Practical :- 1

Aim :- Google and Whois Reconnaissance

- Use Google search techniques to gather information about a specific target or organization.
- Utilize advanced search operators to refine search results and access hidden information.
- Perform Whois lookups to retrieve domain registration information and gather details about the target's infrastructure.

Using Google:

Because of various web server misconfigurations, sensitive information gets indexed by the search engines when spiders crawl them. The sensitive information may include: password files, confidential directories, logon portals, log files etc.

A Google dork query is a search string that uses advanced search operators to find information that is not readily available on a website. Google dorking, also known as Google hacking, can return information that is difficult to locate through simple search queries. To locate sensitive information, attackers use advanced sear 1ch strings called Google dork queries.

Some Google Dork Queries:

i)Files Containing Passwords

Search string: "whoops! there was an error." "db_password"

URL:
https://www.google.com/search?q=%22whoops!%20there%20was%20an%20error.%22%20%22db_pa ssword%22

Result: reveals database passwords as a result of the error raised by the PP Framework Laravel

Search string: intext:"login" department | admin | manager | company | host filetype:xls | xlsx community -github

URL:
https://www.google.com/search?q=intext:%22login%22%20department%20|%20admin%20|%20mana ger%20|%20com pany%20|%20host%20filetype:xls%20|%20xlsx%20-community%20-github

Result: reveals spreadsheets containing passwords

Search String: inurl:"build.xml" intext:"tomcat.manager.password"

URL:
https://www.google.com/search?q=inurl:%22build.xml%22%20intext:%22tomcat.manager.password% 22

Result: reveals the password of tomcat manager

Search String: intitle:"index of" intext:login.csv

URL:

https://www.google.com/search?q=intitle:%22index%20of%22%20intext:login.

csv **Result:** reveals servers with open directories exposing login information

files **ii) Pages Containing Login Portals**

Search String: inurl:admin.php inurl:admin ext:php

URL:

https://www.google.com/search?q=inurl:admin.php%20inurl:admin%20ext:php

Result: reveals the admin login page of sites

iii) Various Online Devices **Search String:** intitle:"VB Viewer"

URL:

https://www.google.com/search?q=intitle:%22VB%20Viewer%22

Result: reveals several online webcams or IPcams

File Containing Juicy Info

Search String: ext:env intext:APP_ENV= | intext:APP_DEBUG= | intext:APP_KEY=

URL:
https://www.google.com/search?q=ext:env%20intext:APP_ENV=%20|%20intext:APP_DEBUG=%20 | %20intext:APP_KEY=

Result: finds the environment configuration files (.env) of Laravel Framework which reveal credentials of database and SMTP servers

Whois:

WHOIS is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block or an autonomous system, but is also used for a wider range of other information. The protocol stores and delivers database content in a human-readable format. The WHOIS protocol is documented in RFC 3912.

Online Whois query:

