INFORMATION GATHERING

Information gathering plays a crucial part in preparation for any professional social engineering engagement. Information gathering is the most time-consuming and laborious phase of the attack cycle but is often a major determinant of the success or failure of the engagement.

- Information-gathering tools freely available online
- Online locations that house valuable pieces of data
- Software to aid in finding and collating the data
- The value or use of seemly insignificant data which collected online, over the phone, or in-person

WHOIS LOOKUP

Whois can be defined as an internet service which provides registration details of domains. The domains are registered with the help of registrars like Go Daddy. While the user registers their domain. The information they enter is publically available on the internet. This information can be easily looked up using the whois service.

Since there is no central database available for whois information. Thus the search engines collect the whois information form multiple registrars and provide them.

shein.in

Updated 53 seconds ago

Domain Information

Domain:	shein.in
Registrar:	GoDaddy.com, LLC
Registered On:	2016-05-22
Expires On:	2022-05-22
Updated On:	2020-11-06
Status:	clientDeleteProhibited clientRenewProhibited clientTransferProhibited clientUpdateProhibited
Name Servers:	ns-2033.awsdns-62.co.uk dns1.p07.nsone.net dns2.p07.nsone.net ns-250.awsdns-31.com

Registrant Contact

Organization:	Zoetop Business Co., Limited
State:	HONG KONG
Country:	HK
Email:	Please contact the Registrar listed above

Administrative Contact

Email:	Please contact the Registrar listed above

Technical Contact

Email:	Please contact the Registrar listed above

Raw Whois Data

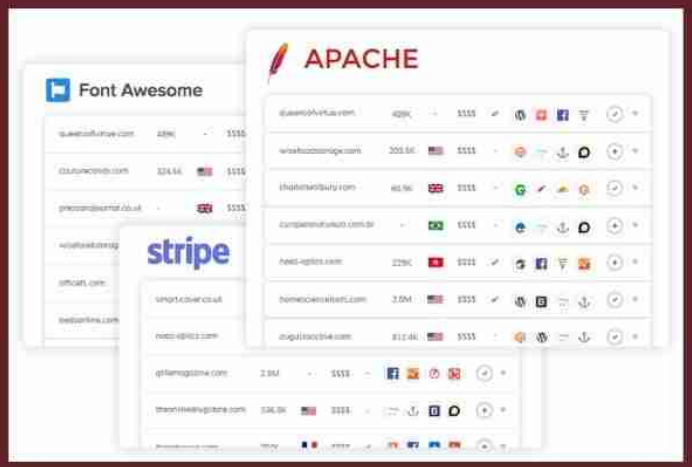
```
Domain Name: shein.in
Registry Domain ID: D414400000000969651-
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2020-11-06T07:42:16Z
Creation Date: 2016-05-22T23:04:41Z
Registry Expiry Date: 2022-05-22T23:04:4
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited ht
Domain Status: clientRenewProhibited htt
Domain Status: clientTransferProhibited
Domain Status: clientUpdateProhibited ht
Registry Registrant ID: REDACTED FOR PRI
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Zoetop Business
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: HONG KONG
Registrant Postal Code: REDACTED FOR PRI
Registrant Country: HK
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVA
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Reg
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVA
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registra
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVAC
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar
Name Server: ns-2033.awsdns-62.co.uk
Name Server: dns1.p07.nsone.net
Name Server: dns2.p07.nsone.net
Name Server: ns-250.awsdns-31.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Compla
>>> Last update of WHOIS database: 2021-

For more information on Whois status coc

Access to .IN WHOIS information is provi
```

TECHNOLOGY LOOKUP

We can find out what technologies a website or application is using for doing this there are various tools for example wappalyzer .



WAPPALYZER

Wappalyzer is a technology profiler that shows you what websites are built with. Find out what CMS a website is using, as well as any framework, ecommerce platform, JavaScript libraries and many more. Wappalyzer is more than a CMS detector or framework detector: it uncovers more than a thousand technologies in dozens of categories such as programming languages, analytics, marketing tools, payment processors, CRM, CDN and others.

