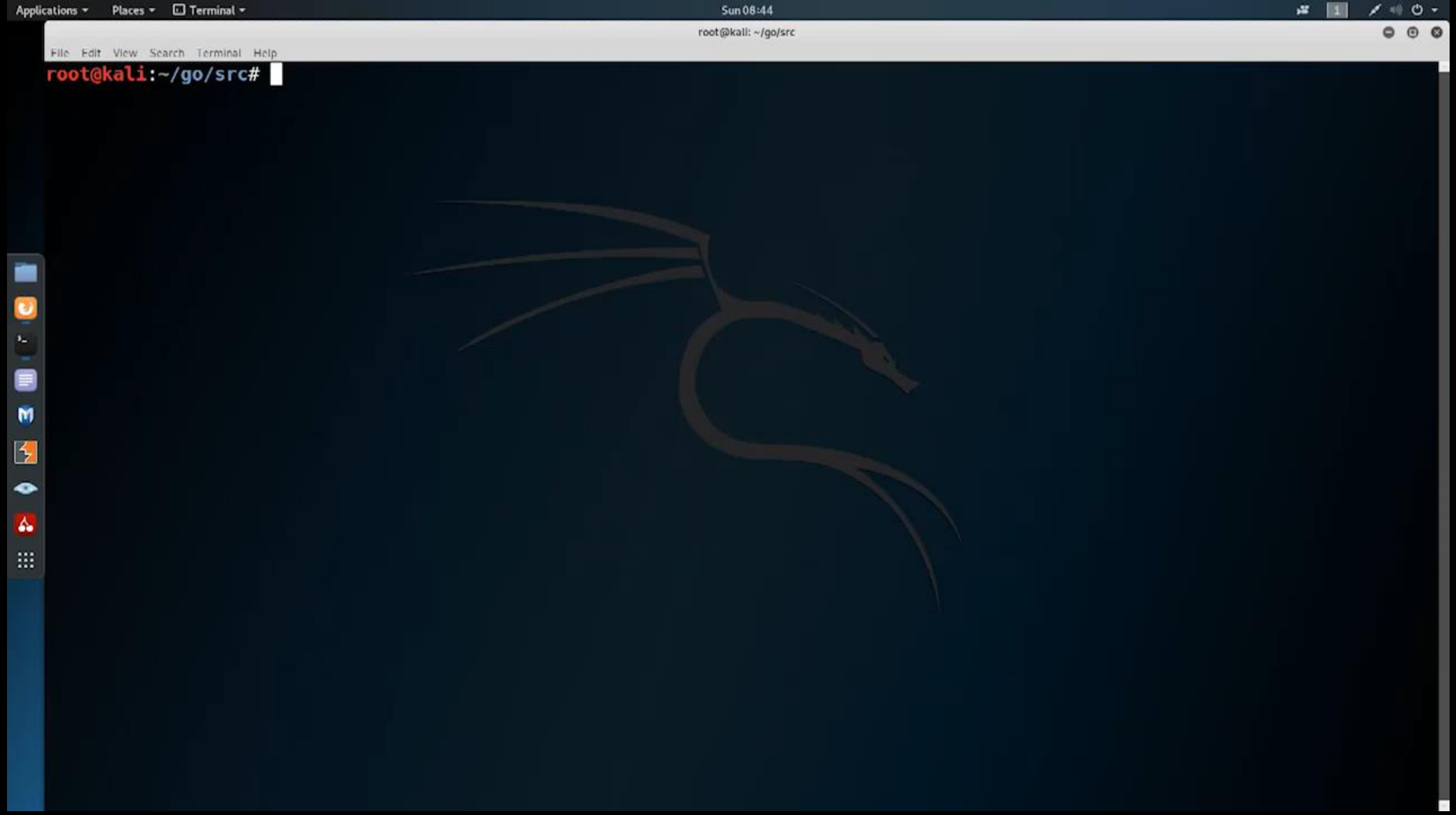
Brute Forcing

bugcrowd



https://github.com/C-Sto/recursebuster

bugcrowd



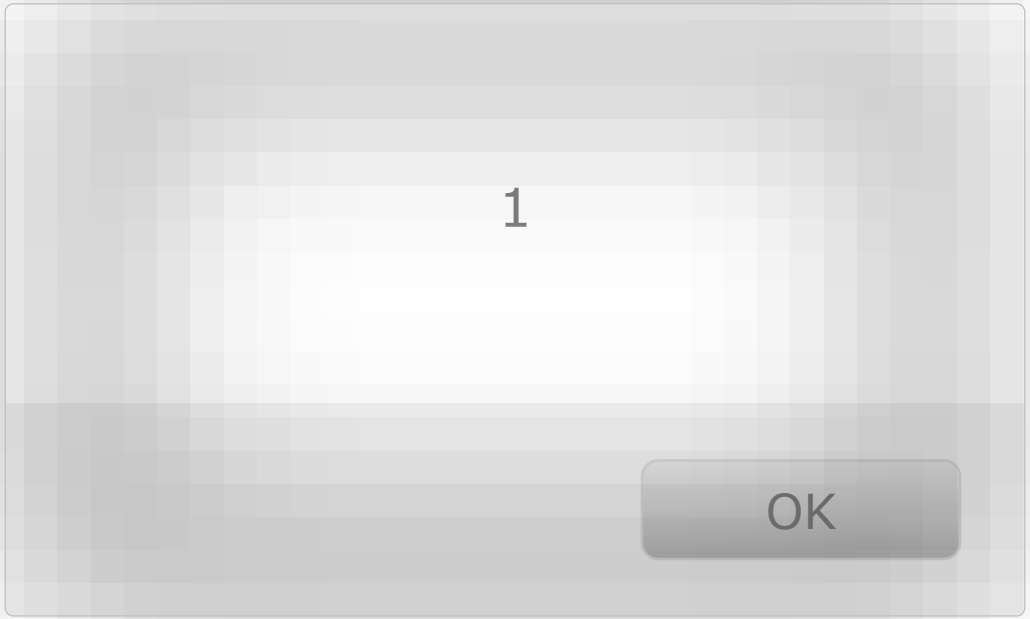
https://github.com/ffuf/ffuf

bugcrowd

XSS

Stop 👏 Doing 👏 This

Always fully explore an XSS vector
look for elevation, page redresses or other avenues before submitting an alert(1)



Weaponized

XSS Payloads

https://github.com/hakluke/weaponised-XSS-payloads

https://medium.com/@hakluke/upgrade-xss-from-medium-to-critical-cb96597b6cc4

- WordPress Create Admin
- WordPress Create new Page
- WordPress Create Post
- My BB Create new Admin
- Drupal Create new Admin
- CSRF bypass for XSS using Iframe Injection Template

