**Test performed on:**

Website Security Scan Report

──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://facebook.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( W00f! )

\ \_\_\_\_/

,, \_\_ 404 Hack Not Found

|`-.\_\_ / / \_\_ \_\_

/" \_/ /\_/ \ \ / /

\*===\* / \ \\_/ / 405 Not Allowed

/ )\_\_// \ /

/| / /---` 403 Forbidden

\\/` \ | / \_ \

`\ /\_\\\_ 502 Bad Gateway / / \ \ 500 Internal Error

`\_\_\_\_\_``-` /\_/ \\_\

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://facebook.com

[+] Generic Detection results:

[\*] The site https://facebook.com seems to be behind a WAF or some sort of security solution

[~] Reason: The server returns a different response code when an attack string is used.

Normal response code is "400", while the response code to cross-site scripting attack is "200"

[~] Number of requests: 5

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Vary: Accept-Encoding

Content-Encoding: br

Set-Cookie: fr=0TH8Oh450yQ25acv3..BnYSzj..AAA.0.0.BnYSzj.AWUrrRJMqaM; expires=Mon, 17-Mar-2025 07:48:51 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly, sb=4yxhZ2gCNOkgxFwonMGAJ2xF; expires=Wed, 21-Jan-2026 07:48:51 GMT; Max-Age=34560000; path=/; domain=.facebook.com; secure; httponly

reporting-endpoints: coop\_report="https://www.facebook.com/browser\_reporting/coop/?minimize=0", default="https://www.facebook.com/ajax/browser\_error\_reports/?device\_level=unknown&brsid=7449284613904369131", permissions\_policy="https://www.facebook.com/ajax/browser\_error\_reports/"

report-to: {"max\_age":2592000,"endpoints":[{"url":"https:\/\/www.facebook.com\/browser\_reporting\/coop\/?minimize=0"}],"group":"coop\_report","include\_subdomains":true}, {"max\_age":259200,"endpoints":[{"url":"https:\/\/www.facebook.com\/ajax\/browser\_error\_reports\/?device\_level=unknown&brsid=7449284613904369131"}]}, {"max\_age":3600,"endpoints":[{"url":"https:\/\/www.facebook.com\/ajax\/browser\_error\_reports\/?device\_level=unknown&brsid=7449284613904369131"}],"group":"network-errors"}, {"max\_age":21600,"endpoints":[{"url":"https:\/\/www.facebook.com\/ajax\/browser\_error\_reports\/"}],"group":"permissions\_policy"}

content-security-policy: default-src data: blob: 'self' https://\*.fbsbx.com \*.facebook.com \*.fbcdn.net;script-src \*.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

nel: {"report\_to":"network-errors","max\_age":3600,"failure\_fraction":0.01}

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

origin-agent-cluster: ?1

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

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

X-FB-Debug: zX/wzzSHiZwGvLTfgKy6BqgiUAu4+1jqV+vhvjVt+MLVq2TBMiAJrkqNG3RhoM9Nj38/md4EyFFTffbwsn+4vA==

Date: Tue, 17 Dec 2024 07:48:51 GMT

X-FB-Connection-Quality: GOOD; q=0.7, rtt=73, rtx=0, c=10, mss=1268, tbw=3425, tp=-1, tpl=-1, uplat=268, ullat=0

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

Transfer-Encoding: chunked

Connection: keep-alive

[+] All important security headers are present.

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 02:48 EST

Nmap scan report for facebook.com (163.70.139.35)

Host is up (0.078s latency).

Other addresses for facebook.com (not scanned): 2a03:2880:f34f:1:face:b00c:0:25de

rDNS record for 163.70.139.35: edge-star-mini-shv-02-tir3.facebook.com

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http proxygen-bolt

443/tcp open ssl/https

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.91%I=7%D=12/17%Time=67612CF0%P=x86\_64-pc-linux-gnu%r(Get

SF:Request,B3,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nLocation:\x20ht

SF:tps:///\r\nContent-Type:\x20text/plain\r\nServer:\x20proxygen-bolt\r\nD

SF:ate:\x20Tue,\x2017\x20Dec\x202024\x2007:49:05\x20GMT\r\nConnection:\x20

SF:close\r\nContent-Length:\x200\r\n\r\n")%r(HTTPOptions,B3,"HTTP/1\.1\x20

SF:301\x20Moved\x20Permanently\r\nLocation:\x20https:///\r\nContent-Type:\

SF:x20text/plain\r\nServer:\x20proxygen-bolt\r\nDate:\x20Tue,\x2017\x20Dec

SF:\x202024\x2007:49:05\x20GMT\r\nConnection:\x20close\r\nContent-Length:\

SF:x200\r\n\r\n")%r(RTSPRequest,C21,"HTTP/1\.1\x20400\x20Bad\x20Request\r\

SF:nContent-Type:\x20text/html;\x20charset=utf-8\r\nDate:\x20Tue,\x2017\x2

SF:0Dec\x202024\x2007:49:05\x20GMT\r\nConnection:\x20close\r\nContent-Leng

SF:th:\x202959\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en\"\x20id=\"fac

SF:ebook\">\n\x20\x20<head>\n\x20\x20\x20\x20<title>Facebook\x20\|\x20Erro

SF:r</title>\n\x20\x20\x20\x20<meta\x20charset=\"utf-8\">\n\x20\x20\x20\x2

SF:0<meta\x20http-equiv=\"cache-control\"\x20content=\"no-cache\">\n\x20\x

SF:20\x20\x20<meta\x20http-equiv=\"cache-control\"\x20content=\"no-store\"

SF:>\n\x20\x20\x20\x20<meta\x20http-equiv=\"cache-control\"\x20content=\"m

SF:ax-age=0\">\n\x20\x20\x20\x20<meta\x20http-equiv=\"expires\"\x20content

SF:=\"-1\">\n\x20\x20\x20\x20<meta\x20http-equiv=\"pragma\"\x20content=\"n

SF:o-cache\">\n\x20\x20\x20\x20<meta\x20name=\"robots\"\x20content=\"noind

SF:ex,nofollow\">\n\x20\x20\x20\x20<style>\n\x20\x20\x20\x20\x20\x20html,\

SF:x20body\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#141823;\n\x20\

SF:x20\x20\x20\x20\x20\x20\x20background-color:\x20#e9eaed;\n\x20\x20\x20\

SF:x20\x20\x20\x20\x20font-family:\x20Helvetica,\x20Lucida\x20Grande,\x20A

SF:rial,\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

SF:\x20\x20\x20\x20\x20Tahoma,\x20Verdana,\x20sans-serif;\n\x20\x20\x20\x2

SF:0\x20\x20\x20\x20margin:\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20padding

