Name: Iyiola, Oluwaleke

Student ID: IDEAS/24/21635

Course: INT 302Kali Linux Tools and System Security – Lab 1: Reconnaissance (Information Gathering)

Lab Steps

Step 1: Get the IP Address of a Domain Using ping

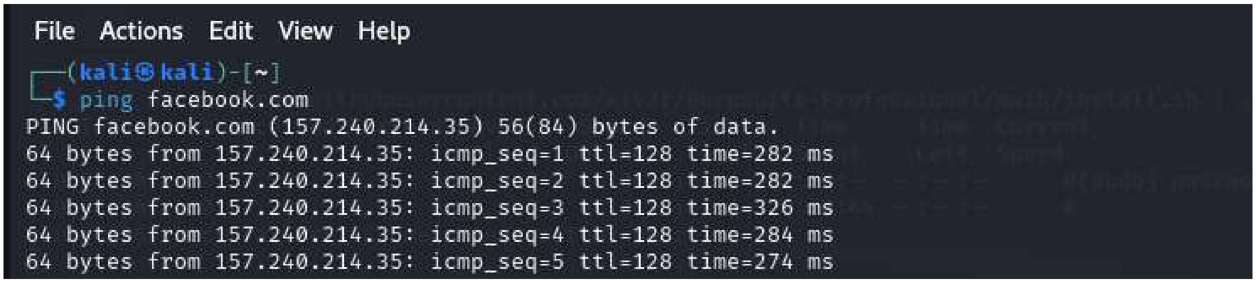
Exercise 1:

Use the ping command to find the IP addresses of the following domains:

- facebook.com twitter.com amazon.com

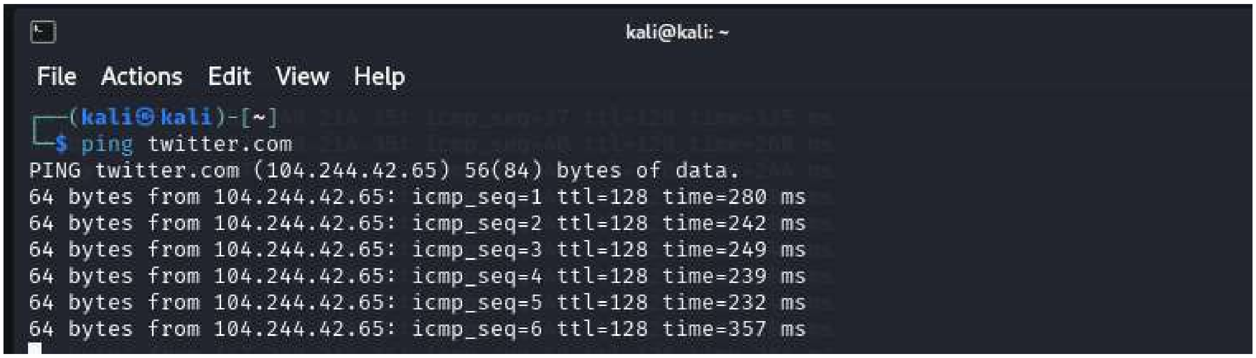
Record Your Answers:

1. facebook.com: __________104.244.42.129



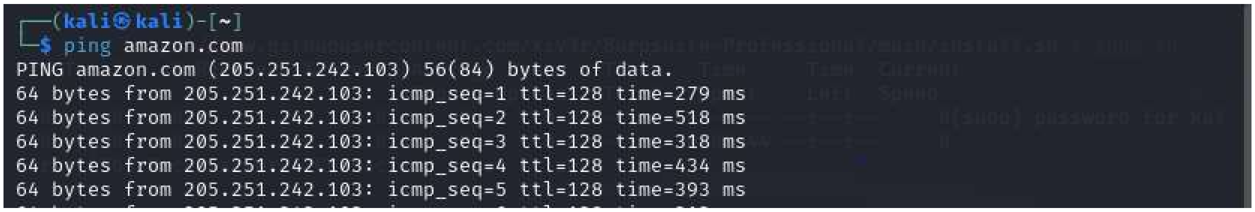
```
┌──(kali㉿kali)-[~]
└─$ ping facebook.com
PING facebook.com (157.240.214.35) 56(84) bytes of data.
64 bytes from 157.240.214.35: icmp_seq=1 ttl=128 time=282 ms
64 bytes from 157.240.214.35: icmp_seq=2 ttl=128 time=282 ms
64 bytes from 157.240.214.35: icmp_seq=3 ttl=128 time=326 ms
64 bytes from 157.240.214.35: icmp_seq=4 ttl=128 time=284 ms
64 bytes from 157.240.214.35: icmp_seq=5 ttl=128 time=274 ms
```

2. twitter.com: __________104.244.42.129



```
┌──(kali㉿kali)-[~]
└─$ ping twitter.com
PING twitter.com (104.244.42.65) 56(84) bytes of data.
64 bytes from 104.244.42.65: icmp_seq=1 ttl=128 time=280 ms
64 bytes from 104.244.42.65: icmp_seq=2 ttl=128 time=242 ms
64 bytes from 104.244.42.65: icmp_seq=3 ttl=128 time=249 ms
64 bytes from 104.244.42.65: icmp_seq=4 ttl=128 time=239 ms
64 bytes from 104.244.42.65: icmp_seq=5 ttl=128 time=232 ms
64 bytes from 104.244.42.65: icmp_seq=6 ttl=128 time=357 ms
```

amazon.com: __________205.251.242.103



```
┌──(kali㉿kali)-[~]
└─$ ping amazon.com
PING amazon.com (205.251.242.103) 56(84) bytes of data.
64 bytes from 205.251.242.103: icmp_seq=1 ttl=128 time=279 ms
64 bytes from 205.251.242.103: icmp_seq=2 ttl=128 time=518 ms
64 bytes from 205.251.242.103: icmp_seq=3 ttl=128 time=318 ms
64 bytes from 205.251.242.103: icmp_seq=4 ttl=128 time=434 ms
64 bytes from 205.251.242.103: icmp_seq=5 ttl=128 time=393 ms
```

Exercise 2: Retrieve Domain Registration Details Using whois

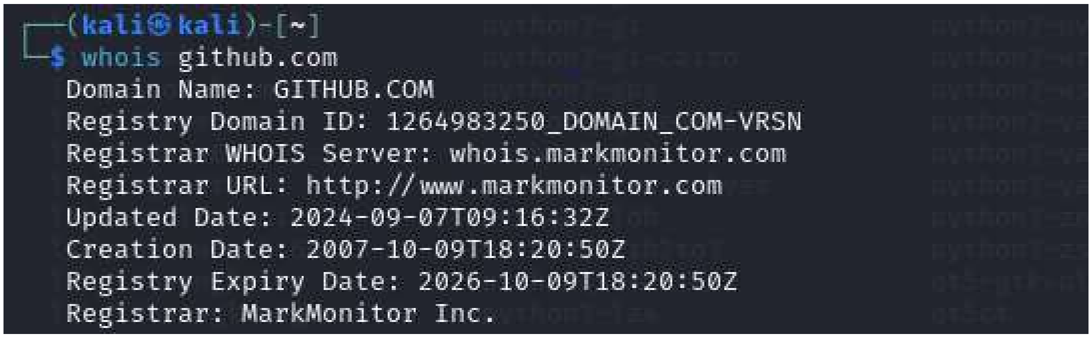
Run the whois command for the following domains:

- **github.com**
- linkedin.com

- apple.com

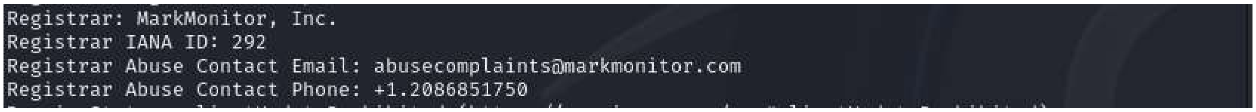
Answer These Questions:

1. What is the registration expiration date for github.com? 2026-10-09T18:20:50Z



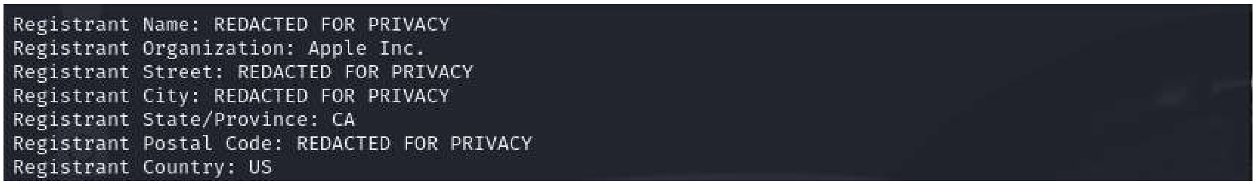
```
┌──(kali㉿kali)-[~]
└─$ whois github.com
   Domain Name: GITHUB.COM
   Registry Domain ID: 1264983250_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2024-09-07T09:16:32Z
   Creation Date: 2007-10-09T18:20:50Z
   Registry Expiry Date: 2026-10-09T18:20:50Z
   Registrar: MarkMonitor Inc.
```

2. Who is the registrar for linkedin.com? MarkMonitor, Inc.



```
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
```

3. What country is the registrant of apple.com from? CA/US



```
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Apple Inc.
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: CA
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
```

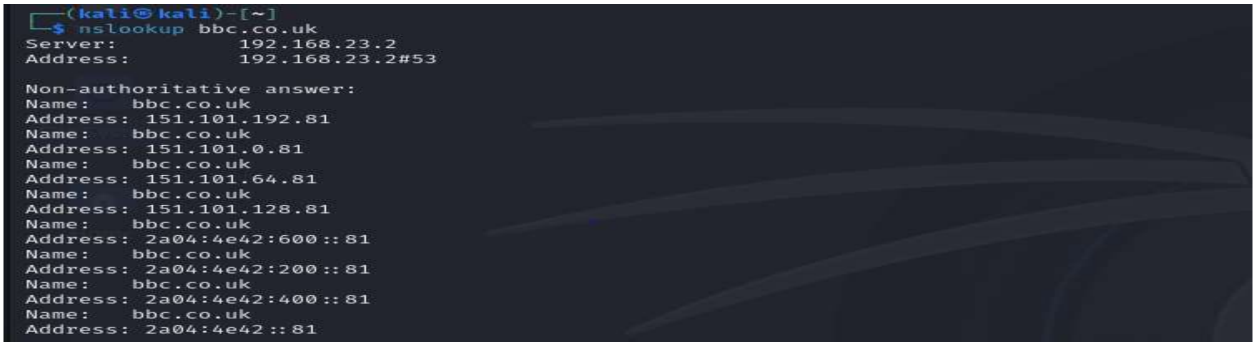
Exercise 3: Perform a DNS Lookup Using nslookup

Use nslookup to look up DNS information for the following domains:

- bbc.co.uk
- netflix.com

Answer These Questions:

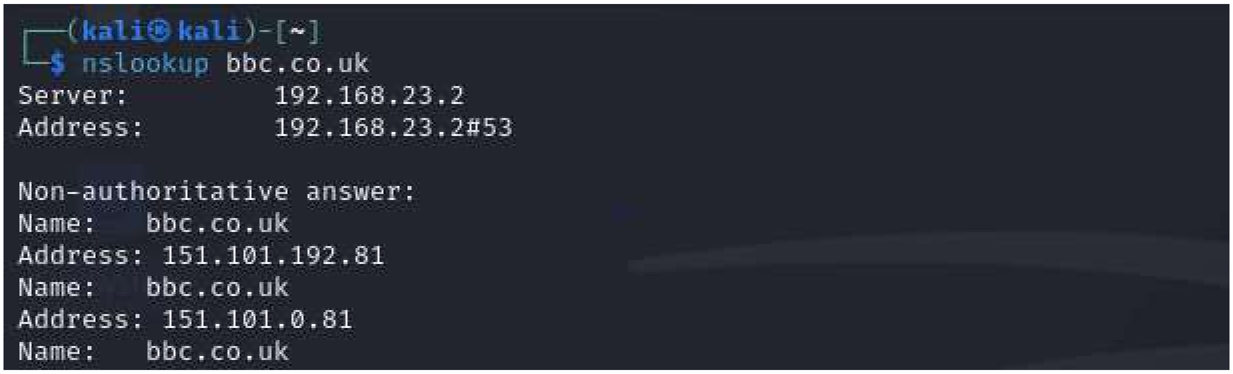
1. What is the IP address for bbc.co.uk? 192.168.23.2



```
┌──(kali㉿kali)-[~]
└─$ nslookup bbc.co.uk
Server:         192.168.23.2
Address:        192.168.23.2#53

Non-authoritative answer:
Name:   bbc.co.uk
Address: 151.101.192.81
Name:   bbc.co.uk
Address: 151.101.0.81
Name:   bbc.co.uk
Address: 151.101.64.81
Name:   bbc.co.uk
Address: 151.101.128.81
Name:   bbc.co.uk
Address: 2a04:4e42:600::81
Name:   bbc.co.uk
Address: 2a04:4e42:200::81
Name:   bbc.co.uk
Address: 2a04:4e42:400::81
Name:   bbc.co.uk
Address: 2a04:4e42::81
```

2. What are the name servers (NS) for netflix.com? 192.168.23.2



```
┌──(kali㉿kali)-[~]
└─$ nslookup bbc.co.uk
Server:         192.168.23.2
Address:        192.168.23.2#53

Non-authoritative answer:
Name:   bbc.co.uk
Address: 151.101.192.81
Name:   bbc.co.uk
Address: 151.101.0.81
Name:   bbc.co.uk
```