Credit balance: 48 Buy credits

Website URL or company name

http://www.Shein.in

Spend 1 credit.

Security

Technologies

Emarsys		
Branch	2.58.2	Marketing automation
Aimtell		
Emarsys		Personalisation
Google Analytics		
Branch	2.58.2	
Sensors Data		
Facebook Pixel		Analytics
Akamai mPulse		
Google Analytics Enhanced eCommerce		
Vue.js	2.5.17	JavaScript frameworks
Choices		
Swiper Slider		Miscellaneous
webpack		
jQuery	1.12.4	JavaScript libraries
Boomerang		
Twitter Ads		
Microsoft Advertising		Advertising
Criteo		
Nginx		Web servers
Nginx		Reverse proxies
Akamai		CDN
Facebook		Widgets
Google Tag Manager		Tag managers
Boomerang		RUM
Akamai mPulse		
Cart Functionality		Ecommerce
Facebook Login		Social logins
Criteo		Retargeting

CACHE INFORMATION

There are tools through which we can get information about a website like traffic on that website ,sells of that site and many more informations.one of them are wayback.

WAYBACK

Software has been developed to "crawl" the Web and download all publicly accessible information and data files on webpages, the Gopher hierarchy, the Netnews (Usenet) bulletin board system, and downloadable software.The information collected by these "crawlers" does not include all the information available on the Internet, since much of the data is restricted by the publisher or stored in databases that are not accessible. To overcome inconsistencies in partially cached websites, Archive-It.org was developed in 2005 by the Internet Archive as a means of allowing institutions and content creators to voluntarily harvest and preserve collections of digital content, and create digital archives.

SUB-DOMAIN INFORMATION

Finding subdomains is an important step in the information gathering phase of a penetration test. Subdomains are interesting because they point to various (less-known) applications and indicate different external network ranges used by the target company.

For instance, subdom1.company.com points to IP 1.1.1.1 and subdom2.company.com points to IP 2.2.2.2. Now you know two different IP ranges possibly owned by your target organization and you can extend the attack surface.

Furthermore, subdomains sometimes host 'non-public' applications (e.g. test, development, restricted) which are usually less secure than the public/official applications so they can be the primary attack targets.

File Machine View Input Devices Help

kali@kali: ~/Desktop/Su...

File Actions Edit View Help

Coded By Ahmed Aboul-Ela - @aboul3la

```
[-] Enumerating subdomains now for m.shein.in
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
HTTPSConnectionPool(host='searchdns.netcraft.com', port=443): Max retries exc
eeded with url: /?restriction=site+ends+with&host=example.com (Caused by NewC
onnectionError('<urllib3.connection.HTTPSConnection object at 0x7fa75be00940>
: Failed to establish a new connection: [Errno -3] Temporary failure in name
resolution'))
HTTPSConnectionPool(host='www.virustotal.com', port=443): Max retries exceede
d with url: /ui/domains/m.shein.in/subdomains (Caused by NewConnectionError('
<urllib3.connection.HTTPSConnection object at 0x7fa75bdfebe0>: Failed to esta
blish a new connection: [Errno -3] Temporary failure in name resolution'))
Process GoogleEnum-4:
Traceback (most recent call last):
  File "/usr/lib/python3.9/multiprocessing/process.py", line 315, in _bootstr
ap
    self.run()
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 240, in enumerate
    if not self.check_response_errors(resp):
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 303, in check_respon
se_errors
    if (type(resp) is str or type(resp) is unicode) and 'Our systems have det
ected unusual traffic' in resp:
NameError: name 'unicode' is not defined
HTTPSConnectionPool(host='dnsdumpster.com', port=443): Max retries exceeded w
ith url: / (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection
 object at 0x7fa75bdfeb50>: Failed to establish a new connection: [Errno -3]
Temporary failure in name resolution'))
```