Automating Application Security Bug Hunting

Improving coverage with better automation

@JCRAN

Information Security Professional?

Research:
@KennaSecurity

Janitor:
@intrigueio

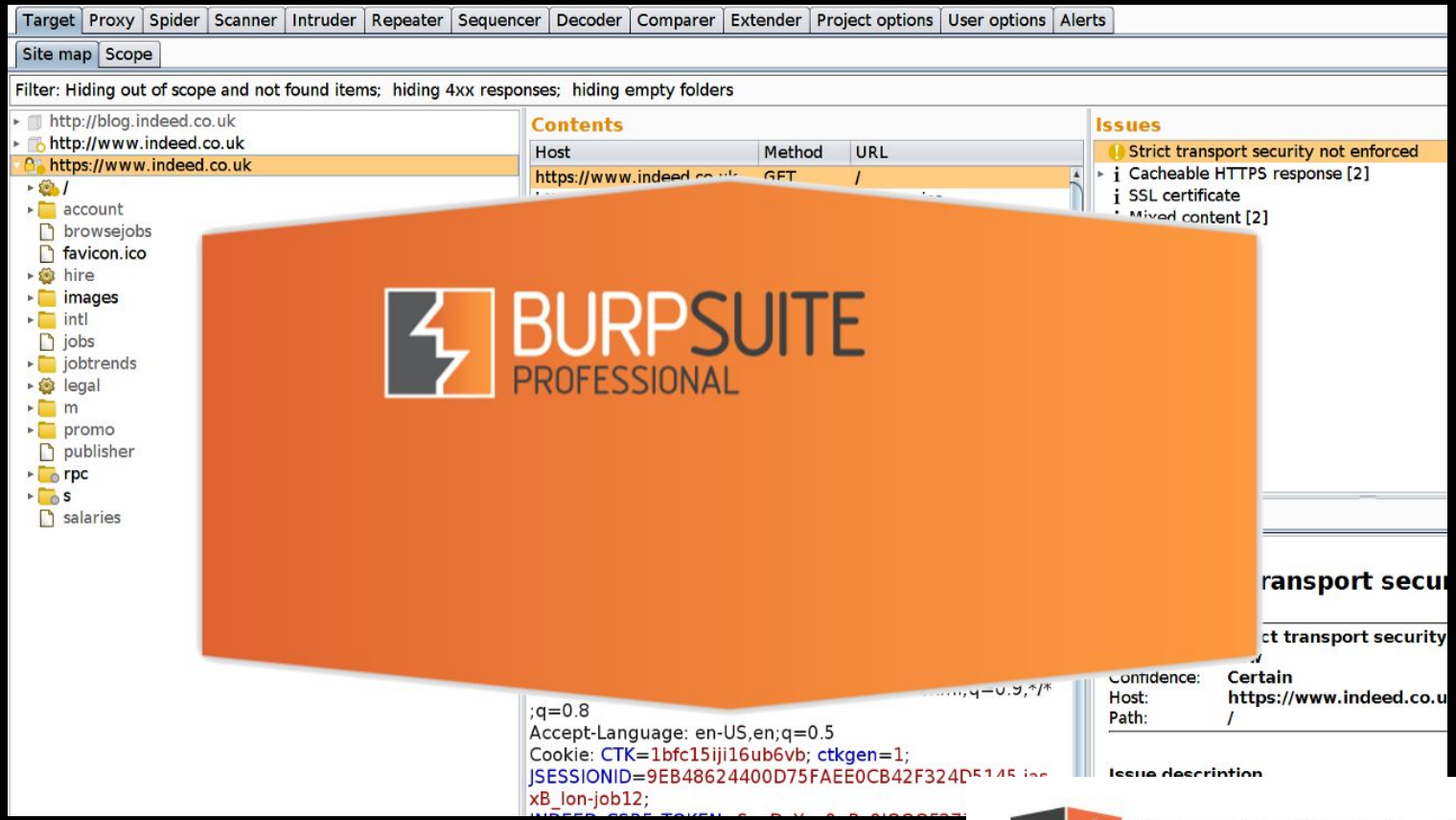
Previously:
@bugcrowd, @rapid7

@JGAMBLIN

Information Secuirty Rank Amature

Principal Security Engineer:
@KennaSecurity

Jerrygamblin.com
Internal.dev
Questionable.dev
(Coming Soon!)

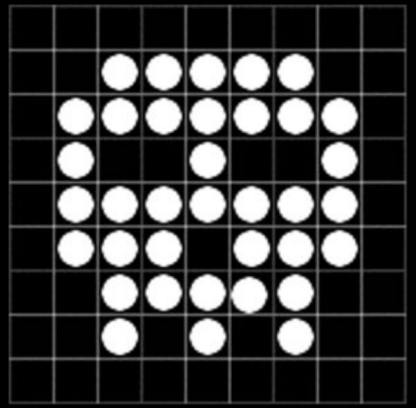


When you think of web application automation....

PORTSWIGGER
WEB SECURITY

There are many great extensions...

Attack Surface Detector



ActiveScan++

TURBO INTRUDER

And If You Want To Dig Into More...

- https://portswigger.net/bappstore
- http://offsecbyautomation.com/Worthwhile-BurpSuite-Plugins/
- https://securityonline.info/top-8-burp-suite-extensions-burpsuite-web-app-pentest/
- https://github.com/snoopysecurity/awesome-burp-extensions


Exploitable Legacy Systems
Shadow IT Services
Exposed Web Vulnerabilities
Leaked Secrets & Accounts
Misconfigured Services
Unauthenticated Databases

Forward DNS
Reverse DNS
Search Engines
Certificate Transparency
BGP
Security Trails
Censys
Binary Edge
SHODAN
Project Sonar
Parsing PDFs
PublicWWW
Passive DNS
BuiltWith
Historical WHOIS
SpyOnWeb
VirusTotal
Robtex
DNSDumpster

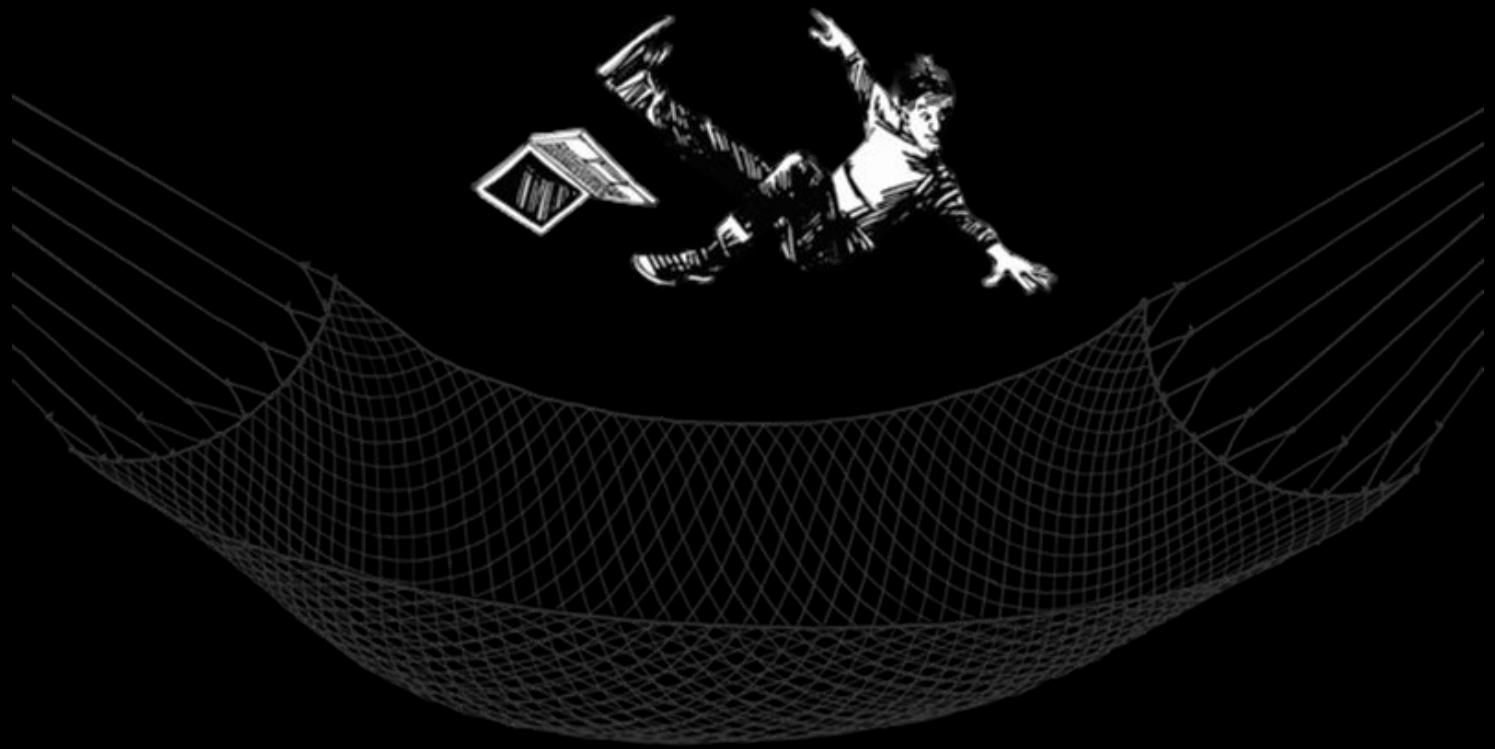
Xforce Exchange
Alienvault
AbuseIPDB
Archive.org
RIRs (ARIN,RIPE,etc)
Bing
Circl.lu
Clearbit
CommonCrawl
EDGAR
OpenCorporates
CRT.sh
Cymon
CiberCrimeTracker
FullContact
Dehashed
HIBP
Google
Whoisology
WhoisXMLAPI