INT302: Kali Linux Tools and System Security

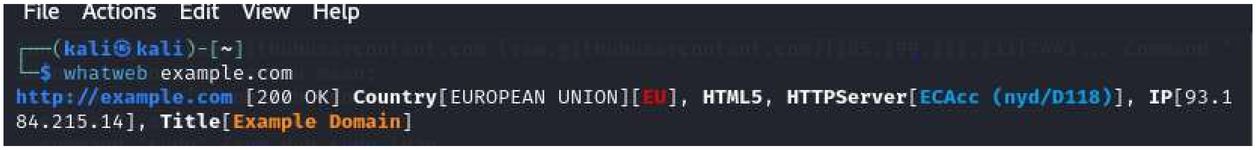
Lab 2: Website Enumeration and Information Gathering

Exercise 1:

Run the whatweb command to detect technologies for the following targets:

- **example.com**

  http://example.com [200 OK] Country [EUROPEAN UNION] [EU], HTML5, HTTPServer [ECAcc (nyd/D166)], IP [93.184.215.14], Title [Example Domain]

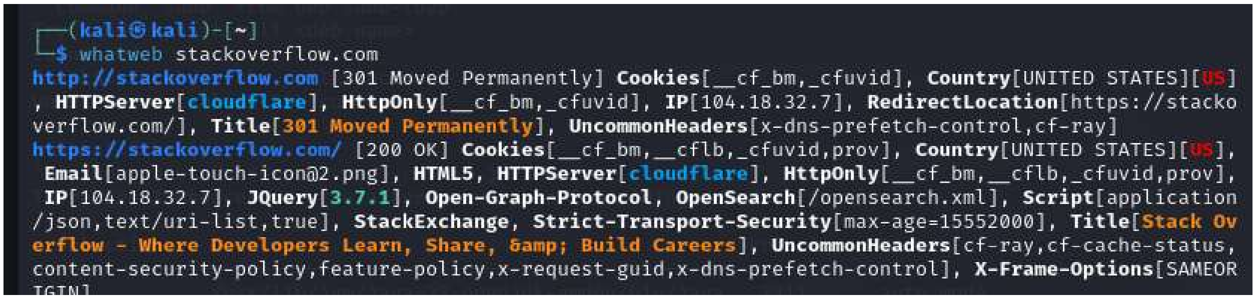


```
┌──(kali㉿kali)-[~]
└─$ whatweb example.com
http://example.com [200 OK] Country[EUROPEAN UNION][EU], HTML5, HTTPServer[ECAcc (nyd/D118)], IP[93.1
84.215.14], Title[Example Domain]
```

- **stackoverflow.com**

  http://stackoverflow.com [301 Moved Permanently] Cookies[__cf_bm,_cfuvid], Country[UNITED STATES][US], HTTPServer[cloudflare], HttpOnly[__cf_bm,_cfuvid], IP[104.18.32.7], RedirectLocation[https://stackoverflow.com/], Title[301 Moved Permanently], UncommonHeaders[x-dns-prefetch-control,cf-ray]

  https://stackoverflow.com/ [200 OK] Cookies[__cf_bm,__cflb,_cfuvid,prov], Country[UNITED STATES][US], Email[apple-touch-icon@2.png], HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm,__cflb,_cfuvid,prov], IP[104.18.32.7], JQuery[3.7.1], Open-Graph-Protocol, OpenSearch[/opensearch.xml], Script[application/json,text/uri-list,true], StackExchange, Strict-Transport-Security[max-age=15552000], Title[Stack Overflow - Where Developers Learn, Share, &amp; Build Careers], UncommonHeaders[cf-ray,cf-cache-status,content-security-policy,feature-policy,x-request-guid,x-dns-prefetch-control], X-Frame-Options[SAMEORIGIN]

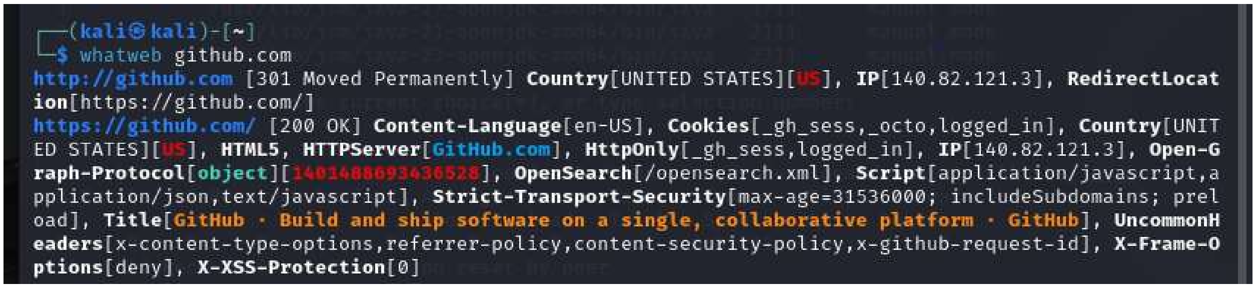


```
┌──(kali㉿kali)-[~]
└─$ whatweb stackoverflow.com
http://stackoverflow.com [301 Moved Permanently] Cookies[__cf_bm,_cfuvid], Country[UNITED STATES][US]
, HTTPServer[cloudflare], HttpOnly[__cf_bm,_cfuvid], IP[104.18.32.7], RedirectLocation[https://stacko
verflow.com/], Title[301 Moved Permanently], UncommonHeaders[x-dns-prefetch-control,cf-ray]
https://stackoverflow.com/ [200 OK] Cookies[__cf_bm,__cflb,_cfuvid,prov], Country[UNITED STATES][US],
 Email[apple-touch-icon@2.png], HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm,__cflb,_cfuvid,prov],
 IP[104.18.32.7], JQuery[3.7.1], Open-Graph-Protocol, OpenSearch[/opensearch.xml], Script[application
/json,text/uri-list,true], StackExchange, Strict-Transport-Security[max-age=15552000], Title[Stack Ov
erflow - Where Developers Learn, Share, &amp; Build Careers], UncommonHeaders[cf-ray,cf-cache-status,
content-security-policy,feature-policy,x-request-guid,x-dns-prefetch-control], X-Frame-Options[SAMEOR
IGIN]
```

