Sri Lanka Institute of Information Technology

Penetration Testing Report

IE3022 - Applied Information Assurance

B.Sc. (Hons) in Information Technology

Specializing Cyber Security

Student Details

Student ID	Student Name
IT19961118	W.M.J.P. Wijesekara

Executive Summary

The target system was examined and analyzed using a variety of standardized tools and utilities. Overall, we agree that the implementations under review have reached an acceptable level of security, while we believe that corrective action is necessary due to medium and low risk concerns. The investigation's findings revealed traits that are well-protected against a number of well-known vulnerabilities.

I discovered high, medium, and low-level vulnerabilities and flaws on alibaba.com, including Session Cookie Not Marked as Secure, Weak Ciphers Enabled.

Following tools that I used to do this penetration testing report.

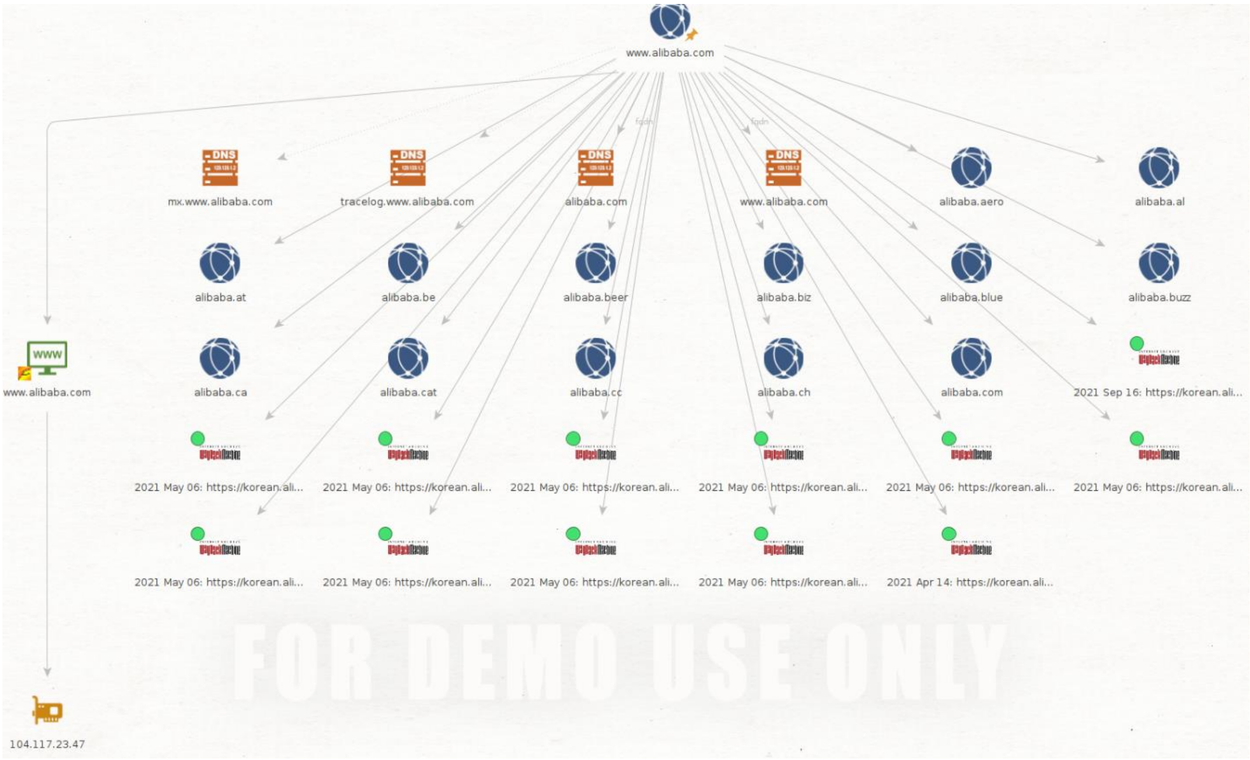
1. Nmap
2. Maltego
3. Nslookup
4. recon-ng
5. sublist3r
6. theHarvester
7. angry ip
8. (Zenmap)nmap
9. legion tool
10. netsparker
11. nikto

1. <u>Foot printing and Reconnaissance</u>

Foot printing is a type of reconnaissance that involves gathering information about a target computer system or network. Both passive and aggressive foot printing are possible. Examining a company's website is an example of passive information gathering but using social engineering to get access to classified material is an example of active information gathering.

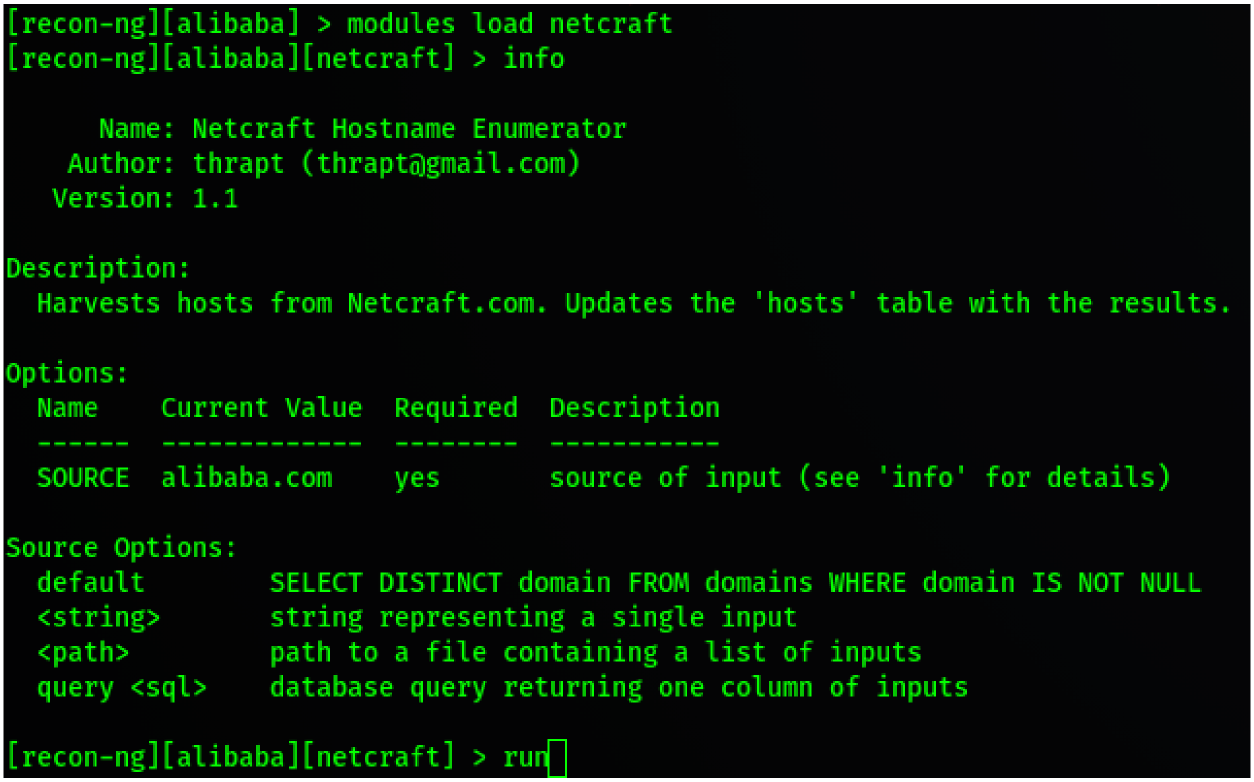
- **Maltego**

Using Maltego, we may determine the ties to which persons are related, such as their social profile, common acquaintances, companies based on the information gathered, and websites.

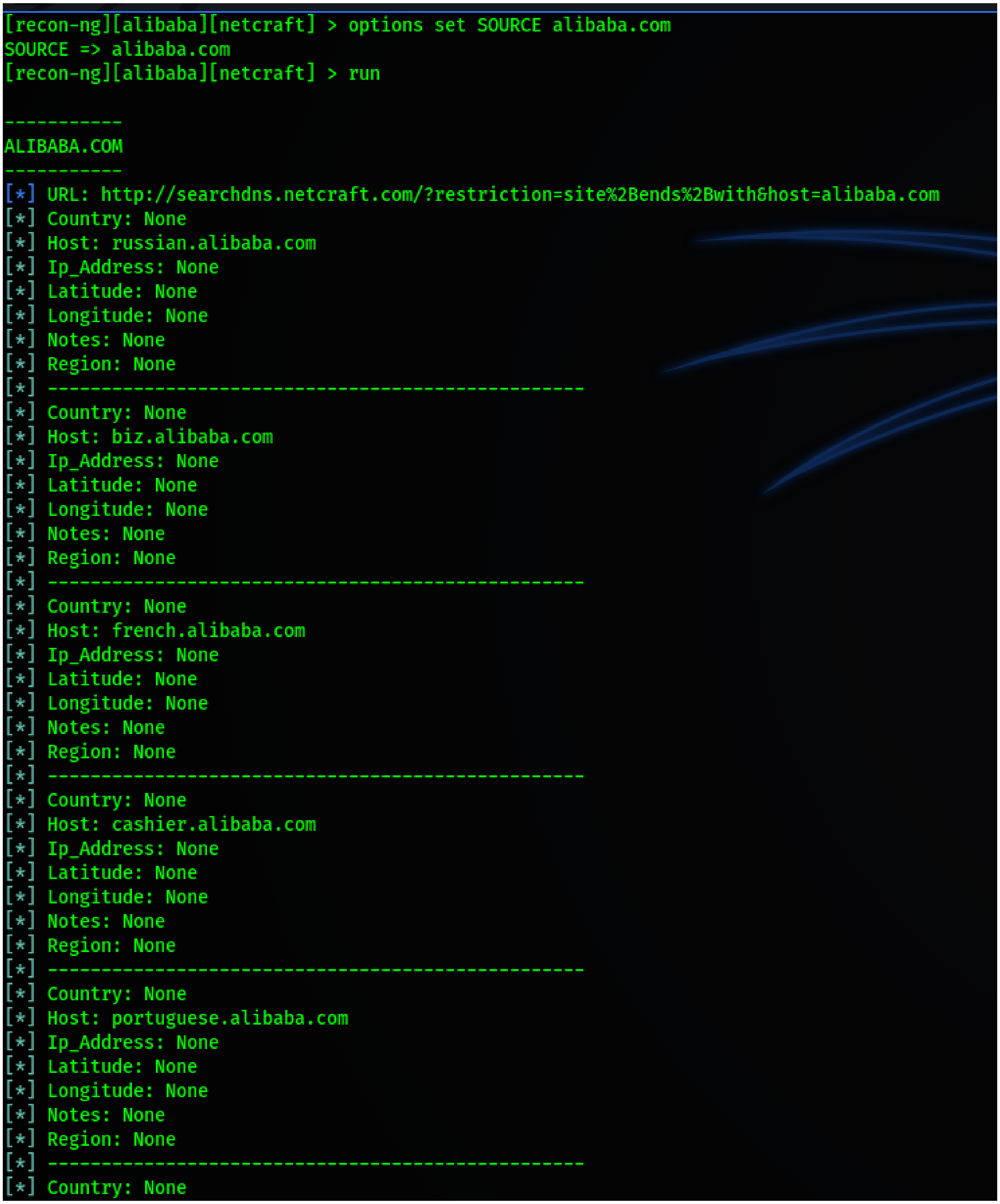

www.alibaba.com
mx.www.alibaba.com
tracelog.www.alibaba.com
alibaba.com
www.alibaba.com
alibaba.aero
alibaba.al
alibaba.at
alibaba.be
alibaba.beer
alibaba.biz
alibaba.blue
alibaba.buzz
www.alibaba.com
alibaba.ca
alibaba.cat
alibaba.cc
alibaba.ch
alibaba.com
2021 Sep 16: https://korean.ali...
2021 May 06: https://korean.ali...
2021 May 06: https://korean.ali...
2021 May 06: https://korean.ali...
2021 May 06: https://korean.ali...
2021 May 06: https://korean.ali...
2021 May 06: https://korean.ali...
2021 May 06: https://korean.ali...
2021 May 06: https://korean.ali...
2021 May 06: https://korean.ali...
2021 May 06: https://korean.ali...
2021 Apr 14: https://korean.ali...
FOR DEMO USE ONLY
104.117.23.47

- **Recon-ng**

Recon-ng is a Python Web Reconnaissance framework with a lot of features. Recon-ng provides a powerful environment for conducting open-source web-based reconnaissance quickly and completely, with distinct modules, database interface, built-in convenience functions, interactive help, and command completion.



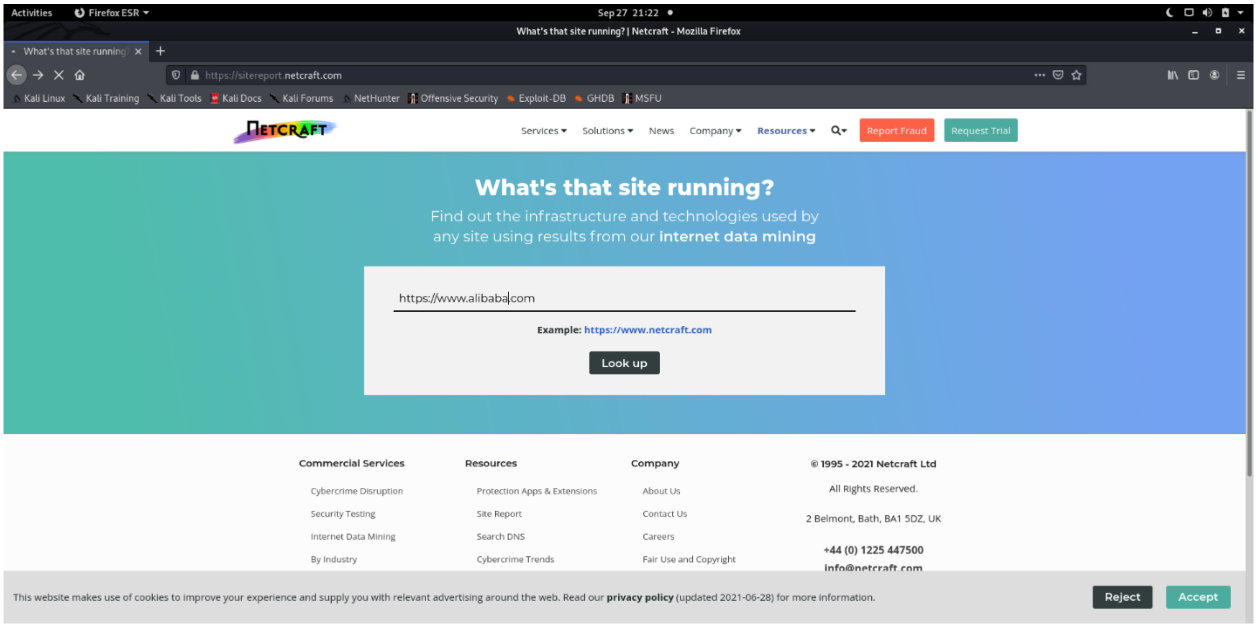
```
[recon-ng][alibaba] > modules load netcraft
[recon-ng][alibaba][netcraft] > info

      Name: Netcraft Hostname Enumerator
    Author: thrapt (thrapt@gmail.com)
   Version: 1.1

Description:
  Harvests hosts from Netcraft.com. Updates the 'hosts' table with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  alibaba.com    yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][alibaba][netcraft] > run
```



```
[recon-ng][alibaba][netcraft] > options set SOURCE alibaba.com
SOURCE => alibaba.com
[recon-ng][alibaba][netcraft] > run

-----------
ALIBABA.COM
-----------
[*] URL: http://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=alibaba.com
[*] Country: None
[*] Host: russian.alibaba.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: biz.alibaba.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: french.alibaba.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: cashier.alibaba.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
[*] Host: portuguese.alibaba.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] --------------------------------------------------
[*] Country: None
```

- ## Netcraft.com

Netcraft provides cybercrime disruption and anti-phishing services, as well as application security testing, code reviews, automated penetration testing, research data, and research on a wide range of internet issues.



What's that site running?

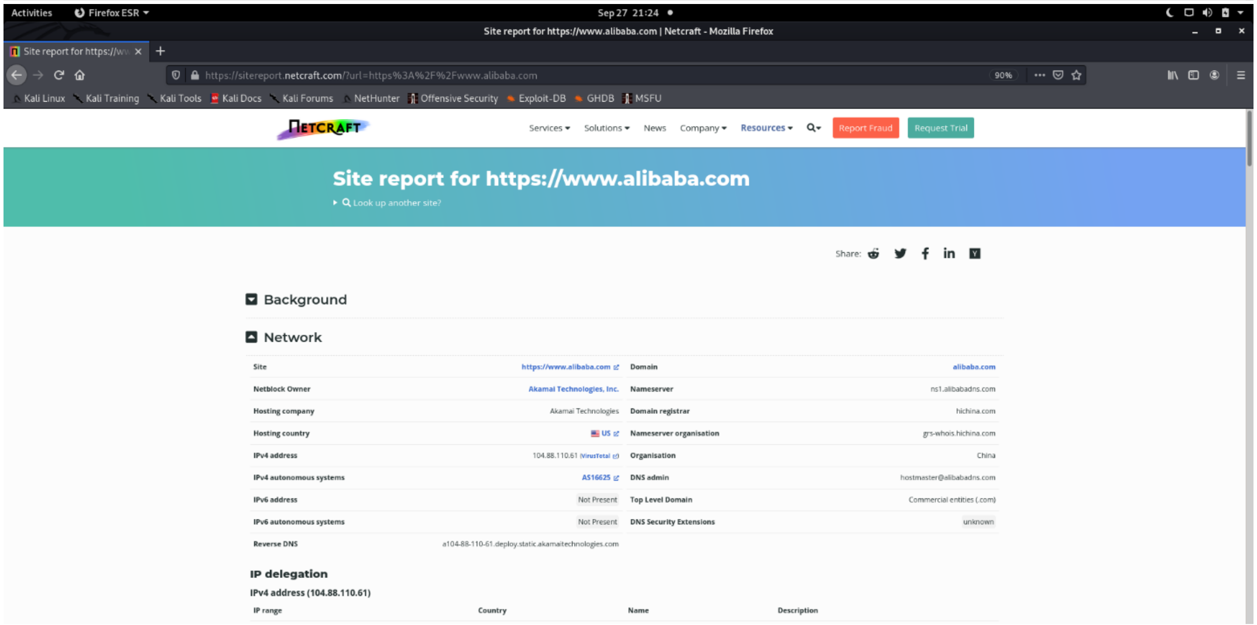
Find out the infrastructure and technologies used by any site using results from our **internet data mining**

https://www.alibaba.com

Example: https://www.netcraft.com

Commercial Services	Resources	Company	© 1995 - 2021 Netcraft Ltd
Cybercrime Disruption	Protection Apps & Extensions	About Us	All Rights Reserved.
Security Testing	Site Report	Contact Us	2 Belmont, Bath, BA1 5DZ, UK
Internet Data Mining	Search DNS	Careers	+44 (0) 1225 447500
By Industry	Cybercrime Trends	Fair Use and Copyright	info@netcraft.com

This website makes use of cookies to improve your experience and supply you with relevant advertising around the web. Read our **privacy policy** (updated 2021-06-28) for more information.