WordPress

Admin Call Payloads

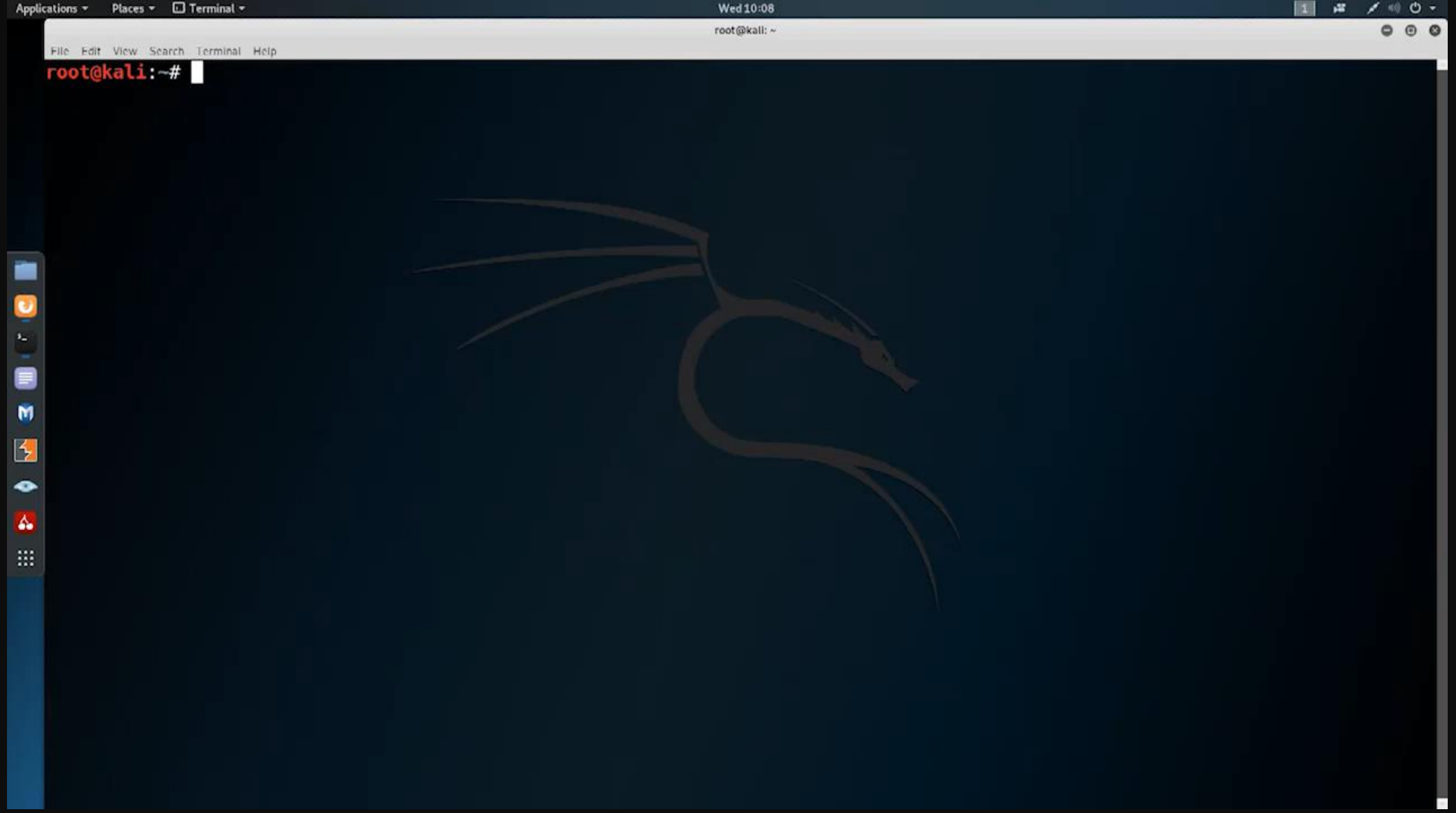
https://github.com/hoodoer/WP-XSS-Admin-Funcs

- Add new administrator user
- Exfiltrate WordPress site content export
- WordPress plugin installation