- **github.com**

  http://github.com [301 Moved Permanently] Country[UNITED STATES][US], IP[140.82.121.3], RedirectLocation[https://github.com/]

  https://github.com/ [200 OK] Content-Language[en-US], Cookies[_gh_sess,_octo,logged_in], Country[UNITED STATES][US], HTML5, HTTPServer[GitHub.com], HttpOnly[_gh_sess,logged_in], IP[140.82.121.3], Open-Graph-Protocol[object][1401488693436528], OpenSearch[/opensearch.xml], Script[application/javascript,application/json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubdomains; preload], Title[GitHub · Build and ship software on a single, collaborative platform · GitHub], UncommonHeaders[x-content-type-options,referrer-policy,content-security-policy,x-github-request-id], X-Frame-Options[deny], X-XSS-Protection[0]



```
┌──(kali㉿kali)-[~]
└─$ whatweb github.com
http://github.com [301 Moved Permanently] Country[UNITED STATES][US], IP[140.82.121.3], RedirectLocat
ion[https://github.com/]
https://github.com/ [200 OK] Content-Language[en-US], Cookies[_gh_sess,_octo,logged_in], Country[UNIT
ED STATES][US], HTML5, HTTPServer[GitHub.com], HttpOnly[_gh_sess,logged_in], IP[140.82.121.3], Open-G
raph-Protocol[object][1401488693436528], OpenSearch[/opensearch.xml], Script[application/javascript,a
pplication/json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubdomains; prel
oad], Title[GitHub · Build and ship software on a single, collaborative platform · GitHub], UncommonH
eaders[x-content-type-options,referrer-policy,content-security-policy,x-github-request-id], X-Frame-O
ptions[deny], X-XSS-Protection[0]
```

Exercise 2: Perform Aggressive Scanning Using whatweb

Perform an aggressive scan on the following targets:

- **google.com**
  - WhatWeb http://google.com
  - Status   : 301 Moved Permanently
  - Title   : 301 Moved
  - IP   : 172.217.17.14
  - Country   : UNITED STATES, US
  - Summary   : HTTPServer[gws], RedirectLocation[http://www.google.com/], UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]
  - Detected Plugins:
  - [HTTPServer]
  - HTTP server header string. This plugin also attempts to
  - identify the operating system from the server header.
  - String   : gws (from server string)
  - [RedirectLocation]
  - HTTP Server string location. used with http-status 301 and 302
  - String   : http://www.google.com/ (from location)
  - [UncommonHeaders]
  - Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version. Info about headers can be found at www.http-stats.com
  - String   : content-security-policy-report-only (from headers)
  -
  - [X-Frame-Options]

```
•           This plugin retrieves the X-Frame-Options value from the
•           HTTP header. - More Info:
•           http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
•           aspx
•
•           String      : SAMEORIGIN
•
•       [ X-XSS-Protection ]
•           This plugin retrieves the X-XSS-Protection value from the
•           HTTP header. - More Info:
•           http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
•           aspx
•
•           String      : 0
•
•       HTTP Headers:
•           HTTP/1.1 301 Moved Permanently
•           Location: http://www.google.com/
•           Content-Type: text/html; charset=UTF-8
•           Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-lk7kWABEWk8muHd2D5qIIg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
•           Date: Sat, 02 Nov 2024 19:40:55 GMT
•           Expires: Mon, 02 Dec 2024 19:40:55 GMT
•           Cache-Control: public, max-age=2592000
•           Server: gws
•           Content-Length: 219
•           X-XSS-Protection: 0
•           X-Frame-Options: SAMEORIGIN
•           Connection: close
•
•       WhatWeb report for http://www.google.com/
•       Status    : 200 OK
•       Title     : Google
•       IP        : 142.250.178.164
•       Country   : UNITED STATES, US
•
•       Summary   : Cookies[AEC,NID], HTML5, HTTPServer[gws], HttpOnly[AEC,NID], Script, UncommonHeaders[content-security-policy-report-only], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]
•
•       Detected Plugins:
•       [ Cookies ]
•           Display the names of cookies in the HTTP headers. The
•           values are not returned to save on space.
•
•           String      : AEC
•           String      : NID
•
•       [ HTML5 ]
•           HTML version 5, detected by the doctype declaration
•
```

```

[ HTTPServer ]
	HTTP server header string. This plugin also attempts to
	identify the operating system from the server header.

	String       : gws (from server string)

[ HttpOnly ]
	If the HttpOnly flag is included in the HTTP set-cookie
	response header and the browser supports it then the cookie
	cannot be accessed through client side script - More Info:
	http://en.wikipedia.org/wiki/HTTP_cookie

	String       : AEC,NID

[ Script ]
	This plugin detects instances of script HTML elements and
	returns the script language/type.


[ UncommonHeaders ]
	Uncommon HTTP server headers. The blacklist includes all
	the standard headers and many non standard but common ones.
	Interesting but fairly common headers should have their own
	plugins, eg. x-powered-by, server and x-aspnet-version.
	Info about headers can be found at www.http-stats.com

	String       : content-security-policy-report-only (from headers)

[ X-Frame-Options ]
	This plugin retrieves the X-Frame-Options value from the
	HTTP header. - More Info:
	http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
	aspx

	String       : SAMEORIGIN

[ X-XSS-Protection ]
	This plugin retrieves the X-XSS-Protection value from the
	HTTP header. - More Info:
	http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
	aspx

	String       : 0

HTTP Headers:
	HTTP/1.1 200 OK
	Date: Sat, 02 Nov 2024 19:40:57 GMT
	Expires: -1
	Cache-Control: private, max-age=0
	Content-Type: text/html; charset=ISO-8859-1
```

- Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-mk9ZD562ADjFOMytzt4mjw' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp
- P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
- Content-Encoding: gzip
- Server: gws
- Content-Length: 9038
- X-XSS-Protection: 0
- X-Frame-Options: SAMEORIGIN
- Set-Cookie: AEC=AVYB7coGaxNT5aA0F5qg9CUVoTXvocvUkOu1nw3nR4Rxxy357slM7H67tw; expires=Thu, 01-May-2025 19:40:57 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax
- Set-Cookie: NID=518=kXLNMvC5qMkixoOjof3UPEyTApzOrNKlIqSr3hIX2B6rsUjHibpBZi8A0nD_9FSAewrzKkHbbnxgKhZiAqzdjigtXb9mw2AzuL5y4IX7zdareglRw3ZaccVVgPTZg5lYVBLmZRpB2kSqZn7e53bF_joP7GWmKR3_ckZxi-qkyheJdPct28jljyFcvaPu0ezyDZit; expires=Sun, 04-May-2025 19:40:57 GMT; path=/; domain=.google.com; HttpOnly
- Connection: close

- **facebook.com**

WhatWeb report for http://facebook.com

Status : 301 Moved Permanently

Title : <None>

IP : <Unknown>

Country : <Unknown>

Summary : HTTPServer[proxygen-bolt], RedirectLocation[https://facebook.com/]

Detected Plugins:

[HTTPServer]

HTTP server header string. This plugin also attempts to

identify the operating system from the server header.