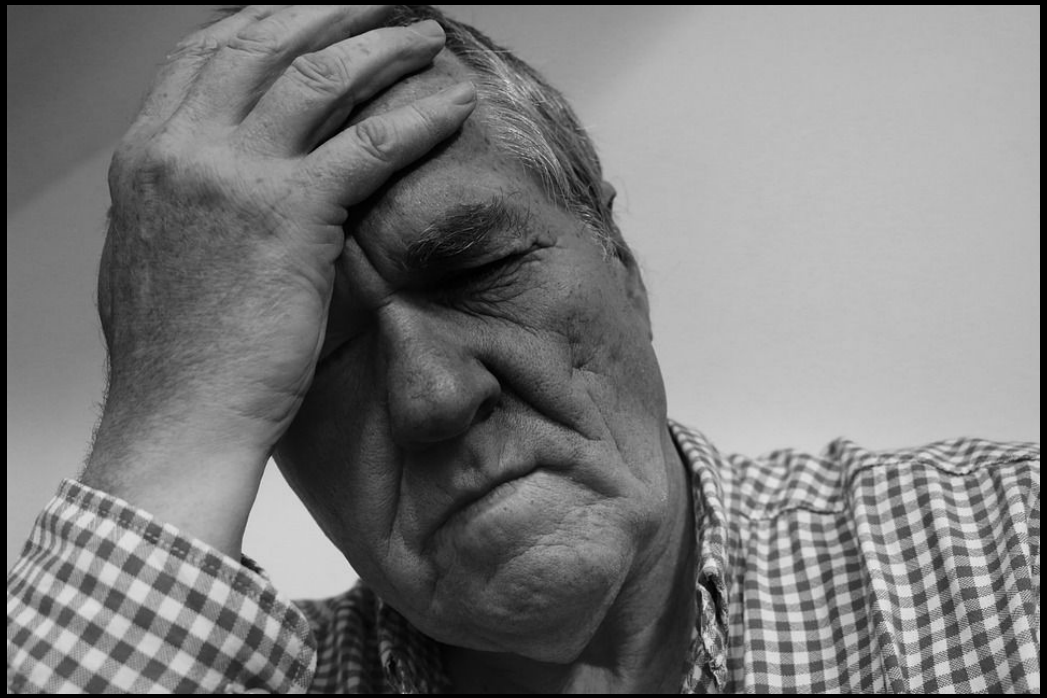
Many Many High Quality Sources And Tools

Smbmap
XRay
Scanless
Racoon
DataSploit
amass
fierce
Aquatone
Sublis3r
nmap
Dnsrecon
Altdns
Sublist3r
subquest
SubScraper
xray
Lazyrecon

masscan
anubis
bluto
censys-subdomain-finder
DMitry
dnscan
dnsenum.pl
dnsrecon
Domain analyzer
DomainRecon
gobuster
Knockpy
ldns-walk
massdns
nsec3walker
recon-ng
subbrute
SubFinder

Bug bounties provide an important **safety net!**





So what’s missing?!?


Inherent Complexity.
Missing fundamentals.

Rich Mogull
@rmogull

The hardest problem in security is solving the simple problems at scale.

4:16 PM - 22 Feb 2019

63 Retweets **191** Likes

14 63 191


Better automation can help improve coverage and visibility

3 Keys For Better Automation **

Broad Array of Sources
An Ontology
Recursion

** Coverage-focused Automation

INTRIGUE CORE

OPEN SECURITY AUTOMATION FRAMEWORK

Tasks provide a Broad Array of **Sources**
Entities provide An **Ontology**
Machines provide **Recursion**

aws_ec2_gather_instances
aws_s3_brute
convert_entity
create_entity
create_service
dns_brute_srv
dns_brute_sub
dns_brute_sub_async
dns_brute_sub_over_http
dns_brute_tld
dns_lookup_mx
dns_lookup_txt
dns_permute
dns_recurse_spf
dns_search_sonar
dns_snoop_cache
dns_transfer_zone
email_brute_gmail_glxu
email_harvest
email_validate
enrich/aws_s3_bucket
enrich/dns_record
enrich/domain
enrich/generic
enrich/github_account
enrich/ip_address
enrich/nameserver
enrich/net_block
enrich/network_service
enrich/organization
enrich/ssl_certificate
enrich/uri
enumerate_nameservers
finger_extraction
ftp_enumerate
gitrob
import/arin_ipv4_ranges
import/aws_ipv4_ranges
import/data_file
import/domainlist_domains
import/shodan_json_tmp
import/umbrella_top_domains
import/umbrella_top_sites
ip_geolocate
masscan_scan
net_block_expand
network_service_fuzz
nmap_scan
phone_number_lookup
saas_google_calendar_check
saas_google_groups_check
saas_jira_check
saas_trello_check
scrape_publicwww
search_bgp
search_bing
search_builtwith
search_censys
search_crt
search_edgar
search_github
search_github_code
search_have_i_been_pwned
search_opencorporates
search_phishtank
search_project_honeypot
search_robtex
search_shodan
search_sublister
search_threatcrowd
search_towerdata
search_virustotal
search_whoisology
security_trails_historical_dns
security_trails_historical_whois
security_trails_nameserver_search
security_trails_subdomain_search
snmp_walk
tcp_bind_and_collect
uri_analyze_target
uri_brute
uri_brute_common_content
uri_brute_creds
uri_brute_focused_content
uri_check_security_headers
uri_check_subdomain_hijack
uri_enumerate_js
uri_extract_metadata
uri_gather_linked_content
uri_gather_robots
uri_gather_sitemap
uri_gather_ssl_certificate
uri_screenshot
uri_spider
uri_youtube_metadata
vulns/apache_struts_jakarta_parser
vulns/cisco_smart_install_scan
vulns/etcd_harvester
vulns/ssrf_brute_parameter
vulns/ssrf_proxy_host_header
vulns/tomcat_put_jsp
web_account_check
whois_lookup

Intrigue Core Built-in Tasks

aws_ec2_gather_instances
aws_s3_brute
convert_entity
create_entity
create_service
dns_brute_srv
dns_brute_sub
dns_brute_sub_async
dns_brute_sub_over_http
dns_brute_tld
dns_lookup_mx
dns_lookup_txt
dns_permute
dns_recurse_spf
dns_search_sonar
dns_snoop_cache
dns_transfer_zone
email_brute_gmail_glxu
email_harvest
email_validate
enrich/aws_s3_bucket
enrich/dns_record
enrich/domain
enrich/generic
enrich/github_account
enrich/ip_address
enrich/nameserver
enrich/net_block
enrich/network_service
enrich/organization
enrich/ssl_certificate
enrich/uri
enumerate_nameservers
finger_extraction
ftp_enumerate
gitrob
import/arin_ipv4_ranges
import/aws_ipv4_ranges
import/data_file
import/domainlist_domains
import/shodan_json_tmp
import/umbrella_top_domains
import/umbrella_top_sites
ip_geolocate
masscan_scan
net_block_expand
network_service_fuzz
nmap_scan
phone_number_lookup
saas_google_calendar_check
saas_google_groups_check
saas_jira_check
saas_trello_check
scrape_publicwww
search_bgp
search_bing
search_builtwith
search_censys
search_crt
search_edgar
search_github
search_github_code
search_have_i_been_pwned
search_opencorporates
search_phishtank
search_project_honeypot
search_robtex
search_shodan
search_sublister
search_threatcrowd
search_towerdata
search_virustotal
search_whoisology
security_trails_historical_dns
security_trails_historical_whois
security_trails_nameserver_search
security_trails_subdomain_search
snmp_walk
tcp_bind_and_collect
uri_analyze_target
uri_brute
uri_brute_common_content
uri_brute_creds
uri_brute_focused_content
uri_check_security_headers
uri_check_subdomain_hijack
uri_enumerate_js
uri_extract_metadata
uri_gather_linked_content
uri_gather_robots
uri_gather_sitemap
uri_gather_ssl_certificate
uri_screenshot
uri_spider
uri_youtube_metadata
vulns/apache_struts_jakarta_parser
vulns/cisco_smart_install_scan
vulns/etcd_harvester
vulns/ssrf_brute_parameter
vulns/ssrf_proxy_host_header
vulns/tomcat_put_jsp
web_account_check
whois_lookup

Intrigue Core Built-in Tasks

aws_ec2_gather_instances
aws_s3_brute
convert_entity
create_entity
create_service
dns_brute_srv
dns_brute_sub
dns_brute_sub_async
dns_brute_sub_over_http
dns_brute_tld
dns_lookup_mx
dns_lookup_txt
dns_permute
dns_recurse_spf
dns_search_sonar
dns_snoop_cache
dns_transfer_zone
email_brute_gmail_glxu
email_harvest
email_validate
enrich/aws_s3_bucket
enrich/dns_record
enrich/domain
enrich/generic
enrich/github_account

enrich/ip_address
enrich/nameserver
enrich/net_block
enrich/network_service
enrich/organization
enrich/ssl_certificate
enrich/uri
enumerate_nameservers
finger_extraction
ftp_enumerate
gitrob **
import/arin_ipv4_ranges
import/aws_ipv4_ranges
import/data_file
import/domainlist_domains
import/shodan_json_tmp
import/umbrella_top_domains
import/umbrella_top_sites
ip_geolocate
masscan_scan
net_block_expand
network_service_fuzz
nmap_scan
phone_number_lookup
saas_google_calendar_check
saas_google_groups_check
saas_jira_check

saas_trello_check
scrape_publicwww
search_bgp
search_bing
search_builtwith
search_censys
search_crt
search_edgar
search_github
search_github_code
search_have_i_been_pwned
search_opencorporates
search_phishtank
search_project_honeypot
search_robtex
search_shodan
search_sublister
search_threatcrowd
search_towerdata
search_virustotal
search_whoisology
security_trails_historical_dns
security_trails_historical_whois
security_trails_nameserver_search
security_trails_subdomain_search
snmp_walk

tcp_bind_and_collect
uri_analyze_target
uri_brute
uri_brute_common_content
uri_brute_creds
uri_brute_focused_content
uri_check_security_headers
uri_check_subdomain_hijack
uri_enumerate_js
uri_extract_metadata
uri_gather_linked_content
uri_gather_robots
uri_gather_sitemap
uri_gather_ssl_certificate
uri_screenshot
uri_spider
uri_youtube_metadata
vulns/apache_struts_jakarta_parser
vulns/cisco_smart_install_scan
vulns/etcd_harvester
vulns/ssrf_brute_parameter
vulns/ssrf_proxy_host_header
vulns/tomcat_put_jsp
web_account_check
whois_lookup

