

SEMINAR 1

TOOLS FOR INTERNET RESEARCH



Getting information about machines,
people and...source code!



JOSÉ MANUEL REDONDO LÓPEZ "S-81 ISAAC PERAL" PROJECT V4.0



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

Logo: @creative_vanesa (Instagram)

● You may wonder why all current focus on security these days...

- Even with no technical knowledge, you can have a lot of information about people / companies that can be exploited to obtain advantages
- All is over the Internet for you to pick up...if you know where (and how) to look
- This seminar will show you tools explaining how to do it
- If you are serious about uses (and misuses) of the information over the Internet, you should enroll in the optional course Web Information Systems (**SIW**)
 - If you contact Daniel Gayo, he can give you access to the course materials and videos for you to check!

● Let's do something that does not require a lot of technical skill 😊

- **OSINT (Open-Source INTelligence)**
- Some of these applications will be used in laboratories
- But, above all, we will exploit this branch more in the **Group Work** of the course

● **NOTE:** If, using these tools, you find yourself exposing too many information on Internet (“egosurfing”), there are ways of recovering your privacy

- You can follow this guide: <https://open.nytimes.com/how-to-dox-yourself-on-the-internet-d2892b4c5954?gi=57af4dc583d>



INDEX

- ▶ OSINT with machines
- ▶ OSINT with people
 - Social networks
 - Reconnaissance from multiple sources
- ▶ OSINT with source code

[< Go to Index](#)

OSINT AGAINST THE MACHINE

Investigating machines using only public information



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

● Machine (not web) search engine

- Routers, servers, cameras... (IoT)
- Reports the type of service found, version, etc.
- Finds SCADA (Supervisory Control And Data Acquisition)
 - Industrial engineering devices

● Search for up to 10 devices

- Free registration allows more and using logical operators
- Used to view devices exposed to the Internet and if they pose a danger
 - They have management software that can be accessed, and attacked

● Tutorials

- <https://danielmiessler.com/study/shodan/>
- <https://hacking-etico.com/2016/02/12/4979/>

Web Technologies

 MOODLE

 PHP

 REQUIREJS

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ("/), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0215	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38. a bug in mod_ssl when using per-location

Apache httpd 2.4.38

HTTP/1.1 200 OK
Date: Mon, 21 Feb 2022 02:36:16 GMT
Server: Apache/2.4.38 (Debian)
Set-Cookie: MoodleSession=j25o9m0cman8dkarptfvspemup; path=/; secure
Expires:
Cache-Control: private, pre-check=0, post-check=0, max-age=0, no-transform
Pragma: no-cache
Content-Language: es
Content-Script-Type: text/javascript
Content-Style-Type: text/css
X-UA-Compatible: IE=edge
Accept-Ranges: none
X-Frame-Options: sameorigin
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8

SSL Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

03:b7:b4:45:4c:85:40:a2:1d:c9:b0:fd:06:bf:c0:61:e8:f3

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=Let's Encrypt, CN=R3

Validity

Not Before: Jan 12 04:06:45 2022 GMT

Not After : Apr 12 04:06:44 2022 GMT

Subject: CN=virtual.ingenieriainformatica.uniovi.es

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public-Key: (2048 bit)

Modulus:

00:df:4c:d6:9c:50:19:04:39:96:05:61:cb:0d:2b:

ab:4f:cd:0a:9f:66:33:3b:66:07:a8:61:8a:ac:25:

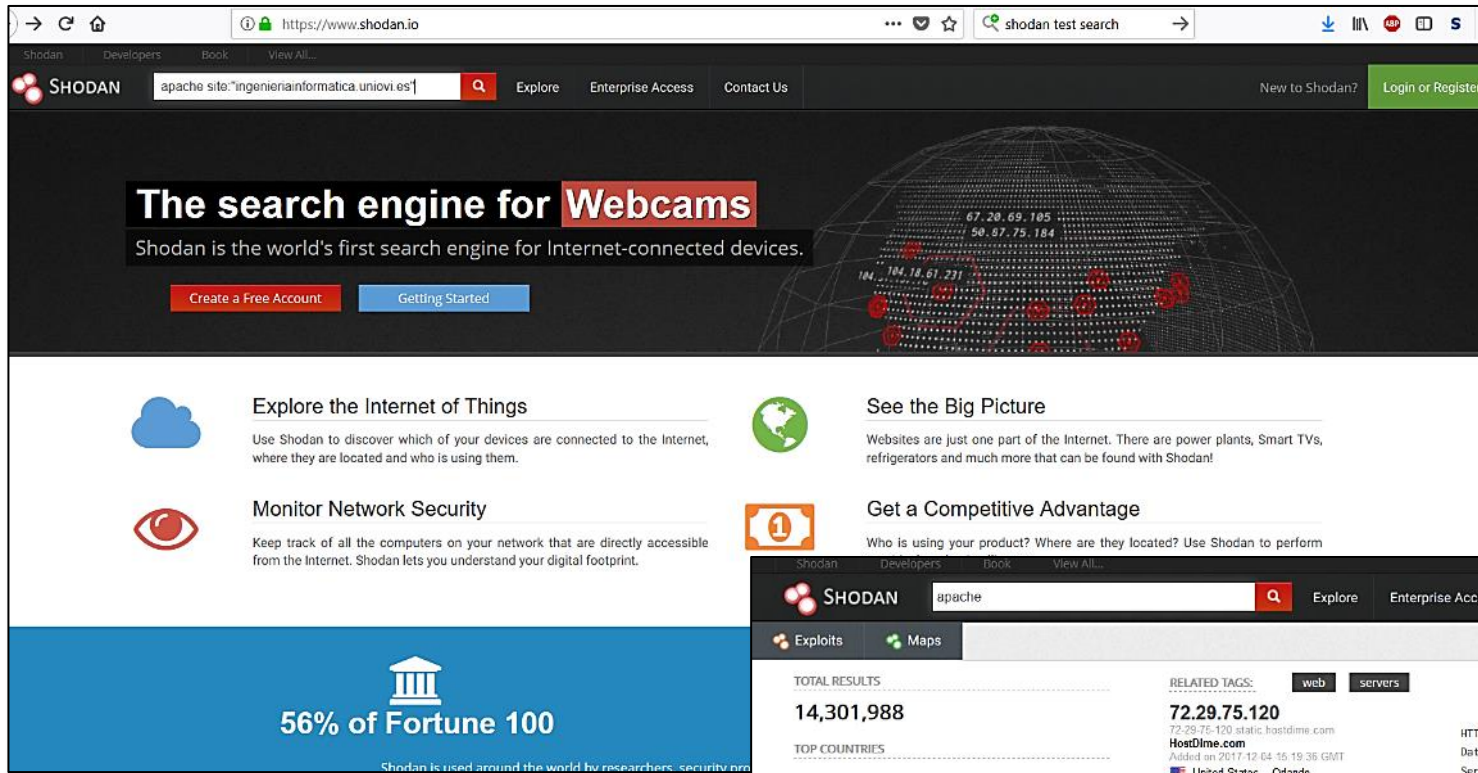
c7:ab:08:38:d9:36:05:de:2d:43:58:d5:eb:0c:e1:

55:04:5f:70:79:f5:f4:44:1a:fa:d2:77:e4:38:75:

4c:51:3a:3e:f7:02:95:c6:cd:96:f7:3a:2d:ae:48:

fe:8a:5a:df:cb:d5:52:eb:e3:d1:b3:87:b2:35:67:

5f:0d:e1:44:05:3b:c1:3f:a0:43:62:86:9b:3f:ea:



The search engine for **Webcams**

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started

Explore the Internet of Things
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

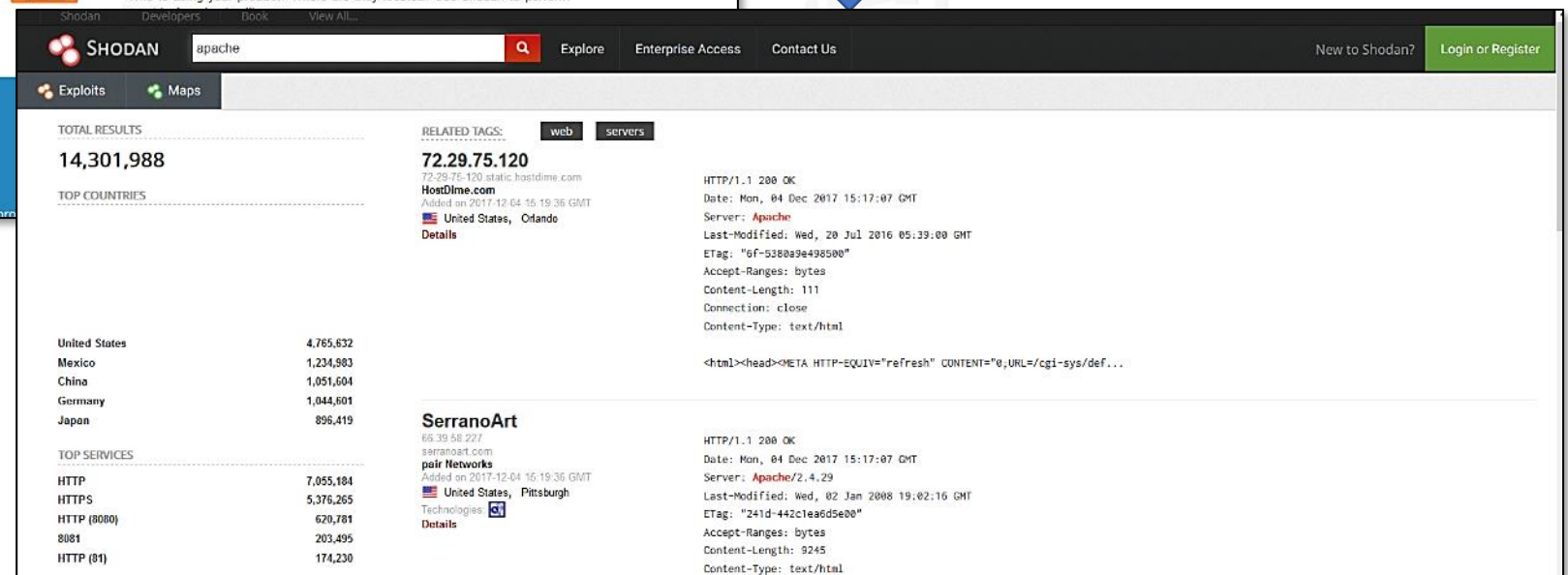
See the Big Picture
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage
Who is using your product? Where are they located? Use Shodan to perform

56% of Fortune 100
Shodan is used around the world by researchers, security pros

Search these service's banners

- HTTP/HTTPS
- FTP
- SSH
- Telnet
- SNMP
- SIP (IP telephony)
- RTSP (video *streaming* and webcams)
- ...



