

Automating Application Security Bug Hunting

Improving coverage with better automation

@JCRAN

Information Security Professional?

Research:

@KennaSecurity

Janitor:

@intrigueio

Previously:

@bugcrowd, @rapid7



@JGAMBLIN

Information Security Rank Amature

Principal Security Engineer:

@KennaSecurity

Jerrygamblin.com

Internal.dev

Questionable.dev

(Coming Soon!)





Filter: Hiding out of scope and not found items; hiding 4xx responses; hiding empty folders

- > http://blog.indeed.co.uk
- > http://www.indeed.co.uk
- https://www.indeed.co.uk**
- >  /
- >  account
- >  browsejobs
- >  favicon.ico
- >  hire
- >  images
- >  intl
- >  jobs
- >  jobtrends
- >  legal
- >  m
- >  promo
- >  publisher
- >  rpc
- >  s
- >  salaries

Contents

Host	Method	URL
https://www.indeed.co.uk	GET	/

Issues

-  Strict transport security not enforced
- >  Cacheable HTTPS response [2]
- >  SSL certificate
- >  Mixed content [2]



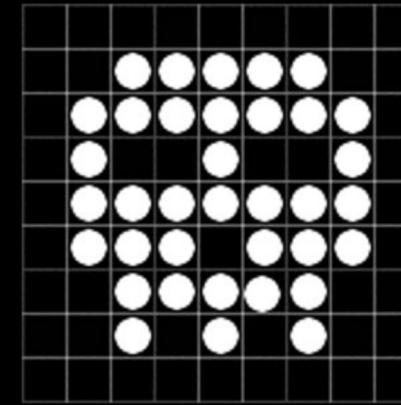
;q=0.8
Accept-Language: en-US,en;q=0.5
Cookie: CTK=1bfc15iji16ub6vb; ctkgem=1;
JSESSIONID=9EB48624400D75FAEE0CB42F324DE1A5; inc
XB_Ion-job12;
WEBSERVICE_TOKEN=6...D...Y...C...B...G...S...E...T...I...

Confidence: Certain
Host: https://www.indeed.co.uk
Path: /

Issue description

When you think of web application automation....

There are many great extensions...