Site report for https://www.alibaba.com

Background

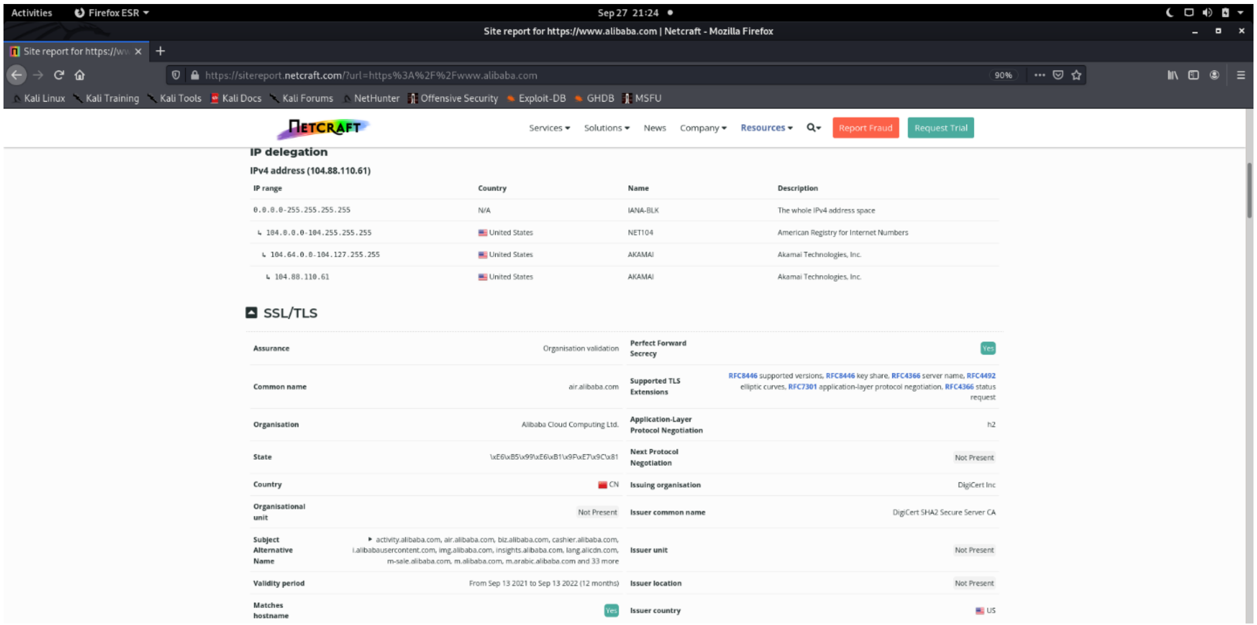
Network

Site	https://www.alibaba.com	Domain	alibaba.com
Netblock Owner	Akamai Technologies, Inc.	Nameserver	ns1.alibabadns.com
Hosting company	Akamai Technologies	Domain registrar	hichina.com
Hosting country	US	Nameserver organisation	grs-whois.hichina.com
IPv4 address	104.88.110.61 (VirusTotal)	Organisation	China
IPv4 autonomous systems	AS16625	DNS admin	hostmaster@alibabadns.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	a104-88-110-61.deploy.static.akamaitechnologies.com		

IP delegation

IPv4 address (104.88.110.61)

IP range	Country	Name	Description



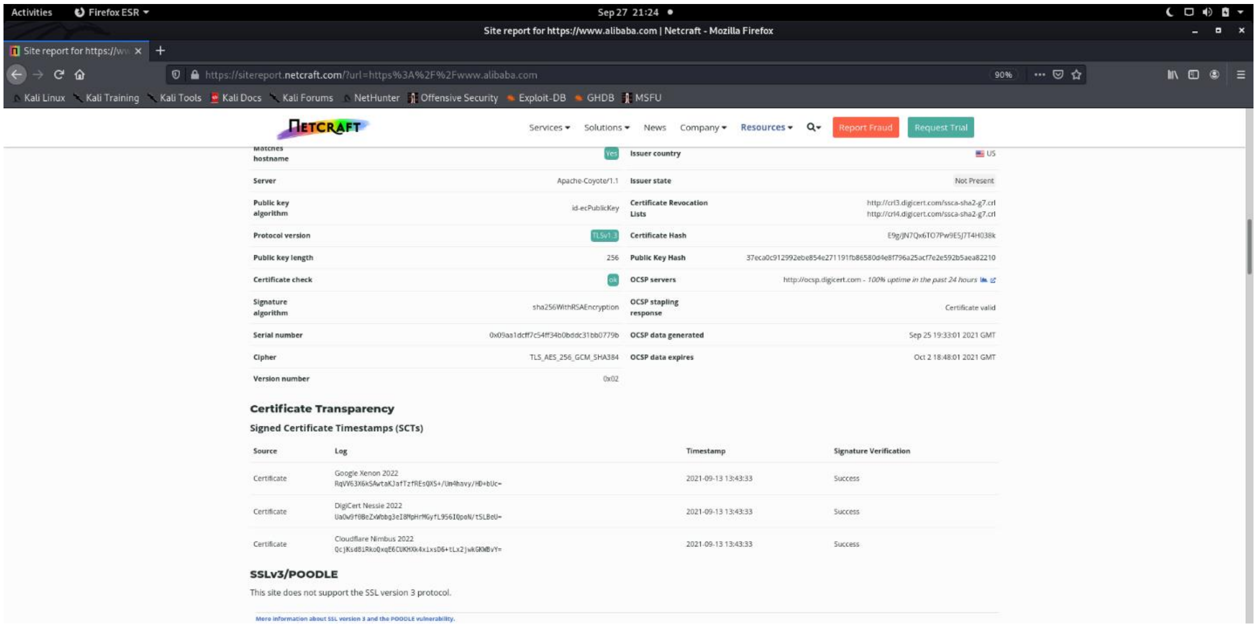
IP delegation

IPv4 address (104.88.110.61)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 104.0.0.0-104.255.255.255	United States	NET104	American Registry for Internet Numbers
↳ 104.64.0.0-104.127.255.255	United States	AKAMAI	Akamai Technologies, Inc.
↳ 104.88.110.61	United States	AKAMAI	Akamai Technologies, Inc.

SSL/TLS

Assurance	Organisation validation	**Perfect Forward Secrecy**	Yes
Common name	air.alibaba.com	**Supported TLS Extensions**	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC4492 elliptic curves, RFC7301 application-layer protocol negotiation, RFC4366 status request
Organisation	Alibaba Cloud Computing Ltd.	**Application-Layer Protocol Negotiation**	h2
State	\xE6\xB5\x99\xE6\xB1\x9F\xE7\x9C\x81	**Next Protocol Negotiation**	Not Present
Country	CN	**Issuing organisation**	DigiCert Inc
Organisational unit	Not Present	**Issuer common name**	DigiCert SHA2 Secure Server CA
Subject Alternative Name	▸ activity.alibaba.com, air.alibaba.com, biz.alibaba.com, cashier.alibaba.com, i.alibabausercontent.com, img.alibaba.com, insights.alibaba.com, lang.alicdn.com, m-sale.alibaba.com, m.alibaba.com, m.arabic.alibaba.com and 33 more	**Issuer unit**	Not Present
Validity period	From Sep 13 2021 to Sep 13 2022 (12 months)	**Issuer location**	Not Present
Matches hostname	Yes	**Issuer country**	US



Matches hostname	Yes	**Issuer country**	US
Server	Apache-Coyote/1.1	**Issuer state**	Not Present
Public key algorithm	id-ecPublicKey	**Certificate Revocation Lists**	http://crl3.digicert.com/ssca-sha2-g7.crl http://crl4.digicert.com/ssca-sha2-g7.crl
Protocol version	TLSv1.3	**Certificate Hash**	E9g/JN7Qx6TO7Pw9E5J7T4H038k
Public key length	256	**Public Key Hash**	37eca0c912992ebe854e271191fb86580d4e8f796a25acf7e2e592b5aea82210
Certificate check	ok	**OCSP servers**	http://ocsp.digicert.com - *100% uptime in the past 24 hours*
Signature algorithm	sha256WithRSAEncryption	**OCSP stapling response**	Certificate valid
Serial number	0x09aa1dcff7c54ff34b0bddc31bb0779b	**OCSP data generated**	Sep 25 19:33:01 2021 GMT
Cipher	TLS_AES_256_GCM_SHA384	**OCSP data expires**	Oct 2 18:48:01 2021 GMT
Version number	0x02		

Certificate Transparency

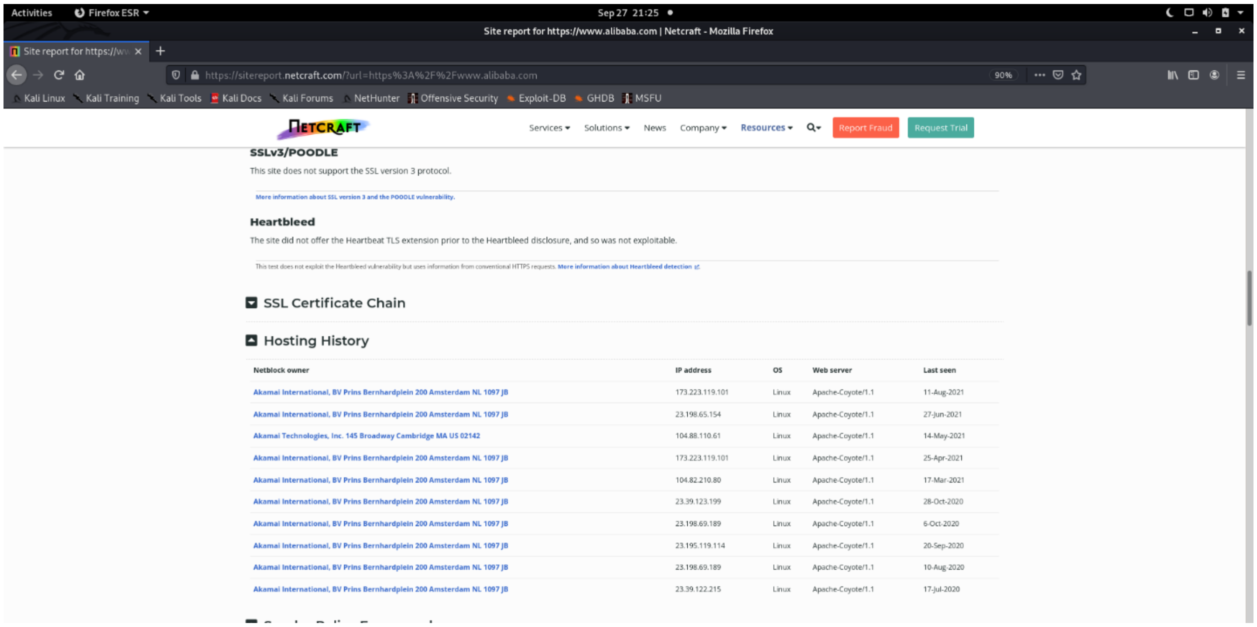
Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Xenon 2022 RqVV63X6kSAwtaKJafTzfREsQXS+/Um4havy/HD+bUc=	2021-09-13 13:43:33	Success
Certificate	DigiCert Nessie 2022 UaOw9f0BeZxWbbg3eI8MpHrMGyfL956IQpoN/tSLBeU=	2021-09-13 13:43:33	Success
Certificate	Cloudflare Nimbus 2022 QcjKsd8iRkoQxqE6CUKHXk4xixsD6+tLx2jwkGKWBvY=	2021-09-13 13:43:33	Success

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.



SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

Heartbleed

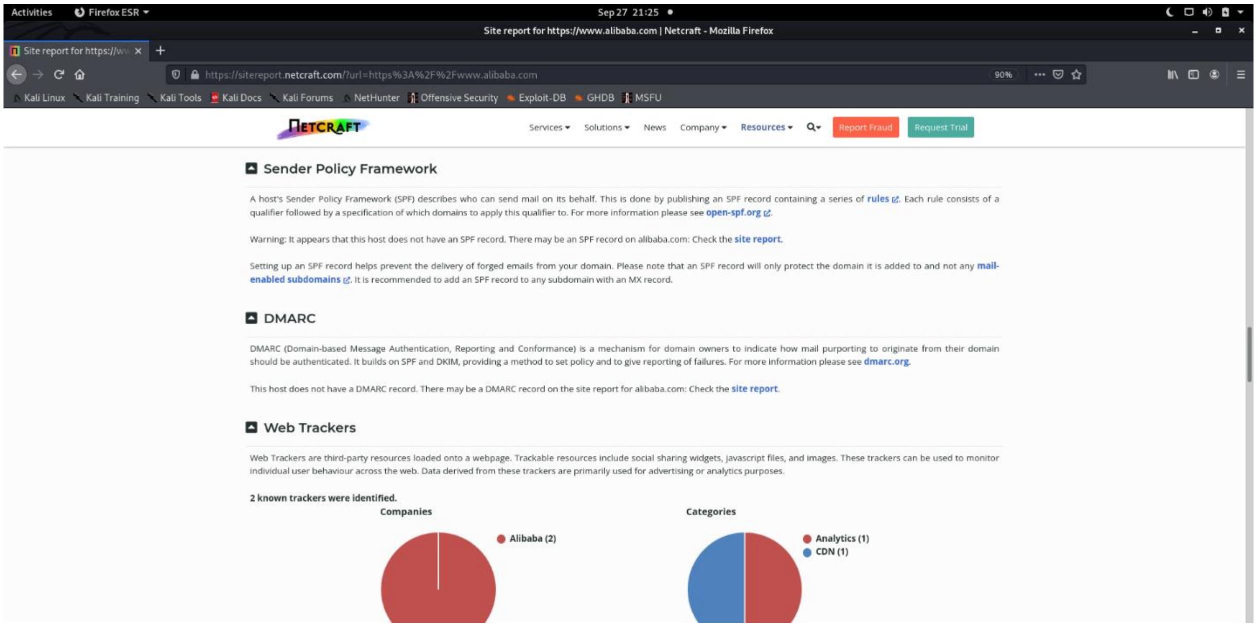
The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. More information about Heartbleed detection

SSL Certificate Chain

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	173.223.119.101	Linux	Apache-Coyote/1.1	11-Aug-2021
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.198.65.154	Linux	Apache-Coyote/1.1	27-Jun-2021
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.88.110.61	Linux	Apache-Coyote/1.1	14-May-2021
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	173.223.119.101	Linux	Apache-Coyote/1.1	25-Apr-2021
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.82.210.80	Linux	Apache-Coyote/1.1	17-Mar-2021
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.39.123.199	Linux	Apache-Coyote/1.1	28-Oct-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.198.69.189	Linux	Apache-Coyote/1.1	6-Oct-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.119.114	Linux	Apache-Coyote/1.1	20-Sep-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.198.69.189	Linux	Apache-Coyote/1.1	10-Aug-2020
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.39.122.215	Linux	Apache-Coyote/1.1	17-Jul-2020



Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see open-spf.org.

Warning: It appears that this host does not have an SPF record. There may be an SPF record on alibaba.com: Check the site report.

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any mail-enabled subdomains. It is recommended to add an SPF record to any subdomain with an MX record.