SF::\x200;\n\x20\x20\x20\x20\x20\x20\x20\x20text-align:\x20center;\n\x20\x

SF:20\x20\x20\x20\x20}\n\n\x20\x20\x20\x20\x20\x20#header\x20{\n\x20\x20\x

SF:20\x20\x20\x20\x20\x20height:\x2030px;\n\x20\x20\x20\x20\x20\x20\x20\x2

SF:0");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port443-TCP:V=7.91%T=SSL%I=7%D=12/17%Time=67612CF6%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,16A1,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nVary:\x20Acc

SF:ept-Encoding\r\nPragma:\x20no-cache\r\nCache-Control:\x20private,\x20no

SF:-cache,\x20no-store,\x20must-revalidate\r\nExpires:\x20Sat,\x2001\x20Ja

SF:n\x202000\x2000:00:00\x20GMT\r\ncontent-security-policy:\x20default-src

SF:\x20'self'\x20data:\x20blob:;script-src\x20'nonce-VEORUFFw'\x20blob:\x2

SF:0data:\x20'self'\x20\\*\.facebook\.com\x20\\*\.fbcdn\.net\x20\\*\.facebook

SF:\.net\x20127\.0\.0\.1:\\*\x20https://\\*\.google-analytics\.com\x20\\*\.go

SF:ogle\.com;style-src\x20data:\x20blob:\x20'unsafe-inline';connect-src\x2

SF:0blob:\x20'self'\x20\\*\.facebook\.com\x20facebook\.com\x20\\*\.fbcdn\.ne

SF:t\x20\\*\.facebook\.net\x20wss://\\*\.facebook\.com:\\*\x20wss://\\*\.whats

SF:app\.com:\\*\x20wss://\\*\.fbcdn\.net\x20attachment\.fbsbx\.com\x20ws://l

SF:ocalhost:\\*\x20\\*\.cdninstagram\.com\x20https://\\*\.google-analytics\.c

SF:om;img-src\x20'self'\x20data:\x20blob:\x20https://\\*\.google-analytics\

SF:.com;block-all-mixed-content;upgrade-insecure-requests;\r\nreporting-en

SF:dpoints:\x20coop\_report=\"https://www\.facebook\.com/browser\_reporting/

SF:coop/\?minimize=0\"\r\nreport-to:\x20{\"max\_age\":2592000,\"endpoints\"

SF::\[{\"url\":\"http")%r(HTTPOptions,1617,"HTTP/1\.1\x20500\x20Internal\x

SF:20Server\x20Error\r\nVary:\x20Accept-Encoding\r\nerror-mid:\x20c7c8b69f

SF:e9b6faa81409f203767d7880\r\nPragma:\x20no-cache\r\nCache-Control:\x20pr

SF:ivate,\x20no-cache,\x20no-store,\x20must-revalidate\r\nExpires:\x20Sat,

SF:\x2001\x20Jan\x202000\x2000:00:00\x20GMT\r\ncontent-security-policy:\x2

SF:0default-src\x20'self'\x20data:\x20blob:;script-src\x20'nonce-3qum1oaq'

SF:\x20blob:\x20data:\x20'self'\x20\\*\.facebook\.com\x20\\*\.fbcdn\.net\x20

SF:\\*\.facebook\.net\x20127\.0\.0\.1:\\*\x20https://\\*\.google-analytics\.c

SF:om\x20\\*\.google\.com;style-src\x20data:\x20blob:\x20'unsafe-inline';co

SF:nnect-src\x20blob:\x20'self'\x20\\*\.facebook\.com\x20facebook\.com\x20\

SF:\*\.fbcdn\.net\x20\\*\.facebook\.net\x20wss://\\*\.facebook\.com:\\*\x20wss

SF:://\\*\.whatsapp\.com:\\*\x20wss://\\*\.fbcdn\.net\x20attachment\.fbsbx\.c

SF:om\x20ws://localhost:\\*\x20\\*\.cdninstagram\.com\x20https://\\*\.google-

SF:analytics\.com;img-src\x20'self'\x20data:\x20blob:\x20https://\\*\.googl

SF:e-analytics\.com;block-all-mixed-content;upgrade-insecure-requests;\r\n

SF:X-Frame-Options:\x20DENY\r\nX-Content-Type-Options:\x20nosniff\r\nX-XSS

SF:-Protection:\x200\r\nreporting-endpoints");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 38.76 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website is relatively safe with no critical issues detected.

[+] Keep monitoring and maintaining security configurations.

------------------------------

Scan Completed!

─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://snapchat.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://snapchat.com

[+] Generic Detection results:

[\*] The site https://snapchat.com seems to be behind a WAF or some sort of security solution

[~] Reason: The server returns a different response code when an attack string is used.

Normal response code is "200", while the response code to cross-site scripting attack is "403"

[~] Number of requests: 5

[+] Checking HTTP Headers...

Security Headers:

------------------------------

content-type: text/html; charset=UTF-8

Content-Length: 134

via: 1.1 google

date: Tue, 17 Dec 2024 07:49:11 GMT

Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

[!] Missing Security Headers:

- Content-Security-Policy

- Strict-Transport-Security

- X-Frame-Options

- X-XSS-Protection

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 02:49 EST

Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 4.70% done; ETC: 02:49 (0:00:41 remaining)

Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 4.95% done; ETC: 02:49 (0:00:38 remaining)

Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 9.15% done; ETC: 02:49 (0:00:20 remaining)

Nmap scan report for snapchat.com (34.149.46.130)

Host is up (0.067s latency).

rDNS record for 34.149.46.130: 130.46.149.34.bc.googleusercontent.com

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http

443/tcp open ssl/https API Gateway

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.91%I=7%D=12/17%Time=67612D04%P=x86\_64-pc-linux-gnu%r(Get

SF:Request,C0,"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nCache-Control:\