SHODAN apache

Exploits | Maps

TOTAL RESULTS: 14,301,988

RELATED TAGS: web servers

72.29.75.120
72-29-75-120.static.hostdime.com
HostDime.com
Added on 2017-12-04 15:19:36 GMT
United States, Orlando
Details

HTTP/1.1 200 OK
Date: Mon, 04 Dec 2017 15:17:07 GMT
Server: Apache
Last-Modified: Wed, 20 Jul 2016 05:39:00 GMT
ETag: "6f-5380a3e498500"
Accept-Ranges: bytes
Content-Length: 111
Connection: close
Content-Type: text/html

<html><head><META HTTP-EQUIV="refresh" CONTENT="0;URL=/cgi-sys/def...

TOP COUNTRIES	Count
United States	4,765,632
Mexico	1,234,583
China	1,051,604
Germany	1,044,601
Japan	896,419

TOP SERVICES

Service	Count
HTTP	7,055,184
HTTPS	5,376,265
HTTP (8080)	620,781
8081	203,495
HTTP (81)	174,230

SerranoArt
66.39.58.227
serranoart.com
pair Networks
Added on 2017-12-04 15:19:36 GMT
United States, Pittsburgh
Technologies: 61
Details

HTTP/1.1 200 OK
Date: Mon, 04 Dec 2017 15:17:07 GMT
Server: Apache/2.4.29
Last-Modified: Wed, 02 Jan 2008 19:02:16 GMT
ETag: "241d-442c1ea6d5e00"
Accept-Ranges: bytes
Content-Length: 9245
Content-Type: text/html

- The best part of having a Shodan account is the power of its search filter
 - It is like a Google for machines!
- You can search machines using an enormous amount of criteria
- Including advanced HTTP and SSL features
 - That is, specially against web servers and remote accessible machines over Internet

General

- all
- asn
- city
- country
- cpe
- device
- geo
- has_ipv6
- has_screenshot
- has_ssl
- has_vuln
- hash
- hostname
- ip
- isp
- link
- net
- org
- os

HTTP

- http.component
- http.component_category
- http.favicon.hash
- http.headers_hash
- http.html
- http.html_hash
- http.robots_hash
- http.securitytxt
- http.status
- http.title
- http.waf

Bitcoin

- bitcoin.ip
- bitcoin.ip_count
- bitcoin.port
- bitcoin.version

SSL

- ssl
- ssl.alpn
- ssl.cert.alg
- ssl.cert.expired
- ssl.cert.extension
- ssl.cert.fingerprint
- ssl.cert.issuer.cn
- ssl.cert.pubkey.bits
- ssl.cert.pubkey.type
- ssl.cert.serial
- ssl.cert.subject.cn
- ssl.chain_count
- ssl.cipher.bits
- ssl.cipher.name
- ssl.cipher.version
- ssl.ja3s
- ssl.jarm
- ssl.version

SHODAN CLI

<https://cli.shodan.io/>



Computer Security

- **Python library providing Shodan's capabilities from the command line**
 - Useful in GUI-less contexts
- **Allows to integrate Shodan's features into our own scripts or programs**
 - Or automate pentesting tasks including Shodan
 - The official website has usage examples
- **Its capabilities are equivalent to the web interface**
- **Set of useful searches**
 - <https://github.com/jakejarvis/awesome-shodan-queries>

```
81.171.175.68 80 Star Technology Services Limited
178.73.238.43 80 Portlane Networks AB
113.245.76.199 5900 China Telecom HUNAN
149.210.160.163 80 Transip B.V. nowarkrengelink.com
23.92.216.117 80 Res.pl Isp S.c. mailingrolout.com
202.69.233.212 443 Verio Web Hosting kubota-rvc23-0727001.com
190.78.179.228 8080 CANTV Servicios, Venezuela 190-78-179-228.dyn.dsl.cantv.net
192.3.4.108 443 ColoCrossing sxi.pw
160.246.182.223 80 Hayashi Telempu Co., Ltd.
198.104.15.120 443 Verio Web Hosting wholesalechildrensclothing.com.au
208.64.139.67 80 Desync Networks 119-a.webmasters.com
212.227.51.115 443 1&1 Internet AG s535322526.online.de
75.98.17.22 443 Internap Network Services Corporation
178.208.77.241 81 McHost.Ru v112059.vps.modir.ru
63.249.80.153 443 Cruzio www12153.cruzio.com
87.243.209.223 8080 HotChilli Internet static-87-243-209-223.adsl.hotchilli.net
183.89.74.87 81 3BB Broadband mx-11-183.89.74-87.dynamic.3bb.co.th
178.236.77.90 80 Excellent Hosting Sweden AB
54.201.193.170 80 Amazon.com ec2-54-201-193-170.us-west-2.compute.amazonaws.com
106.186.28.222 80 Linode, LLC li608-222.members.linode.com
54.85.166.63 80 Merck and Co. ec2-54-85-166-63.compute-1.amazonaws.com
208.131.128.136 80 WestHost greenstreetstudios.org
```

● Like Shodan, but with structured info

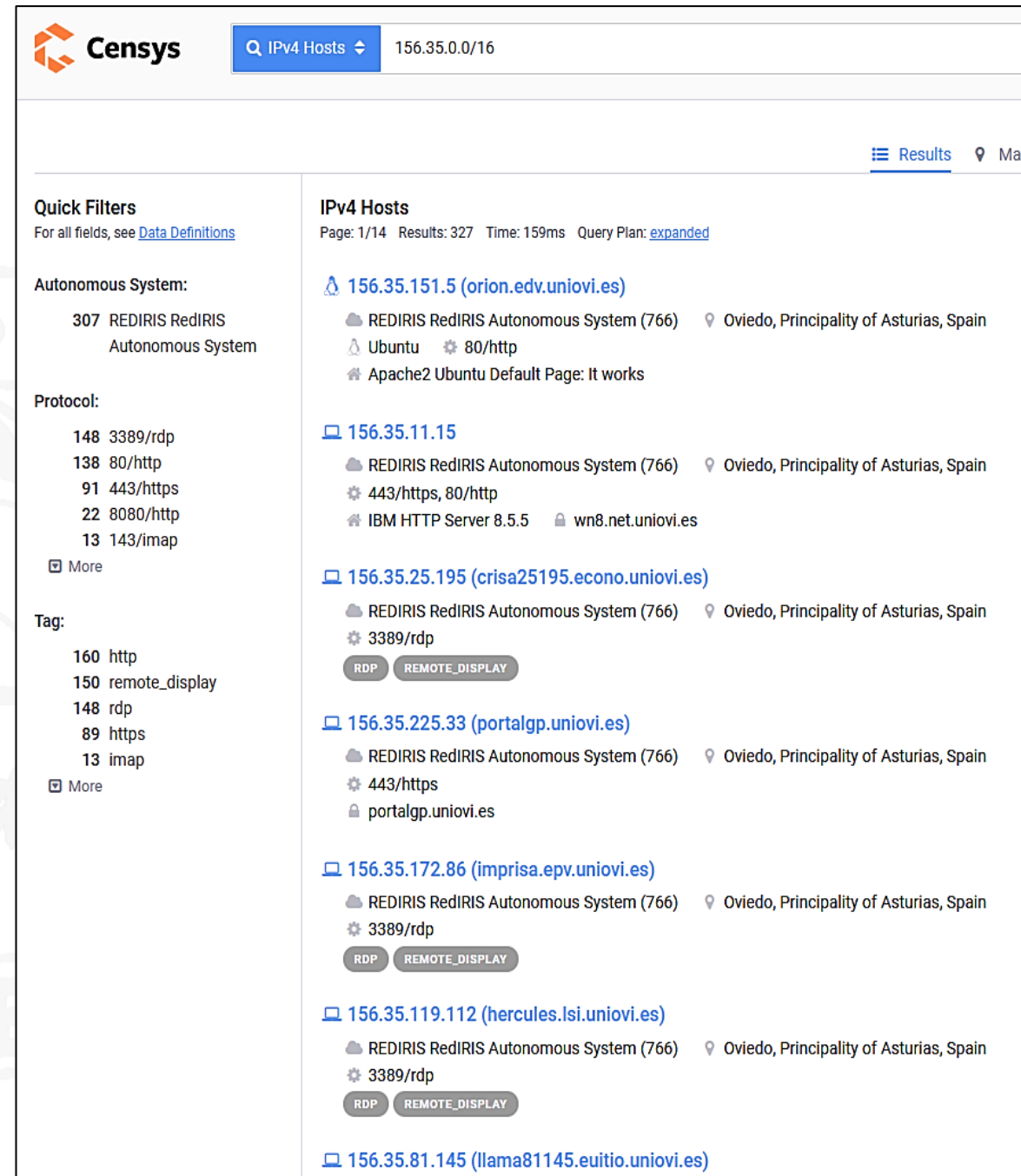
- Searches server features: interesting running services (RDP), OS/web server banners...
- Multiple search criteria
 - IP (v4 only) and networks: <https://censys.io/ipv4/>
 - Website domain names: <https://censys.io/domain?q=>
 - Certificates: <https://censys.io/certificates?q=>