ActiveScan++



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**

Many Many High Quality Sources And Tools

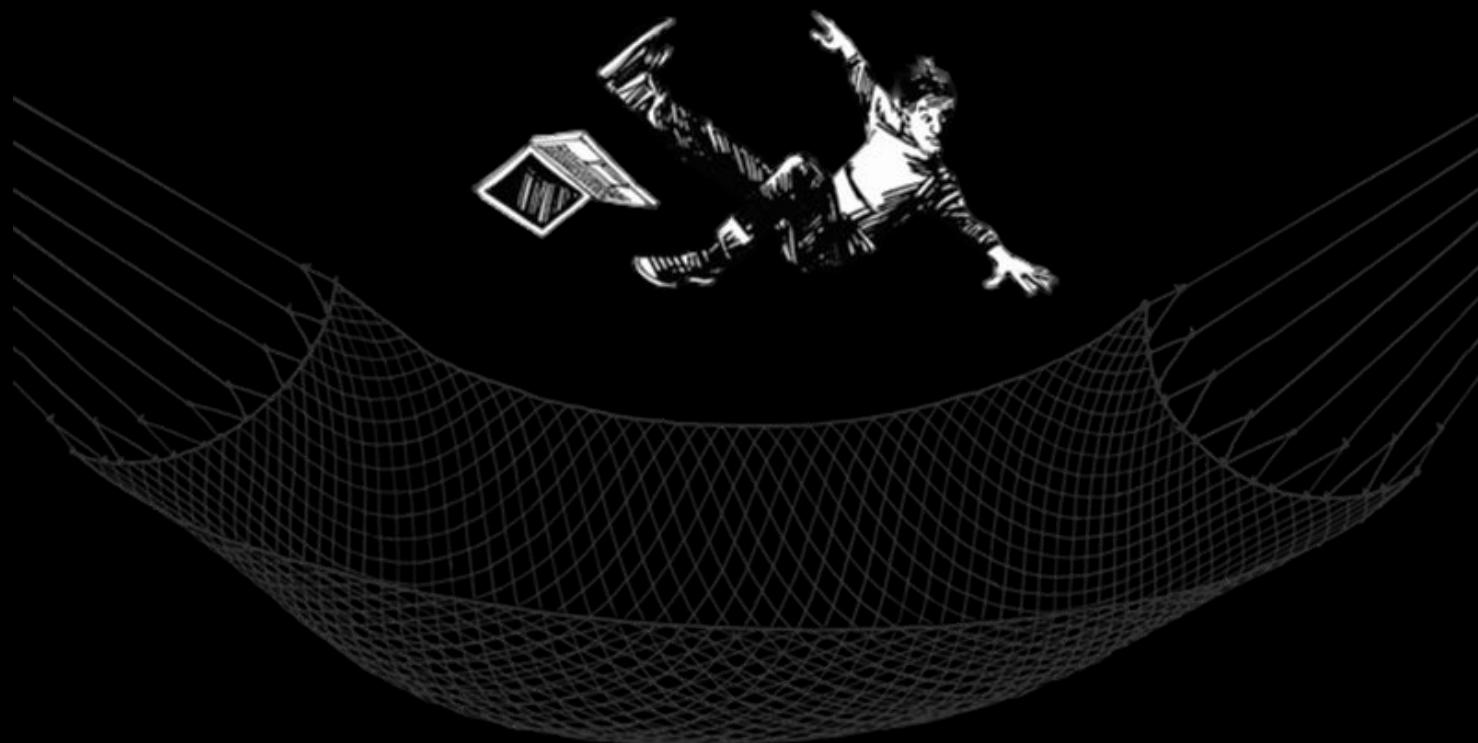
Forward DNS
Reverse DNS
Search Engines
 Certificate
 Transparency
 BGP
Security Trails
 Censys
Binary Edge
 SHODAN
Project Sonar
Parsing PDFs
PublicWWW
Passive DNS
 BuiltWith
Historical WHOIS
 SpyOnWeb
 VirusTotal
 Robtex
 DNSDumpster

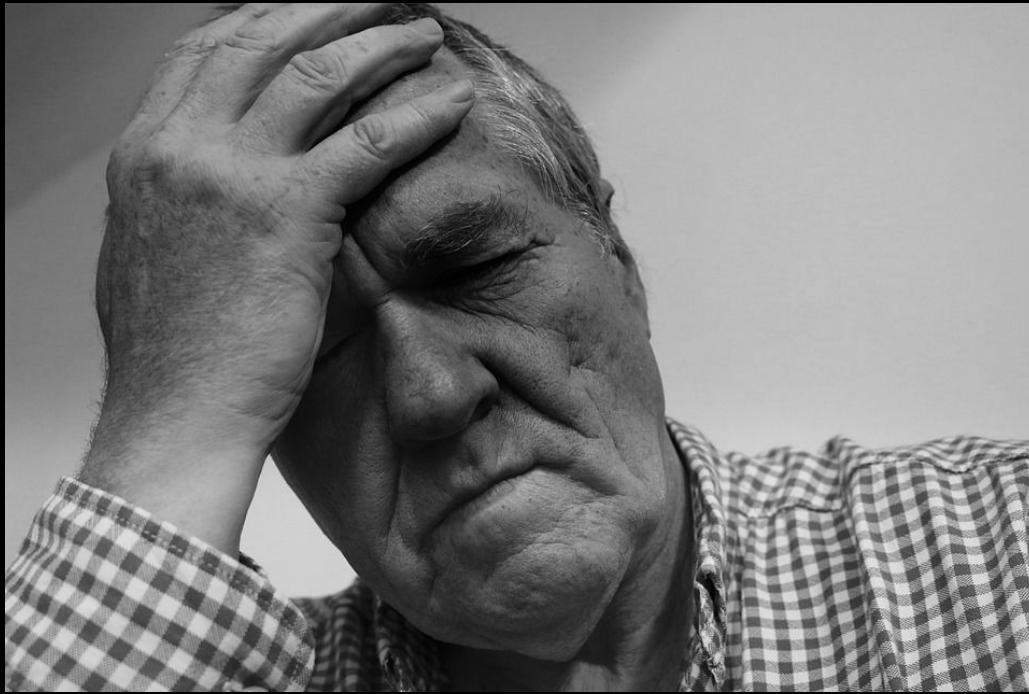
Xforce Exchange
Alienvault
AbuseIPDB
Archive.org
RIRs (ARIN,RIPE,etc)
 Bing
 Circl.lu
 Clearbit
CommonCrawl
 EDGAR
OpenCorporates
 CRT.sh
 Cymon
CiberCrimeTracker
 FullContact
 Dehashed
 HIBP
 Google
 Whoisology
 WhoisXMLAPI