Intrigue Core Built-in Tasks

aws_ec2_gather_instances
aws_s3_brute
convert_entity
create_entity
create_service
dns_brute_srv
dns_brute_sub
dns_brute_sub_async
dns_brute_sub_over_http
dns_brute_tld
dns_lookup_mx
dns_lookup_txt
dns_permute
dns_recurse_spf
dns_search_sonar
dns_snoop_cache
dns_transfer_zone
email_brute_gmail_glxu
email_harvest
email_validate
enrich/aws_s3_bucket
enrich/dns_record
enrich/domain
enrich/generic
enrich/github_account

enrich/ip_address
enrich/nameserver
enrich/net_block
enrich/network_service
enrich/organization
enrich/ssl_certificate
enrich/uri
enumerate_nameservers
finger_extraction
ftp_enumerate
gitrob
import/arin_ipv4_ranges
import/aws_ipv4_ranges
import/data_file
import/domainlist_domains
import/shodan_json_tmp
import/umbrella_top_domains
import/umbrella_top_sites
ip_geolocate
masscan_scan
net_block_expand
network_service_fuzz
nmap_scan
phone_number_lookup
saas_google_calendar_check
saas_google_groups_check
saas_jira_check

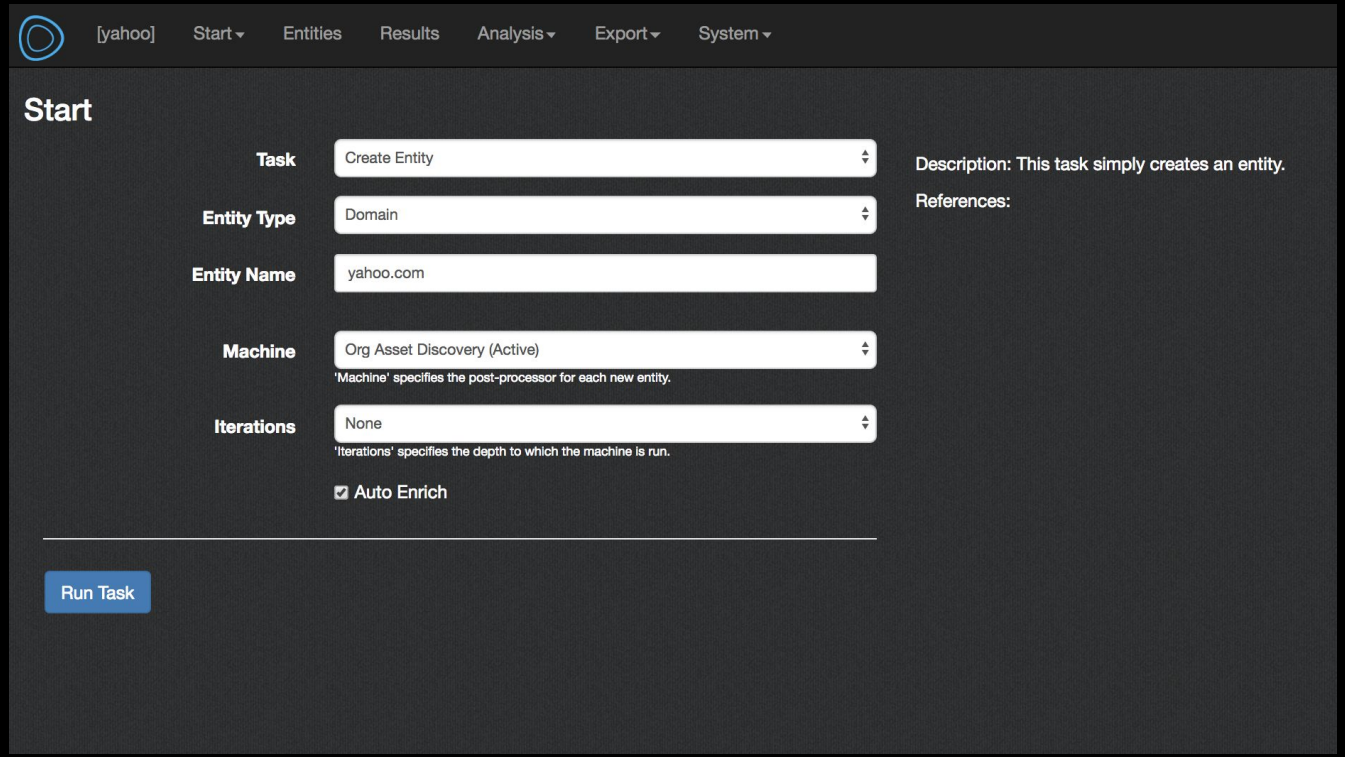
saas_trello_check
scrape_publicwww
search_bgp
search_bing
search_builtwith
search_censys
search_crt
search_edgar
search_github
search_github_code
search_have_i_been_pwned
search_opencorporates
search_phishtank
search_project_honeypot
search_robtex
search_shodan
search_sublister
search_threatcrowd
search_towerdata
search_virustotal
search_whoisology
security_trails_historical_dns
security_trails_historical_whois
security_trails_nameserver_search
security_trails_subdomain_search
snmp_walk

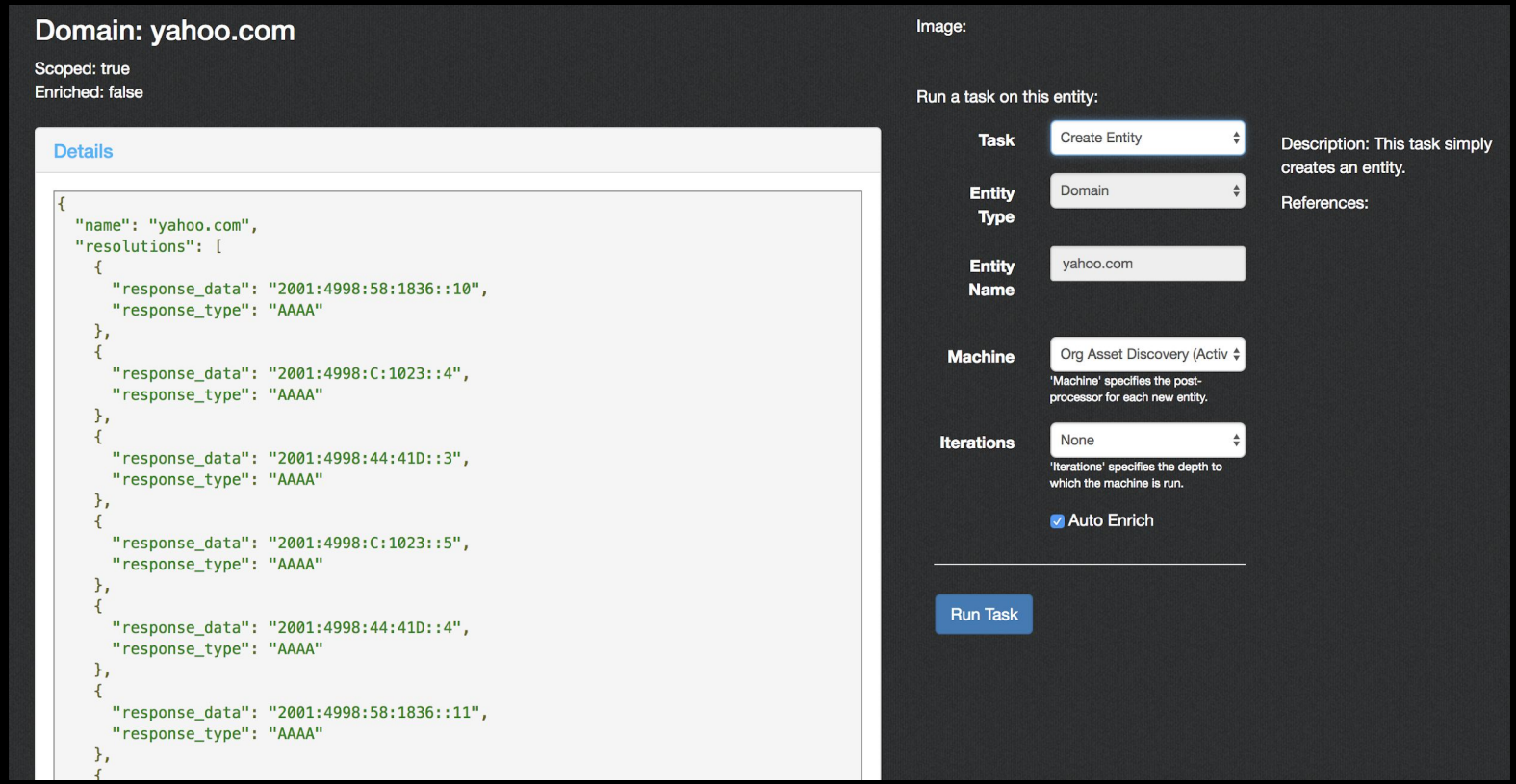
tcp_bind_and_collect
uri_analyze_target
uri_brute
uri_brute_common_content
uri_brute_creds
uri_brute_focused_content
uri_check_security_headers
uri_check_subdomain_hijack
uri_enumerate_js
uri_extract_metadata
uri_gather_linked_content
uri_gather_robots
uri_gather_sitemap
uri_gather_ssl_certificate
uri_screenshot
uri_spider
uri_youtube_metadata
vulns/apache_struts_jakarta_parser
vulns/cisco_smart_install_scan
vulns/etcd_harvester
vulns/ssrf_brute_parameter
vulns/ssrf_proxy_host_header
vulns/tomcat_put_jsp
web_account_check
whois_lookup