- Automatically hide the malicious plugin after it's installed
- Upload PHP meterpreter shell and execute

Subdomain

Discovery

bugcrowd



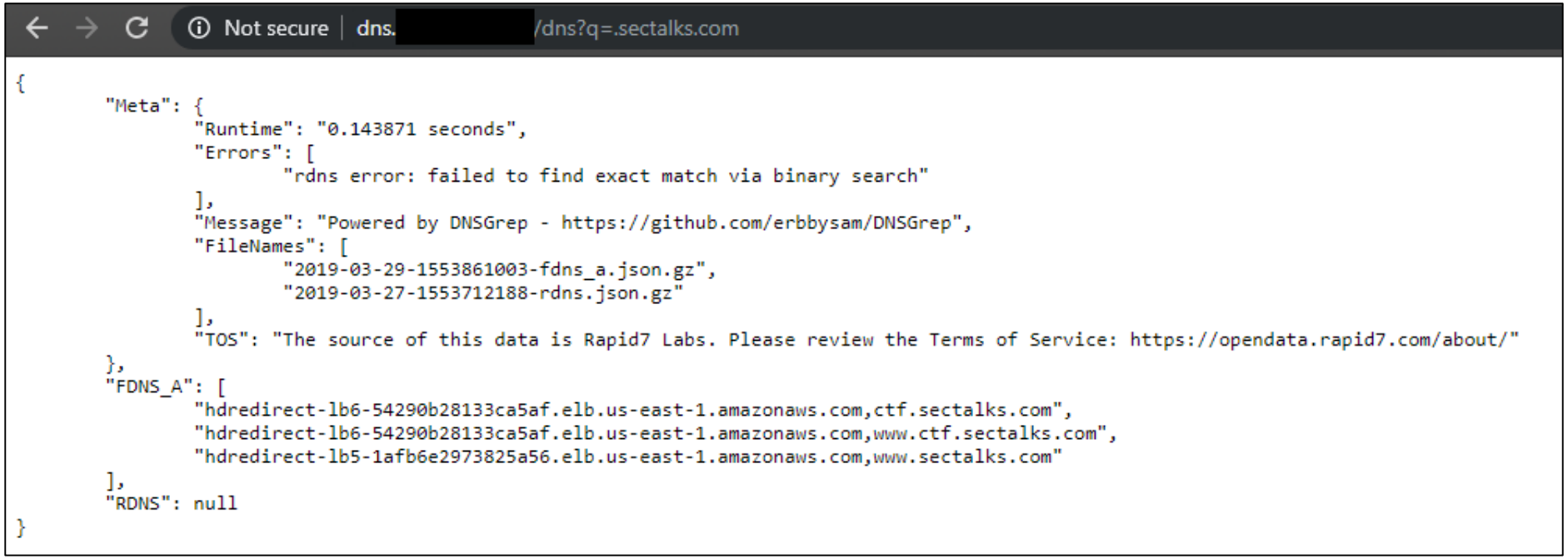
https://github.com/vortexau/dnsvalidator