SF:x20private\r\nLocation:\x20https://34\.149\.46\.130:443/\r\nContent-Len

SF:gth:\x200\r\nDate:\x20Tue,\x2017\x20Dec\x202024\x2007:49:25\x20GMT\r\nC

SF:ontent-Type:\x20text/html;\x20charset=UTF-8\r\n\r\n")%r(HTTPOptions,C0,

SF:"HTTP/1\.0\x20301\x20Moved\x20Permanently\r\nCache-Control:\x20private\

SF:r\nLocation:\x20https://34\.149\.46\.130:443/\r\nContent-Length:\x200\r

SF:\nDate:\x20Tue,\x2017\x20Dec\x202024\x2007:49:25\x20GMT\r\nContent-Type

SF::\x20text/html;\x20charset=UTF-8\r\n\r\n")%r(RTSPRequest,1AD,"HTTP/1\.0

SF:\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/html;\x20charset=UTF

SF:-8\r\nReferrer-Policy:\x20no-referrer\r\nContent-Length:\x20273\r\nDate

SF::\x20Tue,\x2017\x20Dec\x202024\x2007:49:26\x20GMT\r\n\r\n\n<html><head>

SF:\n<meta\x20http-equiv=\"content-type\"\x20content=\"text/html;charset=u

SF:tf-8\">\n<title>400\x20Bad\x20Request</title>\n</head>\n<body\x20text=#

SF:000000\x20bgcolor=#ffffff>\n<h1>Error:\x20Bad\x20Request</h1>\n<h2>Your

SF:\x20client\x20has\x20issued\x20a\x20malformed\x20or\x20illegal\x20reque

SF:st\.</h2>\n<h2></h2>\n</body></html>\n")%r(FourOhFourRequest,DF,"HTTP/1

SF:\.0\x20301\x20Moved\x20Permanently\r\nCache-Control:\x20private\r\nLoca

SF:tion:\x20https://34\.149\.46\.130:443/nice%20ports%2C/Trinity\.txt\.bak

SF:\r\nContent-Length:\x200\r\nDate:\x20Tue,\x2017\x20Dec\x202024\x2007:49

SF::31\x20GMT\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\n\r\n")%r(

SF:DNSVersionBindReqTCP,B3,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-

SF:Length:\x2054\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nDate:\

SF:x20Tue,\x2017\x20Dec\x202024\x2007:49:41\x20GMT\r\n\r\n<html><title>Err

SF:or\x20400\x20\(Bad\x20Request\)!!1</title></html>")%r(DNSStatusRequestT

SF:CP,B3,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Length:\x2054\r\nC

SF:ontent-Type:\x20text/html;\x20charset=UTF-8\r\nDate:\x20Tue,\x2017\x20D

SF:ec\x202024\x2007:49:42\x20GMT\r\n\r\n<html><title>Error\x20400\x20\(Bad

SF:\x20Request\)!!1</title></html>")%r(Help,1AD,"HTTP/1\.0\x20400\x20Bad\x

SF:20Request\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nReferrer-P

SF:olicy:\x20no-referrer\r\nContent-Length:\x20273\r\nDate:\x20Tue,\x2017\

SF:x20Dec\x202024\x2007:49:42\x20GMT\r\n\r\n\n<html><head>\n<meta\x20http-

SF:equiv=\"content-type\"\x20content=\"text/html;charset=utf-8\">\n<title>

SF:400\x20Bad\x20Request</title>\n</head>\n<body\x20text=#000000\x20bgcolo

SF:r=#ffffff>\n<h1>Error:\x20Bad\x20Request</h1>\n<h2>Your\x20client\x20ha

SF:s\x20issued\x20a\x20malformed\x20or\x20illegal\x20request\.</h2>\n<h2><

SF:/h2>\n</body></html>\n");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port443-TCP:V=7.91%T=SSL%I=7%D=12/17%Time=67612D0A%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,C8,"HTTP/1\.0\x20404\x20Not\x20Found\r\ndate:\x20Tue,\x2

SF:017\x20Dec\x202024\x2007:49:31\x20GMT\r\nserver:\x20API\x20Gateway\r\nv

SF:ia:\x201\.1\x20google\r\nvary:\x20Accept-Encoding\r\nContent-Length:\x2

SF:00\r\nAlt-Svc:\x20h3=\":443\";\x20ma=2592000,h3-29=\":443\";\x20ma=2592

SF:000\r\n\r\n")%r(HTTPOptions,C8,"HTTP/1\.0\x20404\x20Not\x20Found\r\ndat

SF:e:\x20Tue,\x2017\x20Dec\x202024\x2007:49:32\x20GMT\r\nserver:\x20API\x2

SF:0Gateway\r\nvia:\x201\.1\x20google\r\nvary:\x20Accept-Encoding\r\nConte

SF:nt-Length:\x200\r\nAlt-Svc:\x20h3=\":443\";\x20ma=2592000,h3-29=\":443\

SF:";\x20ma=2592000\r\n\r\n")%r(FourOhFourRequest,C8,"HTTP/1\.0\x20404\x20

SF:Not\x20Found\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x2007:49:32\x20GMT\r

SF:\nserver:\x20API\x20Gateway\r\nvia:\x201\.1\x20google\r\nvary:\x20Accep

SF:t-Encoding\r\nContent-Length:\x200\r\nAlt-Svc:\x20h3=\":443\";\x20ma=25

SF:92000,h3-29=\":443\";\x20ma=2592000\r\n\r\n")%r(tor-versions,B3,"HTTP/1

SF:\.0\x20400\x20Bad\x20Request\r\nContent-Length:\x2054\r\nContent-Type:\

SF:x20text/html;\x20charset=UTF-8\r\nDate:\x20Tue,\x2017\x20Dec\x202024\x2

SF:007:49:33\x20GMT\r\n\r\n<html><title>Error\x20400\x20\(Bad\x20Request\)

SF:!!1</title></html>")%r(RTSPRequest,1AD,"HTTP/1\.0\x20400\x20Bad\x20Requ

SF:est\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nReferrer-Policy:

SF:\x20no-referrer\r\nContent-Length:\x20273\r\nDate:\x20Tue,\x2017\x20Dec

SF:\x202024\x2007:49:39\x20GMT\r\n\r\n\n<html><head>\n<meta\x20http-equiv=

SF:\"content-type\"\x20content=\"text/html;charset=utf-8\">\n<title>400\x2

SF:0Bad\x20Request</title>\n</head>\n<body\x20text=#000000\x20bgcolor=#fff

SF:fff>\n<h1>Error:\x20Bad\x20Request</h1>\n<h2>Your\x20client\x20has\x20i

SF:ssued\x20a\x20malformed\x20or\x20illegal\x20request\.</h2>\n<h2></h2>\n

SF:</body></html>\n")%r(DNSVersionBindReqTCP,B3,"HTTP/1\.0\x20400\x20Bad\x

SF:20Request\r\nContent-Length:\x2054\r\nContent-Type:\x20text/html;\x20ch

SF:arset=UTF-8\r\nDate:\x20Tue,\x2017\x20Dec\x202024\x2007:49:44\x20GMT\r\

SF:n\r\n<html><title>Error\x20400\x20\(Bad\x20Request\)!!1</title></html>"