Intrigue Core Built-in Tasks

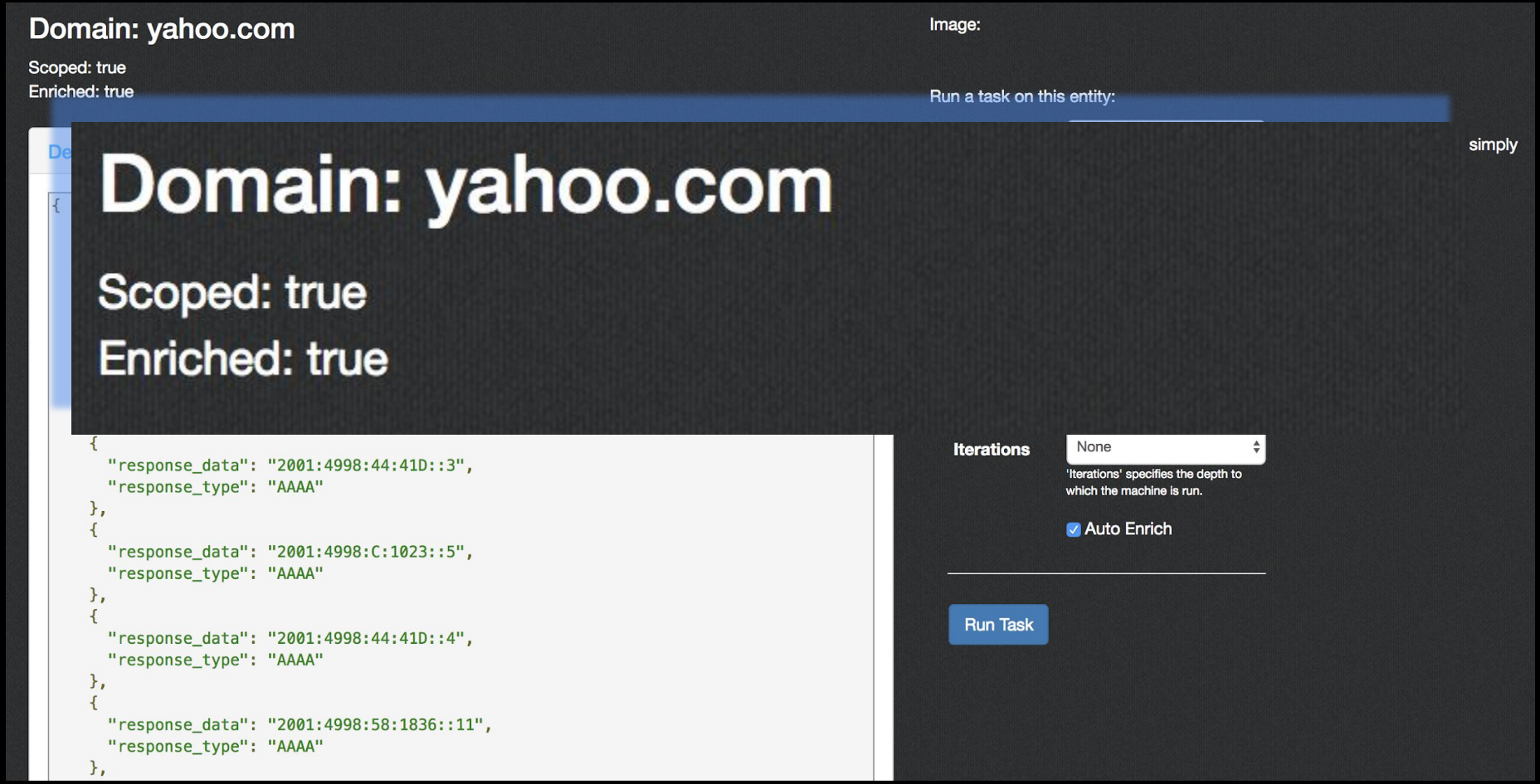
autonomous_system	github_account	person
aws_credential	github_repository	phone_number
aws_s3_bucket	info	physical_location
credential	ip_address	screenshot
dns_record	nameserver	software_package
document	net_block	ssl_certificate
domain	network_service	string
email_address	organization	uri
file		web_account

Intrigue Core Built-In Entities


[yahoo]
Start
Entities
Results
Analysis
Export
System
Start
Task
Create Entity
Entity Type
Domain
Entity Name
yahoo.com
Machine
Org Asset Discovery (Active)
'Machine' specifies the post-processor for each new entity.
Iterations
None
'Iterations' specifies the depth to which the machine is run.
Auto Enrich
Run Task
Description: This task simply creates an entity.
References:



Enrichment builds out the entity.


Domain: yahoo.com
Scoped: true
Enriched: true
Image:
Run a task on this entity:
simply
Domain: yahoo.com
Scoped: true
Enriched: true
{
"response_data": "2001:4998:44:41D::3",
"response_type": "AAAA"
},
{
"response_data": "2001:4998:C:1023::5",
"response_type": "AAAA"
},
{
"response_data": "2001:4998:44:41D::4",
"response_type": "AAAA"
},
{
"response_data": "2001:4998:58:1836::11",
"response_type": "AAAA"
},
Iterations
None
'Iterations' specifies the depth to which the machine is run.
Auto Enrich
Run Task

Domain: yahoo.com

Scoped: true
Enriched: true

Details

Alias Group: 11414
Aliases:
- Domain: yahoo.com

Ancestors:

Tasks that created this entity:
- create_entity (Domain: yahoo.com)

Tasks run on this entity:
- enrich/domain (Domain: yahoo.com)
- create_entity (Domain: yahoo.com)

Entities discovered from this entity:
- Domain: yahoo.com

Alias Group: 11414
Aliases:
- Domain: yahoo.com

Ancestors:

Tasks that created this entity:
- create_entity (Domain: yahoo.com)

Tasks run on this entity:
- enrich/domain (Domain: yahoo.com)
- create_entity (Domain: yahoo.com)

Entities discovered from this entity:
- Domain: yahoo.com

Description: This task simply creates an entity.

References:

Page: 1 Results: 0 .. 28 previous next

timestamp	result	entity count	complete
2019-03-03 01:09:42 -0600	enrich/domain on Domain: yahoodns.net	1	complete
2019-03-03 01:09:38 -0600	enrich/domain on Domain: 2.ip6.arpa	0	complete
2019-03-03 01:09:38 -0600	enrich/domain on Domain: 2.ip6.arpa	0	complete
2019-03-03 01:09:37 -0600	enrich/ip_address on IpAddress: 72.30.35.10	2	complete
2019-03-03 01:09:37 -0600	enrich/dns_record on DnsRecord: 3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.1.4.0.4.4.0.0.8.9.9.4.1.0.0.2.ip6.arpa	2	complete
2019-03-03 01:09:37 -0600	enrich/dns_record on DnsRecord: 4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.1.4.0.4.4.0.0.8.9.9.4.1.0.0.2.ip6.arpa	2	complete
2019-03-03 01:09:37 -0600	enrich/dns_record on DnsRecord: 0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.3.8.1.8.5.0.0.8.9.9.4.1.0.0.2.ip6.arpa	2	complete
2019-03-03 01:09:37 -0600	enrich/ip_address on IpAddress: 98.137.246.8	2	complete
2019-03-03 01:09:37 -0600	enrich/dns_record on DnsRecord: 4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.2.0.1.c.0.0.0.8.9.9.4.1.0.0.2.ip6.arpa	2	complete
2019-03-03 01:09:37 -0600	enrich/dns_record on DnsRecord: media-router-fp1.prod1.media.vip.ne1.yahoo.com	3	complete
2019-03-03 01:09:37 -0600	enrich/dns_record on DnsRecord: 5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.2.0.1.c.0.0.0.8.9.9.4.1.0.0.2.ip6.arpa	2	complete
2019-03-03 01:09:37 -0600	enrich/dns_record on DnsRecord: media-router-fp2.prod1.media.vip.ne1.yahoo.com	3	complete
2019-03-03 01:09:37 -0600	enrich/dns_record on DnsRecord: 1.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.3.8.1.8.5.0.0.8.9.9.4.1.0.0.2.ip6.arpa	2	complete
2019-03-03 01:09:37 -0600	enrich/dns_record on DnsRecord: media-router-fp1.prod1.media.vip.gq1.yahoo.com	3	complete
2019-03-03 01:09:36 -0600	enrich/dns_record on DnsRecord: media-router-fp1.prod1.media.vip.bf1.yahoo.com	3	complete
2019-03-03 01:09:36 -0600	enrich/ip_address on IpAddress: 72.30.35.9	2	complete
2019-03-03 01:09:36 -0600	enrich/dns_record on DnsRecord: media-router-fp2.prod1.media.vip.gq1.yahoo.com	3	complete
2019-03-03 01:09:36 -0600	enrich/dns_record on DnsRecord: media-router-fp2.prod1.media.vip.bf1.yahoo.com	3	complete
2019-03-03 01:09:36 -0600	enrich/ip_address on IpAddress: 98.138.219.231	2	complete
2019-03-03 01:09:36 -0600	enrich/ip_address on IpAddress: 98.137.246.7	2	complete
2019-03-03 01:09:36 -0600	enrich/ip_address on IpAddress: 98.138.219.232	2	complete
2019-03-03 01:09:36 -0600	enrich/ip_address on IpAddress: 2001:4998:44:41d::3	2	complete
2019-03-03 01:09:35 -0600	enrich/ip_address on IpAddress: 2001:4998:c:1023::4	2	complete
2019-03-03 01:09:35 -0600	enrich/ip_address on IpAddress: 2001:4998:c:1023::5	2	complete
2019-03-03 01:09:35 -0600	enrich/ip_address on IpAddress: 2001:4998:44:41d::4	2	complete
2019-03-03 01:09:35 -0600	enrich/ip_address on IpAddress: 2001:4998:58:1836::11	2	complete
2019-03-03 01:09:35 -0600	enrich/ip_address on IpAddress: 2001:4998:58:1836::10	2	complete
2019-03-03 01:09:34 -0600	enrich/domain on Domain: yahoo.com	14	complete
2019-03-03 01:09:34 -0600	create_entity on Domain: yahoo.com	1	complete

Cancel All

Enrichment can trigger new tasks too.