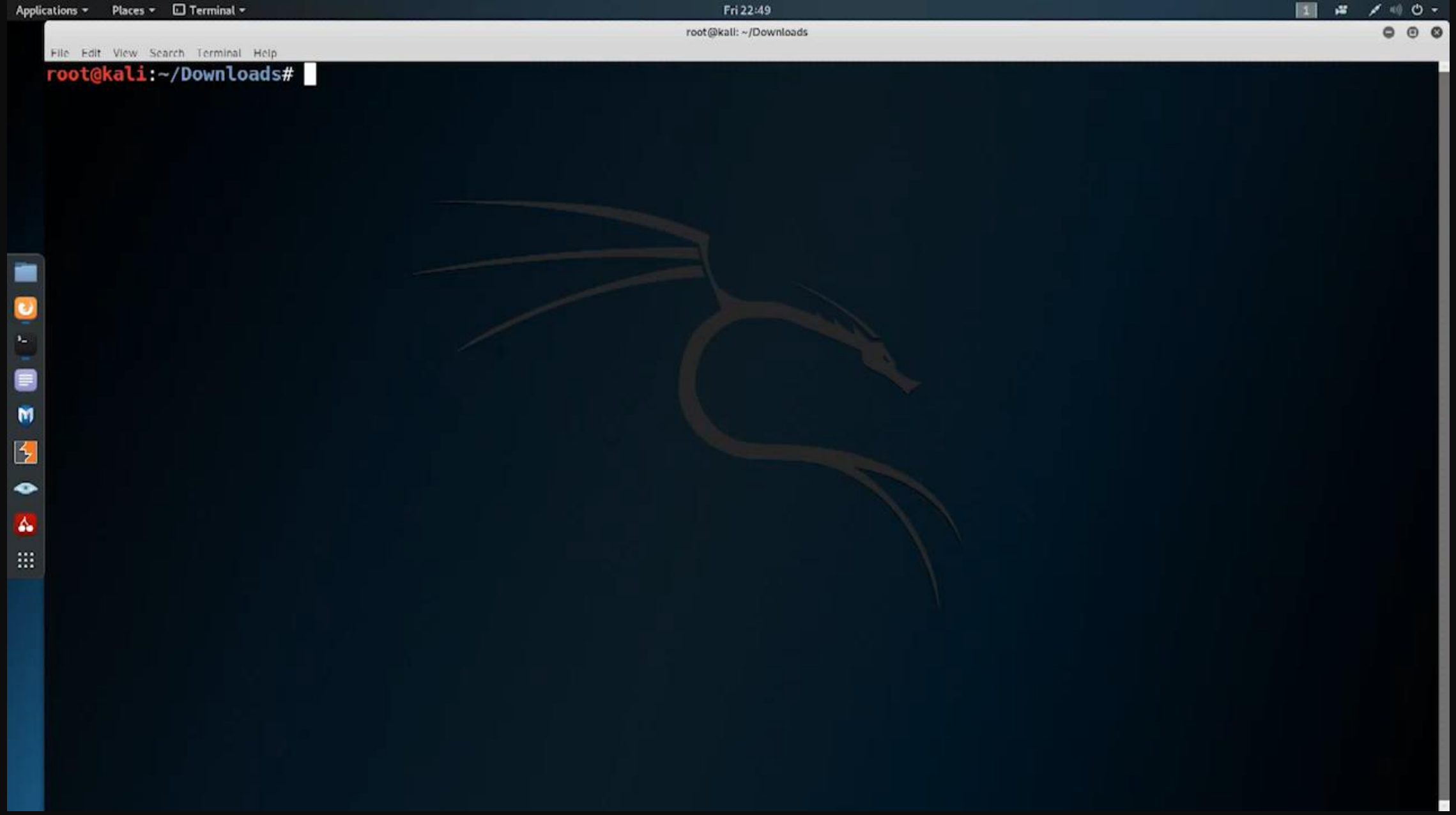
bugcrowd

DNSGrep

Utility for quickly searching presorted DNS names—Built around the Rapid7 rdns & fdns dataset

https://github.com/erbbysam/DNSGrep





https://github.com/Edu4rdSHL/findomain

bugcrowd

API Keys

and Build Logs

bugcrowd

Keyhacks

Safe testing to verify authenticity of 47 API keys

https://github.com/streaak/keyhacks

Slack Webhook

If the below command returns `missing_text_or_fallback_or_attachments`, it means that the URL is valid, any other responses would mean that the URL is invalid.

```
curl -s -X POST -H "Content-type: application/json" -d '{"text":""}' "https://hooks.slack.com/services/T00000000/B00
```

Slack API token

```
curl -sX POST "https://slack.com/api/auth.test?token=xoxp-TOKEN_HERE&pretty=1"
```

SauceLabs Username and access Key

```
curl -u USERNAME:ACCESS_KEY https://saucelabs.com/rest/v1/users/USERNAME
```

Facebook AppSecret

You can generate access tokens by visiting the URL below.

```
https://graph.facebook.com/oauth/access_token?client_id=ID_HERE&client_secret=SECRET_HERE&redirect_uri=&grant_type=c
```