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

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

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





So what's missing?!?

An aerial night photograph of the San Francisco skyline, featuring the illuminated city buildings and the Bay Bridge in the background.

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

A photograph of a person from behind, wearing a backpack and holding a camera, taking a picture of a vast tea plantation on a hillside. The sun is low on the horizon, casting long shadows and creating a warm, golden glow over the green terraced fields. In the distance, more hills and mountains are visible under a clear blue sky.

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

Intrigue Core Built-in Tasks

autonomous_system
aws_credential
aws_s3_bucket
credential
dns_record
document
domain
email_address
file

github_account
github_repository
info
ip_address
nameserver
net_block
network_service
organization

person
phone_number
physical_location
screenshot
software_package
ssl_certificate
string
uri
web_account

Intrigue Core Built-In Entities



[yahoo]

Start ▾

Entities

Results

Analysis ▾

Export ▾

System ▾

Start

Task

Create Entity

Description: This task simply creates an entity.

Entity Type

Domain

Entity Name

yahoo.com

References:**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

Domain: yahoo.com

Scoped: true

Enriched: false

Details

```
{  
  "name": "yahoo.com",  
  "resolutions": [  
    {  
      "response_data": "2001:4998:58:1836::10",  
      "response_type": "AAAA"  
    },  
    {  
      "response_data": "2001:4998:C:1023::4",  
      "response_type": "AAAA"  
    },  
    {  
      "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"  
    },  
  ]  
}
```

Image:

Run a task on this entity:

Task	<input type="button" value="Create Entity"/>	Description: This task simply creates an entity.
Entity Type	<input type="button" value="Domain"/>	References:
Entity Name	<input type="text" value="yahoo.com"/>	
Machine	<input type="button" value="Org Asset Discovery (Activ"/>	'Machine' specifies the post-processor for each new entity.
Iterations	<input type="button" value="None"/>	'Iterations' specifies the depth to which the machine is run.
<input checked="" type="checkbox"/> Auto Enrich		

Enrichment builds out the entity.

Domain: yahoo.com

Scoped: true

Enriched: true

Image:

Run a task on this entity:

De

Domain: yahoo.com

simply

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:

Description: This task simply creates an entity.

References:

Tasks that created this entity:

- [create_entity \(Domain: yahoo.com\)](#)

(Activ

st-

epth to

Tasks run on this entity:

- [enrich/domain \(Domain: yahoo.com\)](#)
- [create_entity \(Domain: yahoo.com\)](#)

Entities discovered from this entity:

- [Domain: yahoo.com](#)

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.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.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: 0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.3.8.1.8.5.0.0.8.9.9.4.1.0.0.2.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: 4.0.0.0.0.0.0.0.0.0.0.0.0.0.3.2.0.1.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: 5.0.0.0.0.0.0.0.0.0.0.0.0.3.2.0.1.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: 1.1.0.0.0.0.0.0.0.0.0.0.6.3.8.1.8.5.0.0.8.9.9.4.1.0.0.2.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:c1023::4	2	complete
2019-03-03 01:09:35 -0600	enrich/ip_address on ipAddress: 2001:4998:c1023::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