● Search tutorial

- <https://developerinsider.co/censys-find-and-analyze-any-server-and-device-on-the-internet/>

● A similar tool is Onhype.io:

- <https://fwhibbit.es/descubrimiento-y-recopilacion-de-activos-con-onyphe-io>
- Comparison with other tools (ZMap, Mr Looquer)
 - <https://www.dragonjar.org/shodan-vs-scans-io-vs-censys-io-vs-zmap-vs-mr-looquer.shtml>



The screenshot shows the Censys IPv4 Hosts search results page. The search query is "156.35.0.0/16". The page displays a list of results, each representing an IP address and its associated information. The results are filtered by "Quick Filters" and "Autonomous System".

Quick Filters
For all fields, see [Data Definitions](#)

Autonomous System:
307 REDIRIS RedIRIS Autonomous System

Protocol:
148 3389/rdp
138 80/http
91 443/https
22 8080/http
13 143/imap
[More](#)

Tag:
160 http
150 remote_display
148 rdp
89 https
13 imap
[More](#)

IPv4 Hosts
Page: 1/14 Results: 327 Time: 159ms Query Plan: [expanded](#)

[156.35.151.5 \(orion.edv.uniovi.es\)](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
Ubuntu 80/http
Apache2 Ubuntu Default Page: It works

[156.35.11.15](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
443/https, 80/http
IBM HTTP Server 8.5.5 wn8.net.uniovi.es

[156.35.25.195 \(crisa25195.econo.uniovi.es\)](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
3389/rdp
[RDP](#) [REMOTE_DISPLAY](#)

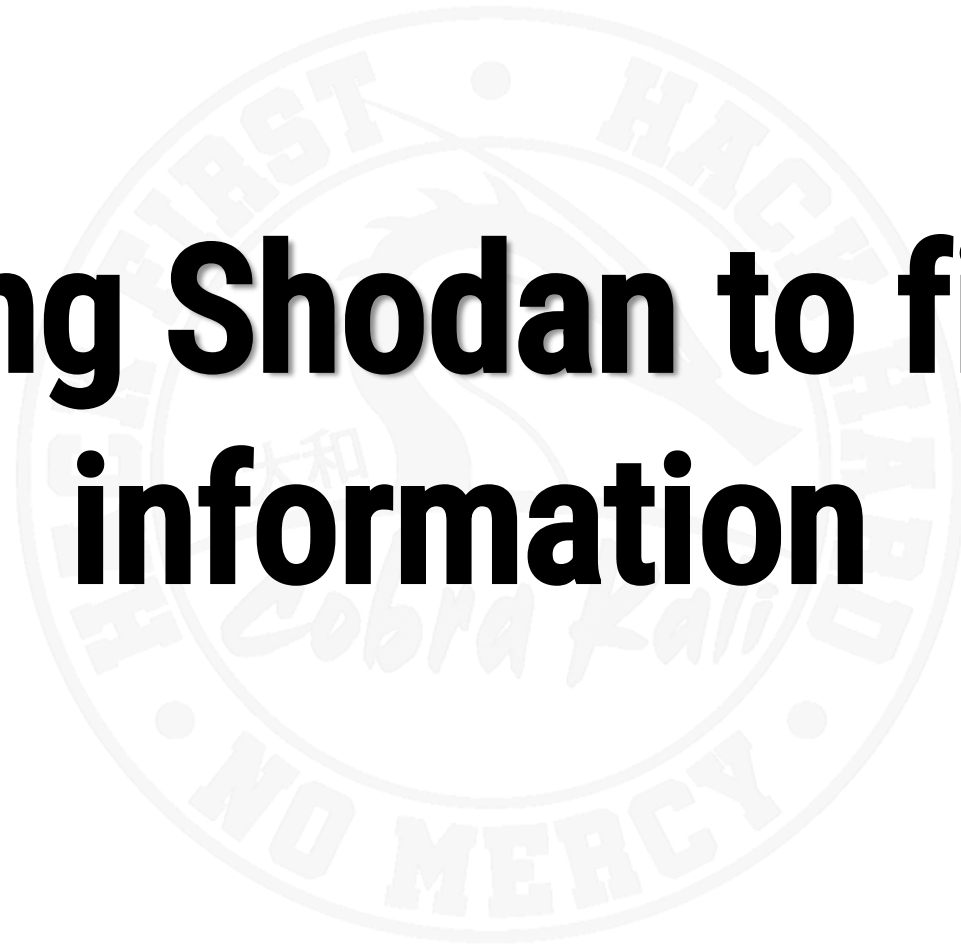
[156.35.225.33 \(portalgp.uniovi.es\)](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
443/https
portalgp.uniovi.es

[156.35.172.86 \(imprisa.epv.uniovi.es\)](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
3389/rdp
[RDP](#) [REMOTE_DISPLAY](#)

[156.35.119.112 \(hercules.lsi.uniovi.es\)](#)
REDIRIS RedIRIS Autonomous System (766) Oviedo, Principality of Asturias, Spain
3389/rdp
[RDP](#) [REMOTE_DISPLAY](#)

[156.35.81.145 \(llama81145.eutio.uniovi.es\)](#)

Using Shodan to find information



GOOGLE HACKING OR “GOOGLE DORKING”



- **Ability of doing certain searches that reveal compromising information**
 - Using standard search engines (normally targeting a concrete domain with the `site:` operator)
 - These queries find information leading to vulnerabilities, configuration issues, or facilitate an attack
 - It can be done in other search engines too (although Google is the most used one)
- **There is a database of organized prebuilt searches: Google Hacking Database**
 - These are called “Google Dorks” : <https://www.exploit-db.com/google-hacking-database>
 - Choose the right search category: each one represents a possible vulnerability!
 - Search the target with the chosen query (`site:`)
- **“Dorking” can also be used with other products**
 - <https://github.com/cipher387/Dorks-collections-list>
- **Examples**
 - <https://wifibit.com/google-hacking/>
 - <https://ciberpatrulla.com/osint-con-google/>
 - <https://ciberpatrulla.com/buscar-google/>
 - https://medium.com/@logicbomb_1/one-misconfig-jira-to-leak-them-all-including-nasa-and-hundreds-of-fortune-500-companies-a70957ef03c7

GOOGLE HACKING: PROCESS



Computer Security

EXPLOIT DATABASE

Google Hacking Database

Show 15

Date Added	Dork	Category	Author
2020-01-17	intitle:"WS02 Management Console"	Various Online Devices	Alfie
2020-01-10	intitle:"webview login" alcatel lucent	Pages Containing Login Portals	Bruno Schmid
2020-01-09	intitle:"LAS VANTAGE Login"	Pages Containing Login Portals	Reza Abasi
2020-01-09	site:"cgi/domadmin.cgi"	Pages Containing Login Portals	Reza Abasi
2020-01-09	inurl:"8080/login.jsp?os_destination="	Pages Containing Login Portals	Reza Abasi
2020-01-09	intitle:"index of" "wp-security-audit-log"	Files Containing Juicy Info	Reza Abasi
2020-01-09	intext:"powered by codoforum" inurl:"/user/login"	Pages Containing Login Portals	Prasanth
2020-01-06	inurl:"/index.php?enter=guest"	Various Online Devices	Reza Abasi
2020-01-06	intitle:"Zabbix" intext:"username" intext:"password" inurl:"/zabbix/index.php"	Pages Containing Login Portals	Reza Abasi

Category: Any

Author: Begin typing...

Filters

Web Server Detection

intitle:"Apache2 Ubuntu Default Page: It works"

GHDB-ID: 5311

Author: REZA ABASI

Published: 2019-07-31

Google Dork Description: intitle:"Apache2 Ubuntu Default Page: It works"

Google Search: intitle:"Apache2 Ubuntu Default Page: It works"

web server detection: intitle:"Apache2 Ubuntu Default Page: It works"

Reza Abasi(Turku)

EXPLOIT DATABASE

Google Hacking Database

Show 15

Date Added	Dork	Category
2019-09-24	site:"/server-status" intext:"Apache server status for"	Web Server Detection
2019-09-02	inurl:/iisstart.htm intitle:"IIS7"	Web Server Detection
2019-08-30	inurl:/phpmyadmin/change_log.php -github -gitlab	Web Server Detection
2019-08-12	inurl:"WebPortal?bankin"	Web Server Detection
2019-07-31	intitle:"Apache2 Ubuntu Default Page: It works"	Web Server Detection
2019-07-31	intitle:"IIS Windows Server" -inurl:"IIS Windows Server"	Web Server Detection
2019-07-29	inurl:/server-status + "Server MPM:"	Web Server Detection
2019-06-24	inurl:phpinfo.php intext:build 2600	Web Server Detection
2019-06-17	inurl:OrganizationChart.cc	Web Server Detection
2019-06-17	intext:"Brought to you by eVetSites"	Web Server Detection
2019-06-06	intext:"Powered by GetSimple" -site:get-simple.info	Web Server Detection
2019-05-30	inurl:ismol.php	Web Server Detection

intitle:"Apache2 Ubuntu Default Page: It works"

Aproximadamente 27.000 resultados (0,40 segundos)

Traducir esta página

Apache2 Ubuntu Default Page: It works Annex02!