DMARC

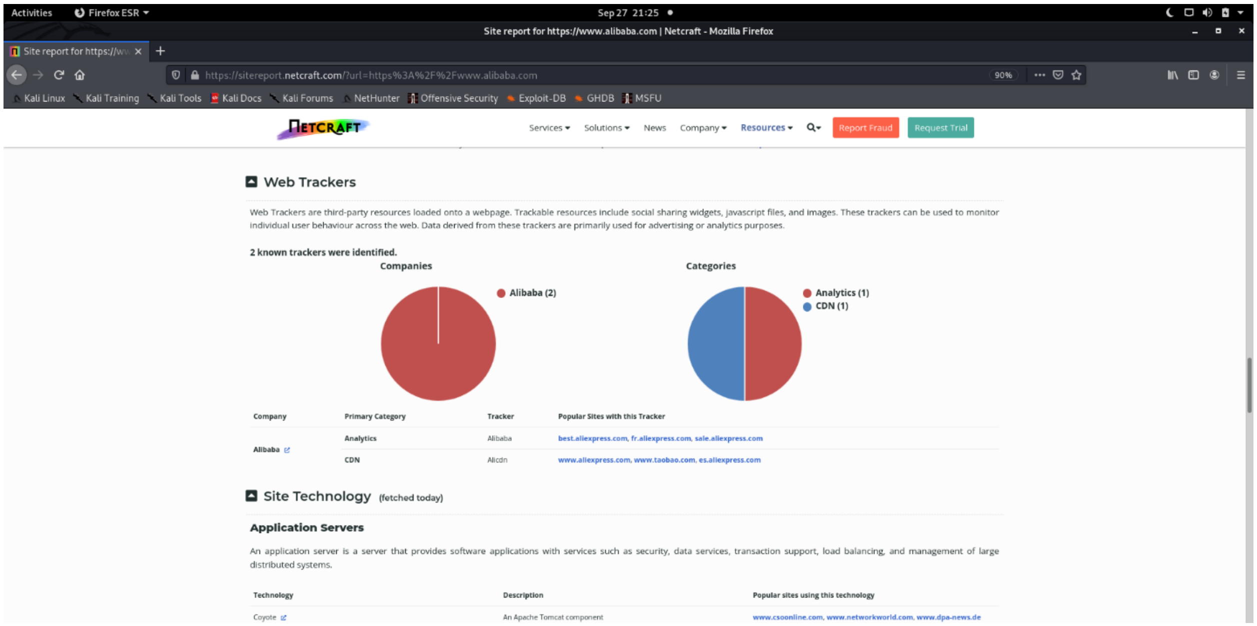
DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.

This host does not have a DMARC record. There may be a DMARC record on the site report for alibaba.com: Check the site report.

Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

2 known trackers were identified.



Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

2 known trackers were identified.

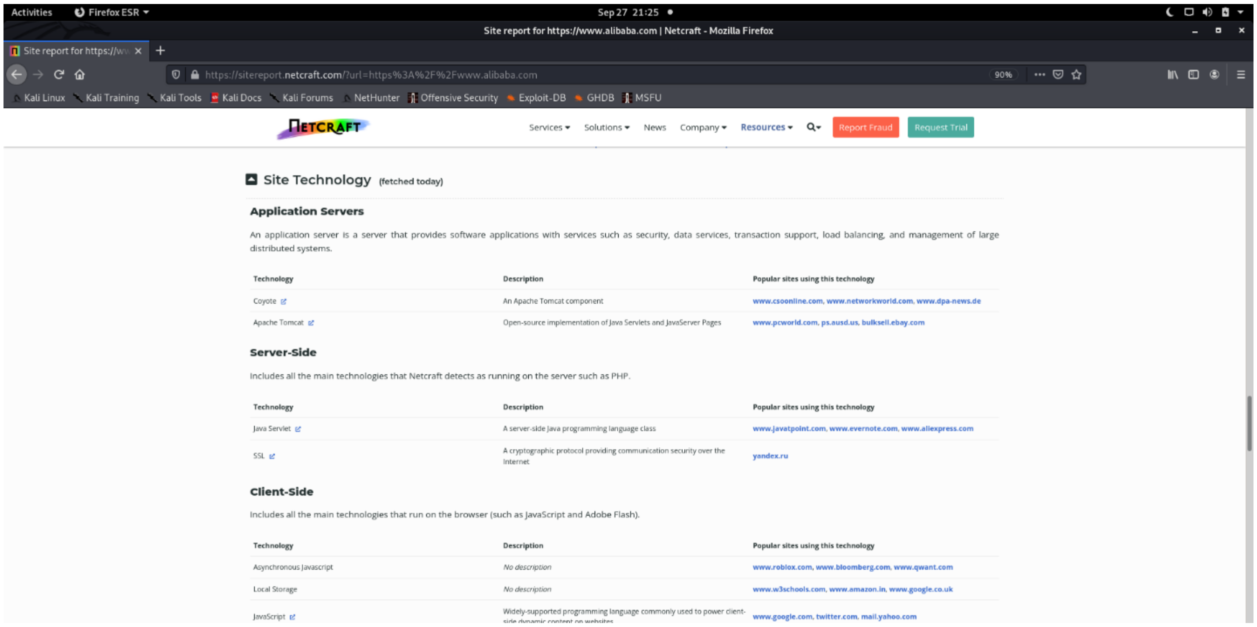
Company	Primary Category	Tracker	Popular Sites with this Tracker
Alibaba	Analytics	Alibaba	best.aliexpress.com, fr.aliexpress.com, sale.aliexpress.com
	CDN	Alicdn	www.aliexpress.com, www.taobao.com, es.aliexpress.com

Site Technology (fetched today)

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
Coyote	An Apache Tomcat component	www.csoonline.com, www.networkworld.com, www.dpa-news.de



Site Technology (fetched today)

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
Coyote	An Apache Tomcat component	www.csoonline.com, www.networkworld.com, www.dpa-news.de
Apache Tomcat	Open-source implementation of Java Servlets and JavaServer Pages	www.pcworld.com, ps.ausd.us, bulksell.ebay.com

Server-Side

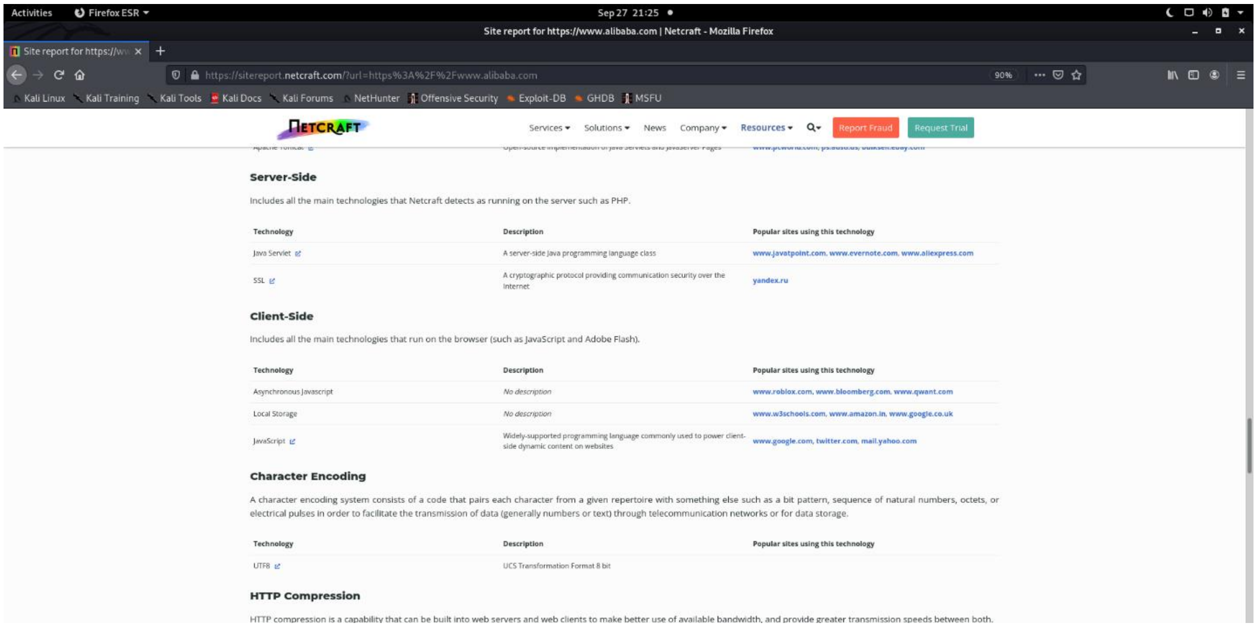
Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
Java Servlet	A server-side Java programming language class	www.javatpoint.com, www.evernote.com, www.aliexpress.com
SSL	A cryptographic protocol providing communication security over the Internet	yandex.ru

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Asynchronous Javascript	*No description*	www.roblox.com, www.bloomberg.com, www.qwant.com
Local Storage	*No description*	www.w3schools.com, www.amazon.in, www.google.co.uk
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.google.com, twitter.com, mail.yahoo.com



Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
Java Servlet	A server-side Java programming language class	www.javatpoint.com, www.evernote.com, www.aliexpress.com
SSL	A cryptographic protocol providing communication security over the Internet	yandex.ru

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Asynchronous Javascript	*No description*	www.roblox.com, www.bloomberg.com, www.qwant.com
Local Storage	*No description*	www.w3schools.com, www.amazon.in, www.google.co.uk
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.google.com, twitter.com, mail.yahoo.com

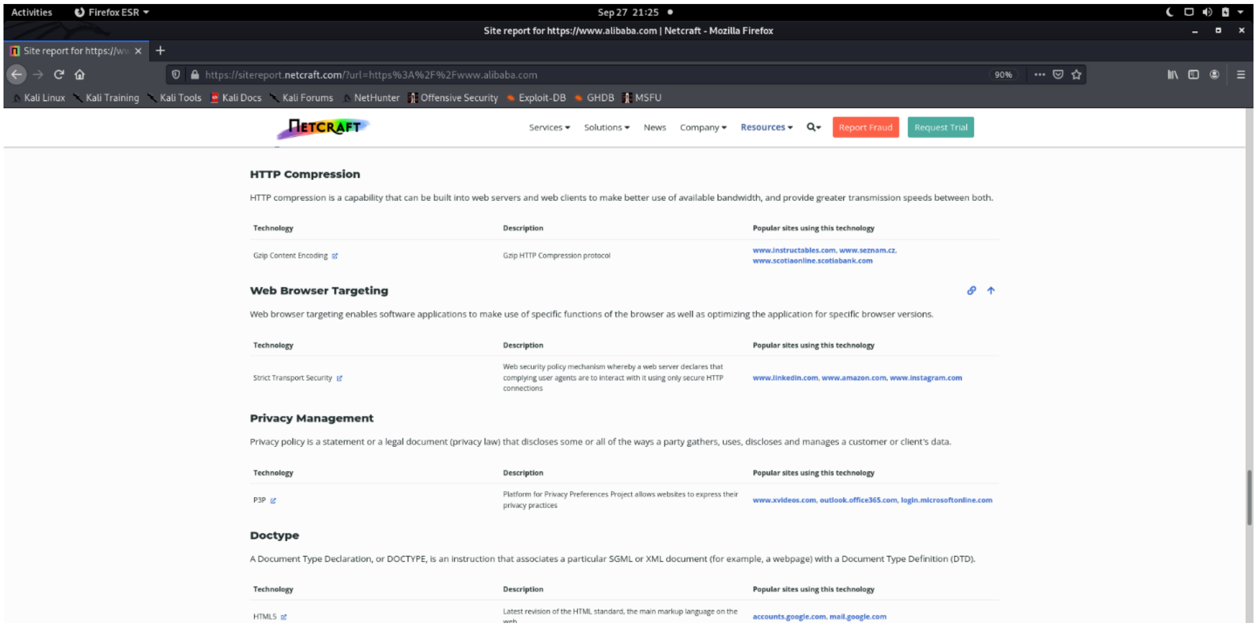
Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTF8	UCS Transformation Format 8 bit	

HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.



HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.instructables.com, www.seznam.cz, www.scotiaonline.scotiabank.com

Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	www.linkedin.com, www.amazon.com, www.instagram.com

Privacy Management

Privacy policy is a statement or a legal document (privacy law) that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's data.

Technology	Description	Popular sites using this technology
P3P	Platform for Privacy Preferences Project allows websites to express their privacy practices	www.xvideos.com, outlook.office365.com, login.microsoftonline.com

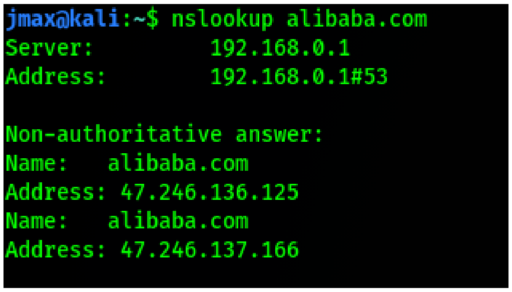
Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	accounts.google.com, mail.google.com

- ## Nslookup

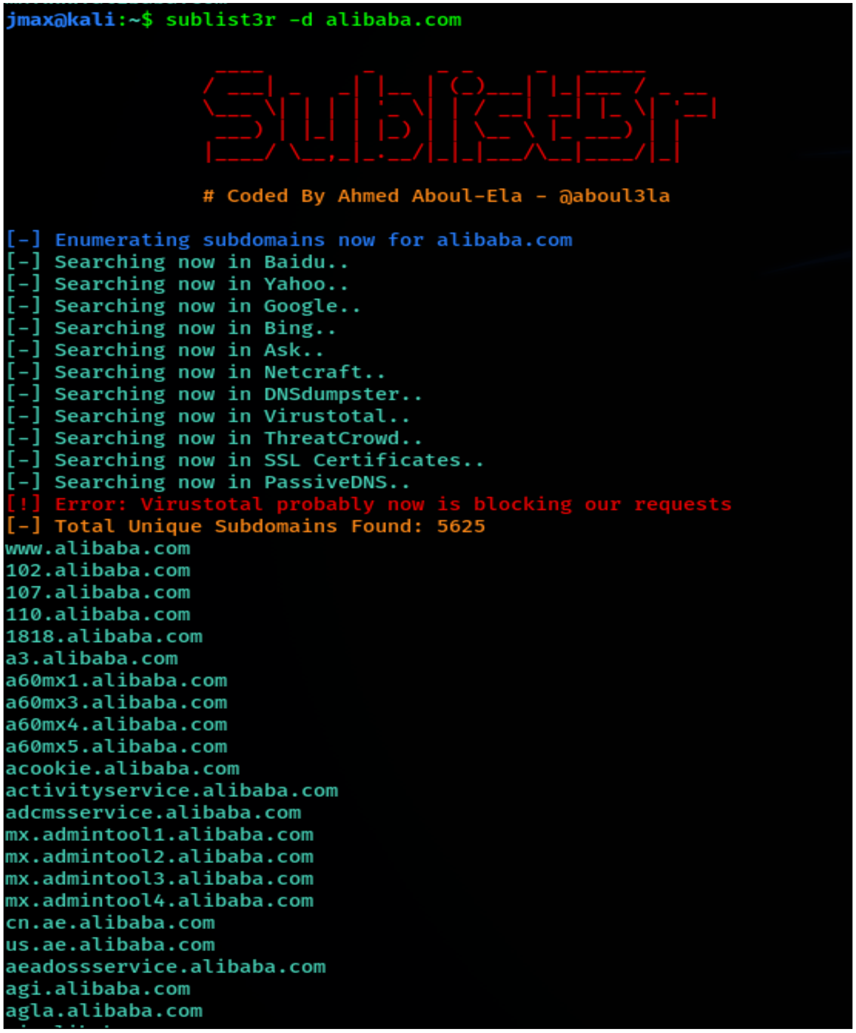
nslookup is a network administration command-line tool that looks up the mapping between a domain name and an IP address, as well as other DNS records, in the Domain Name System.



```
jmax@kali:~$ nslookup alibaba.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   alibaba.com
Address: 47.246.136.125
Name:   alibaba.com
Address: 47.246.137.166
```

- ## Sublist3r

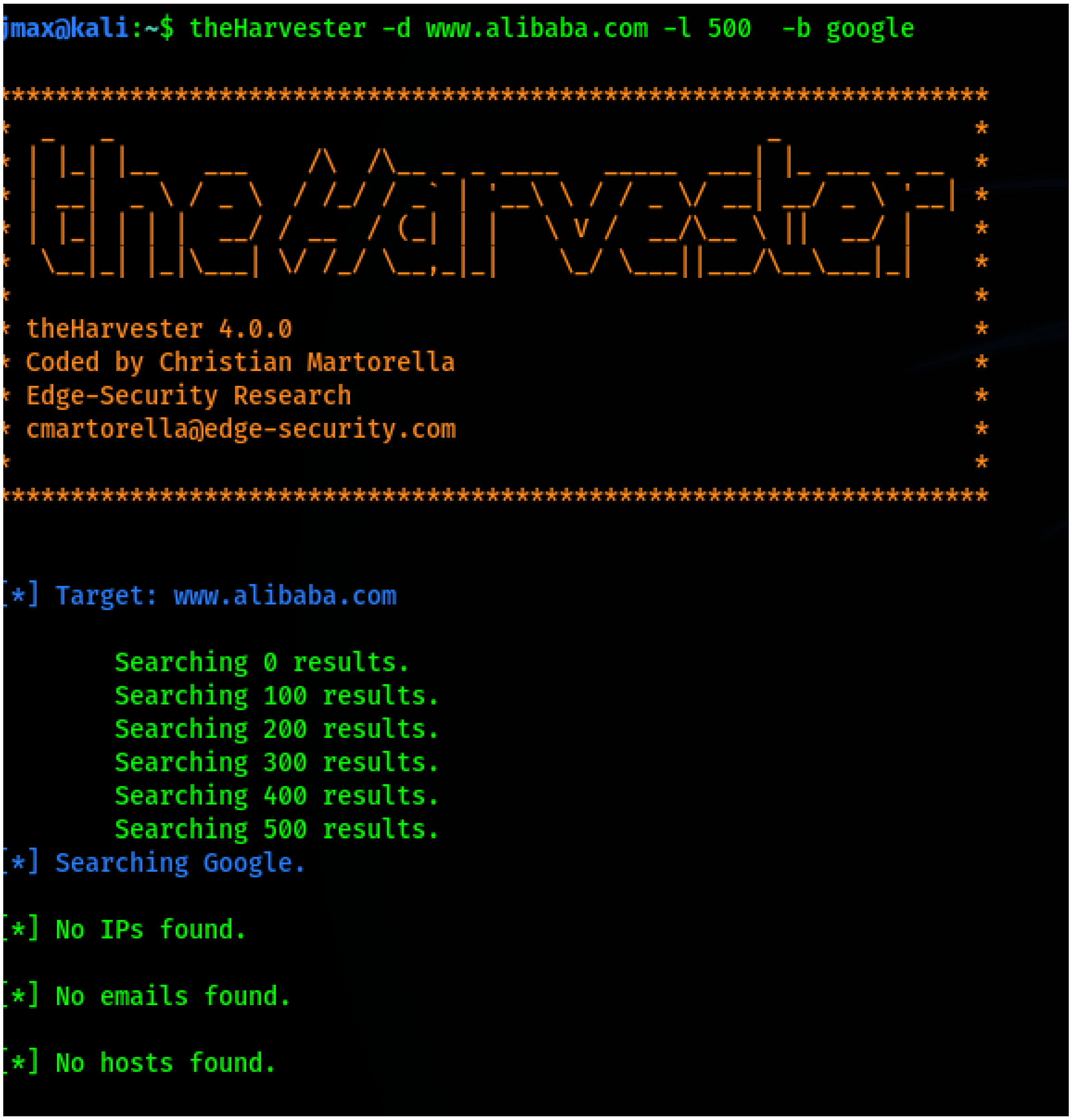
Sublist3r is a Python application that enumerates website subdomains using OSINT. It helps penetration testers and bug hunters collect and aggregate subdomains for the specified site. Sublist3r uses a number of search engines to count subdomains.



```
jmax@kali:~$ sublist3r -d alibaba.com

                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for alibaba.com
[-] 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..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 5625
www.alibaba.com
102.alibaba.com
107.alibaba.com
110.alibaba.com
1818.alibaba.com
a3.alibaba.com
a60mx1.alibaba.com
a60mx3.alibaba.com
a60mx4.alibaba.com
a60mx5.alibaba.com
acookie.alibaba.com
activityservice.alibaba.com
adcmsservice.alibaba.com
mx.admintool1.alibaba.com
mx.admintool2.alibaba.com
mx.admintool3.alibaba.com
mx.admintool4.alibaba.com
cn.ae.alibaba.com
us.ae.alibaba.com
aeadossservice.alibaba.com
agi.alibaba.com
agla.alibaba.com
```

- **theHarvester**

The goal of the programmes is to collect email, host names, employee names, subdomains, open ports, and banners from public resources such as search engines, PGP key servers, and computer databases such as Shodan.