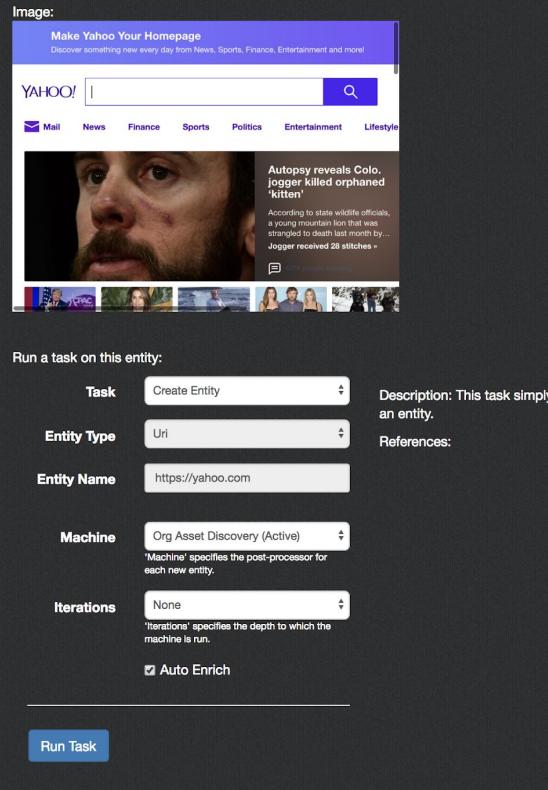
[Cancel All](#)

Enrichment can trigger new tasks too.

Uri: <https://yahoo.com>

Scoped: true
Enriched: true

Details



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
```

```
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
```

VS

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

(thanks @erbbysam!)

Domain: yahoo.com

Scoped: true
Enriched: true

Run a task on this entity:

Task	DNS Search Sonar
Entity Type	Domain
Entity Name	yahoo.com
endpoint	http://ec2-52-91-225
Machine	<p>Org Asset Discovery (Activ</p> <p>'Machine' specifies the post-processor for each new entity.</p>
Iterations	<p>None</p> <p>'Iterations' specifies the depth to which the machine is run.</p>
	<input checked="" type="checkbox"/> Auto Enrich

Description: Search Rapid7's Project Sonar for FDNS and RDNS records matching a given pattern. Utilizes @erbbsam's excellent DNSGrep server to serve results.

References:

Machine Org Asset Discovery (Activ

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

Iterations None

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

Auto Enrich

Run task

Image:

Run a task on this entity:

Task	Create Entity	▼	Description: This task simply creates an entity.
Entity Type	Domain	▼	References:
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.
	<input checked="" type="checkbox"/> Auto Enrich		
<hr/>			
In Task			

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!
[+] 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 srcl.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord basl-1.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord ir-120.basl-1.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord lo0.basl-1.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord ir-121.basl-1.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord ir-108.basl-1.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord ywww-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 11.ycs.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord 12.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 ttfpl-vml.ops.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord yhiipl.ops.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord tftpl1.ops.id1.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord tier1-test-hds-ams01-0.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord tier1-test-hds-ams02-0.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord tier1-test-hds-ams02-0.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-628af810.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce10.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord usw10.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord lo0.cry10.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord lo6.cry10.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce20.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce30.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-628ade30.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce40.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-628ade40.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-d89bce50.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxy-oxygen-628af260.net.yahoo.com. Scoped: true. No-Traverse: false
[+] New Entity: DnsRecord oxv-oxvnen-d89bce60.net.yahoo.com. Scoped: true. No-Traverse: false
```

[Export CSV](#)
[Export JSON](#)

Hint: Use "name:" and "details:" to search specific fields. Separate search tokens with a "|" character.