README.md

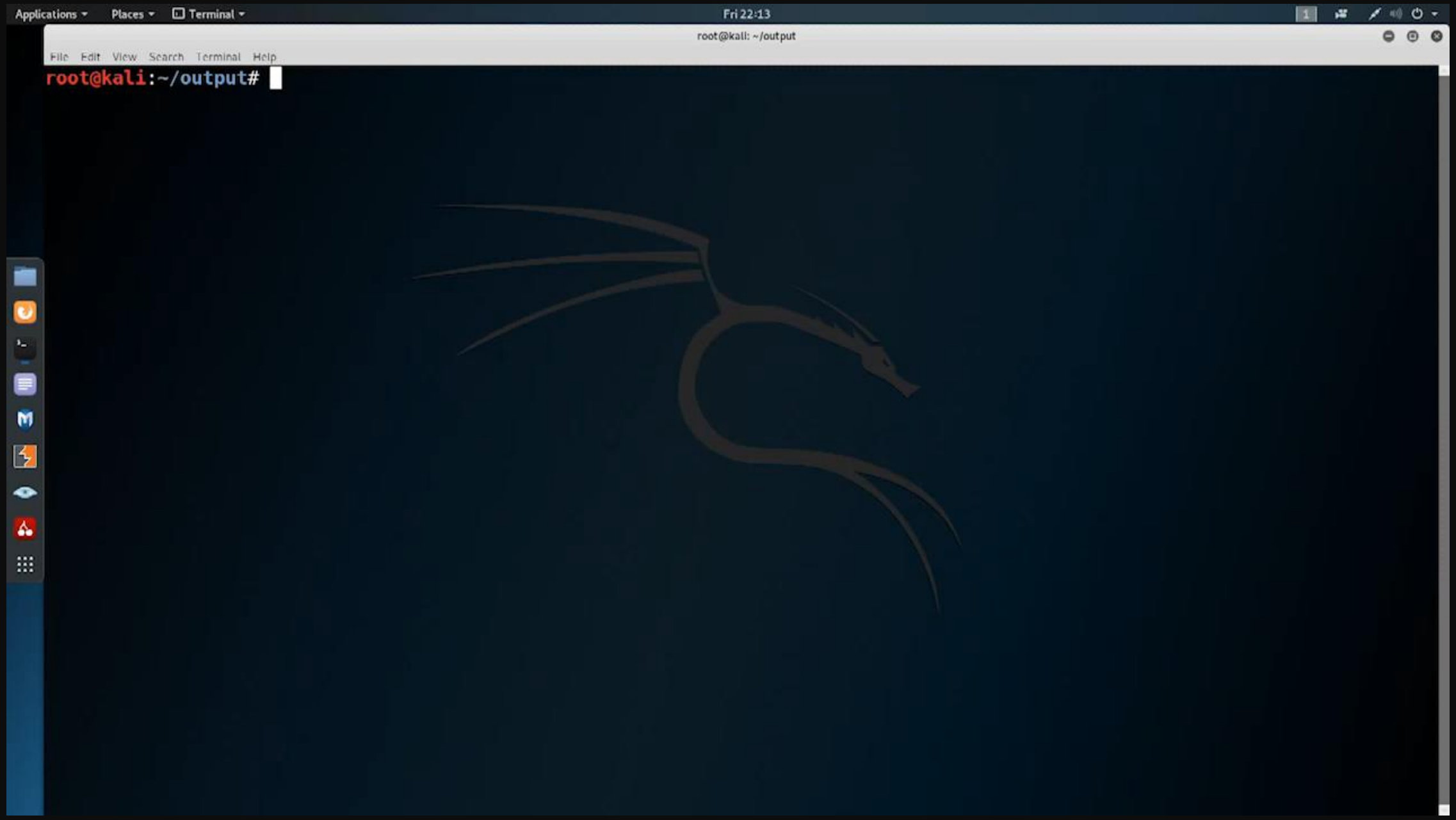
KeyHacks

KeyHacks shows ways in which particular API keys found on a Bug Bounty Program can be used, to check if they are valid.

Table of Contents

API Keys / Build Logs

bugcrowd



https://github.com/lc/secretz

bugcrowd

Dr. Watson

https://github.com/prodigysml/Dr.-Watson

Dr. Watson is a simple Burp Suite extension that helps find assets, keys, subdomains, IP addresses, and other useful information! It's your very own discovery side kick, the Dr. Watson to your Sherlock!