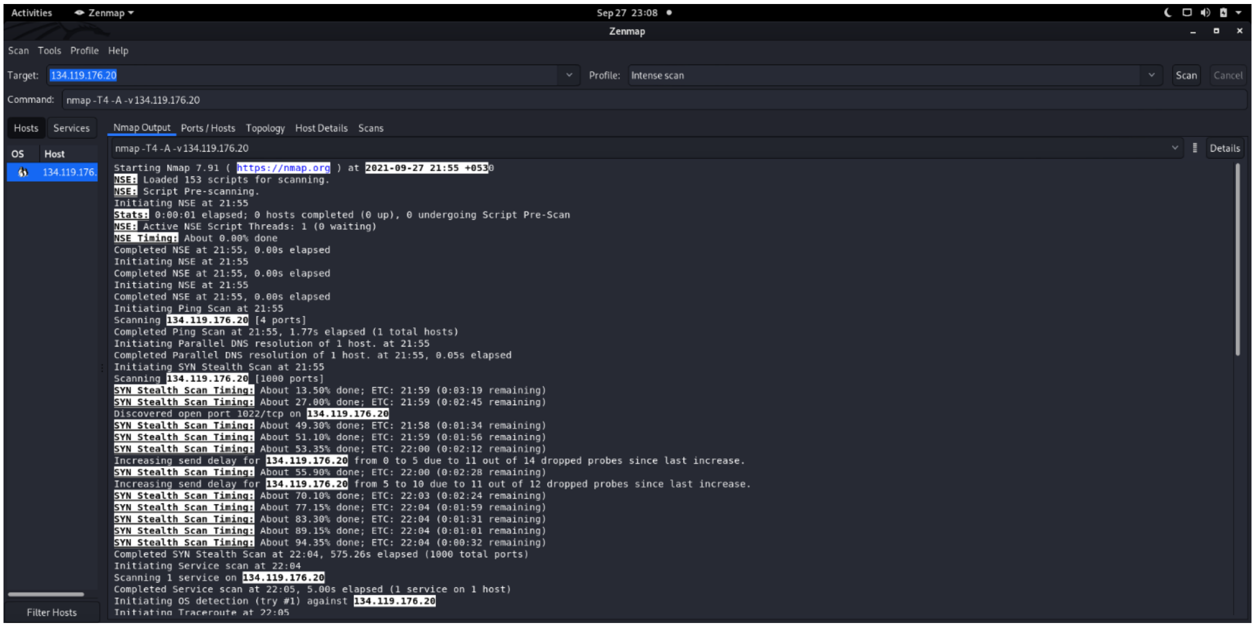
```
jmax@kali:~$ theHarvester -d www.alibaba.com -l 500  -b google

*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.0.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: www.alibaba.com

        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
        Searching 300 results.
        Searching 400 results.
        Searching 500 results.
[*] Searching Google.

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

2. Scanning

- ### Zenmap

  Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner. It is a multi-platform, free and open-source application designed to make Nmap easy for beginners to use while providing advanced features for experienced Nmap user.

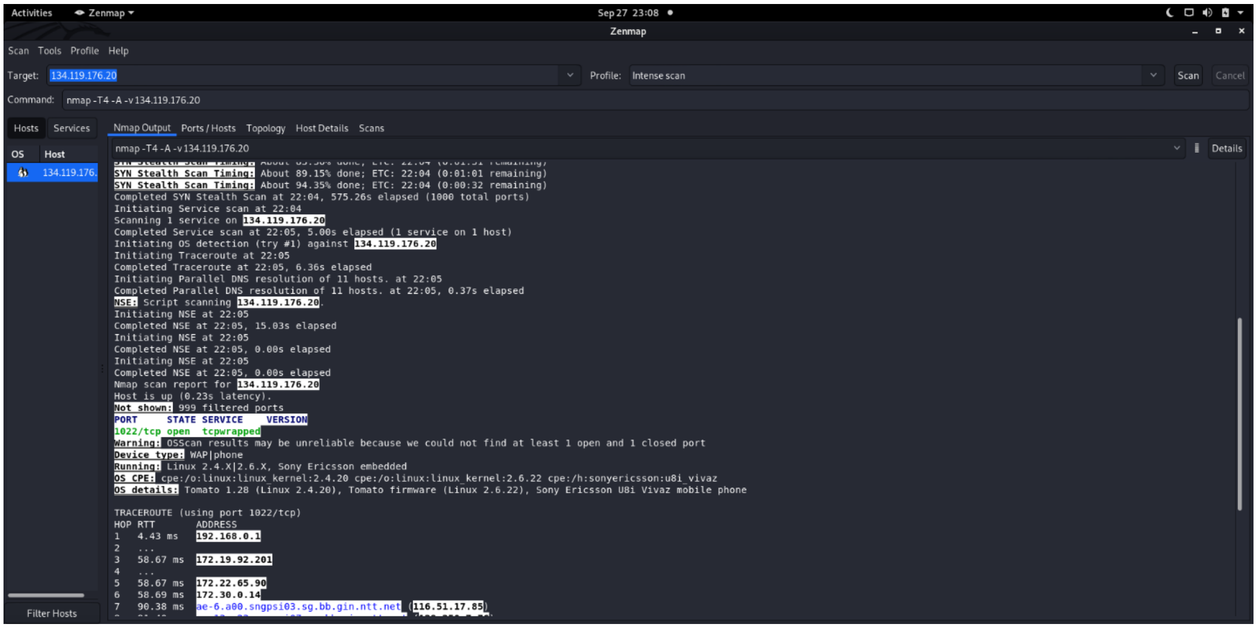
  Below results captured after scanning the domain IP.



Target: 134.119.176.20 Profile: Intense scan

Command: nmap -T4 -A -v 134.119.176.20

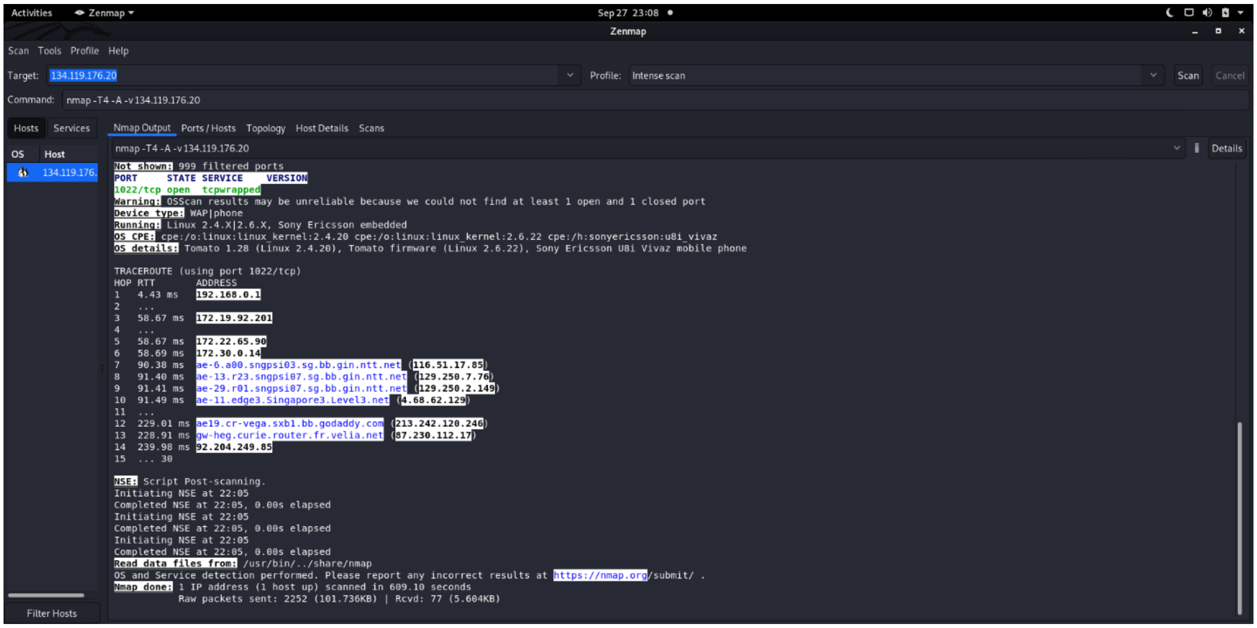
```
nmap -T4 -A -v 134.119.176.20
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 21:55 +0530
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 21:55
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE: Active NSE Script Threads: 1 (0 waiting)
NSE Timing: About 0.00% done
Completed NSE at 21:55, 0.00s elapsed
Initiating NSE at 21:55
Completed NSE at 21:55, 0.00s elapsed
Initiating NSE at 21:55
Completed NSE at 21:55, 0.00s elapsed
Initiating Ping Scan at 21:55
Scanning 134.119.176.20 [4 ports]
Completed Ping Scan at 21:55, 1.77s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:55
Completed Parallel DNS resolution of 1 host. at 21:55, 0.05s elapsed
Initiating SYN Stealth Scan at 21:55
Scanning 134.119.176.20 [1000 ports]
SYN Stealth Scan Timing: About 13.50% done; ETC: 21:59 (0:03:19 remaining)
SYN Stealth Scan Timing: About 27.00% done; ETC: 21:59 (0:02:45 remaining)
Discovered open port 1022/tcp on 134.119.176.20
SYN Stealth Scan Timing: About 49.30% done; ETC: 21:58 (0:01:34 remaining)
SYN Stealth Scan Timing: About 51.10% done; ETC: 21:59 (0:01:56 remaining)
SYN Stealth Scan Timing: About 53.35% done; ETC: 22:00 (0:02:12 remaining)
Increasing send delay for 134.119.176.20 from 0 to 5 due to 11 out of 14 dropped probes since last increase.
SYN Stealth Scan Timing: About 55.90% done; ETC: 22:00 (0:02:28 remaining)
Increasing send delay for 134.119.176.20 from 5 to 10 due to 11 out of 12 dropped probes since last increase.
SYN Stealth Scan Timing: About 70.10% done; ETC: 22:03 (0:02:24 remaining)
SYN Stealth Scan Timing: About 77.15% done; ETC: 22:04 (0:01:59 remaining)
SYN Stealth Scan Timing: About 83.30% done; ETC: 22:04 (0:01:31 remaining)
SYN Stealth Scan Timing: About 89.15% done; ETC: 22:04 (0:01:01 remaining)
SYN Stealth Scan Timing: About 94.35% done; ETC: 22:04 (0:00:32 remaining)
Completed SYN Stealth Scan at 22:04, 575.26s elapsed (1000 total ports)
Initiating Service scan at 22:04
Scanning 1 service on 134.119.176.20
Completed Service scan at 22:05, 5.00s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 134.119.176.20
Initiating Traceroute at 22:05
```



Target: 134.119.176.20 Profile: Intense scan

Command: nmap -T4 -A -v 134.119.176.20

```
nmap -T4 -A -v 134.119.176.20
SYN Stealth Scan Timing: About 89.15% done; ETC: 22:04 (0:01:01 remaining)
SYN Stealth Scan Timing: About 94.35% done; ETC: 22:04 (0:00:32 remaining)
Completed SYN Stealth Scan at 22:04, 575.26s elapsed (1000 total ports)
Initiating Service scan at 22:04
Scanning 1 service on 134.119.176.20
Completed Service scan at 22:05, 5.00s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 134.119.176.20
Initiating Traceroute at 22:05
Completed Traceroute at 22:05, 6.36s elapsed
Initiating Parallel DNS resolution of 11 hosts. at 22:05
Completed Parallel DNS resolution of 11 hosts. at 22:05, 0.37s elapsed
NSE: Script scanning 134.119.176.20.
Initiating NSE at 22:05
Completed NSE at 22:05, 15.03s elapsed
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Nmap scan report for 134.119.176.20
Host is up (0.23s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE    VERSION
1022/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

TRACEROUTE (using port 1022/tcp)
HOP RTT      ADDRESS
1   4.43 ms  192.168.0.1
2   ...
3   58.67 ms 172.19.92.201
4   ...
5   58.67 ms 172.22.65.90
6   58.69 ms 172.30.0.14
7   90.38 ms ae-6.a00.sngpsi03.sg.bb.gin.ntt.net (116.51.17.85)
```

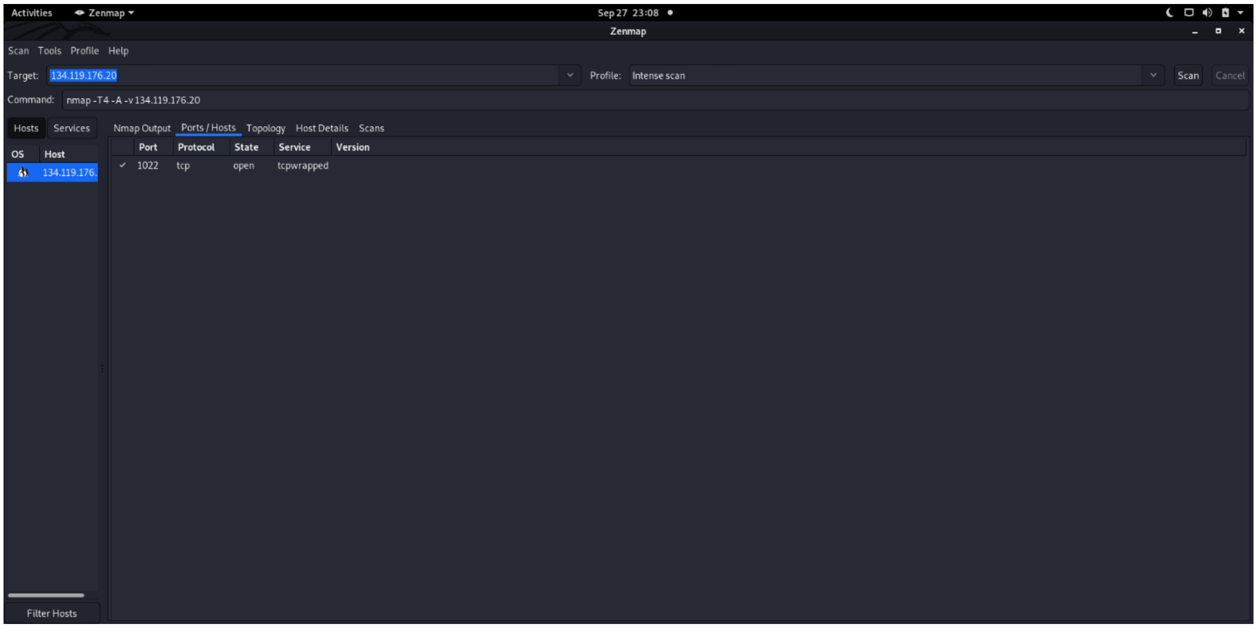


Target: 134.119.176.20

Profile: Intense scan

Command: nmap -T4 -A -v 134.119.176.20

```
nmap -T4 -A -v 134.119.176.20
Not shown: 999 filtered ports
PORT     STATE SERVICE    VERSION
1022/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP|phone
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

TRACEROUTE (using port 1022/tcp)
HOP RTT       ADDRESS
1   4.43 ms   192.168.0.1
2   ...
3   58.67 ms  172.19.92.201
4   ...
5   58.67 ms  172.22.65.90
6   58.69 ms  172.30.0.14
7   90.38 ms  ae-6.a00.sngpsi03.sg.bb.gin.ntt.net (116.51.17.85)
8   91.40 ms  ae-13.r23.sngpsi07.sg.bb.gin.ntt.net (129.250.7.76)
9   91.41 ms  ae-29.r01.sngpsi07.sg.bb.gin.ntt.net (129.250.2.149)
10  91.49 ms  ae-11.edge3.Singapore3.Level3.net (4.68.62.129)
11  ...
12  229.01 ms ae19.cr-vega.sxb1.bb.godaddy.com (213.242.120.246)
13  228.91 ms gw-heg.curie.router.fr.velia.net (87.230.112.17)
14  239.98 ms 92.204.249.85
15  ... 30