SF:)%r(DNSStatusRequestTCP,B3,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nConte

SF:nt-Length:\x2054\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nDat

SF:e:\x20Tue,\x2017\x20Dec\x202024\x2007:49:45\x20GMT\r\n\r\n<html><title>

SF:Error\x20400\x20\(Bad\x20Request\)!!1</title></html>");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 81.32 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- Missing security headers: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, X-XSS-Protection.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://whatsapp.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( W00f! )

\ \_\_\_\_/

,, \_\_ 404 Hack Not Found

|`-.\_\_ / / \_\_ \_\_

/" \_/ /\_/ \ \ / /

\*===\* / \ \\_/ / 405 Not Allowed

/ )\_\_// \ /

/| / /---` 403 Forbidden

\\/` \ | / \_ \

`\ /\_\\\_ 502 Bad Gateway / / \ \ 500 Internal Error

`\_\_\_\_\_``-` /\_/ \\_\

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://whatsapp.com

[+] Generic Detection results:

[\*] The site https://whatsapp.com seems to be behind a WAF or some sort of security solution

[~] Reason: The server returns a different response code when an attack string is used.

Normal response code is "400", while the response code to cross-site scripting attack is "200"

[~] Number of requests: 5

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Vary: Accept-Encoding

Content-Encoding: br

Set-Cookie: wa\_csrf=VF7cxS3-ImC6vd91CdtH3N; path=/; domain=.whatsapp.com; secure; httponly, wa\_lang\_pref=en; expires=Tue, 24-Dec-2024 07:48:11 GMT; Max-Age=604800; path=/; domain=.whatsapp.com; secure, wa\_ul=30abc9a8-61a7-4da4-89bc-38e3a4f61649; expires=Mon, 17-Mar-2025 07:48:11 GMT; Max-Age=7776000; path=/; domain=.www.whatsapp.com; secure; httponly

reporting-endpoints: coop\_report="https://www.facebook.com/browser\_reporting/coop/?minimize=0", coep\_report="https://www.facebook.com/browser\_reporting/coep/?minimize=0", default="https://www.whatsapp.com/whatsapp\_browser\_error\_reports/?device\_level=unknown", permissions\_policy="https://www.whatsapp.com/whatsapp\_browser\_error\_reports/"

report-to: {"max\_age":2592000,"endpoints":[{"url":"https:\/\/www.facebook.com\/browser\_reporting\/coop\/?minimize=0"}],"group":"coop\_report","include\_subdomains":true}, {"max\_age":86400,"endpoints":[{"url":"https:\/\/www.facebook.com\/browser\_reporting\/coep\/?minimize=0"}],"group":"coep\_report"}, {"max\_age":259200,"endpoints":[{"url":"https:\/\/www.whatsapp.com\/whatsapp\_browser\_error\_reports\/?device\_level=unknown"}]}, {"max\_age":21600,"endpoints":[{"url":"https:\/\/www.whatsapp.com\/whatsapp\_browser\_error\_reports\/"}],"group":"permissions\_policy"}

content-security-policy: default-src 'self' data: blob:;script-src \*.whatsapp.com \*.whatsapp.net \*.facebook.com \*.facebook.net 'nonce-ZQbOGMfR' 'self' data: blob: \*.twitter.com;style-src \*.whatsapp.com \*.whatsapp.net 'unsafe-inline' \*.facebook.com 'self' data: blob:;connect-src \*.whatsapp.com \*.whatsapp.net wss://\*.facebook.com:\* \*.fbcdn.net 'self' data: blob:;font-src \*.whatsapp.com \*.whatsapp.net \*.facebook.com static.xx.fbcdn.net data: https://fonts.gstatic.com;img-src \*.whatsapp.com \*.whatsapp.net \*.facebook.com \*.fbcdn.net static.xx.fbcdn.net 'self' data: blob: \*.ytimg.com \*.twitter.com;media-src \*.fbcdn.net 'self' data: blob:;frame-src \*.facebook.com \*.whatsapp.com 'self' data: blob: https://\*.youtube.com \*.youtube-nocookie.com \*.twitter.com;block-all-mixed-content;upgrade-insecure-requests;

permissions-policy: accelerometer=(), attribution-reporting=(), autoplay=(), bluetooth=(), camera=(), 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=(), clipboard-write=(), compute-pressure=(), display-capture=(), encrypted-media=(), fullscreen=(self), gamepad=(), geolocation=(), gyroscope=(), hid=(), idle-detection=(), interest-cohort=(), keyboard-map=(), local-fonts=(), magnetometer=(), microphone=(), midi=(), otp-credentials=(), payment=(), picture-in-picture=(), private-state-token-issuance=(), publickey-credentials-get=(), screen-wake-lock=(), serial=(), shared-storage=(), shared-storage-select-url=(), private-state-token-redemption=(), usb=(), unload=(self), window-management=(), xr-spatial-tracking=();report-to="permissions\_policy"

cross-origin-resource-policy: same-origin

cross-origin-embedder-policy-report-only: require-corp;report-to="coep\_report"

cross-origin-opener-policy: same-origin-allow-popups

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

origin-agent-cluster: ?1

Strict-Transport-Security: max-age=31536000; preload; includeSubDomains

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

X-FB-Debug: 80PIx9aQxhcG0d8RyB3whBB6Sw0MCBHh2zqTXB9N1WeBI57O2en1o2RvYS/KPrdNCMOVe1ScrCW0f/dHw85IfA==

Date: Tue, 17 Dec 2024 07:48:11 GMT

X-FB-Connection-Quality: GOOD; q=0.7, rtt=74, rtx=0, c=14, mss=1268, tbw=3361, tp=-1, tpl=-1, uplat=468, ullat=0

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

Transfer-Encoding: chunked

Connection: keep-alive

[+] All important security headers are present.

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 02:48 EST

Nmap scan report for whatsapp.com (57.144.159.32)

Host is up (0.081s latency).

Other addresses for whatsapp.com (not scanned): 2a03:2880:f284:1cd:face:b00c:0:167

rDNS record for 57.144.159.32: whatsapp-cdn-shv-04-tir3.fbcdn.net

Not shown: 997 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http proxygen-bolt

443/tcp open ssl/https proxygen-bolt

5222/tcp open ssl/xmpp-client?