➢ https://www.whois.com/

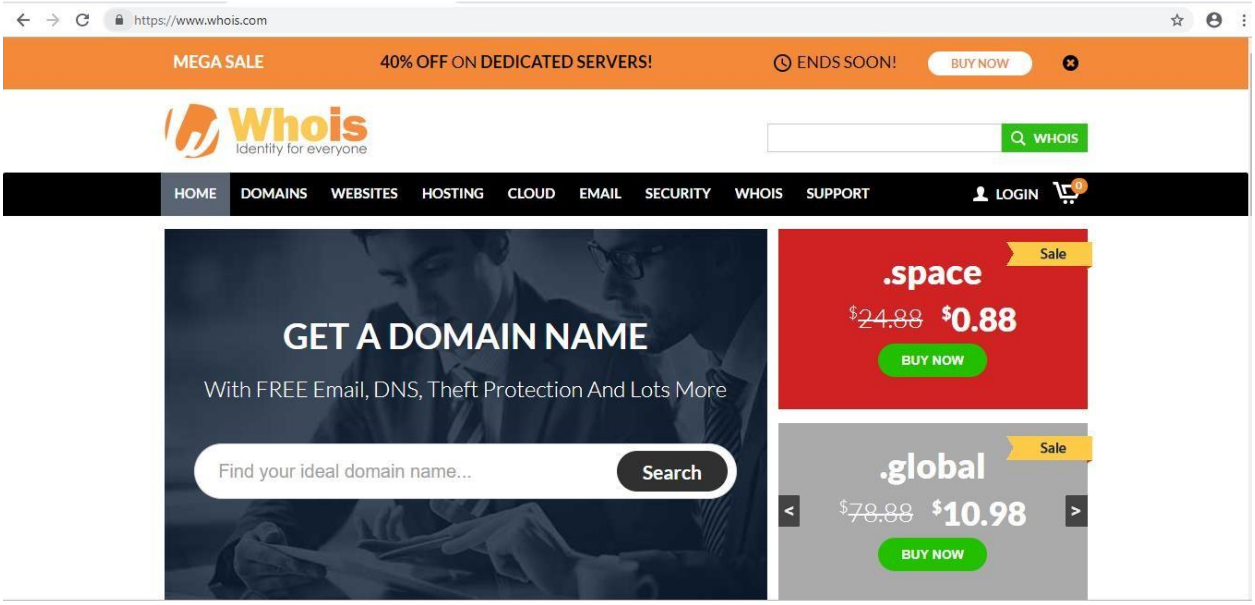
➢ https://www.whois.net/

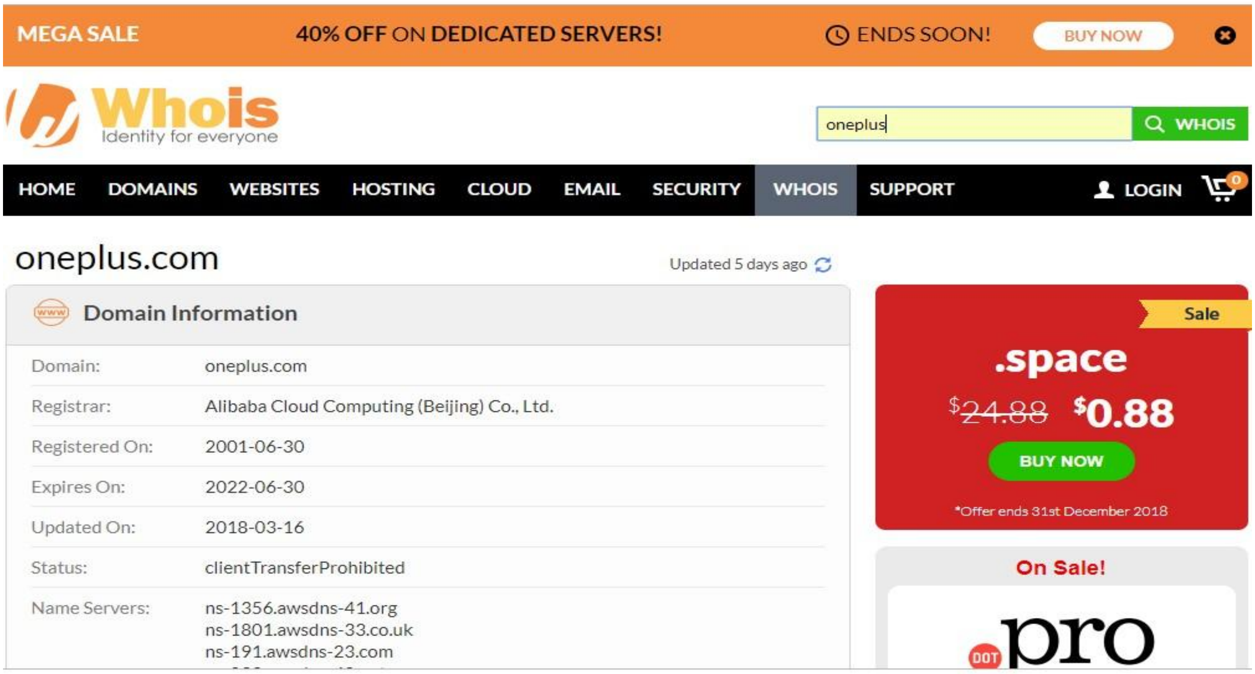
➢ http://whois.domaintools.com/

➢ https://who.is/

➢ https://whois.icann.org/en

➢ A) www.whois.com



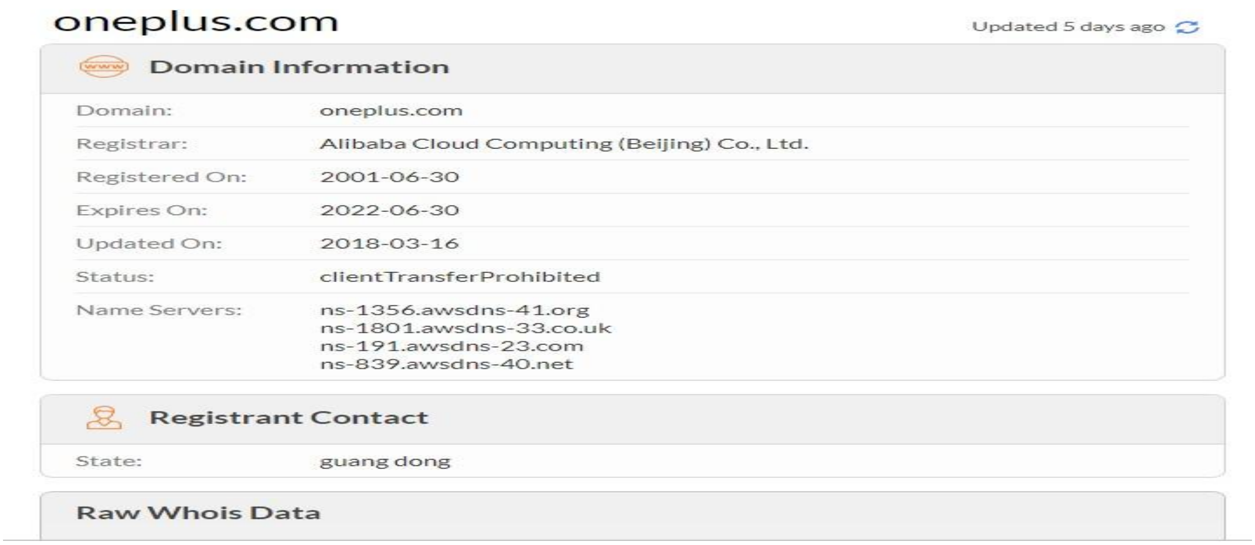


oneplus.com

Updated 5 days ago

Domain Information

Domain:	oneplus.com
Registrar:	Alibaba Cloud Computing (Beijing) Co., Ltd.
Registered On:	2001-06-30
Expires On:	2022-06-30
Updated On:	2018-03-16