NSE: Script Post-scanning.
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Initiating NSE at 22:05
Completed NSE at 22:05, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 609.10 seconds
           Raw packets sent: 2252 (101.736KB) | Rcvd: 77 (5.604KB)
```

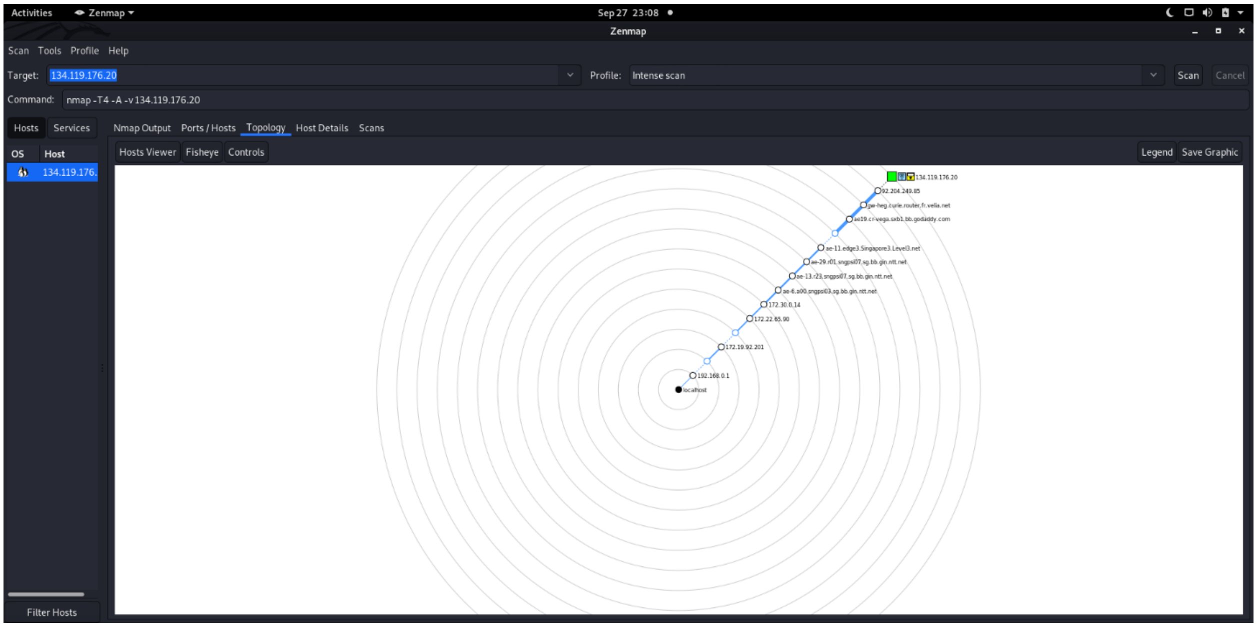


Target: 134.119.176.20

Profile: Intense scan

Command: nmap -T4 -A -v 134.119.176.20

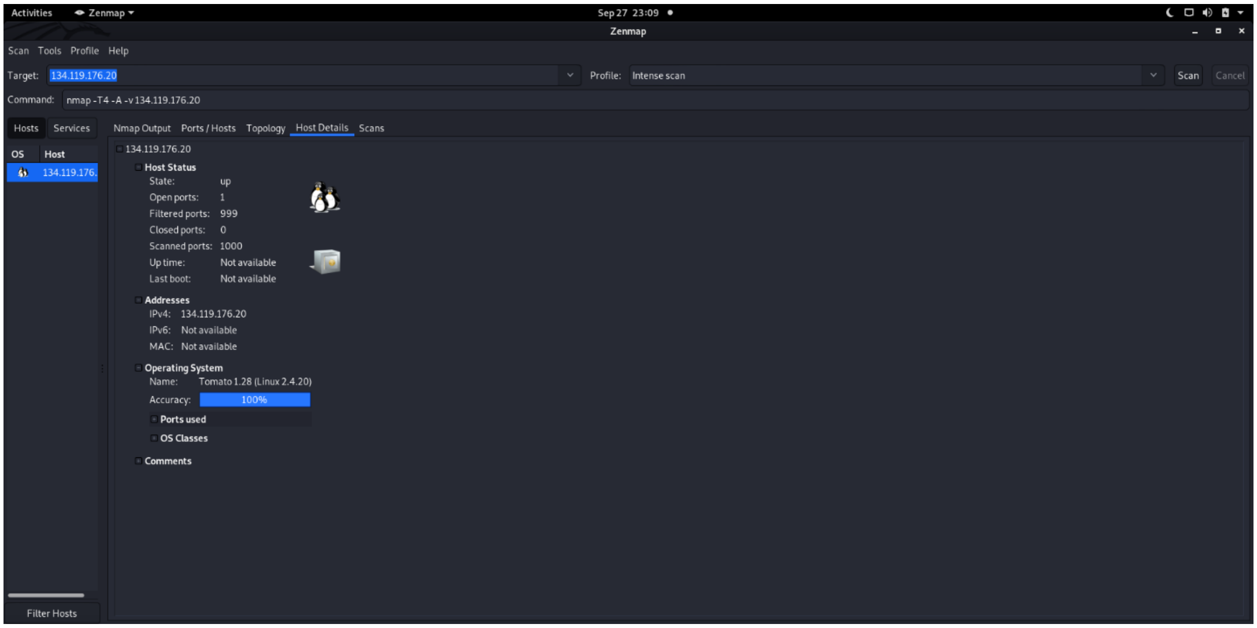
	Port	Protocol	State	Service	Version
✓	1022	tcp	open	tcpwrapped	



Target: 134.119.176.20

Profile: Intense scan

Command: nmap -T4 -A -v 134.119.176.20



Target: 134.119.176.20

Profile: Intense scan

Command: nmap -T4 -A -v 134.119.176.20

134.119.176.20

Host Status

State: up

Open ports: 1

Filtered ports: 999

Closed ports: 0

Scanned ports: 1000

Up time: Not available

Last boot: Not available

Addresses

IPv4: 134.119.176.20

IPv6: Not available

MAC: Not available

Operating System

Name: Tomato 1.28 (Linux 2.4.20)

Accuracy: 100%

Ports used

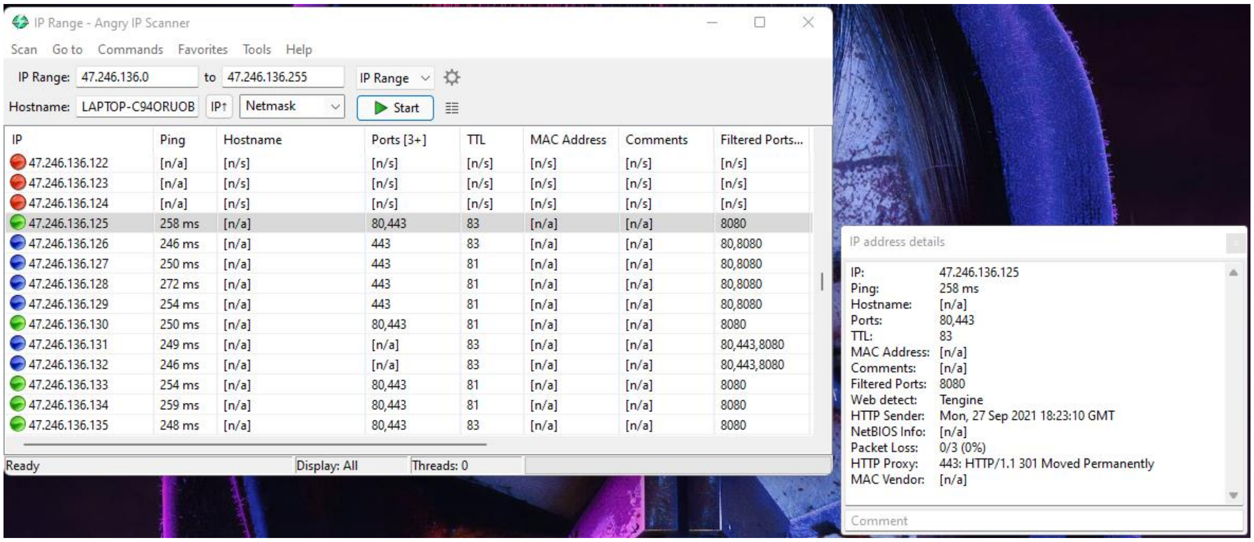
OS Classes

Comments

- **Angry ip**

Angry IP Scanner is a cross-platform, open-source network scanner that is quick and easy to use. It checks IP addresses and ports and has a slew of additional capabilities. It is extensively used by network administrators and ordinary users all over the world, including major and small businesses, banks, and government organizations. It operates on Linux, Windows, and Mac OS X, and it may support additional platforms in the future.

Below results captured after scanning the domain IP.



IP Range: 47.246.136.0 to 47.246.136.255 IP Range

Hostname: LAPTOP-C94ORUOB IP↑ Netmask

IP	Ping	Hostname	Ports [3+]	TTL	MAC Address	Comments	Filtered Ports...
🔴 47.246.136.122	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 47.246.136.123	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🔴 47.246.136.124	[n/a]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]	[n/s]
🟢 47.246.136.125	258 ms	[n/a]	80,443	83	[n/a]	[n/a]	8080
🔵 47.246.136.126	246 ms	[n/a]	443	83	[n/a]	[n/a]	80,8080
🔵 47.246.136.127	250 ms	[n/a]	443	81	[n/a]	[n/a]	80,8080
🔵 47.246.136.128	272 ms	[n/a]	443	81	[n/a]	[n/a]	80,8080
🔵 47.246.136.129	254 ms	[n/a]	443	81	[n/a]	[n/a]	80,8080
🟢 47.246.136.130	250 ms	[n/a]	80,443	81	[n/a]	[n/a]	8080
🔵 47.246.136.131	249 ms	[n/a]	[n/a]	83	[n/a]	[n/a]	80,443,8080
🔵 47.246.136.132	246 ms	[n/a]	[n/a]	83	[n/a]	[n/a]	80,443,8080
🟢 47.246.136.133	254 ms	[n/a]	80,443	81	[n/a]	[n/a]	8080
🟢 47.246.136.134	259 ms	[n/a]	80,443	81	[n/a]	[n/a]	8080
🟢 47.246.136.135	248 ms	[n/a]	80,443	83	[n/a]	[n/a]	8080

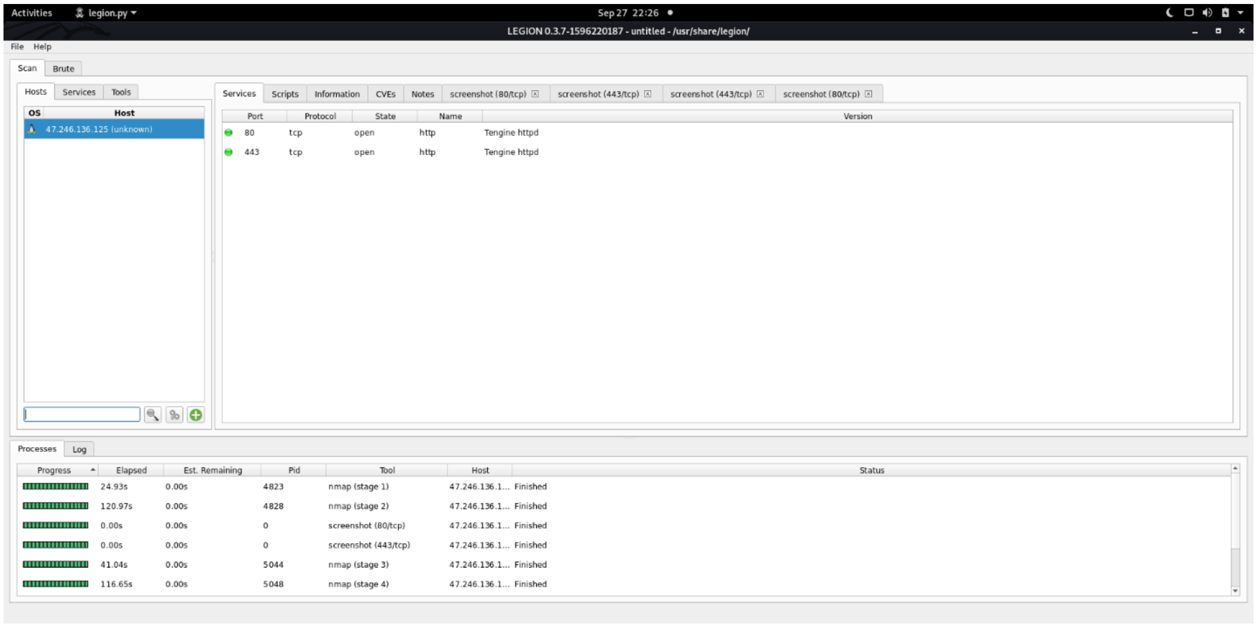
Ready | Display: All | Threads: 0

IP:	47.246.136.125
Ping:	258 ms
Hostname:	[n/a]
Ports:	80,443
TTL:	83
MAC Address:	[n/a]
Comments:	[n/a]
Filtered Ports:	8080
Web detect:	Tengine
HTTP Sender:	Mon, 27 Sep 2021 18:23:10 GMT
NetBIOS Info:	[n/a]
Packet Loss:	0/3 (0%)
HTTP Proxy:	443: HTTP/1.1 301 Moved Permanently
MAC Vendor:	[n/a]

3. Enumeration

- ### Legion Tool

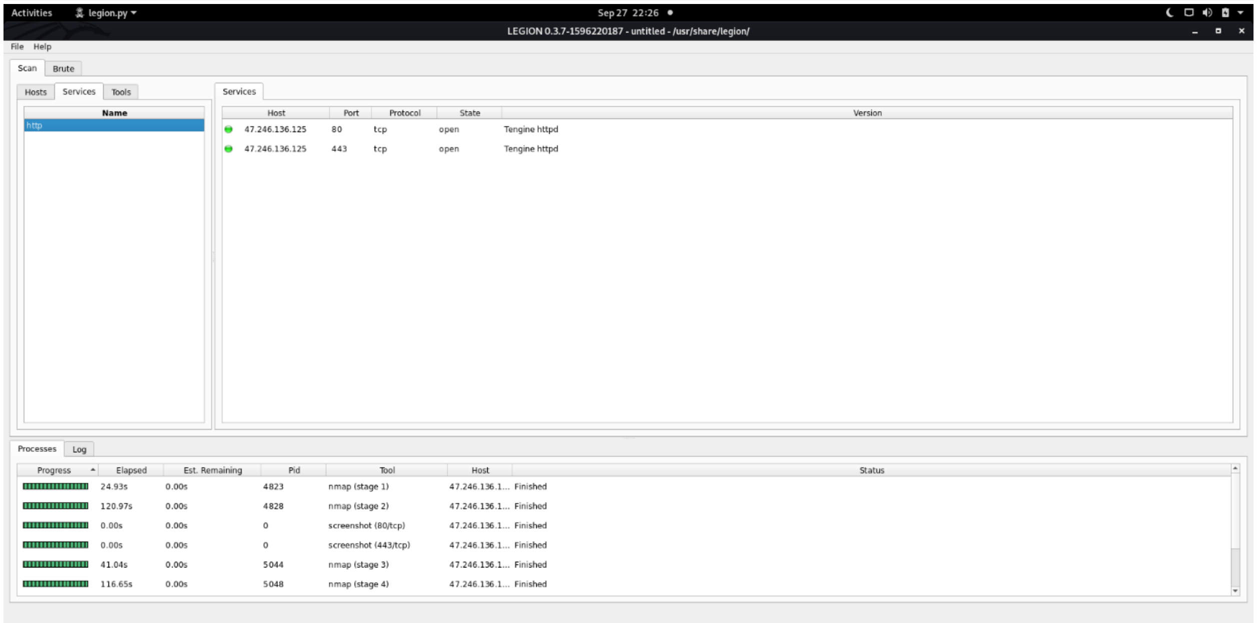
  Legion is a penetration testing platform with a moderate level of difficulty. Legion is a really simple game to play. Legion Tool is a graphical user interface (GUI) with panels and a variety of options that enable pentesters to quickly identify and exploit attack pathways on hosts. Below results captured after scanning the domain IP.



OS	Host
🐧	47.246.136.125 (unknown)

	Port	Protocol	State	Name	Version
●	80	tcp	open	http	Tengine httpd
●	443	tcp	open	http	Tengine httpd

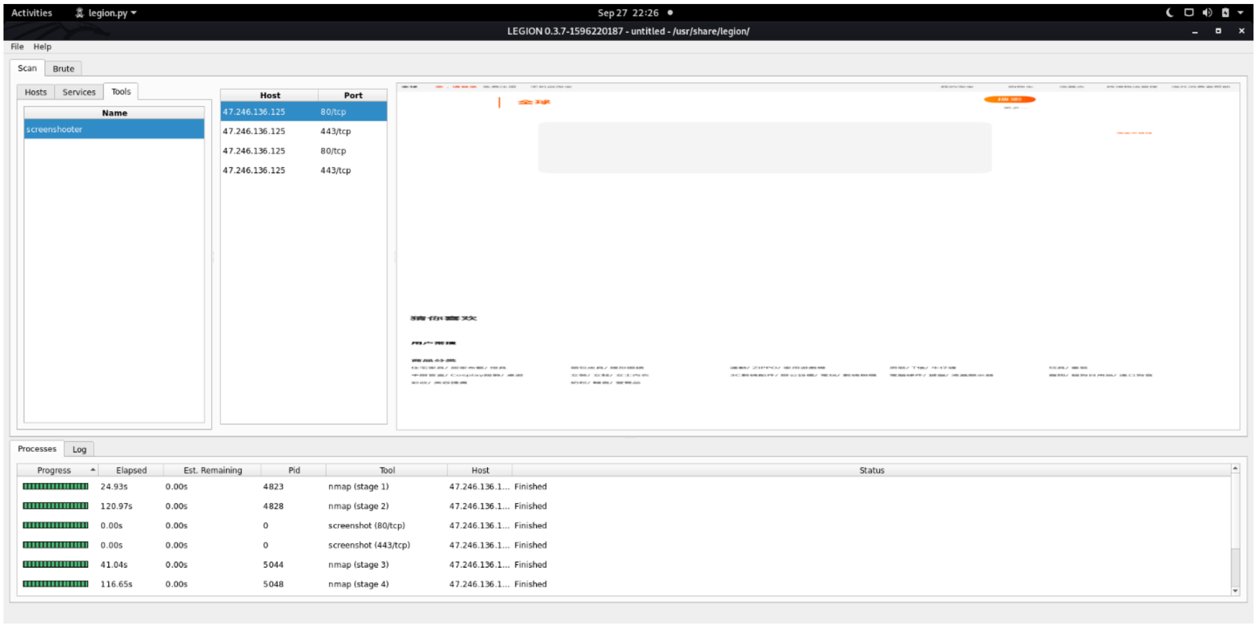
Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	24.93s	0.00s	4823	nmap (stage 1)	47.246.136.1...	Finished
	120.97s	0.00s	4828	nmap (stage 2)	47.246.136.1...	Finished
	0.00s	0.00s	0	screenshot (80/tcp)	47.246.136.1...	Finished
	0.00s	0.00s	0	screenshot (443/tcp)	47.246.136.1...	Finished
	41.04s	0.00s	5044	nmap (stage 3)	47.246.136.1...	Finished
	116.65s	0.00s	5048	nmap (stage 4)	47.246.136.1...	Finished



Name
http

	Host	Port	Protocol	State	Version
●	47.246.136.125	80	tcp	open	Tengine httpd
●	47.246.136.125	443	tcp	open	Tengine httpd

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	24.93s	0.00s	4823	nmap (stage 1)	47.246.136.1...	Finished
	120.97s	0.00s	4828	nmap (stage 2)	47.246.136.1...	Finished
	0.00s	0.00s	0	screenshot (80/tcp)	47.246.136.1...	Finished
	0.00s	0.00s	0	screenshot (443/tcp)	47.246.136.1...	Finished
	41.04s	0.00s	5044	nmap (stage 3)	47.246.136.1...	Finished
	116.65s	0.00s	5048	nmap (stage 4)	47.246.136.1...	Finished



Name
screenshooter

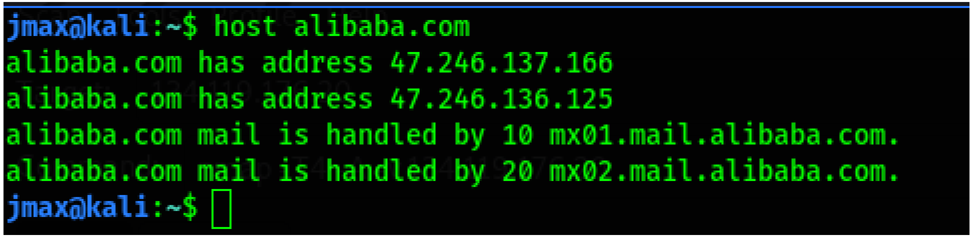
Host	Port
47.246.136.125	80/tcp
47.246.136.125	443/tcp
47.246.136.125	80/tcp
47.246.136.125	443/tcp

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	24.93s	0.00s	4823	nmap (stage 1)	47.246.136.1...	Finished
	120.97s	0.00s	4828	nmap (stage 2)	47.246.136.1...	Finished
	0.00s	0.00s	0	screenshot (80/tcp)	47.246.136.1...	Finished
	0.00s	0.00s	0	screenshot (443/tcp)	47.246.136.1...	Finished
	41.04s	0.00s	5044	nmap (stage 3)	47.246.136.1...	Finished
	116.65s	0.00s	5048	nmap (stage 4)	47.246.136.1...	Finished

- ## Host command

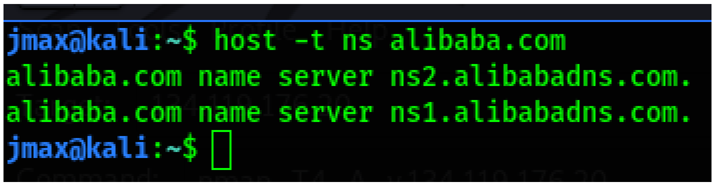
  The host command is used to do DNS (Domain Name System) lookups on a Linux system. In layman's words, the host command is used to locate the domain name of a particular IP address or to discover the IP address of a specific domain name. Below results captured after scanning the domain.

- **public ip and mail servers**



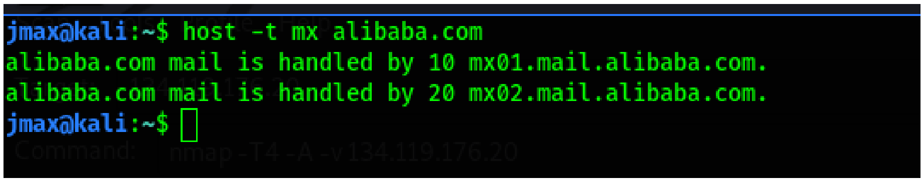
```
jmax@kali:~$ host alibaba.com
alibaba.com has address 47.246.137.166
alibaba.com has address 47.246.136.125
alibaba.com mail is handled by 10 mx01.mail.alibaba.com.
alibaba.com mail is handled by 20 mx02.mail.alibaba.com.
jmax@kali:~$ 
```

- **Name servers**

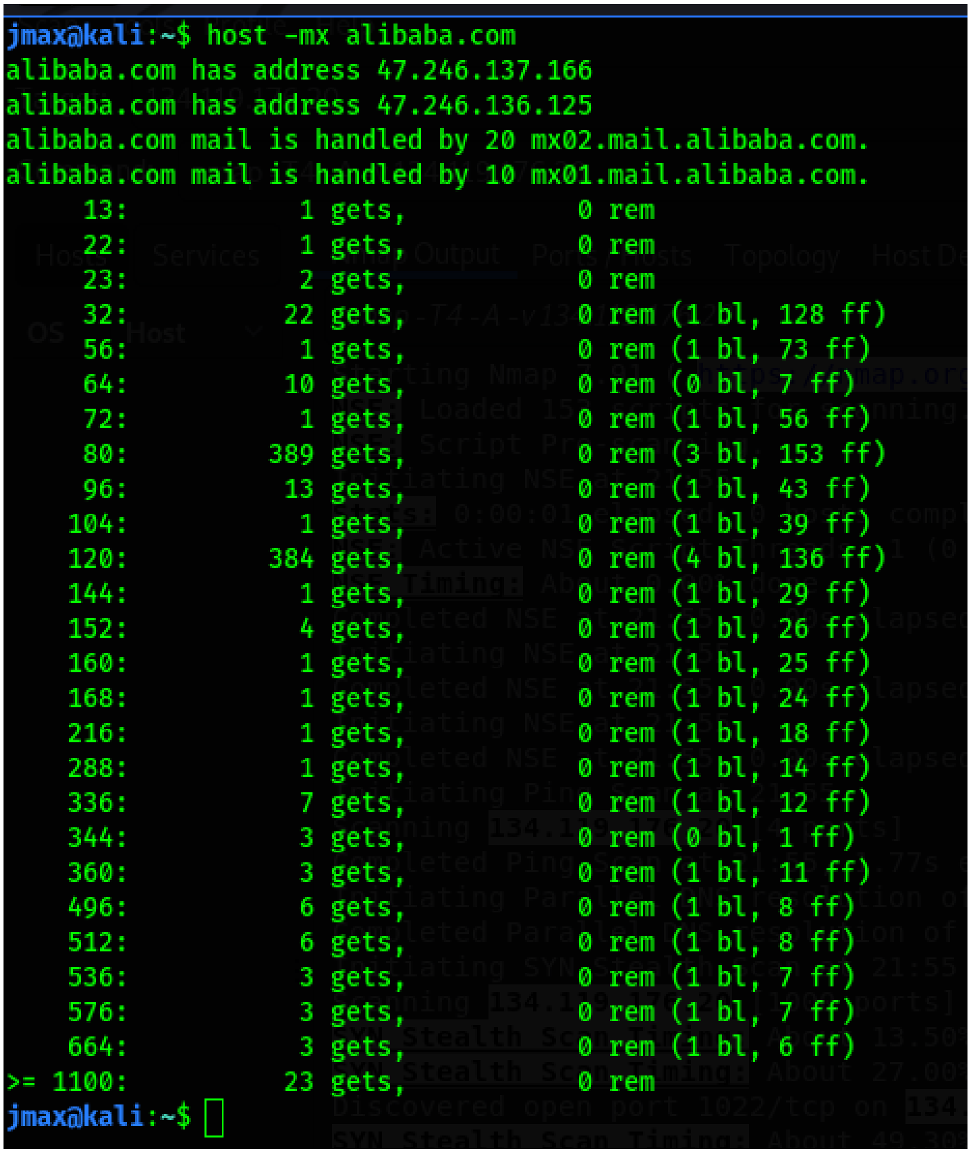