3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.91%I=7%D=12/17%Time=67612CCC%P=x86\_64-pc-linux-gnu%r(Get

SF:Request,845,"HTTP/1\.1\x20403\x20Forbidden\r\nContent-Type:\x20text/pla

SF:in\r\nServer:\x20proxygen-bolt\r\nProxy-Status:\x20http\_request\_error;\

SF:x20e\_fb\_configversion=\"AcKguG6peiYmKL4llJHV99Z9B0nglRmuZsFrMuF7cno-t2J

SF:TEDhHNKcda5d1Lg\";\x20e\_clientaddr=\"AcLCml5TaIBlUVUuK-SFPfGXL70kJhqKOq

SF:EAyG2-WavGTNQHfBB3UQnrIWXcVjQ-DVLIrFqlkvEsahk9Lik\";\x20e\_fb\_vipport=\"

SF:AcJoj5Imfw8fju6KekCRiuW79iw\_5IZFGNWzE4xjAEx8fyMtgqPnNskesKo\";\x20e\_fb\_

SF:vipaddr=\"AcK3VpHPJu7tNKAiTYItAeo02\_z0byXy4zu2Ilw7nAgB6DHP6P6rDVIGTsEXu

SF:dS22W7\_d1u7eQ\";\x20e\_fb\_requestsequencenumber=\"AcLtGijfMOkVrs3dqBeWGL

SF:hvmgnstmUmlND42IAgqUpq4zlV-e7-eYy59g\";\x20e\_fb\_requesttime=\"AcJec\_n8r

SF:R1ae6Q75Q9Nk4No5In9fiGp56YflJ0-UKbvJMesN\_Kb7Rpr84HcjwPSOxczAH2kaQ\";\x2

SF:0e\_fb\_builduser=\"AcI39KMgEPYk8\_RMEb8HL7jOEblRD54p-llD\_CBzJRvuMwDAXYO1m

SF:ksXm-FRI2IZVRs\";\x20e\_fb\_httpversion=\"AcLWraGhYi-HQUvOtRgcDLfNHtNhVKN

SF:KvCIzKdcvZuyA1vnlxfk9tZYu6Bw7\";\x20e\_fb\_binaryversion=\"AcJA48OI5DtLvu

SF:u4fuZeRovspOd\_fOsXWAQT2eAWKX1KJw1cExpEdH9TKV3h4q\_m-3Dgzz")%r(HTTPOption

SF:s,845,"HTTP/1\.1\x20403\x20Forbidden\r\nContent-Type:\x20text/plain\r\n

SF:Server:\x20proxygen-bolt\r\nProxy-Status:\x20http\_request\_error;\x20e\_f

SF:b\_configversion=\"AcIId1OodG2rdSVV1G0Pt\_xi1wIB12ZiTDrADW332arsixjZOQaJj

SF:ZjcQ179RQ\";\x20e\_clientaddr=\"AcLKD19AttwJPyLn2XdjD\_4wnRGgYTTeHUTP3Hky

SF:AtEseLpQGzaCByToeSJDlrSGi9mhoRf99CrLOlRS2Ls\";\x20e\_fb\_vipport=\"AcJwlc

SF:T4tHMIuRNaVTG4sw39atrHI68s7JugVVhTKvaust7vDt-VNZhHCBA\";\x20e\_fb\_vipadd

SF:r=\"AcL9yjdNlgMm3YbuXukbppschh0N1yLKosERrp2QnVBi57lv0x05p2YPiF9FG\_JAa\_w

SF:mTn2pAg\";\x20e\_fb\_requestsequencenumber=\"AcL5lfyLFWtDGRq\_pVlPmbM7jkdL

SF:vbSQ-EcROMAkpTAHbc7oeNUdjyq2KA\";\x20e\_fb\_requesttime=\"AcJ8qPRj1z3TFQi

SF:\_vmwSK9fpN3MrMz0LL9s5ejKSG1oRdDqmx0znPpY0CRiFnABOgXps7ThOqg\";\x20e\_fb\_

SF:builduser=\"AcIN2RVW8yLTV4O3Tw7ocg2upWXc4pwgq2aeBRe57K4-PcTeubbLZfNITFj

SF:RHuksvds\";\x20e\_fb\_httpversion=\"AcKL2NIcdaFepiQHxVhw7Bw0l1H\_I2R5Cmvb\_

SF:Iujqqii7D35D9T5RnM3i6yJ\";\x20e\_fb\_binaryversion=\"AcJJ\_M9cdXMzgfQFCqOU

SF:vN72ZsNno5IHGztYM\_XqxHD\_7PaFSjMOkHZ1gVluK6Sr4au46L")%r(RTSPRequest,F6,"

SF:HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/html;\x20ch

SF:arset=utf-8\r\nDate:\x20Tue,\x2017\x20Dec\x202024\x2007:48:29\x20GMT\r\

SF:nConnection:\x20close\r\nContent-Length:\x20101\r\n\r\n<html>\n<head>\n

SF:<title>WhatsApp\x20Error</title>\n</head>\n\n<body>\n<h1>WhatsApp\x20Er

SF:ror</h1>\n</body>\n\n</html>\n");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port443-TCP:V=7.91%T=SSL%I=7%D=12/17%Time=67612CD2%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,5C7,"HTTP/1\.1\x20400\x20default\_vip\_400\r\nContent-Type