Jenkinz

https://github.com/lc/jenkinz

Jenkinz is a tool to retrieve every build for every job ever created and run on a given Jenkins instance

jLoot *JIRA Secure Attachment Looter*

https://github.com/netspooky/jLoot

jLoot is a tool that can be used to enumerate attachments to JIRA tickets

Cloud

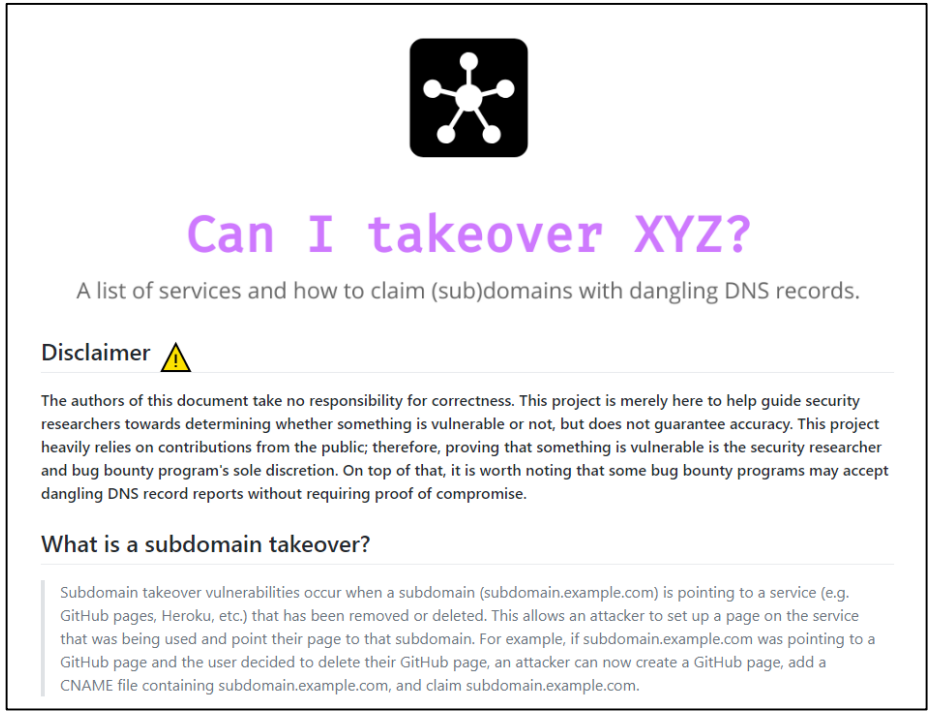
Based Services

bugcrowd

Can I Take Over List

Highlighting Subdomain Takeover Scenarios

https://github.com/edoverflow/can-i-take-over-xyz



Can I takeover XYZ?