Apache2 Ubuntu Default Page: It works Annex02! It works! This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived.

Traducir esta página

Apache2 Ubuntu Default Page: It works * PROXY *****

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page ...

Traducir esta página

Apache2 Ubuntu Default Page: It works

Apache2 Ubuntu Default Page: It works. It works! XXXX This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived.

Traducir esta página

Apache2 Ubuntu Default Page: It works

it works !

FINAL RECON

<https://github.com/thewhiteh4t/FinalRecon>



● Python script for web reconnaissance

● Implements a lot of features to create a full profile of a web page server and its contents

- DNS and WHOIS information
- Full crawler
- Traceroute
- Directory search
- Port scanning the server

● Tutorial:

- <https://hakin9.org/final-recon-osint-tool-for-all-in-one-web-reconnaissance/>

```
python3 finalrecon.py -h
```

```
usage: finalrecon.py [-h] [--headers] [--sslinfo] [--whois] [--crawl] [--dns] [--sub] [--trace] [--dir] [--ps] [--full] [-t T] [-T T] [-w W] [-r] [-s] [-d D] [-e E] [-m M] [-p P] [-tt TT] [-o O] url
```

FinalRecon - The Last Recon Tool You Will Need | v1.0.7

positional arguments:

url Target URL

optional arguments:

-h, --help show this help message and exit
--headers Header Information
--sslinfo SSL Certificate Information
--whois Whois Lookup
--crawl Crawl Target
--dns DNS Enumeration
--sub Sub-Domain Enumeration
--trace Traceroute
--dir Directory Search
--ps Fast Port Scan
--full Full Recon

Extra Options:

-t T Number of Threads [Default : 30]
-T T Request Timeout [Default : 30.0]
-w W Path to Wordlist [Default : wordlists/dirb_common.txt]
-r Allow Redirect [Default : False]
-s Toggle SSL Verification [Default : True]
-d D Custom DNS Servers [Default : 1.1.1.1]
-e E File Extensions [Example : txt, xml, php]
-m M Traceroute Mode [Default : UDP] [Available : TCP, ICMP]
-p P Port for Traceroute [Default : 80 / 33434]
-tt TT Traceroute Timeout [Default : 1.0]
-o O Export Output [Default : txt] [Available : xml, csv]

● Bash script that uses Google Hacking to obtain various types of sensitive information

- Without making queries to the concrete web server
- Files or directories, subdomains...

● Tutorial

- <https://www.youtube.com/watch?v=DY8k-WEravY>

```
> ./GooFuzz -t nasa.gov -e pdf,bak,old -d 10
*****
* GooFuzz 1.2.2 - The Power of Google Dorks *
*****

Target: nasa.gov

=====
Extension: pdf
=====

https://history.nasa.gov/alsj/a11/A11_PressKit.pdf
https://history.nasa.gov/alsj/a13/A13_PressKit.pdf
https://history.nasa.gov/alsj/a14/A14_PressKit.pdf
https://history.nasa.gov/alsj/a15/A15_PressKit.pdf
https://history.nasa.gov/alsj/a410/A07_PressKit.pdf
https://history.nasa.gov/alsj/a410/A09_PressKit.pdf
https://history.nasa.gov/monograph15.pdf
https://www.hq.nasa.gov/alsj/LLRV_Monograph.pdf

=====
Extension: bak
=====

https://bocachica.arc.nasa.gov/ATTREX_2013/rh/rh_omega_oct3.html.bak
https://bocachica.arc.nasa.gov/ATTREX_2013/rh/rh_omega_sep30.html.bak
https://bocachica.arc.nasa.gov/ATTREX_2014/attrex2014_satmap.html.bak
https://bocachica.arc.nasa.gov/ATTREX_2014/schom/schomfigures_20140126.html.bak
https://bocachica.arc.nasa.gov/ATTREX_2014/schom/schomfigures_20140226.html.bak
https://bocachica.arc.nasa.gov/ATTREX_2014/trajfigures/trajfigures.html.bak
https://bocachica.arc.nasa.gov/POSIDON/posidon.html.bak
https://hesperia.gsfc.nasa.gov/hessi/solar_install/installation.bak
https://ndeaa.jpl.nasa.gov/nasa-nde/outreach/outreach.html.bak
https://ndeaa.jpl.nasa.gov/nasa-nde/yosi/yosi.htm.bak

=====
Extension: old
=====

https://bocachica.arc.nasa.gov/HAVE/nmc_rh_omega_plots.html.old
https://echo.jpl.nasa.gov/asteroids/1988TA/1988TA_planning.html.old
https://echo.jpl.nasa.gov/asteroids/1998QE2/1998QE2_planning.html.old
https://echo.jpl.nasa.gov/asteroids/2014J025/2014J025_planning.html.old
https://echo.jpl.nasa.gov/asteroids/goldstone_asteroid_schedule.html.old
https://fits.gsfc.nasa.gov/users_guide/users_guide.ps.old
https://image.msfc.nasa.gov/ChrisDocs/UDFInstall/uLibInstall.old
https://seawifs.gsfc.nasa.gov/OCEAN_PLANET/HTML/titanic.html.old
https://umbra.nascom.nasa.gov/soho/hqa/history.html.old
```

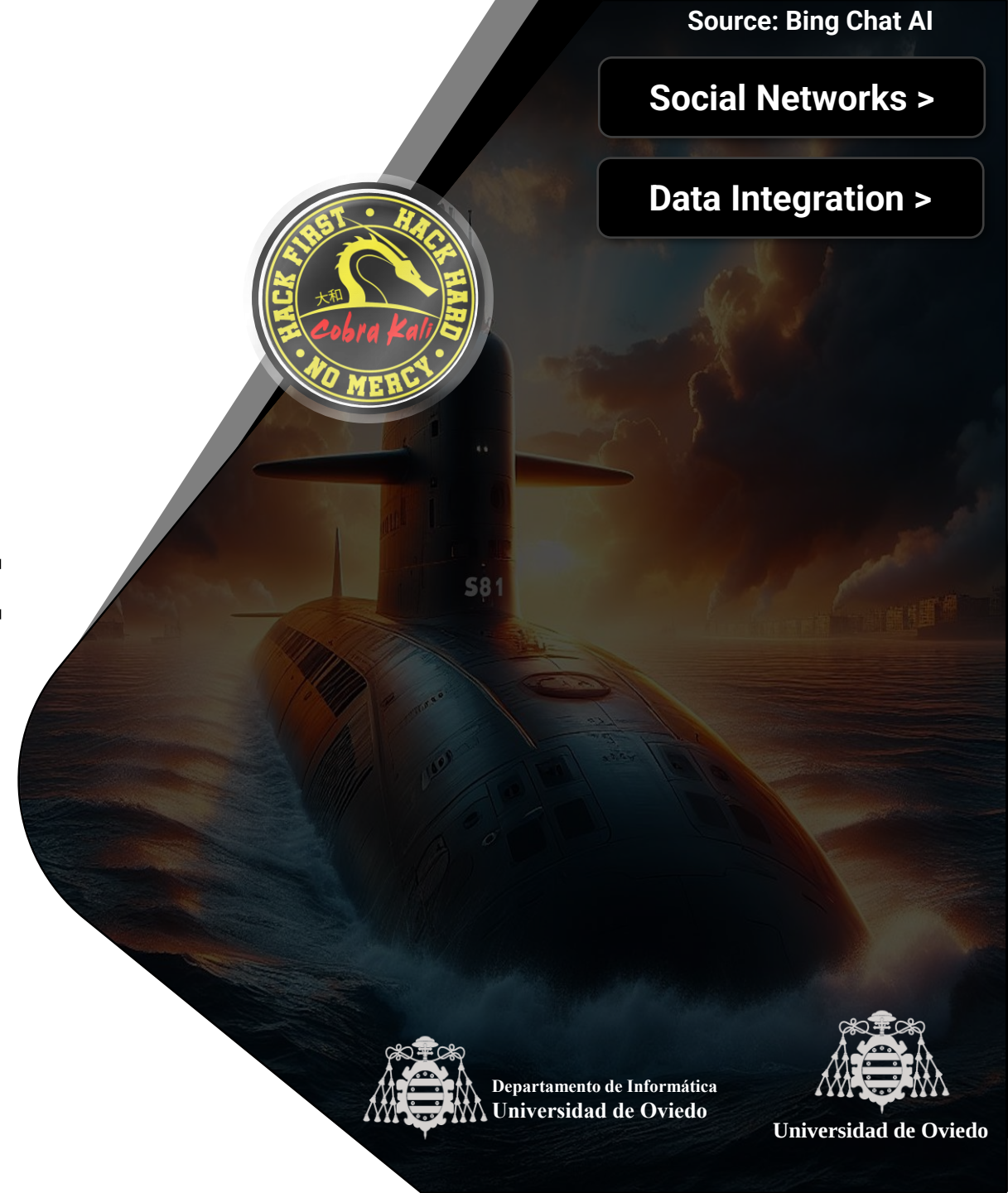
[< Go to Index](#)