SF::\x20text/html;\x20charset=utf-8\r\nAccess-Control-Allow-Origin:\x20\\*\

SF:r\nProxy-Status:\x20proxy\_internal\_response;\x20e\_fb\_responsebytes=\"Ac

SF:L9Y-TymuzrlIuXE3yD448WQqXpHMiOqia2iNAMJs8CV3i\_jJYJYnOobRVT\";\x20e\_fb\_c

SF:onfigversion=\"AcJof0jPIOHE9oZkNwFSqMZ7l\_erhjOmF-JD9nnoMXpjsI-aFSqO0xxX

SF:zDukPQ\";\x20e\_isproxyerr=\"AcJyZd1FBcVrwxOVBBo2fueA1gKhE01hXkqlgTsXDFH

SF:bcO2PfRJTLYIvueRb-A\";\x20e\_clientaddr=\"AcJbQdafo8essCRobBAkfDZXldguev

SF:JpQH0sx6rNGoUChTxMkvKFq-gb0GQ83IA\_1dXnFMlaRFuG-xwTIyo\";\x20e\_fb\_vippor

SF:t=\"AcIDXe5xpi\_4AwVst9-AZDXUjse1RxxtFNn7UEZyALn-kqvoVkpSvpcOUCom\";\x20

SF:e\_fb\_vipaddr=\"AcKL9Ry01iQChMx9hXafgjchytfKmY6f-FcEh7aLZBkNG0dZICfL2RSM

SF:lovx0zItZQVRMO1WvA\";\x20e\_fb\_proxycode=\"AcKXK2Ze2MdVSBvUGZv8pfuMp72S-

SF:6XmiMD89rE6YfmYnnvDFtnojBmuz9j\_\";\x20e\_fb\_requestsequencenumber=\"AcIz

SF:p5Vli1BJL3BkZAdtTNTW0S97rs9z8k6FWZxSIleRvIcDth1I1y26bg\";\x20e\_fb\_reque

SF:sttime=\"AcJXSCOdx9xXg5C-KsHVa8u4oNDoE4YibMumMoNNmFM1BtyuJbC1SBgfxg")%r

SF:(HTTPOptions,5C7,"HTTP/1\.1\x20400\x20default\_vip\_400\r\nContent-Type:\

SF:x20text/html;\x20charset=utf-8\r\nAccess-Control-Allow-Origin:\x20\\*\r\

SF:nProxy-Status:\x20proxy\_internal\_response;\x20e\_fb\_responsebytes=\"AcIB

SF:sndX2ToZIIdribSuInAKxiAzhEZlaFZeabnfsNlqI-8o6SHmwzLL30O3\";\x20e\_fb\_con

SF:figversion=\"AcLcJHZF07LETcdFuXGGBSNnW1O-QSwvOuOE-eTxhYWoUTIVk83Ed5Vuf-

SF:7R5A\";\x20e\_isproxyerr=\"AcLstdYWQCs1yqSVa6GxwgVLh4RZozLi4amKIQYHDHNSj

SF:n20r5dVd2NCg\_N8mg\";\x20e\_clientaddr=\"AcJT199Tt7gm70J1BJ3zZ-yUD\_9CX1WD

SF:hjy1U4IJd2S1bTKKZvD4hY8Vfdn0xi2giXWyyKiMtQ6NStnMGFM\";\x20e\_fb\_vipport=

SF:\"AcLqZv97G9j86N8IzxepptZogkIEM9Z4MMwgXiuzmCNFMR2qLFN9yo\_nMwNF\";\x20e\_

SF:fb\_vipaddr=\"AcIIkoTGBTWxL7QJkkBc3kEqsQGlfXiKxiV43A\_z6LtCF7LRkTyzOOsfo0

SF:SfraI8a7PZpxHYjA\";\x20e\_fb\_proxycode=\"AcLdDFzv9ou1-s5eeevFSixeW3ADhSX

SF:JzRxRP98j0PEUvIPQZ79JMfmdOlEp\";\x20e\_fb\_requestsequencenumber=\"AcLhwI

SF:6qA6BEj3siA98Qp5tk49PiH0cCAQE-TWVUmUJ-eHCb10XyoPey7Q\";\x20e\_fb\_request

SF:time=\"AcJZYsDPMSu3xL1ovRcGKWgVdSZih3IhZCNv9qv90x8PIIvnkNhcVfj\_Hk")%r(F

SF:ourOhFourRequest,5C7,"HTTP/1\.1\x20400\x20default\_vip\_400\r\nContent-Ty

SF:pe:\x20text/html;\x20charset=utf-8\r\nAccess-Control-Allow-Origin:\x20\

SF:\*\r\nProxy-Status:\x20proxy\_internal\_response;\x20e\_fb\_responsebytes=\"

SF:AcKLAY2bnmcN28FAPl8\_DWeNLyDRzB\_CAxzERqAR7zDFA5tbCIbhvv1aUfrs\";\x20e\_fb

SF:\_configversion=\"AcIYaNOARl-DAc72WS5MuHqiE9f\_s4Ey89ced8dqbkMSOwhTCVPgkC

SF:YvPntfyg\";\x20e\_isproxyerr=\"AcIK9qdDVtnGXKNlSb7VeMY1CE1vdTYOEmuK7chRK

SF:egeaaTIimBsRU0G2oPTNA\";\x20e\_clientaddr=\"AcJ6tom3TyOPWfmO98Wh80-hTwHD

SF:\_kp-r1hCH4ggV3ajWRVWzy3HkHFCFHUxR8sQ-Cy4jF5DytRd20H0NBg\";\x20e\_fb\_vipp

SF:ort=\"AcIyCl0\_u5UnLOUKNQB6Z3rgQ1C5X4TKbPZpD99C36fgtFyBeAdDmj1K06Xi\";\x

SF:20e\_fb\_vipaddr=\"AcIEy0nm8too9ozYzc7Kll\_zeKSc7BDudvmPm0\_119zEOhdPT3ChR-

SF:ldB-bWJ3wcCVt7qIIgAA\";\x20e\_fb\_proxycode=\"AcKp6AO3lgqIXTTD9ZiD2Cl8Qm0

SF:gGiK08Dqd6ZqXt\_8vf3HXzFsnOIiQANxF\";\x20e\_fb\_requestsequencenumber=\"Ac

SF:LfOlEU264DbH7ls3-LJz8GAkUBf3Ag1NfkR\_wzu350wsEcSWSrRWUzYw\";\x20e\_fb\_req

SF:uesttime=\"AcL1S0DURoNQ7cjuMxmt1O\_G16DISZc13fXpyBLDXBaxSK9PbZmDFutWh3");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port5222-TCP:V=7.91%T=SSL%I=7%D=12/17%Time=67612CDD%P=x86\_64-pc-linux-g