Status:	clientTransferProhibited
Name Servers:	ns-1356.awsdns-41.org ns-1801.awsdns-33.co.uk ns-191.awsdns-23.com


oneplus.com

Updated 5 days ago

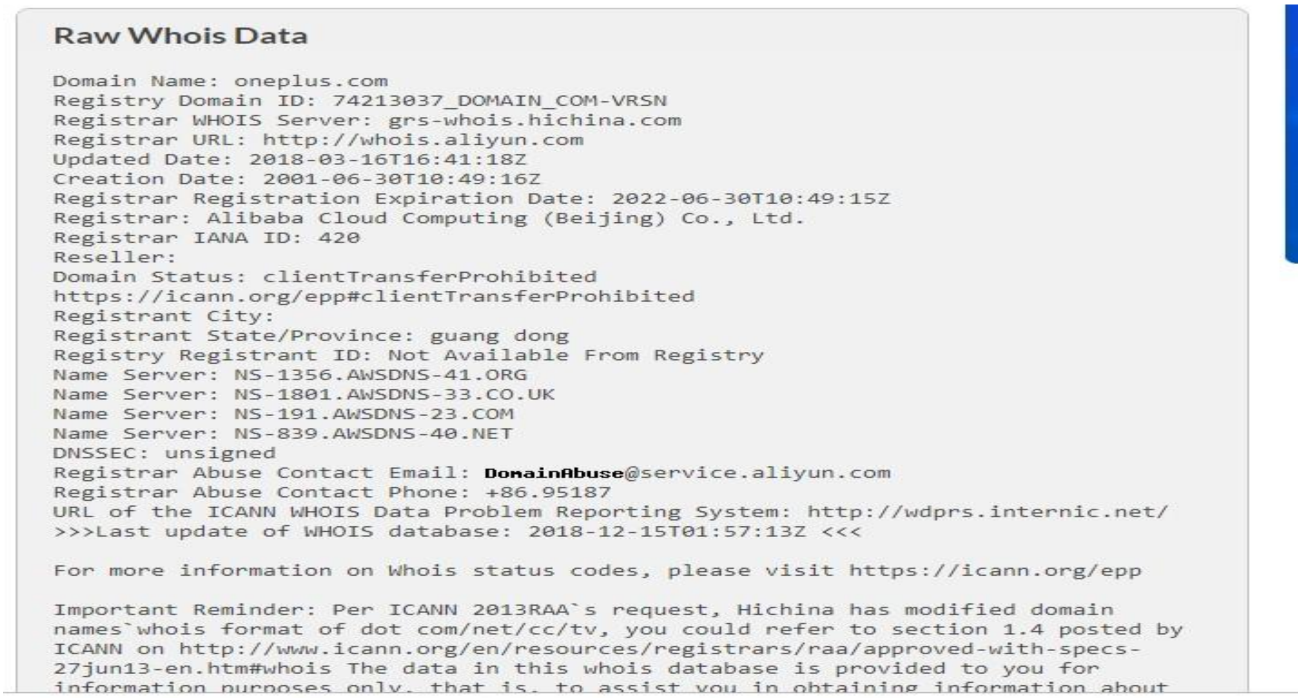
Domain Information

Domain:	oneplus.com
Registrar:	Alibaba Cloud Computing (Beijing) Co., Ltd.
Registered On:	2001-06-30
Expires On:	2022-06-30
Updated On:	2018-03-16
Status:	clientTransferProhibited
Name Servers:	ns-1356.awsdns-41.org ns-1801.awsdns-33.co.uk ns-191.awsdns-23.com ns-839.awsdns-40.net