[Social Networks >](#)

[Data Integration >](#)

OSINT AGAINST THE PEOPLE

Investigating people using public information only



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo

Social networks

Know what the people do...and post 😊



THE PROBLEM OF TOOLS THAT WORK WITH SOCIAL MEDIA

- Social networks don't like tools that extract information from their profiles 😊
 - And that gets us into a cat-and-mouse race
 - Forcing us to look for tools that keep working
- You can find a lot of them in Ciberpatrulla
- Twitter (now X) is a perfect example of this
 - Access to its API became non-free, which killed many research tools
 - This left (some) of the scraping-based ones
 - That is, **processing the content that is displayed on the screen**, acting as if they were normal users
 - Some are (but don't rule out that they stop working)
 - <https://github.com/tweepy/tweepy>
 - <https://github.com/dataquestio/twitter-scrape>

Ciberpatrulla is a huge repository of OSINT tools, among which there are many that work on social networks: <https://ciberpatrulla.com/links/>

Facebook

- 🕒 Descargar videos de Facebook
- 🔍 Whopostedwhat - Busca por fechas
- 📄 Exportador de comentarios a CSV
- 🕒 Socialfy - Exportar comentarios a CSV
- 🕒 FB-Search - Búsqueda en Facebook
- 🔍 Intelx - Búsqueda e Facebook
- 🔍 URLs personalizadas para buscar en Facebook
- new** 🔍 Obtener ID perfil de Facebook

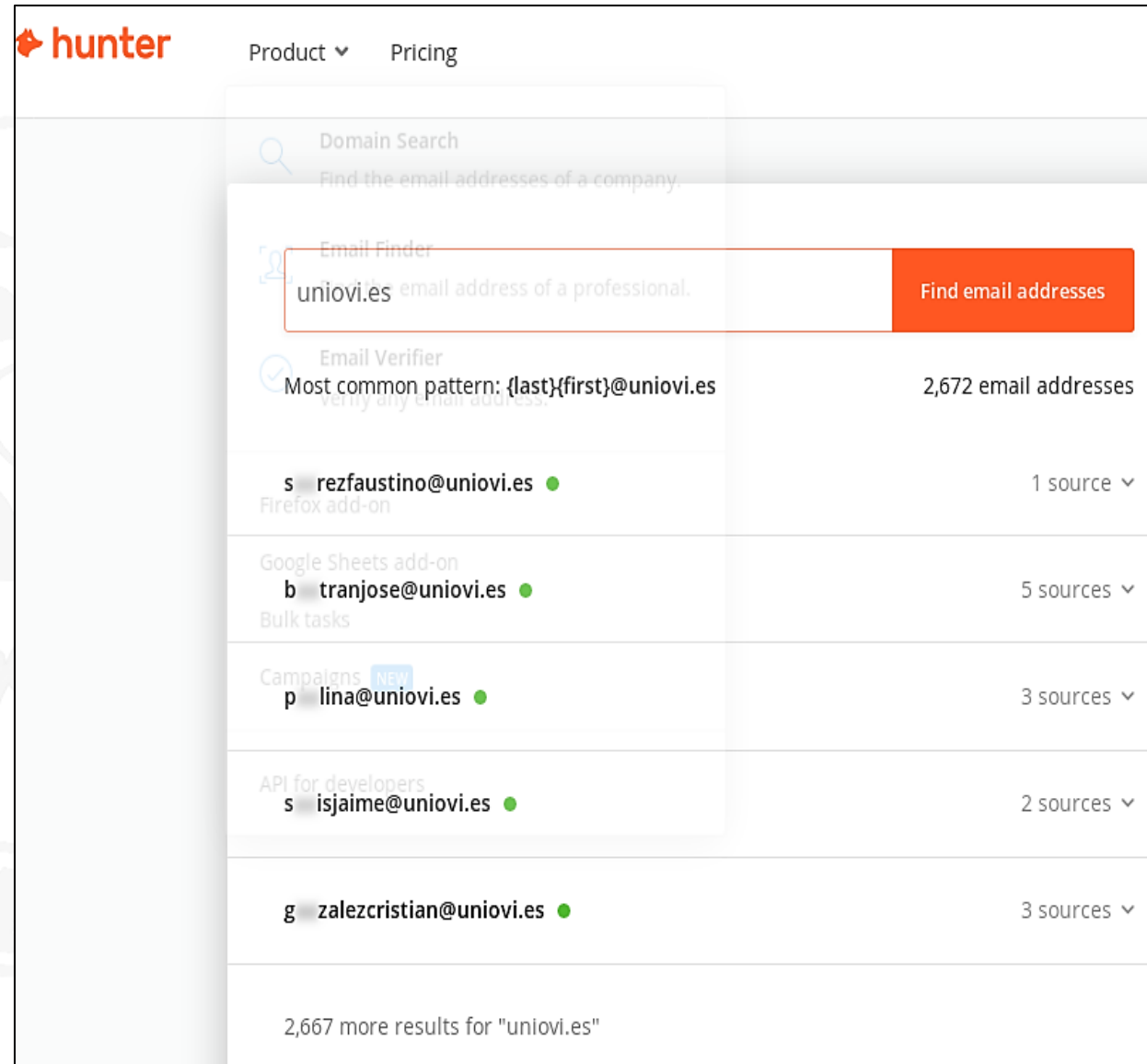
Otras RRSS

- 🕒 Busca en RRSS menos importantes

Instagram

- 🔍 Buscar en google por frase concreta
- 🕒 Cuidado con los avisos de capturas!
- 🔍 Picodash - Búsqueda en Instagram
- 📄 Exportador de comentarios a CSV
- new** 🔍 Tucktools - Descargar Videos de Instagram
- new** 📷 Instafollowers - Obtener ID de Instagram
- new** 📷 Buyinstagramfollowers - Obtener ID de Instagram
- new** 📷 Allsno - Obtener ID de Instagram
- new** 📷 Otzberg - Obtener ID de Instagram
- new** 🔍 Instagram - Buscar por localización
- new** 🔍 Obtener usuario desde la ID

- Website that allows you to discover email addresses related to domains / companies
- With them, OSINT attacks, phishing attempts or APTs (Advanced Persistent Threats) can be started
- It is not a free service
 - Free registration allows limited usage of its features
 - Complete results
 - CSV downloads
 - Up to 50 searches/month



The screenshot displays the Hunter.io web application. At the top, the 'hunter' logo is on the left, and 'Product' and 'Pricing' links are on the right. A search bar is prominently featured, containing the domain 'uniovi.es'. Below the search bar, a table lists various email addresses found for this domain, each with a source icon and a dropdown arrow indicating the number of sources. The table includes entries for 'rezfaustino@uniovi.es' (1 source), 'tranjose@uniovi.es' (5 sources), 'lina@uniovi.es' (3 sources), 'isjaime@uniovi.es' (2 sources), and 'zalezcristian@uniovi.es' (3 sources). A footer note states '2,667 more results for "uniovi.es"'. The interface is clean and modern, with a light gray background and orange accents.

Email Address	Source
s rezfaustino@uniovi.es	1 source
b tranjose@uniovi.es	5 sources
p lina@uniovi.es	3 sources
s isjaime@uniovi.es	2 sources
g zalezcristian@uniovi.es	3 sources

PROJECT SHERLOCK

<https://github.com/sherlock-project/sherlock>



- Finds a username on lots of different social networks and webpages

- More than 320!

- It is very common to find users with the same name on different social networks

- We can use it to collect information from different sources about the same person
- This may reveal data about people with closed profiles only in a network, but an open profile in another one

- Basic usage is simple

- `python3 pherlock.py <username>`

```
(vagrant@kali)~$ sherlock Ibailanos
[*] Checking username Ibailanos on:
[+] Academia.edu: https://independent.academia.edu/Ibailanos
[+] CapFriendly: https://www.capfriendly.com/users/Ibailanos
[+] Chaturbate: https://chaturbate.com/Ibailanos
[+] Coil: https://coil.com/u/Ibailanos
[+] DeviantART: https://Ibailanos.deviantart.com
[+] Duolingo: https://www.duolingo.com/profile/Ibailanos
[+] F3.cool: https://f3.cool/Ibailanos/
[+] Facebook: https://www.facebook.com/Ibailanos
[+] Fiverr: https://www.fiverr.com/Ibailanos
[+] FortniteTracker: https://fortnitetracker.com/profile/all/Ibailanos
[+] Giphy: https://giphy.com/Ibailanos
[+] GitHub: https://www.github.com/Ibailanos
[+] Gumroad: https://www.gumroad.com/Ibailanos
[+] Instagram: https://www.instagram.com/Ibailanos
[+] LeetCode: https://leetcode.com/Ibailanos
[+] Lichess: https://lichess.org/@/Ibailanos
[+] Linktree: https://linktr.ee/Ibailanos
[+] Minecraft: https://api.mojang.com/users/profiles/minecraft/Ibailanos
[+] PSNProfiles.com: https://psnprofiles.com/Ibailanos
[+] Pinterest: https://www.pinterest.com/Ibailanos/
[+] Pokemon Showdown: https://pokemonshowdown.com/users/Ibailanos
[+] Pornhub: https://pornhub.com/users/Ibailanos
[+] Quizlet: https://quizlet.com/Ibailanos
[+] Reddit: https://www.reddit.com/user/Ibailanos
[+] Roblox: https://www.roblox.com/user.aspx?username=Ibailanos
[+] RuneScape: https://apps.runescape.com/runemetrics/profile/profile?user=Ibailanos
[+] Scratch: https://scratch.mit.edu/users/Ibailanos
[+] SlideShare: https://slideshare.net/Ibailanos
[+] Smule: https://www.smule.com/Ibailanos
[+] Spotify: https://open.spotify.com/user/Ibailanos
[+] Telegram: https://t.me/Ibailanos
[+] Tenor: https://tenor.com/users/Ibailanos
[+] TikTok: https://tiktok.com/@Ibailanos
[+] TradingView: https://www.tradingview.com/u/Ibailanos/
[+] Trello: https://trello.com/Ibailanos
[+] Twitch: https://www.twitch.tv/Ibailanos
[+] Twitter: https://twitter.com/Ibailanos
[+] Venmo: https://venmo.com/u/Ibailanos
[+] Wattpad: https://www.wattpad.com/user/Ibailanos
[+] WordPress: https://Ibailanos.wordpress.com/
[+] Xbox Gamertag: https://xboxgamertag.com/search/Ibailanos
[+] YouNow: https://www.younow.com/Ibailanos/
[+] mercadolibre: https://www.mercadolibre.com.br/perfil/Ibailanos
[+] osu!: https://osu.ppy.sh/users/Ibailanos
[+] xHamster: https://xhamster.com/users/Ibailanos
```