Types:

```
Bonneville::Entity::Cve
Intrigue::Entity::AutonomousSystem
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
 - [**DnsRecord:** src.yahoo.com]
 - [**DnsRecord:** src.g03.yahoodns.net]
 - [**IpAddress:** 74.6.136.150]
 - [**DnsRecord:** ca.360.yahoo.com]

Issues

0 issues

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

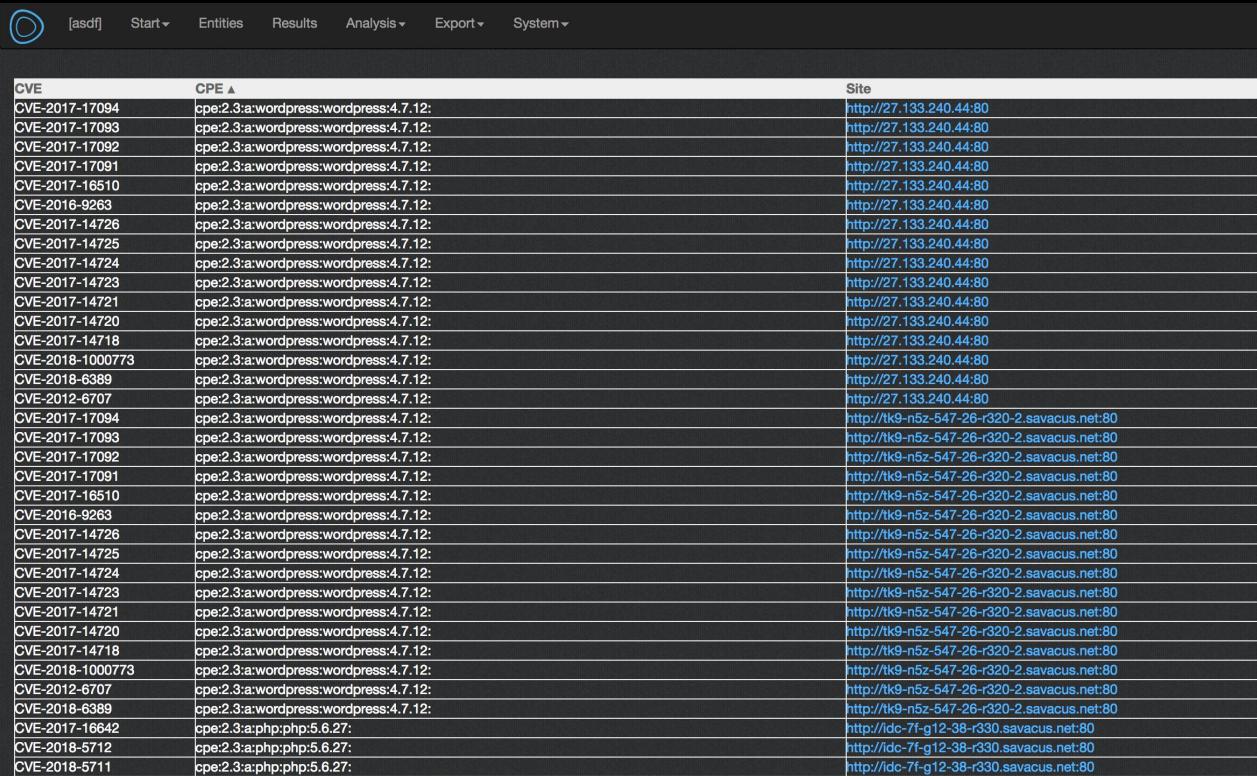
Applications:

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!



The screenshot shows a software application window with a dark theme. At the top, there is a navigation bar with icons and text: a blue circle icon, '[asdf]', 'Start ▾', 'Entities', 'Results', 'Analysis ▾', 'Export ▾', and 'System ▾'. Below the navigation bar is a table with three columns: 'CVE', 'CPE ▾', and 'Site'. The 'CVE' column lists various vulnerability identifiers. The 'CPE' column contains entries like 'cpe:2.3:a:wordpress:wordpress:4.7.12:' repeated many times. The 'Site' column lists URLs such as 'http://27.133.240.44:80', 'http://tk9-n5z-547-26-320-2.savacus.net:80', and 'http://idc-7f-g12-38-r330.savacus.net:80'. The table has a light gray background with alternating darker rows.

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-547-26-320-2.savacus.net:80
CVE-2017-17093	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2017-17092	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2017-17091	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2017-16510	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2016-9263	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2017-14726	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2017-14725	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2017-14724	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2017-14723	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2017-14721	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2017-14720	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2017-14718	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2018-1000773	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2012-6707	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.savacus.net:80
CVE-2018-6389	cpe:2.3:a:wordpress:wordpress:4.7.12:	http://tk9-n5z-547-26-320-2.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

[danielmiessler / SecLists](#)

Unwatch 1,382 Star 16,844 Fork 6,226

Code Issues 5 Pull requests 0 Projects 0 Wiki Insights

SecLists is the security tester's companion. It's a collection of multiple types of lists used during security assessments, collected in one place. List types include usernames, passwords, URLs, sensitive data patterns, fuzzing payloads, web shells, and many more. <https://www.owasp.org/index.php/OWASP...>

646 commits 1 branch 5 releases 75 contributors MIT