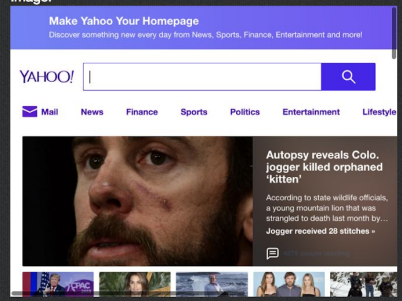
Uri: https://yahoo.com

Scoped: true
Enriched: true

Details


```
{
  "name": "https://yahoo.com",
  "api_endpoint": false,
  "code": "200",
  "title": "Yahoo",
  "generator": null,
  "verbs": null,
  "scripts": [
    "https://s.yimg.com/aaq/cmp/version/2.14.0/cmp.js",
    "https://s.yimg.com/rq/darla/3-6-3/js/g-r-min.js",
    "https://s.yimg.com/aaq/wf/wf-core-1.18.0.js",
    "https://s.yimg.com/zz/combo?yui:/3.18.0/yui/yui-min.js",
    "https://s.yimg.com/ss/rapid-3.53.2.js",
    "https://s.yimg.com/aaq/wf/wf-fetch-1.10.5.js",
    "https://s.yimg.com/aaq/wf/wf-rapid-1.0.7.js",
    "https://s.yimg.com/aaq/wf/wf-toggle-1.3.3.js",
    "https://s.yimg.com/os/mit/td/aperollup-min-c9473dd9_desktop_advance.js",
    "https://s.yimg.com/os/mit/td/td-applet-breakingnews-atomic-0.0.59/r-min.js",
    "https://s.yimg.com/os/mit/td/td-applet-stream-atomic-2.0.1698/r-min.js",
    "https://s.yimg.com/os/mit/td/td-applet-amplify-hpset-1.0.45/r-min.js",
    "https://s.yimg.com/os/mit/td/td-applet-weather-atomic-0.0.210/r-min.js",
    "https://s.yimg.com/os/mit/td/td-applet-yahooview-0.0.25/r-min.js",
    "https://s.yimg.com/os/mit/td/td-applet-astro-atomic-0.0.24/r-min.js",
    "https://s.yimg.com/os/mit/td/td-applet-mega-header-1.0.853/r-min.js",
    "https://s.yimg.com/os/yaft/yaft-0.3.26.min.js",
    "https://s.yimg.com/os/yaft/yaft-plugin-aftnoad-0.1.5.min.js"
  ],
  "headers": [
    "date: Sat, 02 Mar 2019 22:03:10 GMT",
    "p3p: policyref=\"https://policies.yahoo.com/w3c/p3p.xml\", CP=\"CAO DSP COR CUR ADM DEV TAI PSA PSD IVA
i IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA P
RE LOC GOV\"",
    "cache-control: no-store, no-cache, max-age=0, private",
    "strict-transport-security: max-age=31536000",
    "accept-ch: device-memory, dpr, width, viewport-width, rtt, downlink, ect",
    "accept-ch-lifetime: 604800",
    "x-frame-options: SAMEORIGIN",
```


Image:



Run a task on this entity:

Task Create Entity

Entity Type Uri

Entity Name https://yahoo.com

Machine Org Asset Discovery (Active)

'Machine' specifies the post-processor for each new entity.

Iterations None

'Iterations' specifies the depth to which the machine is run.

☑ Auto Enrich

Run Task

Description: This task simply an entity.

References:

Enrichment on an entity of type **Uri.**

Service Fingerprinting with Recog

Ideal Qualities

Application & Network
Comprehensive
Easy to Extend
Version-Aware
Vulnerability-Aware
Browser Enabled
Free (as in Freedom)
XML

```
<fingerprints matches="ssh.banner">
  <fingerprint pattern="^RomSShell_([\d\.]+)$">
    <description>Allegro RomSShell SSH</description>
    <example service.version="4.62">RomSShell_4.62</example>
    <param pos="0" name="service.vendor" value="Allegro"/>
    <param pos="0" name="service.product" value="RomSShell"/>
    <param pos="1" name="service.version"/>
  </fingerprint>
</fingerprints>
```

(Thanks @jonhart and @rapid7!)

Application Fingerprinting with Ident

```
jcran ident master [20190228]$ ./util/check.rb https://www.securitybsides.com
Checking... https://www.securitybsides.com
Fingerprint:
 - PbWorks PbWorks    - unique link (CPE: cpe:2.3:a:pbworks:pbworks::) (Tags: ["SaaS"])
 - Google Analytics    - UA string (CPE: cpe:2.3:s:google:analytics::) (Tags: ["Marketing", "Javascript"])
 - Cloudflare Cloudflare    - Cloudflare Accelerated Page (CPE: cpe:2.3:s:cloudflare:cloudflare::) (Tags: ["CDN"])
Content Checks:
 - Authentication - HTTP: false
 - Authentication - Forms: true
 - Access-Control-Allow-Origin Header: false
 - P3P Header: false
 - X-Frame-Options Header: true
 - X-XSS-Protection Header: false
 - Google Urchin Account Detected: false
 - Directory Listing Detected: false
 - Form Detecteds: true
 - File Upload Form Detected: false
 - Email Addresses Detected: ["jackadaniel@gmail.com"]
```

Application & Network
Comprehensive
Easy to Extend
Version-Aware
Vulnerability-Aware
Browser Enabled
Free (as in Freedom)
JSON

We can use enrichment to match vulnerabilities to the application as soon as fingerprinting is complete.


```
    "hide": null,
    "cpe": "cpe:2.3:a:apache:coyote:1.1:",
    "vulns": [

    ]
  },
  {
    "type": "fingerprint",
    "vendor": "Apache",
    "product": "Tomcat",
    "version": "6.0.14",
    "update": "",
    "tags": [
      "Application Server"
    ],
    "matched_content": "(?-mix:<title>Apache Tomcat)",
    "match_type": "content_body",
    "match_details": "Tomcat Application Server",
    "hide": null,
    "cpe": "cpe:2.3:a:apache:tomcat:6.0.14:",
    "vulns": [
      {
        "cve_id": "CVE-2011-2526",
        "cwe_id": null,
        "cvss_v2": {
          "score": null,
          "vector": null
        },
        "cvss_v3": {
          "score": null,
          "vector": null
        }
      },
      {
        "cve_id": "CVE-2011-2204",
        "cwe_id": null,
        "cvss_v2": {
          "score": null,
          "vector": null
        },
        "cvss_v3": {
          "score": null,
```

Let’s put these concepts in action to…

Broadly Discover Assets
Enumerate App Stacks
Identify Issues

DNSGrep (intrigue-core: dns_search_sonar)

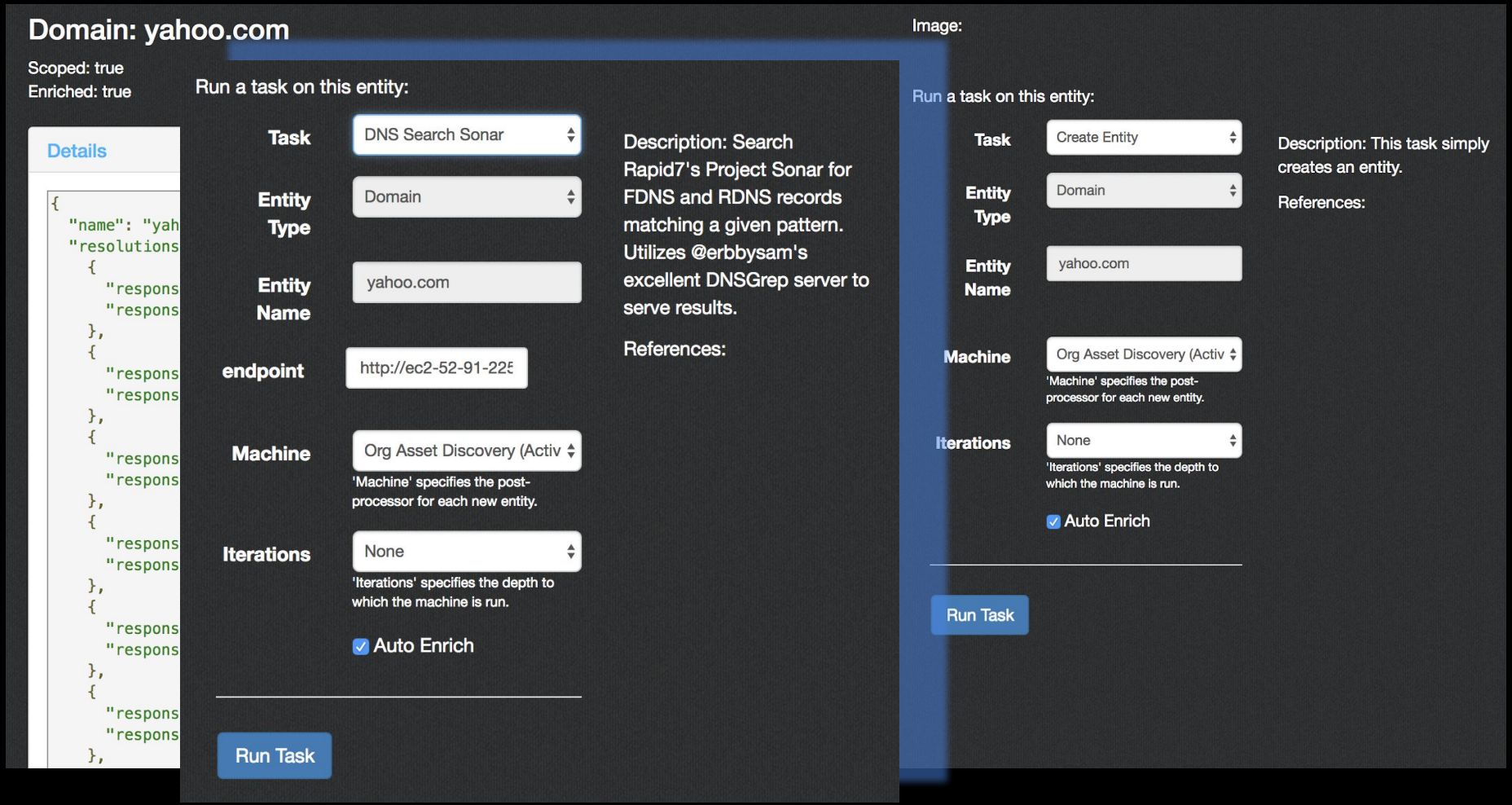
```
ubuntu@client:~$ time gunzip -c fdns_a.json.gz | grep "erbbysam.com"
{"timestamp":"1535127239","name":"blog.erbbysam.com","type":"a","value":"54.190.33.12
5"}
 {"timestamp":"1535133613","name":"erbbysam.com","type":"a","value":"104.154.120.133"}
 {"timestamp":"1535155246","name":"www.erbbysam.com","type":"cname","value":"erbbysam.
com"}
 real    11m31.393s
 user    12m29.212s
 sys     1m37.672s
```

vs

```
ubuntu@client:~$ ls -lath fdns_a.sort.txt
-rw-rw-r-- 1 ubuntu ubuntu 68G Feb  3 09:11 fdns_a.sort.txt
ubuntu@client:~$ time ./dnsgrep -f fdns_a.sort.txt -i "erbbysam.com"
104.154.120.133,erbbysam.com
54.190.33.125,blog.erbbysam.com
erbbysam.com,www.erbbysam.com

real    0m0.002s
user    0m0.000s
sys     0m0.000s
```

(thanks @erbbysam!)