User reconnaissance integration / from multiple sources

Aggregating user data

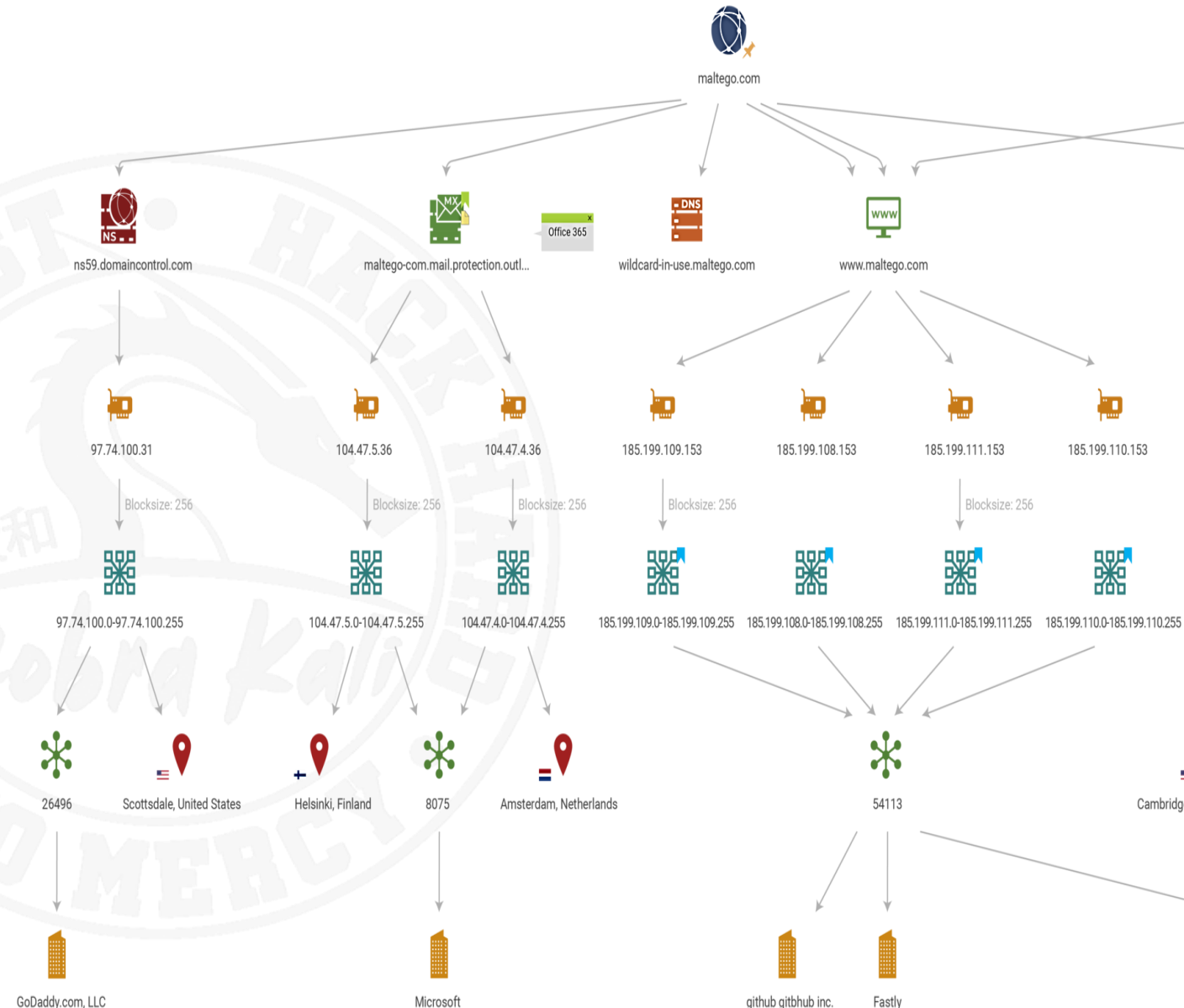


● Collects information from Internet entities

- Creates custom entities that represent any kind of information
- Specializes in finding relationships between them
 - Social networks, computer networks, domains...
- Uses DNS and **whois** records, search engines, known social networks, APIs... as sources

● Tutorials

- <https://www.fwhibbit.es/introduccion-a-maltego>
- <https://ciberpatrulla.com/maltego/>
- www.elladodelmal.com/2010/08/mineria-de-datos-con-maltego-1-de-2.html
- We will see more about it on the **Group Works**



<https://github.com/lanmaster53/recon-ng>

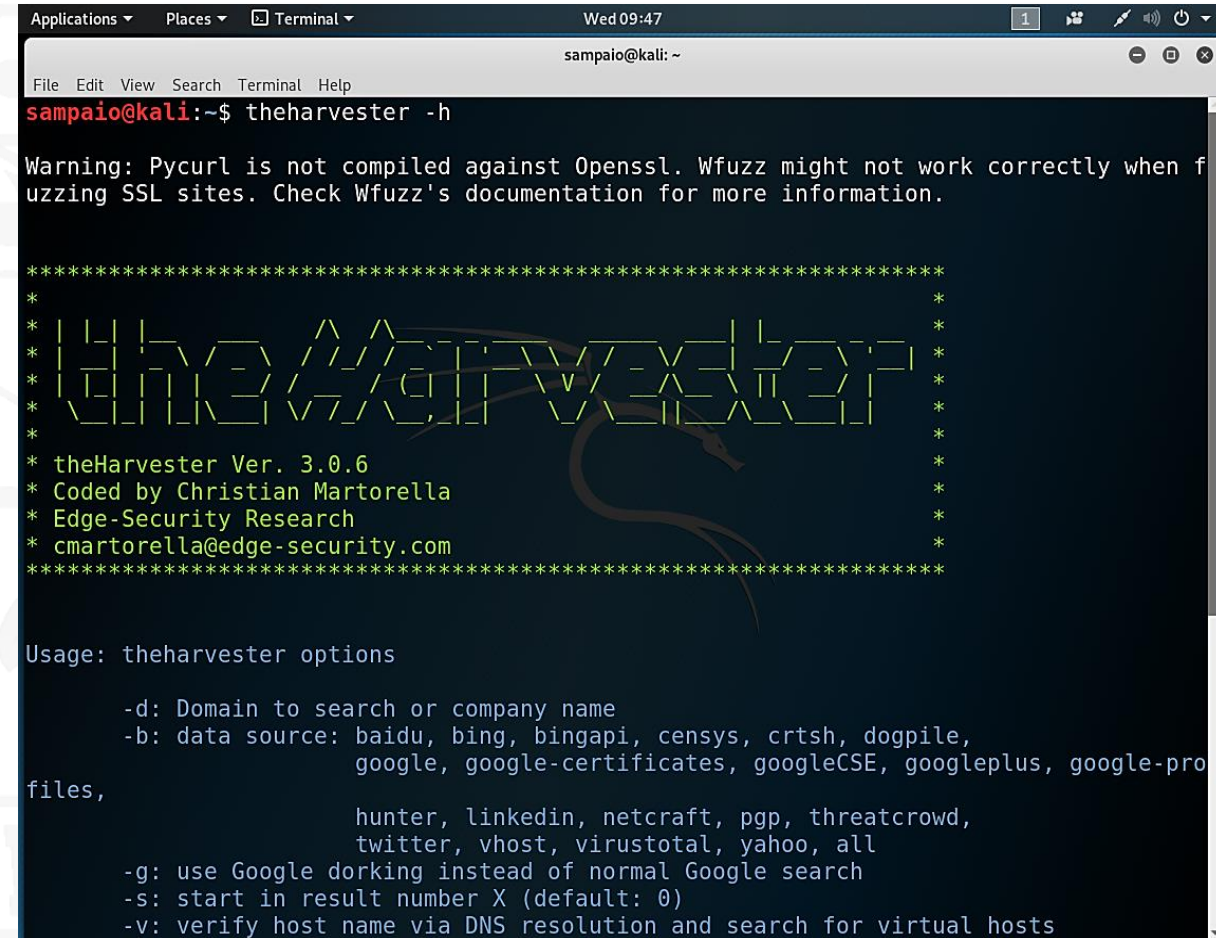


- ```
carlos@NoSoloHacking:~/recon-ng$ sudo ./recon-ng
```
- Sponsored by ...
- ^  
 / \ \ ^  
 ^ / \ \ \ \ \ \  
 / \ \ // \ \ \ \ \ \ \ \  
 // // BLACK HILLS V \ \  
[www.blackhillsinforec.com](http://www.blackhillsinforec.com)
- PRACTISEC  
[www.practisec.com](http://www.practisec.com)
- [recon-ng v5.1.1, Tim Tomes (@lanmaster53)]
- [\*] No modules enabled/installed.
- [recon-ng][default] > █