Branch: master New pull request Create new file Upload files Find file Clone or download

g0tmilk Merge pull request #273 from leesh/master Latest commit 8987c4b 6 days ago

Category	Commit Message	Time Ago
Discovery	Add "admin"	8 days ago
Fuzzing	A wrong payload corrected	20 days ago
IOCs	Fix #259 - Recover from bad merge	2 months ago
Miscellaneous	Fix #259 - Recover from bad merge	2 months ago
Passwords	Update vagrant credentials	8 days ago
Pattern-Matching	removes exec. bits	a month ago
Payloads	Fix #226 - Remove 255+ file names	18 days ago
Usernames	removes exec. bits	a month ago
Web-Shells	Fix #259 - Recover from bad merge	2 months ago
.gitignore	Quick move about	9 months ago

Now let's do some content discovery!



FuzzDB Project

Official FuzzDB Project Repo

[swisskyrepo / PayloadsAllTheThings](#)

Watch 520 Star 6,324 Fork 1,938

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights

A list of useful payloads and bypass for Web Application Security and Pentest/CTF

python pentest payload bypass web-application hacking xss-vulnerability sql-vulnerability-scanner vulnerability useful-payloads useful

301 commits 1 branch 2 releases 26 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

swisskyrepo Web cache deception resources update Latest commit 6d2cd68 a day ago

Category	Commit Message	Time Ago
AWS Amazon Bucket S3	AWS S3 and Open redirect rewritten	2 months ago
CRLF injection	Adding references sectio	2 months ago
CSRF injection	.git/index file parsing + fix CSRF payload typo	23 days ago
CSV injection	SQL wildcard ' + CSV injection reverse shell	2 months ago
CVE Exploits	Use print() function in both Python 2 and Python 3	13 days ago
Command injection	Polyglot Command Injection + XSS HTML file	3 days ago
Directory traversal	Directory traversal / File inclusion rewritten	2 months ago
File inclusion	Use print() function in both Python 2 and Python 3	13 days ago
Insecure deserialization	References added based on @ngalongc bug-bounty-references	2 months ago
Insecure direct object references	References added based on @ngalongc bug-bounty-references	2 months ago
Insecure management interface	Adding references sectio	2 months ago
Insecure source code managem...	.git/index file parsing + fix CSRF payload typo	23 days ago
JSON Web Token	JWT - Payload detail	20 days ago
LDAP injection	Adding references sectio	2 months ago
LaTeX injection	Adding references sectio	2 months ago
Methodology and Resources	Web cache deception resources update	a day ago
NoSQL injection	Adding references sectio	2 months ago
OAuth	References added based on @ngalongc bug-bounty-references	2 months ago
Open redirect	AWS S3 and Open redirect rewritten	2 months ago

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: "/asyncPeople/", :regex => nil },
```