Domain: yahoo.com
Scoped: true
Enriched: true
Details
{
"name": "yah
"resolutions
{
"respons
"respons
},
{
"respons
"respons
},
{
"respons
"respons
},
{
"respons
"respons
},
{
"respons
"respons
},
{
"respons
"respons
},
Run a task on this entity:
Task
DNS Search Sonar
Entity Type
Domain
Entity Name
yahoo.com
endpoint
http://ec2-52-91-225
Machine
Org Asset Discovery (Activ
'Machine' specifies the post-processor for each new entity.
Iterations
None
'Iterations' specifies the depth to which the machine is run.
Auto Enrich
Run Task
Description: Search Rapid7's Project Sonar for FDNS and RDNS records matching a given pattern. Utilizes @erbbysam's excellent DNSGrep server to serve results.
References:
Image:
Run a task on this entity:
Task
Create Entity
Entity Type
Domain
Entity Name
yahoo.com
Machine
Org Asset Discovery (Activ
'Machine' specifies the post-processor for each new entity.
Iterations
None
'Iterations' specifies the depth to which the machine is run.
Auto Enrich
Run Task
Description: This task simply creates an entity.
References:

Task Result: dns_search_sonar

ID: 14715

Start: 2019-03-02 02:15:27 -0600

End:

Elapsed (s):

Job ID: ac8e9c85afec8f3416df7dd7

Handlers: []

Depth: 1

Entity: Domain: yahoo.com

Options: [{"name"=>"endpoint", "value"=>"http://ec2-52-91-225-3.compute-1.amazonaws.com/dns?q="}]

Cancelled: false (Cancel)

Complete: false

Entity Count: 0

Machine:

Max Depth:

Whitelist Strings:

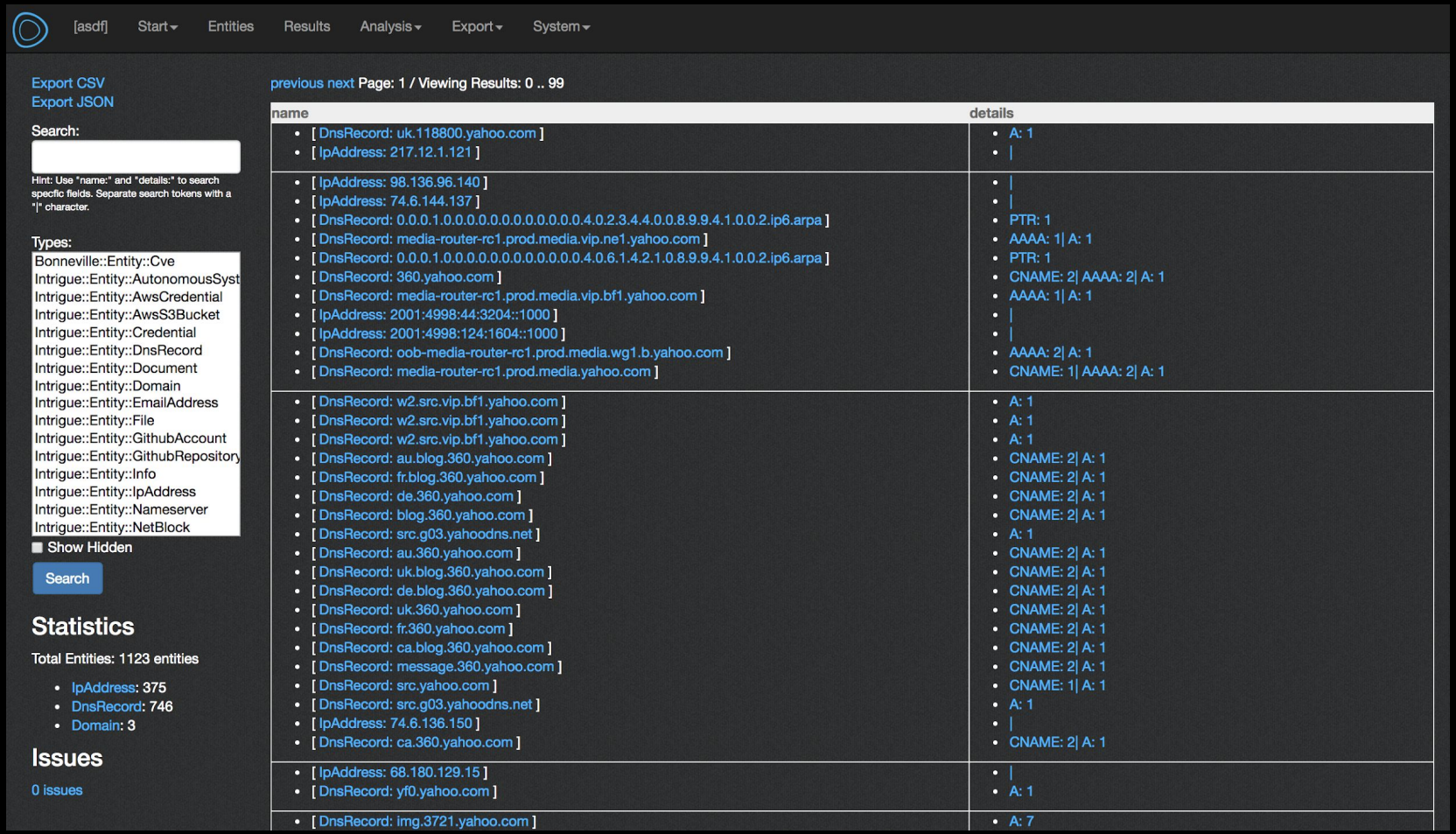
Export:

- JSON

Entities:

- DnsRecord: restore-trad-13.hff01.ne1.yahoo.com
- DnsRecord: flk-udb03.hff01.ne1.yahoo.com
- DnsRecord: restore-trad-12.hff01.ne1.yahoo.com
- DnsRecord: flk-udb02.hff01.ne1.yahoo.com
- DnsRecord: restore-trad-11.hff01.ne1.yahoo.com
- DnsRecord: flk-udb01.hff01.ne1.yahoo.com
- DnsRecord: restore-trad-01.hff01.ne1.yahoo.com
- DnsRecord: restore-trad-10.hff01.ne1.yahoo.com
- DnsRecord: tier1-test-60801.ne1.yahoo.com
- DnsRecord: tier1-test-hds-ams02-1.ne1.yahoo.com

```
[_] Options: [{"endpoint"=>"http://ec2-52-91-225-3.compute-1.amazonaws.com/dns?q="}]
[_] Starting task run at 2019-03-02 02:15:27 UTC!
[+] Searching data for: .yahoo.com
[_] Getting http://ec2-52-91-225-3.compute-1.amazonaws.com/dns?q=.yahoo.com, attempt 0
[_] Skipping enrichment... entity exists!
[_] Skipping enrichment... entity exists!
[_] Skipping enrichment... entity exists!
[_] Skipping enrichment... entity exists!
[_] Skipping enrichment... entity exists!
[_] Skipping enrichment... entity exists!
[+] New Entity: DnsRecord ns21.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord yns21.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord src1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord bas1-1.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord ir-120.bas1-1.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord lo0.bas1-1.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord ir-121.bas1-1.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord ir-108.bas1-1.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord ywvv-01.infra.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord koprol-smtp.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord l1.ycs.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord l2.ycs.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord r1-ops.dns.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord r2-ops.dns.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord tool1.ops.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord ttfp1-vm1.ops.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord ybiip1.ops.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord tftp1.ops.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord tier1-test-hds-ams01-0.ne1.yahoo.com. Scoped: true. No-Traverse:
false
[+] New Entity: DnsRecord tier1-test-hds-ams02-0.ne1.yahoo.com. Scoped: true. No-Traverse:
false
[+] New Entity: DnsRecord oxy-oxygen-628afb10.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce10.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord usw10.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord lo0.cry10.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord lo6.cry10.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce20.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce30.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-628ade30.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce40.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-628ade40.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce50.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-628af260.ne1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce60.ne1.yahoo.com. Scoped: true. No-Traverse: false
```


[asdf]
Start
Entities
Results
Analysis
Export
System
Export CSV
Export JSON
Search:
Hint: Use "name:" and "details:" to search specific fields. Separate search tokens with a "|" character.
Types:
Bonneville::Entity::Cve
Intrigue::Entity::AutonomousSyst
Intrigue::Entity::AwsCredential
Intrigue::Entity::AwsS3Bucket
Intrigue::Entity::Credential
Intrigue::Entity::DnsRecord
Intrigue::Entity::Document
Intrigue::Entity::Domain
Intrigue::Entity::EmailAddress
Intrigue::Entity::File
Intrigue::Entity::GithubAccount
Intrigue::Entity::GithubRepository
Intrigue::Entity::Info
Intrigue::Entity::IpAddress
Intrigue::Entity::Nameserver
Intrigue::Entity::NetBlock
Show Hidden
Search
Statistics
Total Entities: 1123 entities
IpAddress: 375
DnsRecord: 746
Domain: 3
Issues
0 issues
previous next Page: 1 / Viewing Results: 0 .. 99
name
details
[DnsRecord: uk.118800.yahoo.com]
[IpAddress: 217.12.1.121]
A: 1
|
[IpAddress: 98.136.96.140]
[IpAddress: 74.6.144.137]
[DnsRecord: 0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.2.3.4.4.0.0.8.9.9.4.1.0.0.2.ip6.arpa]
[DnsRecord: media-router-rc1.prod.media.vip.ne1.yahoo.com]
[DnsRecord: 0.0.0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.6.1.4.2.1.0.8.9.9.4.1.0.0.2.ip6.arpa]
[DnsRecord: 360.yahoo.com]
[DnsRecord: media-router-rc1.prod.media.vip.bf1.yahoo.com]
[IpAddress: 2001:4998:44:3204::1000]
[IpAddress: 2001:4998:124:1604::1000]
[DnsRecord: oob-media-router-rc1.prod.media.wg1.b.yahoo.com]
[DnsRecord: media-router-rc1.prod.media.yahoo.com]
|
|
PTR: 1
AAAA: 1| A: 1
PTR: 1
CNAME: 2| AAAA: 2| A: 1
AAAA: 1| A: 1
|
|
AAAA: 2| A: 1
CNAME: 1| AAAA: 2| A: 1
[DnsRecord: w2.src.vip.bf1.yahoo.com]
[DnsRecord: w2.src.vip.bf1.yahoo.com]
[DnsRecord: w2.src.vip.bf1.yahoo.com]
[DnsRecord: au.blog.360.yahoo.com]
[DnsRecord: fr.blog.360.yahoo.com]
[DnsRecord: de.360.yahoo.com]
[DnsRecord: blog.360.yahoo.com]
[DnsRecord: src.g03.yahoodns.net]
[DnsRecord: au.360.yahoo.com]
[DnsRecord: uk.blog.360.yahoo.com]
[DnsRecord: de.blog.360.yahoo.com]
[DnsRecord: uk.360.yahoo.com]
[DnsRecord: fr.360.yahoo.com]
[DnsRecord: ca.blog.360.yahoo.com]
[DnsRecord: message.360.yahoo.com]
[DnsRecord: src.yahoo.com]
[DnsRecord: src.g03.yahoodns.net]
[IpAddress: 74.6.136.150]
[DnsRecord: ca.360.yahoo.com]
A: 1
A: 1
A: 1
CNAME: 2| A: 1
CNAME: 2| A: 1
CNAME: 2| A: 1
CNAME: 2| A: 1
A: 1
CNAME: 2| A: 1
CNAME: 2| A: 1
CNAME: 2| A: 1
CNAME: 2| A: 1
CNAME: 2| A: 1
CNAME: 2| A: 1
CNAME: 2| A: 1
CNAME: 1| A: 1
A: 1
|
CNAME: 2| A: 1
[IpAddress: 68.180.129.15]
[DnsRecord: yf0.yahoo.com]
|
A: 1
[DnsRecord: img.3721.yahoo.com]
A: 7