**Source:** <https://www.nosolohacking.info/recon-ng-instalacion/>

<https://github.com/laramies/theHarvester>

- ## ● Also, information from DNS



# SCRUMMAGE

<https://github.com/matamorphosis/Scrummage>



Computer Security

## ● Centralizes OSINT scans

- Provides us a high-level view of sites with information about a target

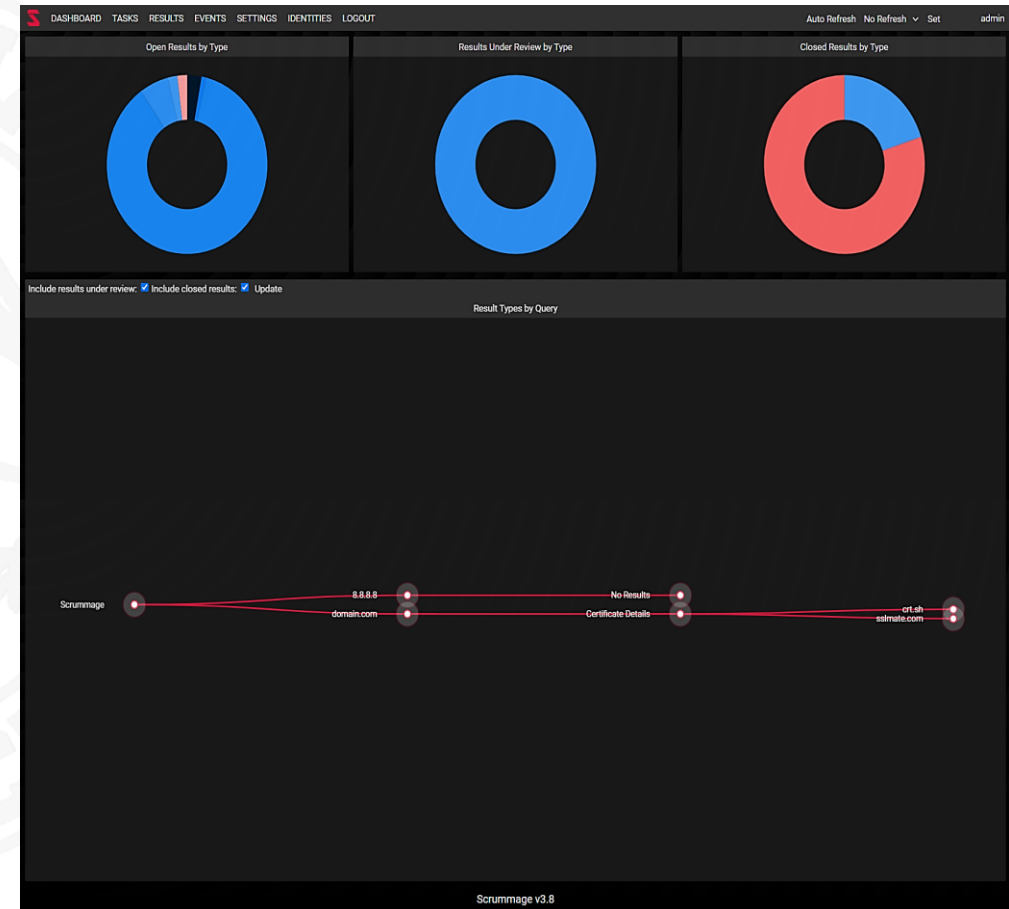
## ● Implements plugins to customize the type of scans and optimize resource usage

## ● Such plugins provide diverse capabilities

- Blockchain search
- Domain fuzzing
- Twitter analytics
- Instagram search
- Search on Have I Been Pwned? (<https://haveibeenpwned.com/>)
  - In case any account identities have been leaked ...

## ● Similar tools

- OSINT Framework: <https://github.com/lockfale/osint-framework>
- Scumblr: <https://portunreachable.com/automated-osint-with-scumblr-a4d81a048e54?gi=ae6ebac43a92>

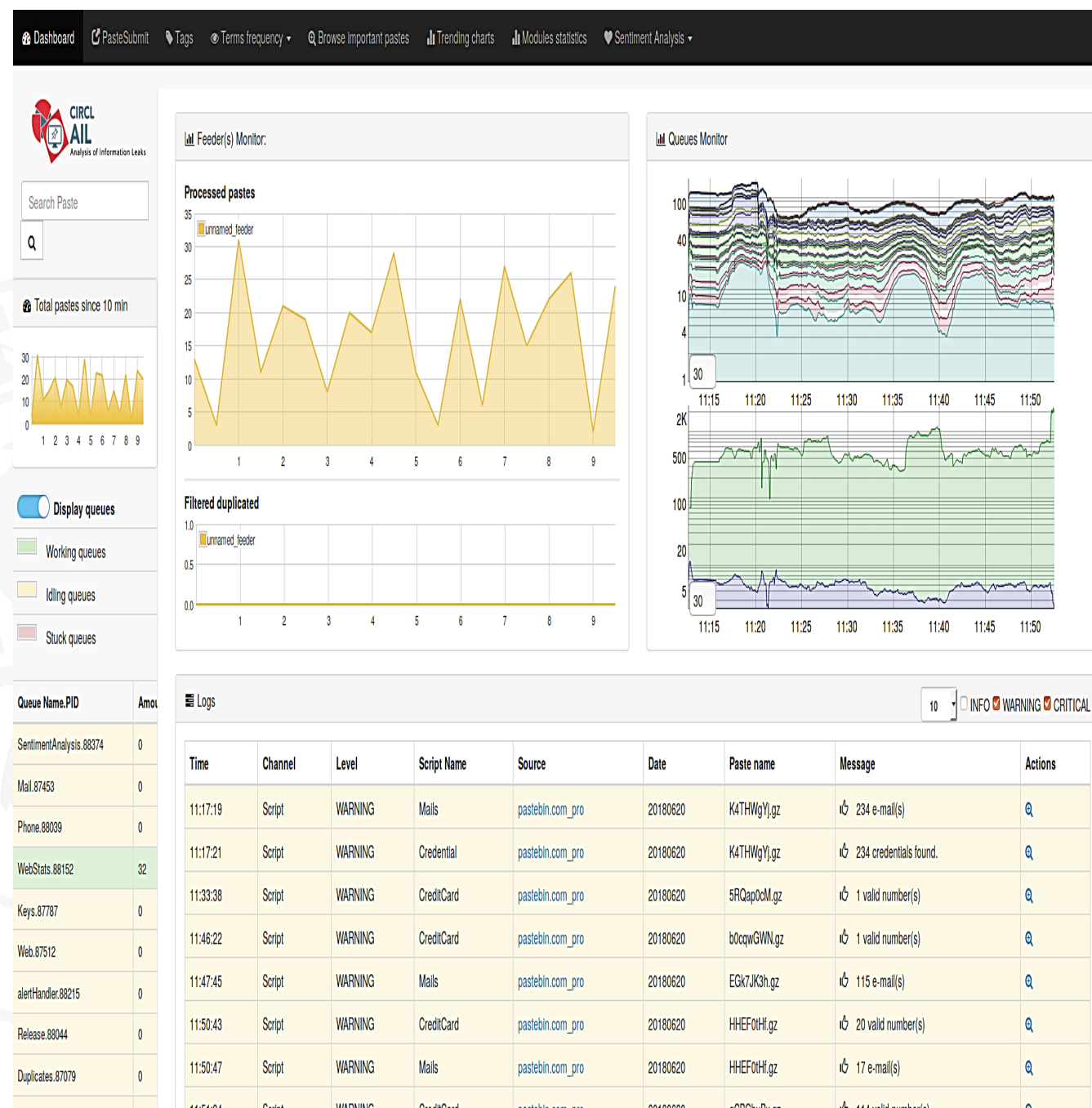


# AIL FRAMEWORK

<https://github.com/CIRCL/AIL-framework>



- **Highly modular framework that analyzes filtered information**
  - From unstructured sources
  - A popular source is Pastebin
- **Its highly modular so it could be extended**
  - And used to mine and process private information of different kinds
  - And therefore, detect and prevent information leakage
- **To find out more**
  - <https://www.kitploit.com/2019/08/ail-framework-framework-for-analysis-of.html>



# MORE OSINT TOOLS...



- OSINT's techniques are very popular and powerful due to the information they can find

- There are a huge number of tools that get information from different media and social networks on Internet
- It's very difficult to list them all

- **Remember:** There's a classified list of tools available: <https://ciberpatrulla.com/links/>

- This web is probably the most complete repository on OSINT tools
- It contains hundreds of tools classified for its basic usage in the OSINT world
- Social networks, vehicles, phones, documents...