```
jmax@kali:~$ host -t ns alibaba.com
alibaba.com name server ns2.alibabadns.com.
alibaba.com name server ns1.alibabadns.com.
jmax@kali:~$ 
```

- **Mail servers**



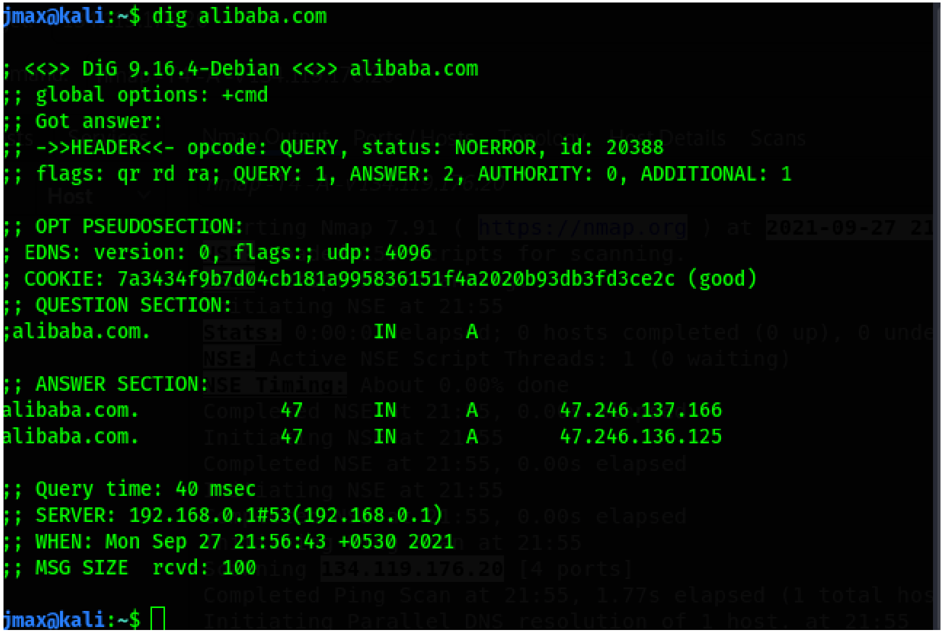
```
jmax@kali:~$ host -t mx alibaba.com
alibaba.com mail is handled by 10 mx01.mail.alibaba.com.
alibaba.com mail is handled by 20 mx02.mail.alibaba.com.
jmax@kali:~$ 
```



```
jmax@kali:~$ host -mx alibaba.com
alibaba.com has address 47.246.137.166
alibaba.com has address 47.246.136.125
alibaba.com mail is handled by 20 mx02.mail.alibaba.com.
alibaba.com mail is handled by 10 mx01.mail.alibaba.com.
     13:          1 gets,          0 rem
     22:          1 gets,          0 rem
     23:          2 gets,          0 rem
     32:         22 gets,          0 rem (1 bl, 128 ff)
     56:          1 gets,          0 rem (1 bl, 73 ff)
     64:         10 gets,          0 rem (0 bl, 7 ff)
     72:          1 gets,          0 rem (1 bl, 56 ff)
     80:        389 gets,          0 rem (3 bl, 153 ff)
     96:         13 gets,          0 rem (1 bl, 43 ff)
    104:          1 gets,          0 rem (1 bl, 39 ff)
    120:        384 gets,          0 rem (4 bl, 136 ff)
    144:          1 gets,          0 rem (1 bl, 29 ff)
    152:          4 gets,          0 rem (1 bl, 26 ff)
    160:          1 gets,          0 rem (1 bl, 25 ff)
    168:          1 gets,          0 rem (1 bl, 24 ff)
    216:          1 gets,          0 rem (1 bl, 18 ff)
    288:          1 gets,          0 rem (1 bl, 14 ff)
    336:          7 gets,          0 rem (1 bl, 12 ff)
    344:          3 gets,          0 rem (0 bl, 1 ff)
    360:          3 gets,          0 rem (1 bl, 11 ff)
    496:          6 gets,          0 rem (1 bl, 8 ff)
    512:          6 gets,          0 rem (1 bl, 8 ff)
    536:          3 gets,          0 rem (1 bl, 7 ff)
    576:          3 gets,          0 rem (1 bl, 7 ff)
    664:          3 gets,          0 rem (1 bl, 6 ff)
>= 1100:         23 gets,          0 rem
jmax@kali:~$ 
```

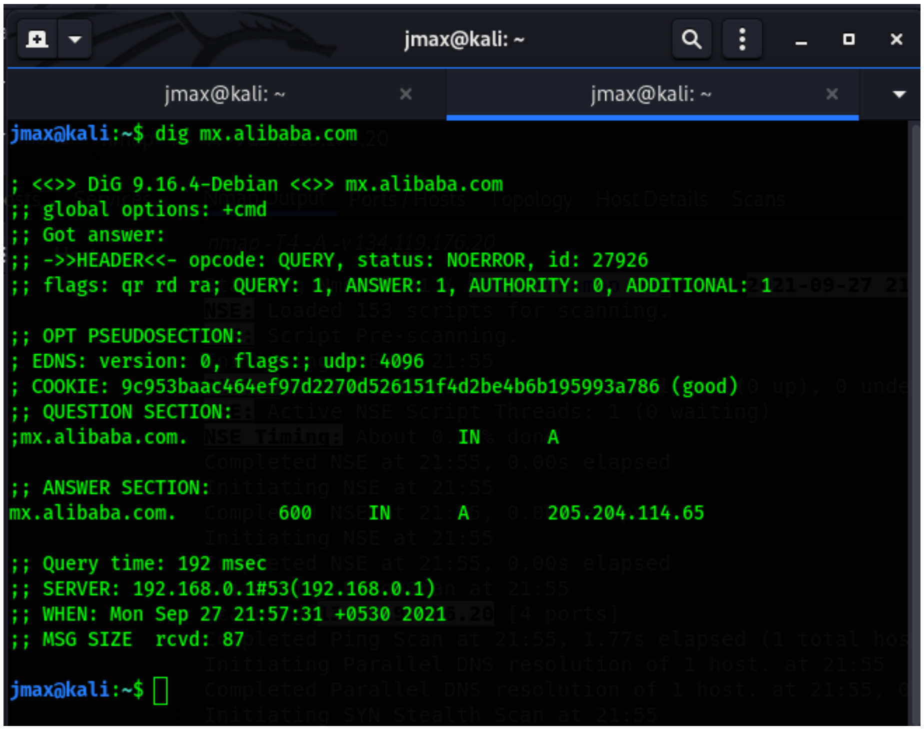
- ## Dig command

dig is a command-line application for network administration that searches the Domain Name System. Dig is useful for both troubleshooting and teaching. It may run in batch mode by reading requests from a file on the operating system, or it can execute based on command line options and flag arguments.



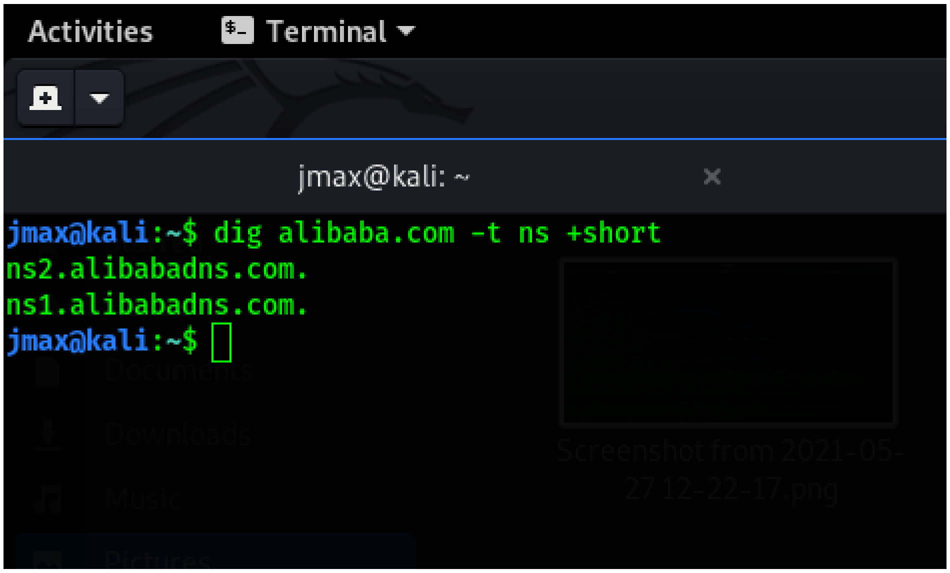
```
jmax@kali:~$ dig alibaba.com