How can we get a list of applications?

```
if domain?
  - dns_search_sonar
  - dns_brute_async
  - search_security_trails

elsif ip_address?
  - check_network_ranges
  - port_scan

elsif network_range?
  - masscan

elsif ftp_server?
  - pull_ftp_server

elsif s3_bucket?
  - check_s3_bucket

else
  #nothing to do!
end
```

Machines use **recursion** to kick off tasks.

Servers:

-/-: 2
ATS/5.3.0: 1
AkamaiGHost: 4
Apache: 286
Apache (Server): 52
Apache-Coyote/1.1: 21
Apache/2.2: 18
Apache/2.2.15 (CentOS): 1
Apache/2.2.15 (Red Hat): 1
Apache/2.2.15 (Red Hat) DAV/2 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips: 3
Apache/2.2.15 (Unix) mod_ssl/2.2.15 OpenSSL/0.9.8l mod_jk/1.2.23 PHP/5.3.0: 1
Apache/2.2.17 (Unix) mod_jk/1.2.31: 5
Apache/2.2.20 (Unix) PHP/5.3.27: 2
Apache/2.2.24 (Unix): 6
Apache/2.2.27 (CentOS): 4
Apache/2.2.3 (CentOS): 4
Apache/2.4.18 (Ubuntu): 22
Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30: 1
Apache/2.4.27 (Unix) CiscoSSL/1.0.2k.6.1.188-fips: 1
Apache/2.4.29 (Ubuntu): 4
Apache/2.4.6 (CentOS): 3
Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips: 3
Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips: 3
Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 mod_wsgi/3.4 Python/2.7.5: 1
Apache/2.4.6 (Red Hat Enterprise Linux) mod_jk/1.2.42 OpenSSL/1.0.2k-fips: 4
Apache/2.4.7 (Ubuntu): 5
CE_C: 3
CE_E: 36
CherryPy/17.0.0: 1
Cisco Stealthwatch 1.0.1: 2

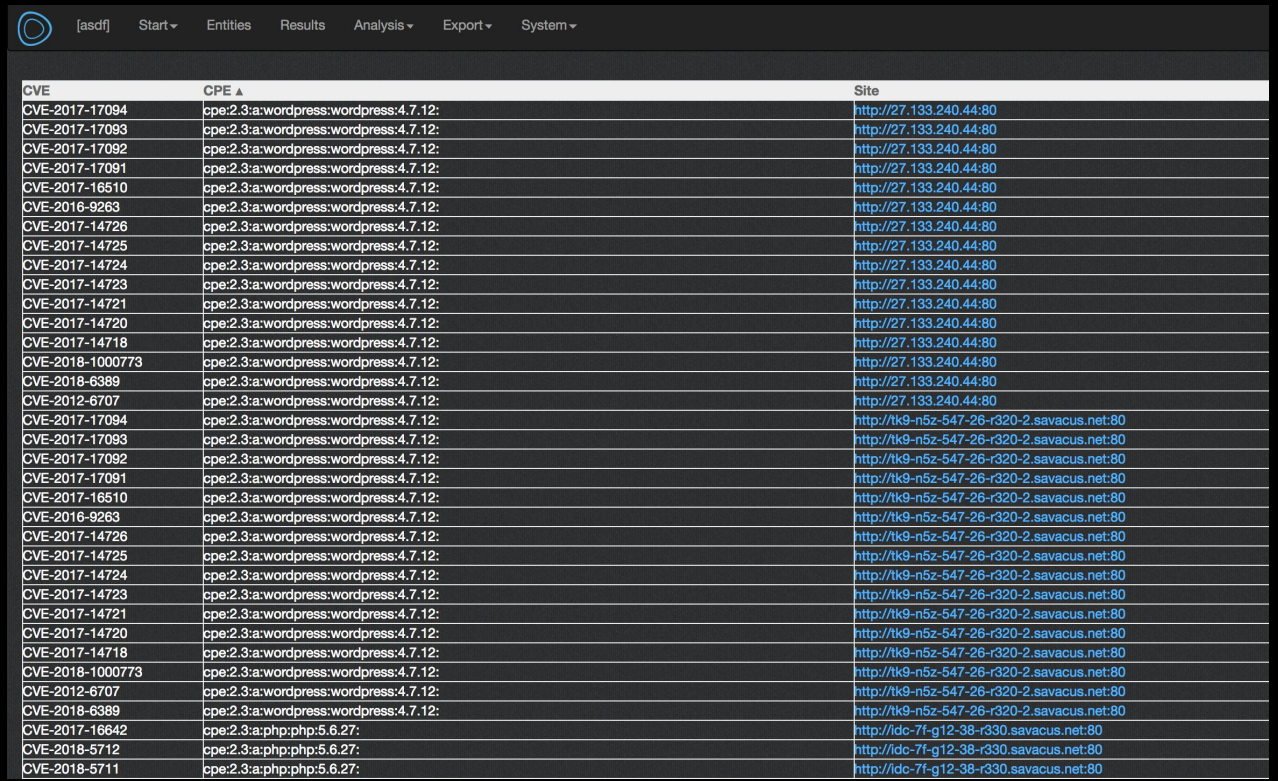
Applications:

4.0.30319: 2
ASP.NET: 37
Akamai Akamai : 6
Amazon Cloudfront : 3
Apache Coyote 1.1: 21
Apache HTTP Server : 283
Apache HTTP Server 2.2: 17
Apache HTTP Server 2.2.15: 6
Apache HTTP Server 2.2.17: 5
Apache HTTP Server 2.2.20: 2
Apache HTTP Server 2.2.24: 6
Apache HTTP Server 2.2.27: 4
Apache HTTP Server 2.2.3: 4
Apache HTTP Server 2.4.18: 22
Apache HTTP Server 2.4.25: 1
Apache HTTP Server 2.4.27: 1
Apache HTTP Server 2.4.29: 4
Apache HTTP Server 2.4.6: 14
Apache HTTP Server 2.4.7: 5
Apache Tomcat 6.0-snapshot: 1
Apache Tomcat 6.0.14: 1
Apache Tomcat 7.0.28: 3
Apache Tomcat 7.0.52: 1
Apache Tomcat 7.0.82: 1
Apache Tomcat 8.0.14 (Ubuntu): 1
Apache Tomcat 8.0.32 (Ubuntu): 2
Apache Tomcat Apache Tomcat: 9
Apache mod_fcgid 2.3.9: 1
Apache mod_jk 1.2.23: 1
Apache mod_jk 1.2.31: 5

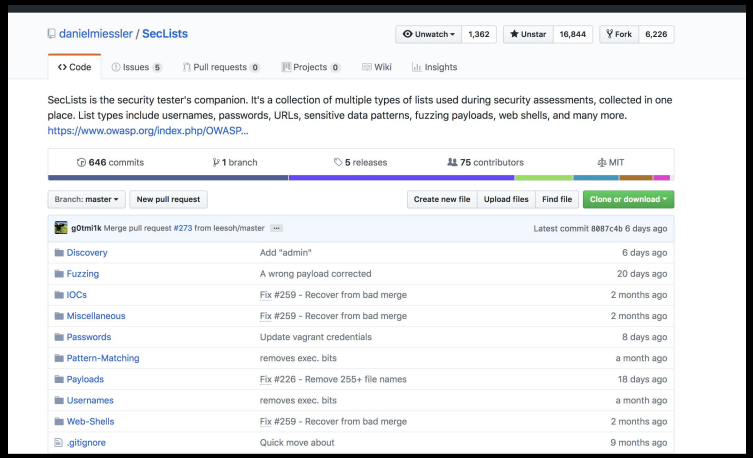
Includes:

Bootstrap: 12
Cloudflare: 11
Drupal: 3
Facebook: 69
Google Analytics: 2
JQuery: 32
Wordpress: 1

Vulns from CPEs!