A list of services and how to claim (sub)domains with dangling DNS records.

Disclaimer ⚠

The authors of this document take no responsibility for correctness. This project is merely here to help guide security researchers towards determining whether something is vulnerable or not, but does not guarantee accuracy. This project heavily relies on contributions from the public; therefore, proving that something is vulnerable is the security researcher and bug bounty program's sole discretion. On top of that, it is worth noting that some bug bounty programs may accept dangling DNS record reports without requiring proof of compromise.

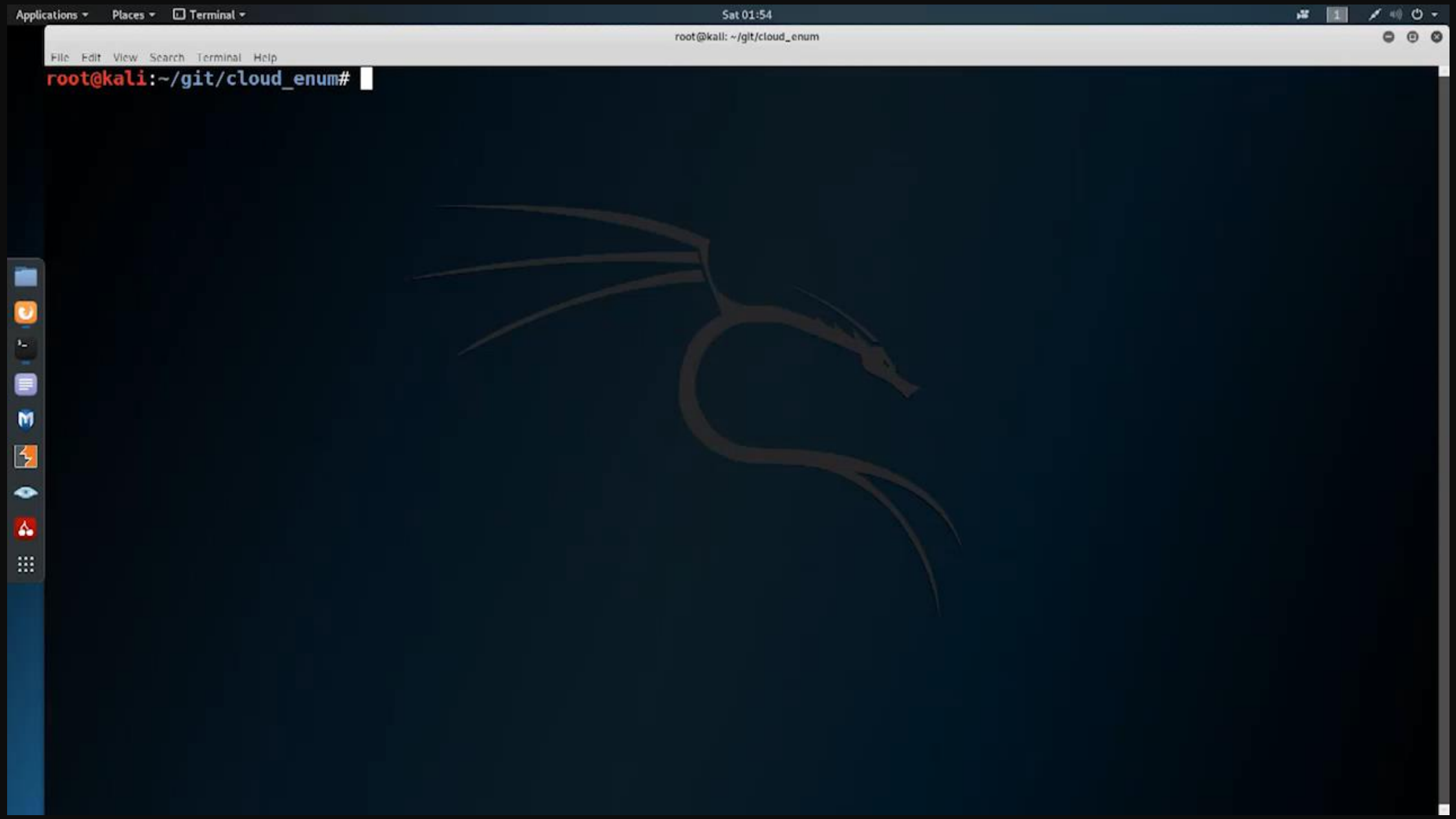
What is a subdomain takeover?