SF:nu%r(GetRequest,5C9,"HTTP/1\.1\x20400\x20default\_vip\_400\r\nContent-Typ

SF:e:\x20text/html;\x20charset=utf-8\r\nAccess-Control-Allow-Origin:\x20\\*

SF:\r\nProxy-Status:\x20proxy\_internal\_response;\x20e\_fb\_responsebytes=\"A

SF:cJUiY7T-5OZV2RgH56JWPvkajOclEK3LOM\_xK-L52SQcCDitsFdFG1kPSlF\";\x20e\_fb\_

SF:configversion=\"AcKWlBY3Lybur2Uy9eyk5LNJhjKM3BEYrLnMrH9t6YO37J\_cd8ShsNQ

SF:1EsMvFQ\";\x20e\_isproxyerr=\"AcI-ODQ8s3D2rLczqv8-f0dnd6rZyBc1e\_Zg5GGQPG

SF:LlUlrXt1gTkelsYdchJQ\";\x20e\_clientaddr=\"AcIWe6QCM9c6MZF2dgzpLvJLBD0hD

SF:PNDUXS9dwp0KtOzC13g2X\_b\_7-pjvfssEZcEuB6p1fYKsy5bOLcBwE\";\x20e\_fb\_vippo

SF:rt=\"AcJYrCwti6oIEFum3V9e\_NjnGhdhOhH4yOIkOjvislfr4d6dYiTpudoVNRAcSg\";\

SF:x20e\_fb\_vipaddr=\"AcL2bPy8yZmtqxMjtv5Eh8hNcl\_oj8Bp8YhoZ0Fwgbf7Uut6Fe4Db

SF:tCWKnlh9MVUPJ1CkHWsSw\";\x20e\_fb\_proxycode=\"AcJACMtJ08Ea8FeRQ5-K4FirtK

SF:McKb2l3lNZPhJmVfbFzvRdxC30zwiw526M\";\x20e\_fb\_requestsequencenumber=\"A

SF:cJdUpHq7ajsyb7B0X7lzG9wnzEqSVAkJFdJpHho4AedrPuMdIR2ODsgLA\";\x20e\_fb\_re

SF:questtime=\"AcKIfgUvdIKylw4rcbUi05Zuvld3JJwsKzgGBkAHWIMA0RYVaaKd\_xIq")%

SF:r(HTTPOptions,5C9,"HTTP/1\.1\x20400\x20default\_vip\_400\r\nContent-Type:

SF:\x20text/html;\x20charset=utf-8\r\nAccess-Control-Allow-Origin:\x20\\*\r

SF:\nProxy-Status:\x20proxy\_internal\_response;\x20e\_fb\_responsebytes=\"AcJ

SF:jMkaOLnLaaKeS0C73m7D0qsbq06j6pzjg0YMdvChSBujdANE8YiGn\_geH\";\x20e\_fb\_co

SF:nfigversion=\"AcL0q7jtAbtcSQGVP3oI7zWV2WjsMkToJQI7wnv9ESItRUqjIm2fO-scE

SF:plD\_A\";\x20e\_isproxyerr=\"AcIcmYVHiAKvw51QINEc0\_jZwVhlraJ1OAUL0wn5DHxI

SF:LsVJFamV1HI-lHa9cw\";\x20e\_clientaddr=\"AcIlhESgYTgfhixhiSs47svJEKugnOr

SF:9lI2t9ngF9X8eprnb14-9sKXux3s3-S-iU1YIxXTsNDmpBX66Vds\";\x20e\_fb\_vipport

SF:=\"AcJ3-R\_jyLldhObeDgamaDX1cU6MQHsQ7Muej-jMsuEdRdgKuihxco2b4Am8XQ\";\x2

SF:0e\_fb\_vipaddr=\"AcJUrh9j2p1q1rrlxraFLFKvQtR5VnCZSAEmEWhlfeM-AScldMab8WH

SF:oVOMh6dwYhCGD1T5rOg\";\x20e\_fb\_proxycode=\"AcK8oS0yS8hTFgSuhxT2mFBiCrCb

SF:-Y5s2-ndylwkHD4-i17q-pLs3HVduCXp\";\x20e\_fb\_requestsequencenumber=\"AcL

SF:ieOPuZaxlVd9yoC1lZhTue\_8J4GmobQu0om-0CNbc\_Yq0CelGepG7ow\";\x20e\_fb\_requ

SF:esttime=\"AcLrpSUfPHIeCAA5L4JZ2X6L-JfV0sTw3GIJDQYdeBbBv5TdgrbA13rX")%r(

SF:RTSPRequest,F6,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20

SF:text/html;\x20charset=utf-8\r\nDate:\x20Tue,\x2017\x20Dec\x202024\x2007

SF::48:47\x20GMT\r\nConnection:\x20close\r\nContent-Length:\x20101\r\n\r\n

SF:<html>\n<head>\n<title>WhatsApp\x20Error</title>\n</head>\n\n<body>\n<h

SF:1>WhatsApp\x20Error</h1>\n</body>\n\n</html>\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 47.26 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website is relatively safe with no critical issues detected.

[+] Keep monitoring and maintaining security configurations.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py 130 ⨯

Enter the target website URL (e.g., https://example.com): https://Tryhackme.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://Tryhackme.com

[+] The site https://Tryhackme.com is behind AWS Elastic Load Balancer (Amazon) WAF.

[~] Number of requests: 2

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Date: Tue, 17 Dec 2024 07:54:40 GMT

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

Transfer-Encoding: chunked

Connection: keep-alive

CF-Ray: 8f3558b3f9dba917-MAA

CF-Cache-Status: DYNAMIC

Set-Cookie: AWSALB=+P/4/a8T9q5qDqTl7UWezdkXSEEy1TPh9znhAQX/B+aJab+8GxpsXhxxLsazbIPIs1oRm1rEmFiMRZp0iwXrzodjZXKxWkEcoB4Yhr/1uL6/8ddlp6fJU/1PiwGx; Expires=Tue, 24 Dec 2024 07:54:40 GMT; Path=/, AWSALBCORS=+P/4/a8T9q5qDqTl7UWezdkXSEEy1TPh9znhAQX/B+aJab+8GxpsXhxxLsazbIPIs1oRm1rEmFiMRZp0iwXrzodjZXKxWkEcoB4Yhr/1uL6/8ddlp6fJU/1PiwGx; Expires=Tue, 24 Dec 2024 07:54:40 GMT; Path=/; SameSite=None, \_csrf=EqYsCPv8dZTjQIqTuesrwTz4; Path=/, connect.sid=s%3AET4-MS0tAGzQBIBjfivML\_262YadapJX.Cbeqo5107XPKzjm7ckVZazrROTcRAeHIp56zISED0pM; Path=/; Expires=Tue, 24 Dec 2024 07:54:40 GMT; HttpOnly

X-Powered-By: Express

Vary: Accept-Encoding

Server: cloudflare

Content-Encoding: br

[!] Missing Security Headers:

- Content-Security-Policy

- Strict-Transport-Security

- X-Frame-Options

- X-XSS-Protection

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 02:54 EST

Nmap scan report for Tryhackme.com (104.22.54.228)

Host is up (0.065s latency).