## Recon Tools for Web Application Pentesting

### Proxy

- Burpsuite
- Zap Proxy

### Webspidering

- Gospider
- Gau
- Linkfinder
- Waybackurls
- Hakrawler
- Paramspider

### Fingerprinting

- Wappalyzer
- Builtwith
- Netcraft
- Whatweb
- Wafw0f

### Email

- Mxtoolbox
- Emkei
- Anonymailer
- Thunderbird

### Sensitive data

- Trufflehog
- Gitsecrets

### Payloads / Wordlists

- Swisskeyrepo
- Seclists

### SSL

- SSLscan
- SSLhopper

### Searchengines

- Shodan
- Censys
- Zoomeye
- Google

### Subdomain

- Subfinder
- Amass
- Dig
- Assetfinder
- Sublist3r
- Chaos

### Directory / Fuzzing

- Ffuf
- Wfuzz
- Gobuster
- Dirbuster

### Vulnerability

- Nuclei
- Wpscan
- Nikto

### Exploit

- Searchsploit
- Exploitdb

### Api

- Postman
- GraphQLmap

### Ports

- Nmap
- Masscan
- Zmap
- Smap
- Hackertarget

### Misc

- HTTPx
- Metasploit
- DNSDumpster
- HTTPrope
- Recon-ng
- Securitytrails

# DO YOU HAVE EXAMPLES?

- With such a number of tools available, it is very easy to get lost when starting an OSINT research
- Therefore, it is best to see examples of how to make one
- You can follow this four-part tutorial
  - <https://navisec.io/a-pentesters-guide-part-1-osint-passive-recon-and-discovery-of-assets/>
  - <https://navisec.io/a-pentesters-guide-part-2-osint-linkedin-is-not-just-for-jobs/>
  - <https://navisec.io/a-pentesters-guide-part-3-osint-breach-dumps-password-spraying/>
  - <https://navisec.io/a-pentesters-guide-part-4-grabbing-hashes-and-forging-external-footholds/>
  - <https://navisec.io/a-pentesters-guide-part-5-unmasking-wafs-and-finding-the-source/>
- Or this OSINT guide
  - <https://www.hackers-arise.com/osint>
- We can find more tools in this web page
  - Metadata extraction, geolocation, subdomain extraction...
  - <https://derechodelared.com/herramientas-osint-recopilatorio/>
- Or in the material that we are going to give you for the **Group Works** 😊

# Using Google Hacking to find Uniovi-bound resources



[< Go to Index](#)

# OSINT AGAINST THE SOURCE

Source code can be an OSINT threat too



Departamento de Informática  
Universidad de Oviedo



Universidad de Oviedo

- ```
https://github.com/intel/pa-blink/blob/98565fea6e44a40fac3901b8d4bdc0029c708032/LayoutTests/fast/url/script-tests/segments.js
["http:example.com/",["http:","example.org","","/example.com/","",""],
["ftp:example.com/",["ftp:","example.com","","/","",""],
["https:example.com/",["https:","example.com","","/","",""],
["madeupscheme:example.com/",["madeupscheme:","","","example.com/","",""],
["file:example.com/",["file:","","","/example.com/","",""],
["ftps:example.com/",["ftps:","","","/example.com/","",""],
["gopher:example.com/",["gopher:","example.com","","/","",""],
["ws:example.com/",["ws:","example.com","","/","",""],
["wss:example.com/",["wss:","example.com","","/","",""],
["data:example.com/",["data:","","","/example.com/","",""],
["javascript:example.com/",["javascript:","","","example.com/","",""],
["mailto:example.com/",["mailto:","","","/example.com/","",""],
["http:example.com/",["http:","example.org","","/foo/example.com/","",""],
["ftp:example.com/",["ftp:","example.com","","/","",""],
["https:example.com/",["https:","example.com","","/","",""],
["madeupscheme:example.com/",["madeupscheme:","","","example.com/","",""],
["file:example.com/",["file:","","","/example.com/","",""],
["ftps:example.com/",["ftps:","","","example.com/","",""],
["gopher:example.com/",["gopher:","example.com","","/","",""],
["ws:example.com/",["ws:","example.com","","/","",""],
["wss:example.com/",["wss:","example.com","","/","",""],
["data:example.com/",["data:","","","example.com/","",""],
["javascript:example.com/",["javascript:","","","example.com/","",""],
["mailto:example.com/",["mailto:","","","example.com/","",""],
End of Matches
(Result 12/1000+)=== Ignore similar [c]ontents/[u]ser/[r]epo/[f]ilename.[p]rint contents.[s]ave state.[a]dd to log. search
```

- Tool to find sensitive data in GitHub repositories
- Includes data from various sources that may have been left in repository files
- Among other information sources it includes
 - Google
 - Amazon (AWS)
 - Paypal
 - Github
 - Facebook
 - Twitter
 - ...

```
root@bugbounty# python3 gitGraber.py -k wordlists/keywords.txt -q "yahoo" -s
[i] Github query : https://api.github.com/search/code?q=yahoo access_key&sort=indexed&o=desc
[i] Status code : 200
[!] POSSIBLE AWS TOKEN FOUND (keyword used:yahoo)
[+] Commit date : 2019-09-10T13:40:08Z by [REDACTED]
[+] RAW URL : https://raw.githubusercontent.com/[REDACTED]/[REDACTED]/cmd_bash.md
[+] Token : [REDACTED]
[+] Repository URL : https://github.com/[REDACTED]/[REDACTED]
[i] Github query : https://api.github.com/search/code?q=yahoo access_token&sort=indexed&o=desc
[i] Status code : 200
[!] POSSIBLE GOOGLE_FIREBASE_OR_MAPS TOKEN FOUND (keyword used:yahoo)
[+] Commit date : 2019-09-11T20:12:28Z by [REDACTED]
[+] RAW URL : https://raw.githubusercontent.com/[REDACTED]/connectApp/[REDACTED]/app.js
[+] Token : [REDACTED]
[+] Repository URL : https://github.com/[REDACTED]/[REDACTED]
[!] POSSIBLE TWILIO TOKEN FOUND (keyword used:yahoo)
[+] Commit date : 2019-07-30T06:28:32Z by [REDACTED]
[+] RAW URL : https://raw.githubusercontent.com/[REDACTED]/[REDACTED]/project.html
[+] Token : [REDACTED]
[+] Repository URL : https://github.com/[REDACTED]/[REDACTED]
```

GITHUB ITSELF!



- The GitHub search feature can also be used to find private information on public repos
- It is a powerful search function that allows searching by multiple terms
 - Like Google Hacking (Google Dorks), but for code
 - In fact, many people call this **GitHub Dorks!**
- The image shows several popular search examples

**Anton**
@therceman

www.therceman.dev

GitHub Dorks for Finding Files

filename:manifest.xml	filename:config.php	filename:.ovpn
filename:travis.yml	filename:config.inc.php	filename:.cscfg
filename:vim_settings.xml	filename:prod.secret.exs	filename:.rdp
filename:database	filename:configuration.php	filename:.mdf
filename:prod.exs	filename:.sh_history	filename:.sdf
filename:prod.secret.exs	filename:shadow	filename:.sqlite
filename:.npmrc_auth	filename:proftpdpasswd	filename:.psafe3
filename:.dockercfg	filename:pgpass	filename:secret_token.rb
filename:WebServers.xml	filename:idea14.key	filename:carrierwave.rb
filename:.bash_history	filename:hub	filename:database.yml
filename:sftp-config.json	filename:.bash_profile	filename:.keychain
filename:sftp.json	filename:.env	filename:.kwallet
filename:secrets.yml	filename:wp-config.php	filename:.exports
filename:.esmtprc	filename:credentials	filename:config.yaml
filename:passwd	filename:id_rsa	filename:settings.py
filename:LocalSettings.php	filename:id_dsa	filename:credentials.xml

GitHub Dorks for Finding API Keys, Tokens and Passwords

api_key	OTP	password
authorization_bearer:	HOMEBREW_GITHUB_API_TOKEN	user_password
oauth	SF_USERNAME	user_pass
auth	HEROKU_API_KEY	passcode
authentication	JEKYLL_GITHUB_TOKEN	client_secret
client_secret	shodan_api_key	secret
api_token:	api.forecast.io	password hash
client_id		user auth

GitHub Dorks Automation Tools

TruggleHog	- https://github.com/dxa4481/truffleHog
Github-Dorks	- https://github.com/techgaun/github-dorks
GitGot	- https://github.com/BishopFox/GitGot
GitMonitor	- https://github.com/Talkaboutcybersecurity/GitMonitor
GitRob	- https://github.com/michenriksen/gitrob
GitHound	- https://github.com/tillson/git-hound
GittyLeaks	- https://github.com/kootenpv/gittyleaks
GitSecrets	- https://github.com/aws-labs/git-secrets
Watchtower	- https://radar.nightfall.ai

SELF-EVALUATION ACHIEVEMENT LIST: SEMINAR 1

- Understand the OSINT concept
- Understand what types of devices we can find on the internet
- Know what type of information you should not put into source code
- Know how to use Shodan and Censys OSINT tools to find machines of a concrete target
- Know how to use Google Hacking to find information of a concrete target
- Know multiple OSINT tools that work with personal information of individuals / companies
- Know tools to study source code in public repositories
- Know how to study a target using Google Hacking
- Know how to study a person on social media and the problem with the tools that do this type of activity



SEMINAR 1

TOOLS FOR INTERNET RESEARCH



Departamento de Informática
Universidad de Oviedo



Universidad de Oviedo