; <<>> DiG 9.16.4-Debian <<>> alibaba.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20388
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 7a3434f9b7d04cb181a995836151f4a2020b93db3fd3ce2c (good)
;; QUESTION SECTION:
;alibaba.com.                   IN      A

;; ANSWER SECTION:
alibaba.com.            47      IN      A       47.246.137.166
alibaba.com.            47      IN      A       47.246.136.125

;; Query time: 40 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Mon Sep 27 21:56:43 +0530 2021
;; MSG SIZE  rcvd: 100

jmax@kali:~$ 
```

- ## Mail Servers



```
jmax@kali:~$ dig mx.alibaba.com

; <<>> DiG 9.16.4-Debian <<>> mx.alibaba.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27926
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9c953baac464ef97d2270d526151f4d2be4b6b195993a786 (good)
;; QUESTION SECTION:
;mx.alibaba.com.                IN      A

;; ANSWER SECTION:
mx.alibaba.com.         600     IN      A       205.204.114.65

;; Query time: 192 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Mon Sep 27 21:57:31 +0530 2021
;; MSG SIZE  rcvd: 87

jmax@kali:~$ 
```

- **Name Servers**

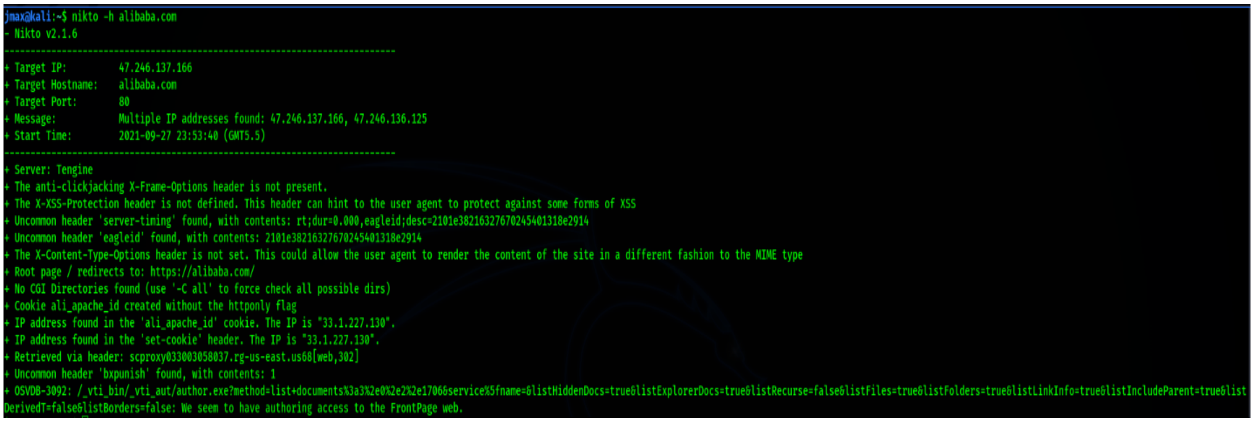


```
jmax@kali:~$ dig alibaba.com -t ns +short
ns2.alibabadns.com.
ns1.alibabadns.com.
jmax@kali:~$ 
```

4. Analyzing Vulnerabilities

- **Nikto scan**

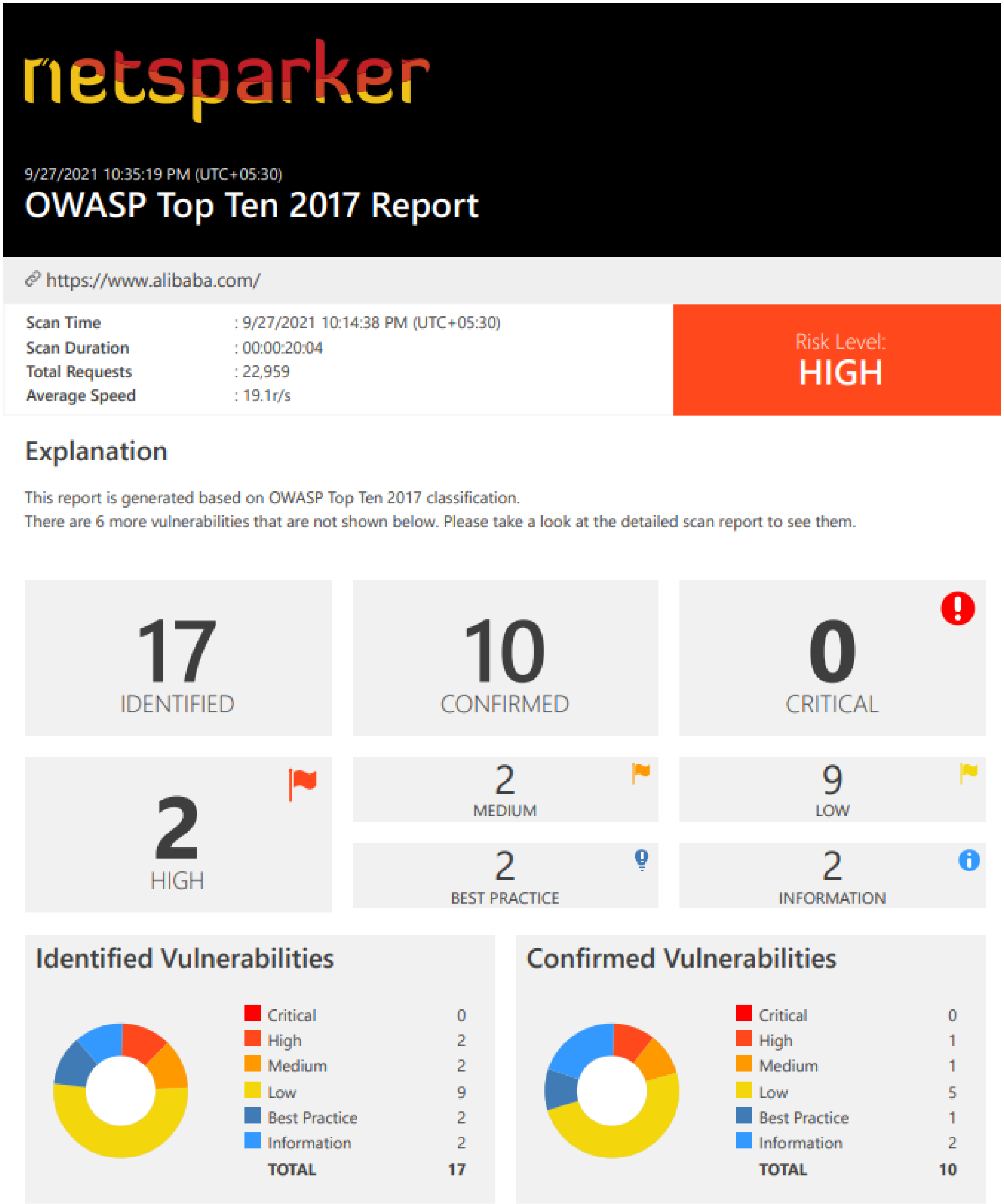
Nikto is a free command-line vulnerability scanner that searches webservers for dangerous files/CGIs, outdated server software, and other problems.



```
jmax@kali:~$ nikto -h alibaba.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          47.246.137.166
+ Target Hostname:    alibaba.com
+ Target Port:        80
+ Message:            Multiple IP addresses found: 47.246.137.166, 47.246.136.125
+ Start Time:         2021-09-27 23:53:40 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Tengine
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'server-timing' found, with contents: rt;dur=0.000,eagleid;desc=2101e38216327670245401318e2914
+ Uncommon header 'eagleid' found, with contents: 2101e38216327670245401318e2914
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://alibaba.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Cookie ali_apache_id created without the httponly flag
+ IP address found in the 'ali_apache_id' cookie. The IP is "33.1.227.130".
+ IP address found in the 'set-cookie' header. The IP is "33.1.227.130".
+ Retrieved via header: scproxy033003058037.rg-us-east.us68[web,302]
+ Uncommon header 'bxpunish' found, with contents: 1
+ OSVDB-3092: /_vti_bin/_vti_aut/author.exe?method=list+documents%3a3%2e0%2e2%2e1706&service%5fname=&listHiddenDocs=true&listExplorerDocs=true&listRecurse=false&listFiles=true&listFolders=true&listLinkInfo=true&listIncludeParent=true&list
DerivedT=false&listBorders=false: We seem to have authoring access to the FrontPage web.
```

- **Netsparker**

Netsparker is an online application security scanner that is fully customizable and enables you to scan and identify security problems in websites, web apps, and web services. Regardless of platform or programming language, Netsparker can scan a wide range of web applications.



netsparker

9/27/2021 10:35:19 PM (UTC+05:30)

OWASP Top Ten 2017 Report

https://www.alibaba.com/

Scan Time	: 9/27/2021 10:14:38 PM (UTC+05:30)
Scan Duration	: 00:00:20:04
Total Requests	: 22,959
Average Speed	: 19.1r/s

Risk Level:
HIGH

Explanation

This report is generated based on OWASP Top Ten 2017 classification.
There are 6 more vulnerabilities that are not shown below. Please take a look at the detailed scan report to see them.

17 IDENTIFIED

10 CONFIRMED

0 CRITICAL

2 HIGH

2 MEDIUM

9 LOW

2 BEST PRACTICE

2 INFORMATION

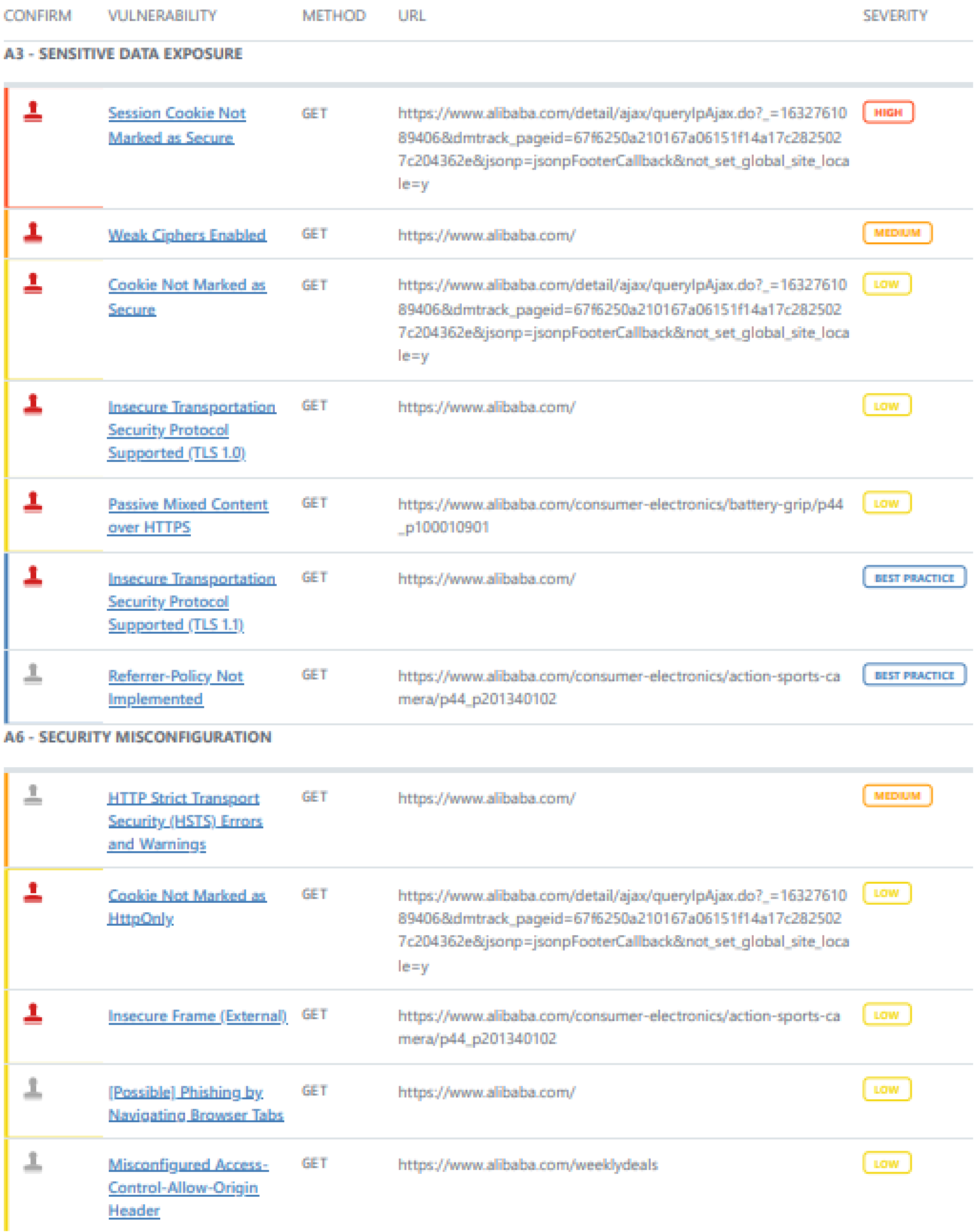
Identified Vulnerabilities

🟥 Critical	0
🟧 High	2
🟧 Medium	2
🟨 Low	9
🟦 Best Practice	2
🟦 Information	2
TOTAL	**17**

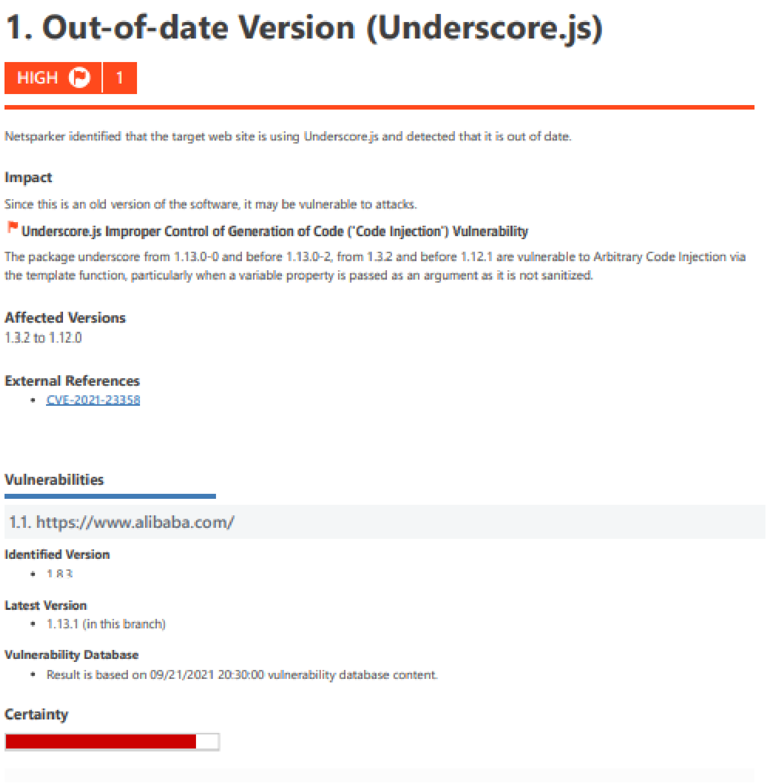
Confirmed Vulnerabilities

🟥 Critical	0
🟧 High	1
🟧 Medium	1
🟨 Low	5
🟦 Best Practice	1
🟦 Information	2
TOTAL	**10**

Vulnerabilities Found



CONFIRM	VULNERABILITY	METHOD	URL	SEVERITY
A3 - SENSITIVE DATA EXPOSURE				
●	Session Cookie Not Marked as Secure	GET	https://www.alibaba.com/detail/ajax/queryIpAjax.do?_=1632761089406&dmtrack_pageid=67f6250a210167a06151f14a17c2825027c204362e&jsonp=jsonpFooterCallback&not_set_global_site_locale=y	HIGH
●	Weak Ciphers Enabled	GET	https://www.alibaba.com/	MEDIUM
●	Cookie Not Marked as Secure	GET	https://www.alibaba.com/detail/ajax/queryIpAjax.do?_=1632761089406&dmtrack_pageid=67f6250a210167a06151f14a17c2825027c204362e&jsonp=jsonpFooterCallback&not_set_global_site_locale=y	LOW
●	Insecure Transportation Security Protocol Supported (TLS 1.0)	GET	https://www.alibaba.com/	LOW
●	Passive Mixed Content over HTTPS	GET	https://www.alibaba.com/consumer-electronics/battery-grip/p44_p100010901	LOW
●	Insecure Transportation Security Protocol Supported (TLS 1.1)	GET	https://www.alibaba.com/	BEST PRACTICE
○	Referrer-Policy Not Implemented	GET	https://www.alibaba.com/consumer-electronics/action-sports-camera/p44_p201340102	BEST PRACTICE
A6 - SECURITY MISCONFIGURATION				
○	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://www.alibaba.com/	MEDIUM
●	Cookie Not Marked as HttpOnly	GET	https://www.alibaba.com/detail/ajax/queryIpAjax.do?_=1632761089406&dmtrack_pageid=67f6250a210167a06151f14a17c2825027c204362e&jsonp=jsonpFooterCallback&not_set_global_site_locale=y	LOW
●	Insecure Frame (External)	GET	https://www.alibaba.com/consumer-electronics/action-sports-camera/p44_p201340102	LOW
○	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.alibaba.com/	LOW
○	Misconfigured Access-Control-Allow-Origin Header	GET	https://www.alibaba.com/weeklydeals	LOW



1. Out-of-date Version (Underscore.js)

HIGH | 1

Netsparker identified that the target web site is using Underscore.js and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Underscore.js Improper Control of Generation of Code ('Code Injection') Vulnerability

The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.

Affected Versions

1.3.2 to 1.12.0

External References

- CVE-2021-23358

Vulnerabilities

1.1. https://www.alibaba.com/

Identified Version

- 1.8.3

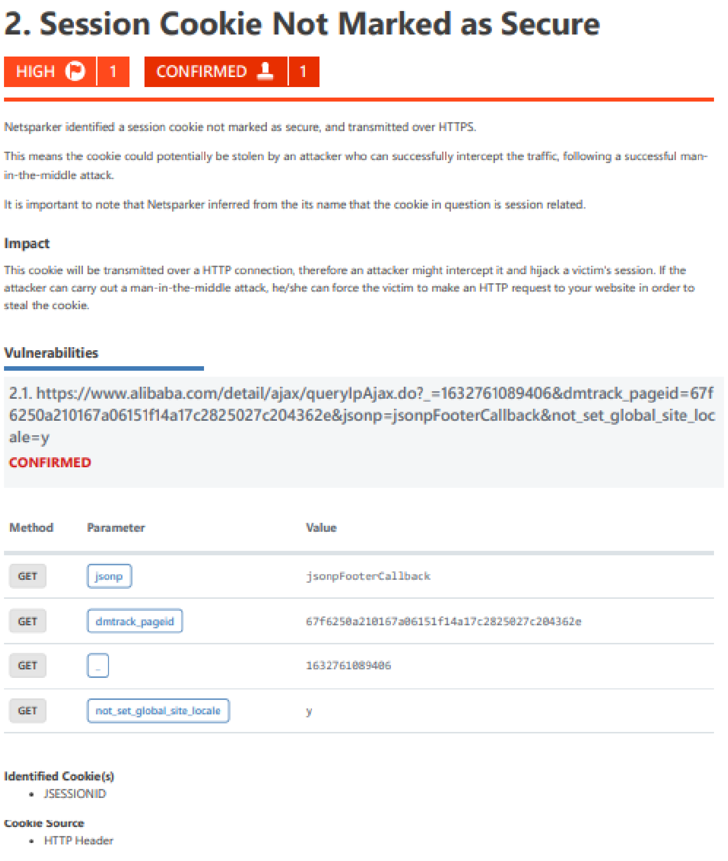
Latest Version

- 1.13.1 (in this branch)

Vulnerability Database

- Result is based on 09/21/2021 20:30:00 vulnerability database content.

Certainty



2. Session Cookie Not Marked as Secure

HIGH | 1 | CONFIRMED | 1

Netsparker identified a session cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept the traffic, following a successful man-in-the-middle attack.

It is important to note that Netsparker inferred from the its name that the cookie in question is session related.

Impact

This cookie will be transmitted over a HTTP connection, therefore an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to your website in order to steal the cookie.

Vulnerabilities

2.1. https://www.alibaba.com/detail/ajax/queryIpAjax.do?_=1632761089406&dmtrack_pageid=67f6250a210167a06151f14a17c2825027c204362e&jsonp=jsonpFooterCallback&not_set_global_site_locale=y

CONFIRMED

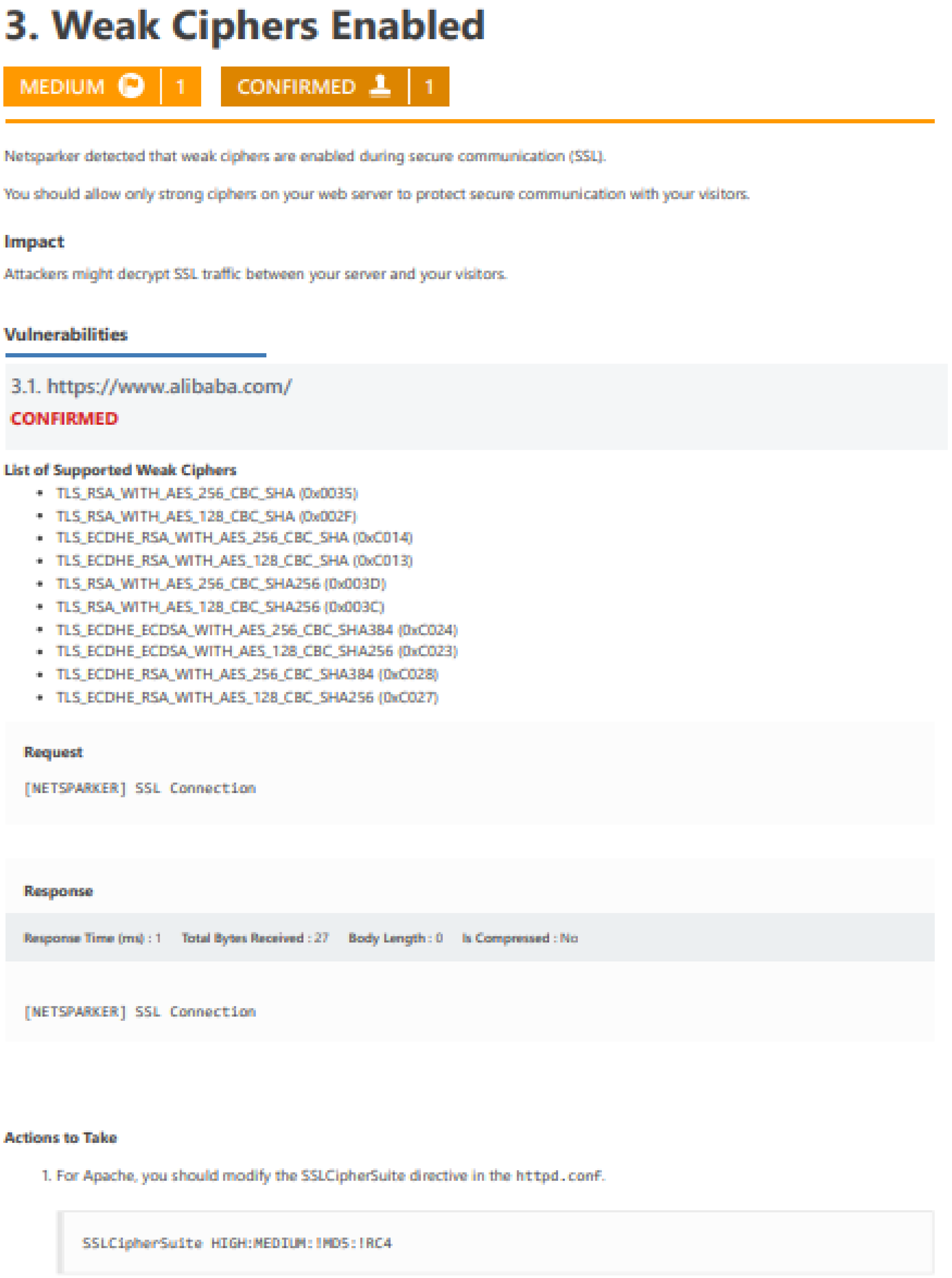
Method	Parameter	Value
GET	jsonp	`jsonpFooterCallback`
GET	dmtrack_pageid	`67f6250a210167a06151f14a17c2825027c204362e`
GET	_	`1632761089406`
GET	not_set_global_site_locale	y

Identified Cookie(s)

- JSESSIONID

Cookie Source

- HTTP Header



3. Weak Ciphers Enabled

MEDIUM | 1   CONFIRMED | 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Vulnerabilities

3.1. https://www.alibaba.com/

CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)

Request