String : proxygen-bolt (from server string)

[RedirectLocation]

HTTP Server string location. used with http-status 301 and

302

String : https://facebook.com/ (from location)

```
HTTP Headers:

        HTTP/1.1 301 Moved Permanently

        Location: https://facebook.com/

        Content-Type: text/plain

        Server: proxygen-bolt

        Date: Tue, 05 Nov 2024 12:00:08 GMT

        Connection: close

        Content-Length: 0


WhatWeb report for https://facebook.com/

Status    : 301 Moved Permanently

Title     : <None>

IP        : <Unknown>

Country   : <Unknown>


Summary   : RedirectLocation[https://www.facebook.com/], Strict-Transport-Security[max-age=15552000; preload], UncommonHeaders[x-fb-debug,x-fb-connection-quality,alt-svc]


Detected Plugins:

[ RedirectLocation ]

        HTTP Server string location. used with http-status 301 and

        302


        String       : https://www.facebook.com/ (from location)


[ Strict-Transport-Security ]

        Strict-Transport-Security is an HTTP header that restricts

        a web browser from accessing a website without the security

        of the HTTPS protocol.


        String       : max-age=15552000; preload


[ UncommonHeaders ]
```

```
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : x-fb-debug,x-fb-connection-quality,alt-svc (from headers)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Location: https://www.facebook.com/
        Strict-Transport-Security: max-age=15552000; preload
        Content-Type: text/html; charset="utf-8"
        X-FB-Debug: x7cEOEN6lcRKqeNkjD0by7uDQH6oehEU5OLqObV+gv9qkVbpi45p6vpvDDK1CMXNoafa6m+1U8uIR2VuIl7i+g==
        Date: Tue, 05 Nov 2024 12:00:11 GMT
        X-FB-Connection-Quality: EXCELLENT; q=0.9, rtt=15, rtx=0, c=10, mss=1392, tbw=2526, tp=-1, tpl=-1, uplat=120, ullat=0
        Alt-Svc: h3=":443"; ma=86400
        Connection: close
        Content-Length: 0

WhatWeb report for https://www.facebook.com/
Status    : 302 Found
Title     : <None>
IP        : <Unknown>
Country   : <Unknown>

Summary   : RedirectLocation[https://web.facebook.com/?_rdc=1&_rdr], Strict-Transport-Security[max-age=15552000; preload], UncommonHeaders[reporting-endpoints,report-to,cross-origin-opener-policy,x-fb-zr-redirect,x-fb-debug,x-fb-connection-quality,alt-svc]

Detected Plugins:
[ RedirectLocation ]
```

```
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://web.facebook.com/?_rdc=1&_rdr (from location)

[ Strict-Transport-Security ]
        Strict-Transport-Security is an HTTP header that restricts
        a web browser from accessing a website without the security
        of the HTTPS protocol.

        String       : max-age=15552000; preload

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : reporting-endpoints,report-to,cross-origin-opener-policy,x-fb-zr-redirect,x-fb-debug,x-fb-connection-quality,alt-svc (from headers)

HTTP Headers:
        HTTP/1.1 302 Found
        Location: https://web.facebook.com/?_rdc=1&_rdr
        reporting-endpoints: coop_report="https://www.facebook.com/browser_reporting/coop/?minimize=0"
        report-to: {"max_age":2592000,"endpoints":[{"url":"https:\/\/www.facebook.com\/browser_reporting\/coop\/?minimize=0"}],"group":"coop_report","include_subdomains":true}
        cross-origin-opener-policy: unsafe-none
        x-fb-zr-redirect: 02|1730894413|
        Strict-Transport-Security: max-age=15552000; preload
        Content-Type: text/html; charset="utf-8"
        X-FB-Debug:
G6oNb6ufM7QsliWsECC70ge+znl4hoCUdyX0rhuyhM/n4aUd6udUHmmgBkJiCZB7IRHJAdSK5Kpl5resyZH
zNg==

        Date: Tue, 05 Nov 2024 12:00:13 GMT

        X-FB-Connection-Quality: EXCELLENT; q=0.9, rtt=14, rtx=0, c=10, mss=1392, tbw=2526, tp=-1, tpl=-
1, uplat=128, ullat=0

        Alt-Svc: h3=":443"; ma=86400

        Connection: close

        Content-Length: 0


WhatWeb report for https://web.facebook.com/?_rdc=1&_rdr

Status    : 200 OK

Title     : <None>

IP        : <Unknown>

Country   : <Unknown>


Summary   : Cookies[fr,sb], HTML5, HttpOnly[fr,sb], Meta-Refresh-
Redirect[/?_rdc=1&_rdr&_fb_noscript=1], PasswordField[pass],
Script[application/ld+json,text/javascript], Strict-Transport-Security[max-age=15552000; preload],
UncommonHeaders[reporting-endpoints,report-to,content-security-policy-report-only,content-security-
policy,document-policy,permissions-policy,cross-origin-resource-policy,cross-origin-opener-policy,x-
content-type-options,x-fb-debug,x-fb-connection-quality,alt-svc], X-Frame-Options[DENY], X-XSS-
Protection[0]


Detected Plugins:

[ Cookies ]

        Display the names of cookies in the HTTP headers. The

        values are not returned to save on space.


        String       : fr

        String       : sb


[ HTML5 ]

        HTML version 5, detected by the doctype declaration



[ HttpOnly ]
```

```
        If the HttpOnly flag is included in the HTTP set-cookie
        response header and the browser supports it then the cookie
        cannot be accessed through client side script - More Info:
        http://en.wikipedia.org/wiki/HTTP_cookie

        String       : fr,sb

[ Meta-Refresh-Redirect ]
        Meta refresh tag is a deprecated URL element that can be
        used to optionally wait x seconds before reloading the
        current page or loading a new page. More info:
        https://secure.wikimedia.org/wikipedia/en/wiki/Meta_refresh

        String       : /?_rdc=1&_rdr&_fb_noscript=1

[ PasswordField ]
        find password fields

        String       : pass (from field name)

[ Script ]
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       : application/ld+json,text/javascript

[ Strict-Transport-Security ]
        Strict-Transport-Security is an HTTP header that restricts
        a web browser from accessing a website without the security
        of the HTTPS protocol.

        String       : max-age=15552000; preload

[ UncommonHeaders ]
```

```
	Uncommon HTTP server headers. The blacklist includes all
	the standard headers and many non standard but common ones.
	Interesting but fairly common headers should have their own
	plugins, eg. x-powered-by, server and x-aspnet-version.
	Info about headers can be found at www.http-stats.com

	String       : reporting-endpoints,report-to,content-security-policy-report-only,content-security-policy,document-policy,permissions-policy,cross-origin-resource-policy,cross-origin-opener-policy,x-content-type-options,x-fb-debug,x-fb-connection-quality,alt-svc (from headers)

[ X-Frame-Options ]
	This plugin retrieves the X-Frame-Options value from the
	HTTP header. - More Info:
	http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
	aspx

	String       : DENY

[ X-XSS-Protection ]
	This plugin retrieves the X-XSS-Protection value from the
	HTTP header. - More Info:
	http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
	aspx

	String       : 0

HTTP Headers:
	HTTP/1.1 200 OK
	Vary: Accept-Encoding
	Content-Encoding: gzip
	Set-Cookie: fr=0WvkSR9EqlKfwmT3y..BnKgjQ..AAA.0.0.BnKgjQ.AWX0WIuA3pA; expires=Mon, 03-Feb-2025 12:00:16 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly
	Set-Cookie: sb=0AgqZ4rhfLquxeP7fYx0ZEO6; expires=Wed, 10-Dec-2025 12:00:16 GMT; Max-Age=34560000; path=/; domain=.facebook.com; secure; httponly
```