> Subdomain takeover vulnerabilities occur when a subdomain (subdomain.example.com) is pointing to a service (e.g. GitHub pages, Heroku, etc.) that has been removed or deleted. This allows an attacker to set up a page on the service that was being used and point their page to that subdomain. For example, if subdomain.example.com was pointing to a GitHub page and the user decided to delete their GitHub page, an attacker can now create a GitHub page, add a CNAME file containing subdomain.example.com, and claim subdomain.example.com.

Engine	Status	Fingerprint	Discussion	Documentation
Airee.ru	Vulnerable		Issue #104	
Akamai	Not vulnerable		Issue #13	
AWS/S3	Vulnerable	`The specified bucket does not exist`	Issue #36	
Bitbucket	Vulnerable	`Repository not found`		
Campaign Monitor	Vulnerable	'Trying to access your account?'		Support Page
Cargo Collective	Vulnerable	`404 Not Found`		Cargo Support Page
Cloudfront	Not vulnerable	ViewerCertificateException	Issue #29	Domain Security on Amazon CloudFront
Desk	Not vulnerable	`Please try again or try Desk.com free for 14 days.`	Issue #9	
Fastly	Edge case	`Fastly error: unknown domain:`	Issue #22	
Feedpress	Vulnerable	`The feed has not been found.`	HackerOne #195350	
Fly.io	Vulnerable	`404 Not Found`	Issue #101	

Cloud Services

bugcrowd



https://github.com/initstring/cloud_enum

bugcrowd

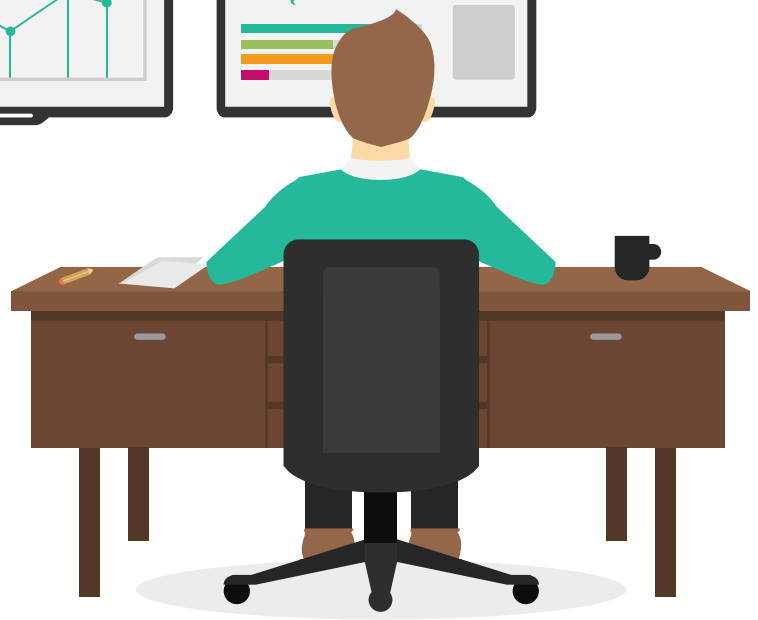
Discovering and Evaluating Tools

Tips and tricks for finding new tools

1. Follow active Github users and pay attention to what they're contributing to, releasing, following or star'ing.

   https://github.com/codingo?tab=following

2. Use time to benchmark tools. Review activity, forks and source as your skillset allows. Use Github Watch on projects when you use them regularly.



bugcrowd

But wait...

There's more!

bugcrowd.com/ask-codingo

February 26, 12:00pm PST

bugcrowd

Questions?

Michael Skelton

Global Head of Security Ops & Researcher Enablement

github.com/codingo

twitter.com/codingo_

bugcrowd

THANK YOU

bugcrowd

#1 Crowdsourced Security Company