```
[NETSPARKER] SSL Connection
```

Response

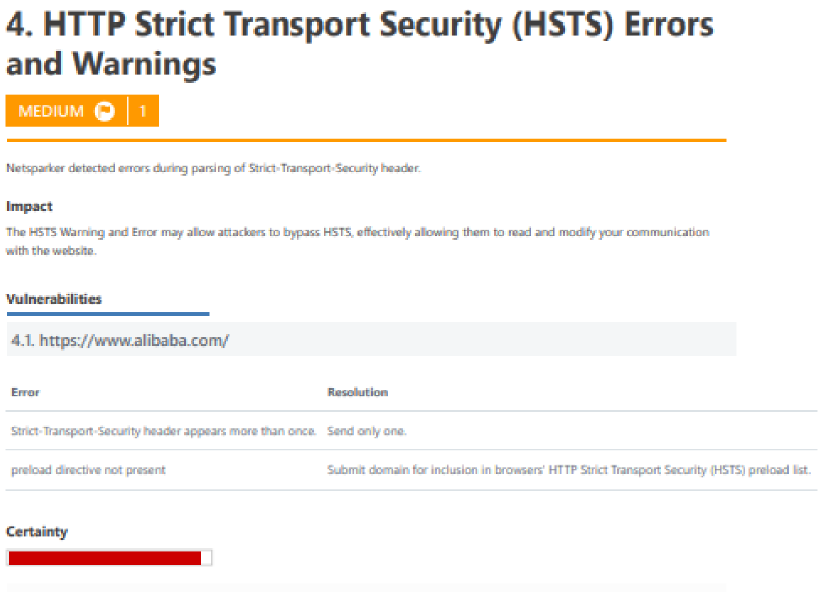
Response Time (ms) : 1   **Total Bytes Received** : 27   **Body Length** : 0   **Is Compressed** : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```



4. HTTP Strict Transport Security (HSTS) Errors and Warnings

Netsparker detected errors during parsing of Strict-Transport-Security header.

Impact

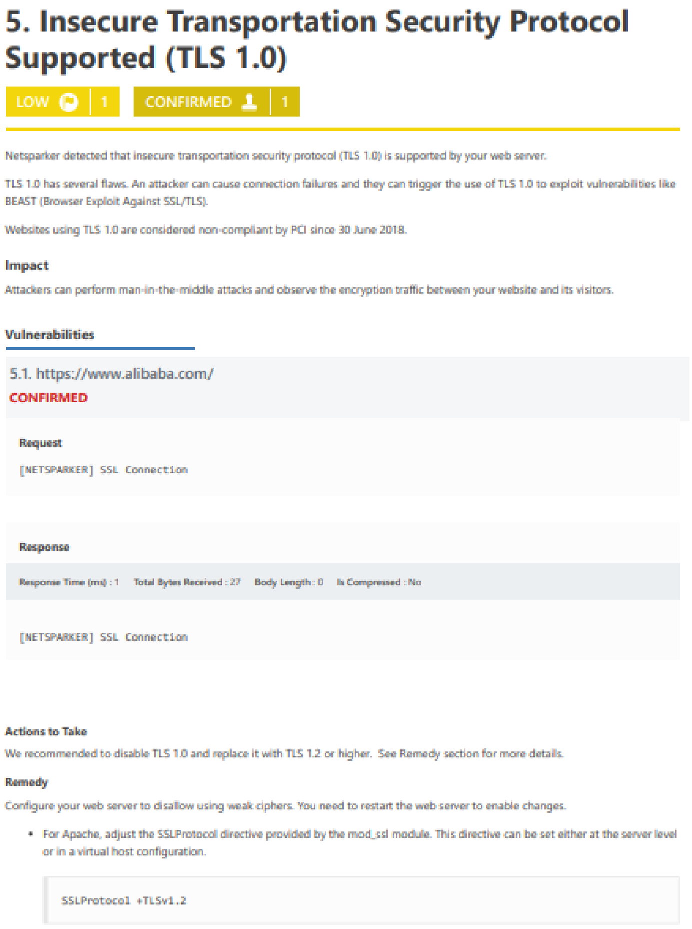
The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.

Vulnerabilities

4.1. https://www.alibaba.com/

Error	Resolution
Strict-Transport-Security header appears more than once.	Send only one.
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

Certainty



5. Insecure Transportation Security Protocol Supported (TLS 1.0)

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 are considered non-compliant by PCI since 30 June 2018.

Impact

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Vulnerabilities

5.1. https://www.alibaba.com/

CONFIRMED

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1   Total Bytes Received : 27   Body Length : 0   Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Actions to Take

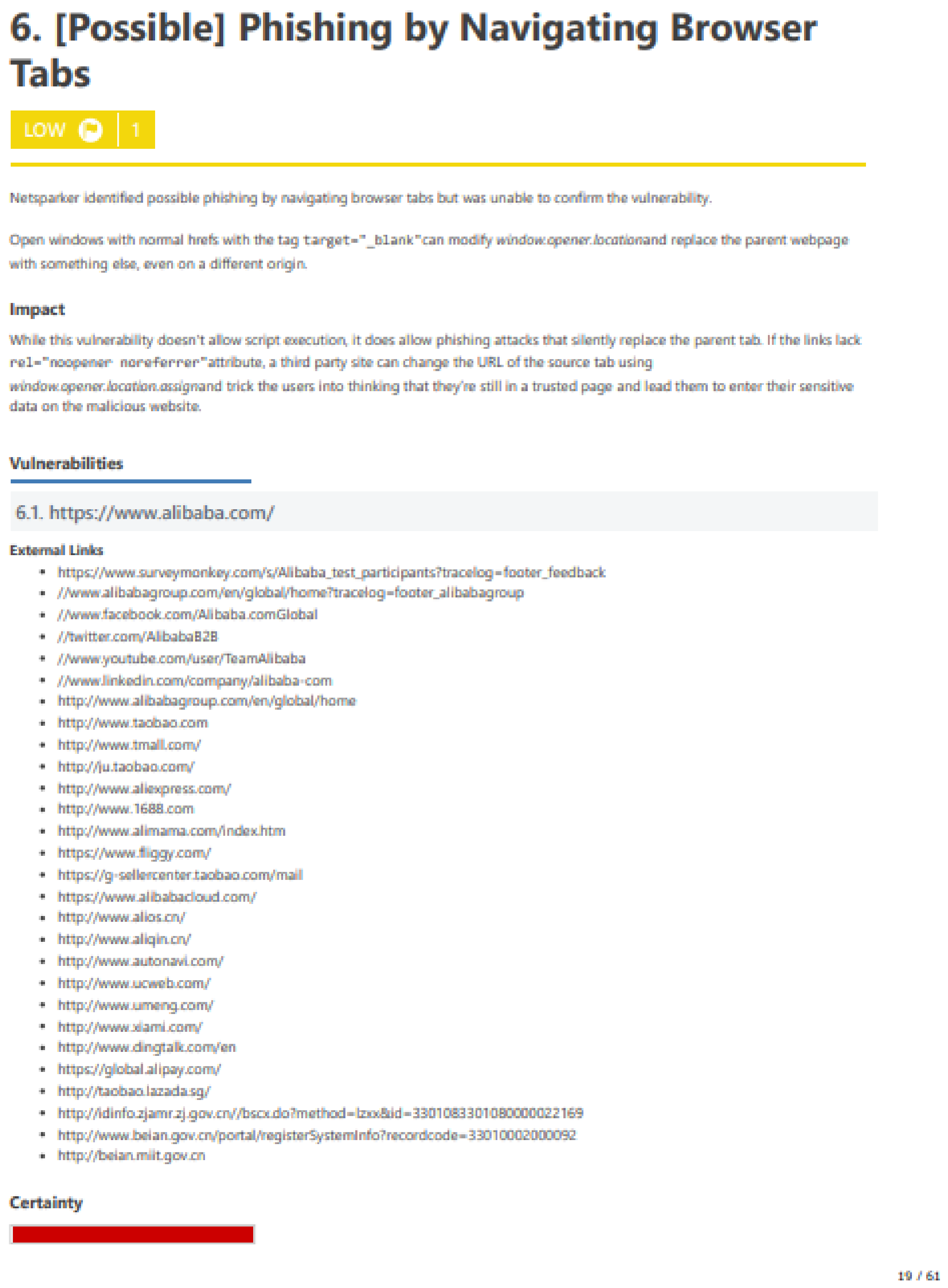
We recommended to disable TLS 1.0 and replace it with TLS 1.2 or higher. See Remedy section for more details.

Remedy

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

```
SSLProtocol +TLSv1.2
```



6. [Possible] Phishing by Navigating Browser Tabs

LOW | 1

Netsparker identified possible phishing by navigating browser tabs but was unable to confirm the vulnerability.

Open windows with normal hrefs with the tag `target="_blank"`can modify *window.opener.location*and replace the parent webpage with something else, even on a different origin.

Impact

While this vulnerability doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab. If the links lack `rel="noopener noreferrer"`attribute, a third party site can change the URL of the source tab using *window.opener.location.assign*and trick the users into thinking that they're still in a trusted page and lead them to enter their sensitive data on the malicious website.

Vulnerabilities

6.1. https://www.alibaba.com/

External Links

- https://www.surveymonkey.com/s/Alibaba_test_participants?tracelog=footer_feedback
- //www.alibabagroup.com/en/global/home?tracelog=footer_alibabagroup
- //www.facebook.com/Alibaba.comGlobal
- //twitter.com/AlibabaB2B
- //www.youtube.com/user/TeamAlibaba
- //www.linkedin.com/company/alibaba-com
- http://www.alibabagroup.com/en/global/home
- http://www.taobao.com
- http://www.tmall.com/
- http://ju.taobao.com/
- http://www.aliexpress.com/
- http://www.1688.com
- http://www.alimama.com/index.htm
- https://www.fliggy.com/
- https://g-sellercenter.taobao.com/mall
- https://www.alibabacloud.com/
- http://www.alios.cn/
- http://www.aliqin.cn/
- http://www.autonavi.com/
- http://www.ucweb.com/
- http://www.umeng.com/
- http://www.xiami.com/
- http://www.dingtalk.com/en
- https://global.alipay.com/
- http://taobao.lazada.sg/
- http://idinfo.zjamr.zj.gov.cn//bscx.do?method=lzxx&id=3301083301080000022169
- http://www.beian.gov.cn/portal/registerSystemInfo?recordcode=33010002000092
- http://beian.miit.gov.cn

Certainty

19 / 61

Conclusion

Following the assessment, it was found that, with the exception of a few loose ends, the application's basic security was not adequately planned and implemented. Overall, due to the employment of security methods and protocols, the web application's dependability and trustworthiness are well-structured.