reporting-endpoints: coop_report="https://web.facebook.com/browser_reporting/coop/?minimize=0", default="https://web.facebook.com/ajax/browser_error_reports/?device_level=unknown&brsid=7433763825315766298", permissions_policy="https://web.facebook.com/ajax/browser_error_reports/"

report-to: {"max_age":2592000,"endpoints":[{"url":"https:\/\/web.facebook.com\/browser_reporting\/coop\/?minimize=0"}],"group":"coop_report","include_subdomains":true}, {"max_age":259200,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/?device_level=unknown&brsid=7433763825315766298"}]}, {"max_age":21600,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/"}],"group":"permissions_policy"}

content-security-policy-report-only: default-src data: blob: 'self' https://*.fbsbx.com 'unsafe-inline' *.facebook.com *.fbcdn.net 'unsafe-eval';script-src 'report-sample' *.facebook.com *.fbcdn.net *.facebook.net 127.0.0.1:* 'unsafe-inline' blob: data: 'self' connect.facebook.net 'unsafe-eval' https://*.google-analytics.com *.google.com;style-src *.fbcdn.net data: *.facebook.com 'unsafe-inline' https://fonts.googleapis.com;connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com https://*.google-analytics.com;font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com https://fonts.gstatic.com;img-src *.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com fbcdn.net connect.facebook.net *.carriersignal.info blob: android-webview-video-poster: *.whatsapp.net *.fb.com *.oculuscdn.com *.tenor.co *.tenor.com *.giphy.com https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net https://*.google-analytics.com;media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data: *.tenor.co *.tenor.com https://*.giphy.com;frame-src *.facebook.com *.fbsbx.com fbsbx.com data: www.instagram.com *.fbcdn.net https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net https://www.google.com https://td.doubleclick.net *.google.com *.doubleclick.net;worker-src blob: *.facebook.com data:;report-uri https://web.facebook.com/csp/reporting/?minimize=0;

content-security-policy: default-src data: blob: 'self' https://*.fbsbx.com 'unsafe-inline' *.facebook.com *.fbcdn.net 'unsafe-eval';script-src 'report-sample' *.facebook.com *.fbcdn.net *.facebook.net 127.0.0.1:* 'unsafe-inline' blob: data: 'self' connect.facebook.net 'unsafe-eval' https://*.google-analytics.com *.google.com;style-src *.fbcdn.net data: *.facebook.com 'unsafe-inline' https://fonts.googleapis.com;connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com https://*.google-analytics.com;font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com https://fonts.gstatic.com;img-src *.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com fbcdn.net connect.facebook.net *.carriersignal.info blob: android-webview-video-poster: *.whatsapp.net *.fb.com *.oculuscdn.com *.tenor.co *.tenor.com *.giphy.com https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net https://*.google-analytics.com;media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data: *.tenor.co *.tenor.com https://*.giphy.com;frame-src *.facebook.com *.fbsbx.com fbsbx.com data: www.instagram.com *.fbcdn.net https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net

```
https://www.google.com https://td.doubleclick.net *.google.com *.doubleclick.net;worker-src blob: *.facebook.com data:;block-all-mixed-content;upgrade-insecure-requests;

    document-policy: force-load-at-top

    permissions-policy: accelerometer=(), attribution-reporting=(self), autoplay=(), bluetooth=(), browsing-topics=(self), camera=(self), ch-device-memory=(), ch-downlink=(), ch-dpr=(), ch-ect=(), ch-rtt=(), ch-save-data=(), ch-ua-arch=(), ch-ua-bitness=(), ch-viewport-height=(), ch-viewport-width=(), ch-width=(), clipboard-read=(self), clipboard-write=(self), compute-pressure=(), display-capture=(self), encrypted-media=(self), fullscreen=(self), gamepad=*, geolocation=(self), gyroscope=(), hid=(), idle-detection=(), interest-cohort=(self), keyboard-map=(), local-fonts=(), magnetometer=(), microphone=(self), midi=(), otp-credentials=(), payment=(), picture-in-picture=(self), private-state-token-issuance=(), publickey-credentials-get=(self), screen-wake-lock=(), serial=(), shared-storage=(), shared-storage-select-url=(), private-state-token-redemption=(), usb=(), unload=(self), window-management=(), xr-spatial-tracking=(self);report-to="permissions_policy"

    cross-origin-resource-policy: same-origin

    cross-origin-opener-policy: unsafe-none

    Pragma: no-cache

    Cache-Control: private, no-cache, no-store, must-revalidate

    Expires: Sat, 01 Jan 2000 00:00:00 GMT

    X-Content-Type-Options: nosniff

    X-XSS-Protection: 0

    X-Frame-Options: DENY

    Strict-Transport-Security: max-age=15552000; preload

    Content-Type: text/html; charset="utf-8"

    X-FB-Debug: 8mf7+K2Kuxo5VUPwrTYeG7ZAJgWPxnw9xTlsmUoReCbRhXRP2IrddOQKAH6bNtq95PpEa7QfI/gT12XmnVsqyA==

    Date: Tue, 05 Nov 2024 12:00:16 GMT

    X-FB-Connection-Quality: EXCELLENT; q=0.9, rtt=15, rtx=0, c=10, mss=1392, tbw=2524, tp=-1, tpl=-1, uplat=207, ullat=0

    Alt-Svc: h3=":443"; ma=86400

    Transfer-Encoding: chunked

    Connection: close


WhatWeb report for https://web.facebook.com/?_rdc=1&_rdr&_fb_noscript=1

Status    : 200 OK

Title     : <None>

IP        : <Unknown>

Country   : <Unknown>
```

```
Summary   : Cookies[fr,noscript,sb], HTML5, HttpOnly[fr,sb], PasswordField[pass],
Script[application/ld+json,text/javascript], Strict-Transport-Security[max-age=15552000; preload],
UncommonHeaders[reporting-endpoints,report-to,content-security-policy-report-only,content-security-
policy,document-policy,permissions-policy,cross-origin-resource-policy,cross-origin-opener-policy,x-
content-type-options,x-fb-debug,x-fb-connection-quality,alt-svc], X-Frame-Options[DENY], X-XSS-
Protection[0]


Detected Plugins:
[ Cookies ]
	Display the names of cookies in the HTTP headers. The
	values are not returned to save on space.


	String       : fr
	String       : noscript
	String       : sb

[ HTML5 ]
	HTML version 5, detected by the doctype declaration



[ HttpOnly ]
	If the HttpOnly flag is included in the HTTP set-cookie
	response header and the browser supports it then the cookie
	cannot be accessed through client side script - More Info:
	http://en.wikipedia.org/wiki/HTTP_cookie


	String       : fr,sb

[ PasswordField ]
	find password fields


	String       : pass (from field name)

[ Script ]
```

```
        This plugin detects instances of script HTML elements and
        returns the script language/type.

        String       : application/ld+json,text/javascript

[ Strict-Transport-Security ]
        Strict-Transport-Security is an HTTP header that restricts
        a web browser from accessing a website without the security
        of the HTTPS protocol.

        String       : max-age=15552000; preload

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : reporting-endpoints,report-to,content-security-policy-report-only,content-security-policy,document-policy,permissions-policy,cross-origin-resource-policy,cross-origin-opener-policy,x-content-type-options,x-fb-debug,x-fb-connection-quality,alt-svc (from headers)

[ X-Frame-Options ]
        This plugin retrieves the X-Frame-Options value from the
        HTTP header. - More Info:
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String       : DENY

[ X-XSS-Protection ]
        This plugin retrieves the X-XSS-Protection value from the
        HTTP header. - More Info:
```

```
        http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.
        aspx

        String      : 0

HTTP Headers:
        HTTP/1.1 200 OK
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Set-Cookie: fr=09rB0ndQYtabCMws3..BnKgjU..AAA.0.0.BnKgjU.AWVML7ceENA; expires=Mon, 03-
Feb-2025 12:00:20 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly
        Set-Cookie: noscript=1; path=/; domain=.facebook.com; secure
        Set-Cookie: sb=1AgqZymh_nGa91XjeYOt_r7r; expires=Wed, 10-Dec-2025 12:00:20 GMT; Max-
Age=34560000; path=/; domain=.facebook.com; secure; httponly
        reporting-endpoints:
coop_report="https://web.facebook.com/browser_reporting/coop/?minimize=0",
default="https://web.facebook.com/ajax/browser_error_reports/?device_level=unknown&brsid=7433
763843639071437", permissions_policy="https://web.facebook.com/ajax/browser_error_reports/"
        report-to:
{"max_age":2592000,"endpoints":[{"url":"https:\/\/web.facebook.com\/browser_reporting\/coop\/?mi
nimize=0"}],"group":"coop_report","include_subdomains":true},
{"max_age":259200,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/?
device_level=unknown&brsid=7433763843639071437"}]},
{"max_age":21600,"endpoints":[{"url":"https:\/\/web.facebook.com\/ajax\/browser_error_reports\/"}]
,"group":"permissions_policy"}
        content-security-policy-report-only: default-src data: blob: 'self' https://*.fbsbx.com 'unsafe-inline'
*.facebook.com *.fbcdn.net 'unsafe-eval';script-src 'report-sample' *.facebook.com *.fbcdn.net
*.facebook.net 127.0.0.1:* 'unsafe-inline' blob: data: 'self' connect.facebook.net 'unsafe-eval'
https://*.google-analytics.com *.google.com;style-src *.fbcdn.net data: *.facebook.com 'unsafe-inline'
https://fonts.googleapis.com;connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net
wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com
ws://localhost:* blob: *.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com
wss://edge-chat.facebook.com wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/
v.whatsapp.net *.fbsbx.com *.fb.com https://*.google-analytics.com;font-src data: *.facebook.com
*.fbcdn.net *.fbsbx.com https://fonts.gstatic.com;img-src *.fbcdn.net *.facebook.com data:
https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com fbcdn.net connect.facebook.net
*.carriersignal.info blob: android-webview-video-poster: *.whatsapp.net *.fb.com *.oculuscdn.com
*.tenor.co *.tenor.com *.giphy.com https://paywithmybank.com/ https://*.paywithmybank.com/
https://www.googleadservices.com https://googleads.g.doubleclick.net https://*.google-
analytics.com;media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com
*.facebook.com data: *.tenor.co *.tenor.com https://*.giphy.com;frame-src *.facebook.com
*.fbsbx.com fbsbx.com data: www.instagram.com *.fbcdn.net https://paywithmybank.com/
https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net
```