Gmail Calendar Documents Photos Reader Web more ▾

hyperboy@gmail.com | Offline Beta Sync | Settings | Help | Sign out

Google Calendar BETA

Create Event Quick Add

Mon 4/6 Tue 4/7 Wed 4/8 Thu 4/9 Fri 4/10 Sat 4/11 Sun 4/12

Today Apr 6 – 12 2009 Refresh

Search My Calendars Show Search Options

My calendars Brian Young Settings Create

Other calendars Add a friend's calendar Hong Kong Holidays Phases of the Moon US Holidays Weather Settings Add

Mon 4/6 (12:00am) Archive Log SUSE Admit Day Dorothy Lau's Birthday

Tue 4/7 Jim's Open Office Hours =

Wed 4/8 DDD STAFF MEETING =

Thu 4/9 10am 10 – 11 a^o Jim's Open Office Hours =

Fri 4/10 12pm 12p – 1p SUSE Admit Day Lunch =

Sat 4/11 1pm 1:15p – 3:05p a^o E281 Media & Design 1:30p – 3p a^o SULAIR DLSS Web Team = .. =

Sun 4/12 10am 10 – 1p Quichester Sunday Kickball TournaMint Julep =

9am =

11am =

12pm 12p – 1p SUSE Admit Day Lunch =

1pm 1:15p – 3:05p a^o E281 Media & Design 1:30p – 3p a^o SULAIR DLSS Web Team = .. =

2pm =

3pm =

4pm 3:45p – 5p Drupal Discussion with SULAIR =

5pm 5:30p – Meeting with Jen =

6pm 5:15p – 6:45 EDUC 229C Learning =

7pm =

8pm 7:30p – 9p Dinner with Bao =

9pm =

10pm =

11pm =

Print Day Week Month 4 Days Agenda

... misconfigurations too: saas_google_calendar_check

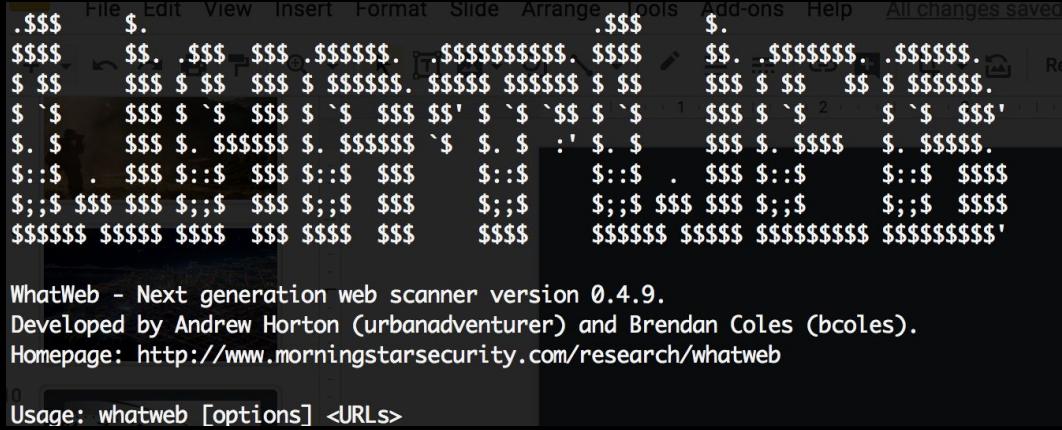
Putting It All Together...
(Demo Time!)

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:          tabletop_gaming
| 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>
|         <br><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
```



Wappalyzer

```
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.cloudflare.com", "categories": [{"31": "CDN"}]}, {"name": "Google Analytics", "confidence": "100", "version": "", "icon": "Google Analytics.svg", "website": "http://google.com/analytics", "categories": [{"10": "Analytics"}]}, {"name": "Prototype", "confidence": "100", "version": "1.7", "icon": "Prototype.png", "website": "http://www.prototypejs.org", "categories": [{"12": "JavaScript Frameworks"}]}, {"name": "Quantcast", "confidence": "100", "version": "", "icon": "Quantcast.png", "website": "http://www.quantcast.com", "categories": [{"10": "Analytics"}]}, {"name": "YUI", "confidence": "100", "version": "", "icon": "YUI.png", "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?



G R E Y N O I S E

DO KNOW EVIL