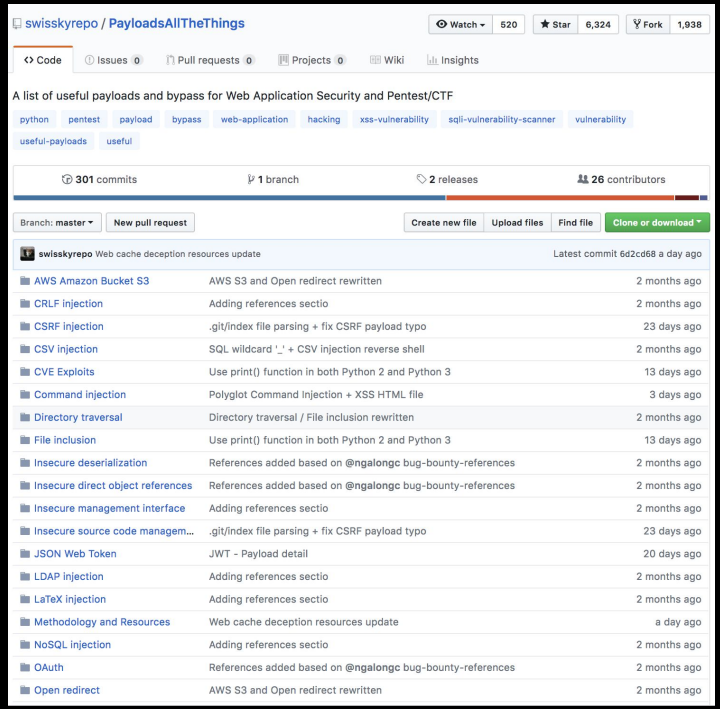
CVE	CPE ▲	Site
CVE-2017-17094	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-17093	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-17092	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-17091	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-16510	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2016-9263	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-14726	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-14725	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-14724	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-14723	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-14721	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-14720	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-14718	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2018-1000773	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2018-6389	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2012-6707	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://27.133.240.44:80
CVE-2017-17094	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-17093	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-17092	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-17091	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-16510	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2016-9263	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-14726	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-14725	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-14724	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-14723	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-14721	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-14720	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-14718	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2018-1000773	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2012-6707	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2018-6389	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-r320-2.savacus.net:80
CVE-2017-16642	cpe:2.3:a:php:php:5.6.27:	http://idc-7f-g12-38-r330.savacus.net:80
CVE-2018-5712	cpe:2.3:a:php:php:5.6.27:	http://idc-7f-g12-38-r330.savacus.net:80
CVE-2018-5711	cpe:2.3:a:php:php:5.6.27:	http://idc-7f-g12-38-r330.savacus.net:80



Now let's do some content discovery!

FuzzDB Project

Official FuzzDB Project Repo



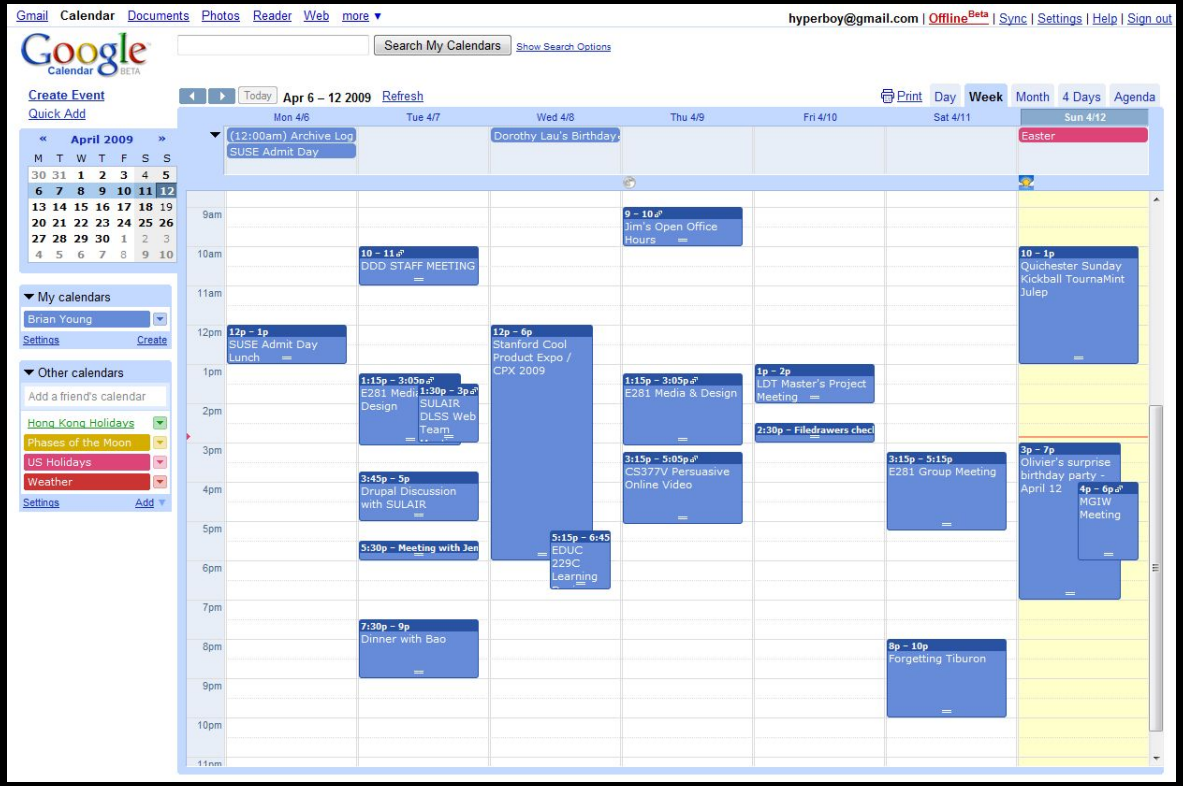
uri_brute_focused_content

```
# technology specifics
apache_list = [
  { path: "/.htaccess", regex: /AuthName/, status: "confirmed" },
  { path: "/.htaccess.bak", regex: /AuthName/, status: "confirmed" },
  { path: "/.htpasswd", regex: /^\w:.*$/ }
]

asp_net_list = [
  { path: "/elmah.axd", regex: nil },
  { path: "/web.config", regex: nil },
  { path: "/Trace.axd", :regex => /Microsoft \.NET Framework Version/, :status => "confirmed" }
]

coldfusion_list = [
  { path: "/CFIDE", regex: nil },
  { path: "CFIDE/administrator/enter.cfm",  :regex => nil }
] # TODO see metasploit for more ideas here


jenkins_list = [
  { path: "/view/All/builds", regex: nil },
  { path: "/view/All/newjob",  :regex => nil },
  { path: "/asynchPeople/",  :regex => nil },
```



… misconfigurations too: saas_google_calendar_check

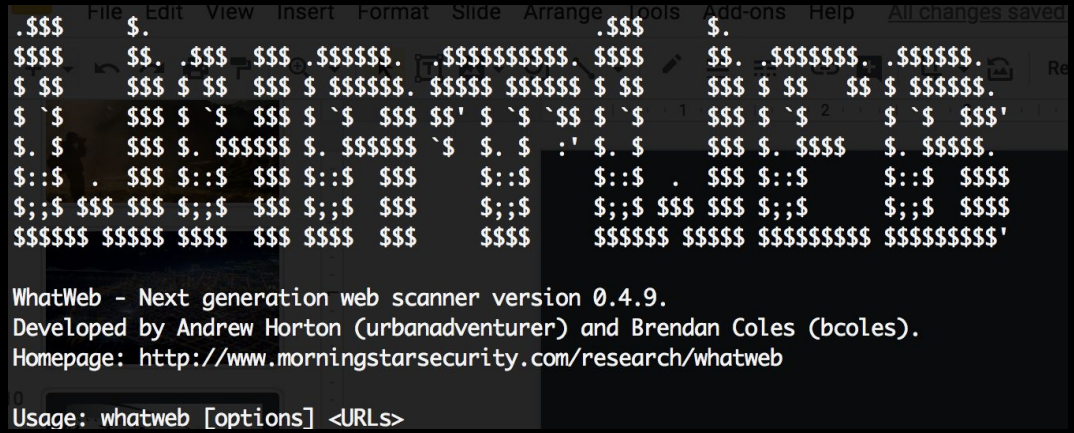
Putting It All Together...
(Demo Time!)

Try it out
Spread the word
Send us ideas
Make a pull request

Thank You!

@jcran
@jgamblin

@intrigueio
https://core.intrigue.io



Ideal Qualities

Application &
Network
Comprehensive
Easy to Extend
Version-Aware
Vulnerability-Aware
Browser Enabled
Free (as in Freedom)

Ideal Qualities

Application & Network

Comprehensive

Easy to Extend

Version-Aware

Vulnerability-Aware

Browser Enabled

Free (as in Freedom)

JSON

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-01 10:05 CST
Nmap scan report for securitybsides.com (104.18.55.114)
Host is up (0.033s latency).
Other addresses for securitybsides.com (not scanned): 104.18.54.114
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        dnsmasq 2.78-82-g804b86b
| dns-nsid:
|   id.server: Answerx_On_austx-dns-cac-304
|_  bind.version: dnsmasq-2.78-82-g804b86b
80/tcp   open  http          cloudflare
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 400 Bad Request
|     Date: Fri, 01 Mar 2019 16:06:22 GMT
|     Content-Type: text/html
|     Content-Length: 171
|     Connection: close
|     Server: cloudflare
|     CF-RAY: 4b0c60b39b9d5843-DFW
|     <html>
|     <head><title>400 Bad Request</title></head>
|     <body bgcolor="white">
|     <center><h1>400 Bad Request</h1></center>
|     <hr><center>cloudflare</center>
|     </body>
|     </html>
|   GetRequest:
|     HTTP/1.1 400 Bad Request
|     Date: Fri, 01 Mar 2019 16:06:21 GMT
|     Content-Type: text/html
```


```
uritybsides.comlop [20190301]$ docker run --rm wappalyzer/cli https://www.secu
{"urls":["https://www.securitybsides.com/"],"applications":[{"name":"CloudFlare","
confidence":"100","version":"","icon":"CloudFlare.svg","website":"http://www.cloud
flare.com","categories":[{"31":"CDN"}]},{"name":"Google Analytics","confidence":"1
00","version":"","icon":"Google Analytics.svg","website":"http://google.com/analyt
ics","categories":[{"10":"Analytics"}]},{"name":"Prototype","confidence":"100","ve
rsion":"1.7","icon":"Prototype.png","website":"http://www.prototypejs.org","catego
ries":[{"12":"JavaScript Frameworks"}]},{"name":"Quantcast","confidence":"100","ve
rsion":"","icon":"Quantcast.png","website":"http://www.quantcast.com","categories"
:[{"10":"Analytics"}]},{"name":"YUI","confidence":"100","version":"","icon":"YUI.p
ng","website":"http://yuilibrary.com","categories":[{"12":"JavaScript Frameworks"}
]}],"meta":{"language":"en"}}
```

Ideal Qualities

Application & Network
Comprehensive
Easy to Extend
Version-Aware
Vulnerability-Aware
Browser Enabled
Free (as in Freedom)

But how can we focus on risk?


GREY NOISE
DO KNOW EVIL