https://www.google.com https://td.doubleclick.net *.google.com *.doubleclick.net;worker-src blob: *.facebook.com data:;report-uri https://web.facebook.com/csp/reporting/?minimize=0;

content-security-policy: default-src data: blob: 'self' https://*.fbsbx.com 'unsafe-inline' *.facebook.com *.fbcdn.net 'unsafe-eval';script-src 'report-sample' *.facebook.com *.fbcdn.net *.facebook.net 127.0.0.1:* 'unsafe-inline' blob: data: 'self' connect.facebook.net 'unsafe-eval' https://*.google-analytics.com *.google.com;style-src *.fbcdn.net data: *.facebook.com 'unsafe-inline' https://fonts.googleapis.com;connect-src *.facebook.com facebook.com *.fbcdn.net *.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'self' http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net *.fbsbx.com *.fb.com https://*.google-analytics.com;font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com https://fonts.gstatic.com;img-src *.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com fbcdn.net connect.facebook.net *.carriersignal.info blob: android-webview-video-poster: *.whatsapp.net *.fb.com *.oculuscdn.com *.tenor.co *.tenor.com *.giphy.com https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net https://*.google-analytics.com;media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data: *.tenor.co *.tenor.com https://*.giphy.com;frame-src *.facebook.com *.fbsbx.com fbsbx.com data: www.instagram.com *.fbcdn.net https://paywithmybank.com/ https://*.paywithmybank.com/ https://www.googleadservices.com https://googleads.g.doubleclick.net https://www.google.com https://td.doubleclick.net *.google.com *.doubleclick.net;worker-src blob: *.facebook.com data:;block-all-mixed-content;upgrade-insecure-requests;

document-policy: force-load-at-top

permissions-policy: accelerometer=(), attribution-reporting=(self), autoplay=(), bluetooth=(), browsing-topics=(self), camera=(self), ch-device-memory=(), ch-downlink=(), ch-dpr=(), ch-ect=(), ch-rtt=(), ch-save-data=(), ch-ua-arch=(), ch-ua-bitness=(), ch-viewport-height=(), ch-viewport-width=(), ch-width=(), clipboard-read=(self), clipboard-write=(self), compute-pressure=(), display-capture=(self), encrypted-media=(self), fullscreen=(self), gamepad=*, geolocation=(self), gyroscope=(), hid=(), idle-detection=(), interest-cohort=(self), keyboard-map=(), local-fonts=(), magnetometer=(), microphone=(self), midi=(), otp-credentials=(), payment=(), picture-in-picture=(self), private-state-token-issuance=(), publickey-credentials-get=(self), screen-wake-lock=(), serial=(), shared-storage=(), shared-storage-select-url=(), private-state-token-redemption=(), usb=(), unload=(self), window-management=(), xr-spatial-tracking=(self);report-to="permissions_policy"

cross-origin-resource-policy: same-origin

cross-origin-opener-policy: unsafe-none

Pragma: no-cache

Cache-Control: private, no-cache, no-store, must-revalidate

Expires: Sat, 01 Jan 2000 00:00:00 GMT

X-Content-Type-Options: nosniff

X-XSS-Protection: 0

X-Frame-Options: DENY

Strict-Transport-Security: max-age=15552000; preload

Content-Type: text/html; charset="utf-8"

```
    X-FB-Debug: q57WJhf9FXh5f+iLoR0+mpplZZLLifrC2XgMHU5Il/epEWLjqG1XUUAganAW5YYdAA3pgjeqLrLkn7e4ujOE6A==

    Date: Tue, 05 Nov 2024 12:00:20 GMT

    X-FB-Connection-Quality: EXCELLENT; q=0.9, rtt=21, rtx=0, c=10, mss=1392, tbw=2524, tp=-1, tpl=-1, uplat=216, ullat=0

    Alt-Svc: h3=":443"; ma=86400

    Transfer-Encoding: chunked

    Connection: close
```