Registrant Contact

State:	guang dong

Raw Whois Data

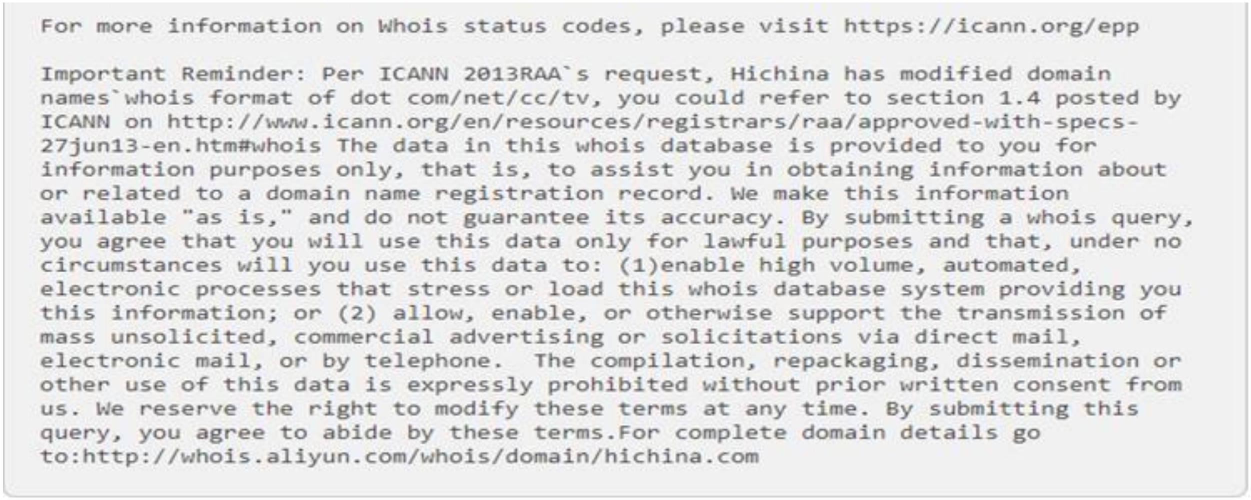


Raw Whois Data

```
Domain Name: oneplus.com
Registry Domain ID: 74213037_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.hichina.com
Registrar URL: http://whois.aliyun.com
Updated Date: 2018-03-16T16:41:18Z
Creation Date: 2001-06-30T10:49:16Z
Registrar Registration Expiration Date: 2022-06-30T10:49:15Z
Registrar: Alibaba Cloud Computing (Beijing) Co., Ltd.
Registrar IANA ID: 420
Reseller:
Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited
Registrant City:
Registrant State/Province: guang dong
Registry Registrant ID: Not Available From Registry
Name Server: NS-1356.AWSDNS-41.ORG
Name Server: NS-1801.AWSDNS-33.CO.UK
Name Server: NS-191.AWSDNS-23.COM
Name Server: NS-839.AWSDNS-40.NET
DNSSEC: unsigned
Registrar Abuse Contact Email: DomainAbuse@service.aliyun.com
Registrar Abuse Contact Phone: +86.95187
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>>Last update of WHOIS database: 2018-12-15T01:57:13Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Important Reminder: Per ICANN 2013RAA`s request, Hichina has modified domain
names`whois format of dot com/net/cc/tv, you could refer to section 1.4 posted by
ICANN on http://www.icann.org/en/resources/registrars/raa/approved-with-specs-
27jun13-en.htm#whois The data in this whois database is provided to you for
information purposes only, that is, to assist you in obtaining information about
```



```
For more information on Whois status codes, please visit https://icann.org/epp

Important Reminder: Per ICANN 2013RAA`s request, Hichina has modified domain
names`whois format of dot com/net/cc/tv, you could refer to section 1.4 posted by
ICANN on http://www.icann.org/en/resources/registrars/raa/approved-with-specs-
27jun13-en.htm#whois The data in this whois database is provided to you for
information purposes only, that is, to assist you in obtaining information about
```

```
or related to a domain name registration record. We make this information
available "as is," and do not guarantee its accuracy. By submitting a whois query,
you agree that you will use this data only for lawful purposes and that, under no
circumstances will you use this data to: (1)enable high volume, automated,
electronic processes that stress or load this whois database system providing you
this information; or (2) allow, enable, or otherwise support the transmission of
mass unsolicited, commercial advertising or solicitations via direct mail,
electronic mail, or by telephone.  The compilation, repackaging, dissemination or
other use of this data is expressly prohibited without prior written consent from
us. We reserve the right to modify these terms at any time. By submitting this
query, you agree to abide by these terms.For complete domain details go
to:http://whois.aliyun.com/whois/domain/hichina.com
```