INT302: Kali Linux Tools and System Security – Lab 3: Subdomain Hunting

Exercise 1:

Run the sublist3r command for the following domains:

- **github.com**

[-] Total Unique Subdomains Found: 95

```
www.github.com

atom-installer.github.com

branch.github.com

brandguide.github.com

camo.github.com

central.github.com

cla.github.com

classroom.github.com

cloud.github.com

f.cloud.github.com

codespaces.github.com

codespaces-dev.github.com

codespaces-ppe.github.com

communication.github.com

www.communication.github.com

m.communication.github.com

res.communication.github.com

t.communication.github.com
```

community.github.com

docs.github.com

docs-front-door.github.com

dodgeball.github.com

edu.github.com

education.github.com

emails.github.com

enterprise.github.com

support.enterprise.github.com

www.support.enterprise.github.com

examregistration.github.com

examregistration-api.github.com

examregistration-uat.github.com

examregistration-uat-api.github.com

fast.github.com

garage.github.com

gist.github.com

graphql.github.com

www.graphql.github.com

graphql-stage.github.com

www.graphql-stage.github.com

help.github.com

helpnext.github.com

hq.github.com

vpn-ca.iad.github.com

id.github.com

import.github.com

import2.github.com

importer2.github.com

jira.github.com

www.jira.github.com

jobs.github.com

lab.github.com

lab-sandbox.github.com

learn.github.com

mac-installer.github.com

maintainers.github.com

www.maintainers.github.com

octostatus-production.github.com

offer.github.com

partnerportal.github.com

www.partnerportal.github.com

pkg.github.com

porter.github.com

porter2.github.com

proxima-review-lab.github.com

raw.github.com

registry.github.com

render.github.com

render-lab.github.com

www.render-lab.github.com

review-lab.github.com

octocaptcha.review-lab.github.com

rs.github.com

schrauger.github.com

api.security.github.com

www.api.security.github.com

skyline.github.com

www.skyline.github.com

slack.github.com

smtp.github.com

www.smtp.github.com

staging-lab.github.com

api.stars.github.com

www.api.stars.github.com

status.github.com

stg.github.com

styleguide.github.com

ws.support.github.com

www.ws.support.github.com

talks.github.com

visualstudio.github.com

www.visualstudio.github.com

vscode-auth.github.com

workspaces.github.com

workspaces-dev.github.com

workspaces-ppe.github.com

- **google.com**

[-] Total Unique Subdomains Found: 97

www.google.com

accounts.google.com

freezone.accounts.google.com

adwords.google.com

qa.adz.google.com

answers.google.com

apps-secure-data-connector.google.com

audioads.google.com

checkout.google.com

mtv-da-1.ad.corp.google.com

ads-compare.eem.corp.google.com

da.ext.corp.google.com

m.guts.corp.google.com

m.gutsdev.corp.google.com

login.corp.google.com

mtv-da.corp.google.com

mygeist.corp.google.com

mygeist2010.corp.google.com

proxyconfig.corp.google.com

reseed.corp.google.com

twdsalesgsa.twd.corp.google.com

uberproxy.corp.google.com

uberproxy-nocert.corp.google.com

uberproxy-san.corp.google.com

ext.google.com

cag.ext.google.com

cod.ext.google.com

da.ext.google.com

eggroll.ext.google.com

fra-da.ext.google.com

glass.ext.google.com

glass-eur.ext.google.com

glass-mtv.ext.google.com

glass-twd.ext.google.com

hot-da.ext.google.com

hyd-da.ext.google.com

ice.ext.google.com

meeting.ext.google.com

mtv-da.ext.google.com

soaproxyprod01.ext.google.com

soaproxytest01.ext.google.com

spdy-proxy.ext.google.com

spdy-proxy-debug.ext.google.com

twd-da.ext.google.com

flexpack.google.com

www.flexpack.google.com

accounts.flexpack.google.com

gaiastaging.flexpack.google.com

mail.flexpack.google.com

plus.flexpack.google.com

search.flexpack.google.com

freezone.google.com

www.freezone.google.com

accounts.freezone.google.com

gaiastaging.freezone.google.com

mail.freezone.google.com

news.freezone.google.com

plus.freezone.google.com

search.freezone.google.com

gmail.google.com

hosted-id.google.com

jmt0.google.com

aspmx.l.google.com

alt1.aspmx.l.google.com

alt2.aspmx.l.google.com

alt3.aspmx.l.google.com

alt4.aspmx.l.google.com

gmail-smtp-in.l.google.com

alt1.gmail-smtp-in.l.google.com

alt2.gmail-smtp-in.l.google.com

alt3.gmail-smtp-in.l.google.com

alt4.gmail-smtp-in.l.google.com

gmr-smtp-in.l.google.com

alt1.gmr-smtp-in.l.google.com

alt2.gmr-smtp-in.l.google.com

alt3.gmr-smtp-in.l.google.com

alt4.gmr-smtp-in.l.google.com

vp.video.l.google.com

m.google.com

freezone.m.google.com

mail.google.com

freezone.mail.google.com

misc.google.com

misc-sni.google.com

mtalk.google.com

mx.google.com

ics.prod.google.com

sandbox.google.com

cert-test.sandbox.google.com

```
ecc-test.sandbox.google.com
services.google.com
talk.google.com
upload.google.com
dg.video.google.com
upload.video.google.com
wifi.google.com
onex.wifi.google.com
```

Step 2: Directory Discovery Using dirb

Exercise 2:

Perform a directory discovery scan on the following targets:

- **http://example.com**

```
└─$ dirb http://example.com
-----------------
DIRB v2.22
By The Dark Raver
-----------------
START_TIME: Tue Nov  5 07:11:24 2024
URL_BASE: http://example.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----------------
```

- **http://example.org**

```
–$ dirb http://example.org
-----------------
DIRB v2.22
By The Dark Raver
-----------------
START_TIME: Tue Nov  5 07:12:40 2024
URL_BASE: http://example.org/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

Step 3: Information Gathering Using theHarvester

Exercise 3:
Use theHarvester to gather information on the following domain:
- example.com

INVALID SOURCE