Other addresses for Tryhackme.com (not scanned): 2606:4700:83b6:d399:f6dd:409:ae35:d89c 172.67.27.10 104.22.55.228

Not shown: 996 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http Cloudflare http proxy

443/tcp open ssl/http Cloudflare http proxy

8080/tcp open http Cloudflare http proxy

8443/tcp open ssl/http Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 21.44 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- Missing security headers: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, X-XSS-Protection.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://apple.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://apple.com

[+] Generic Detection results:

[-] No WAF detected by the generic detection

[~] Number of requests: 7

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Server: Apple

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

Set-Cookie: geo=IN; path=/; domain=.apple.com

X-Frame-Options: SAMEORIGIN

Vary: Accept-Encoding

Content-Security-Policy: default-src 'self' blob: data: \*.akamaized.net \*.apple.com \*.apple-mapkit.com \*.cdn-apple.com \*.organicfruitapps.com; child-src blob: mailto: embed.music.apple.com embed.podcasts.apple.com https://recyclingprogram.apple.com swdlp.apple.com www.apple.com www.instagram.com platform.twitter.com www.youtube-nocookie.com; img-src 'unsafe-inline' blob: data: \*.apple.com \*.apple-mapkit.com \*.cdn-apple.com \*.mzstatic.com; script-src 'unsafe-inline' 'unsafe-eval' blob: \*.apple.com \*.apple-mapkit.com www.instagram.com platform.twitter.com; style-src 'unsafe-inline' \*.apple.com

Referrer-Policy: no-referrer-when-downgrade

Strict-Transport-Security: max-age=31536000; includeSubdomains; preload

X-Content-Type-Options: nosniff

X-Xss-Protection: 1; mode=block

Content-Encoding: gzip

Cache-Control: max-age=0

Expires: Tue, 17 Dec 2024 08:01:47 GMT

Date: Tue, 17 Dec 2024 08:01:47 GMT

Content-Length: 40588

X-Cache: TCP\_HIT from a23-199-67-132.deploy.akamaitechnologies.com (AkamaiGHost/11.7.2.1-35a4fcef889a1f053c9fa641f2ccd99a) (-)

Connection: keep-alive

[+] All important security headers are present.

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:01 EST

Nmap scan report for apple.com (17.253.144.10)

Host is up (0.098s latency).

Other addresses for apple.com (not scanned): 2620:149:af0::10

rDNS record for 17.253.144.10: apple.com.lk

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http

443/tcp open ssl/https

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.91%I=7%D=12/17%Time=67612FF9%P=x86\_64-pc-linux-gnu%r(Get

SF:Request,2ED,"HTTP/1\.0\x20400\x20Host\x20Header\x20Required\r\nDate:\x2

SF:0Tue,\x2017\x20Dec\x202024\x2008:02:02\x20GMT\r\nVia:\x20http/1\.1\x20i

SF:nbom5-edge-bx-005\.ts\.apple\.com\x20\(acdn/14454\.1\)\r\nCache-Control

SF::\x20no-store\r\nContent-Type:\x20text/html\r\nContent-Language:\x20en\

SF:r\nX-Cache:\x20none\r\nCDNUUID:\x201e4bee9a-531e-47bd-9098-9c619f62cbed

SF:-4395988109\r\nContent-Length:\x20447\r\n\r\n<HTML>\n<HEAD>\n<TITLE>Hos

SF:t\x20Header\x20Required</TITLE>\n</HEAD>\n\n<BODY\x20BGCOLOR=\"white\"\

SF:x20FGCOLOR=\"black\">\n<H1>Host\x20Header\x20Required</H1>\n<HR>\n\n<FO

SF:NT\x20FACE=\"Helvetica,Arial\"><B>\nDescription:\x20Your\x20browser\x20

SF:did\x20not\x20send\x20a\x20\"Host\"\x20HTTP\x20header\x20field\nand\x20

SF:therefore\x20the\x20virtual\x20host\x20being\x20requested\x20could\x20n

SF:ot\x20be\x20determined\.\nTo\x20access\x20this\x20web\x20site\x20correc

SF:tly,\x20you\x20will\x20need\x20to\x20upgrade\x20to\x20a\x20browser\ntha

SF:t\x20supports\x20the\x20HTTP\x20\"Host\"\x20header\x20field\.\n</B></FO

SF:NT>\n<HR>\n</BODY>\n")%r(HTTPOptions,2ED,"HTTP/1\.0\x20400\x20Host\x20H

SF:eader\x20Required\r\nDate:\x20Tue,\x2017\x20Dec\x202024\x2008:02:02\x20

SF:GMT\r\nVia:\x20http/1\.1\x20inbom5-edge-bx-001\.ts\.apple\.com\x20\(acd

SF:n/14454\.1\)\r\nCache-Control:\x20no-store\r\nContent-Type:\x20text/htm

SF:l\r\nContent-Language:\x20en\r\nX-Cache:\x20none\r\nCDNUUID:\x208a38215

SF:b-3d80-42a4-8b21-0b4a43554f9c-4396981675\r\nContent-Length:\x20447\r\n\

SF:r\n<HTML>\n<HEAD>\n<TITLE>Host\x20Header\x20Required</TITLE>\n</HEAD>\n

SF:\n<BODY\x20BGCOLOR=\"white\"\x20FGCOLOR=\"black\">\n<H1>Host\x20Header\

SF:x20Required</H1>\n<HR>\n\n<FONT\x20FACE=\"Helvetica,Arial\"><B>\nDescri

SF:ption:\x20Your\x20browser\x20did\x20not\x20send\x20a\x20\"Host\"\x20HTT

SF:P\x20header\x20field\nand\x20therefore\x20the\x20virtual\x20host\x20bei

SF:ng\x20requested\x20could\x20not\x20be\x20determined\.\nTo\x20access\x20

SF:this\x20web\x20site\x20correctly,\x20you\x20will\x20need\x20to\x20upgra

SF:de\x20to\x20a\x20browser\nthat\x20supports\x20the\x20HTTP\x20\"Host\"\x

SF:20header\x20field\.\n</B></FONT>\n<HR>\n</BODY>\n");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port443-TCP:V=7.91%T=SSL%I=7%D=12/17%Time=67612FFF%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,2ED,"HTTP/1\.0\x20400\x20Host\x20Header\x20Required\r\nD

SF:ate:\x20Tue,\x2017\x20Dec\x202024\x2008:02:08\x20GMT\r\nVia:\x20http/1\

SF:.1\x20inbom5-edge-bx-011\.ts\.apple\.com\x20\(acdn/14454\.1\)\r\nCache-

SF:Control:\x20no-store\r\nContent-Type:\x20text/html\r\nContent-Language:

SF:\x20en\r\nX-Cache:\x20none\r\nCDNUUID:\x2009eaaf79-6a88-4635-80cb-c8d9d

SF:f62f50e-4423937514\r\nContent-Length:\x20447\r\n\r\n<HTML>\n<HEAD>\n<TI

SF:TLE>Host\x20Header\x20Required</TITLE>\n</HEAD>\n\n<BODY\x20BGCOLOR=\"w

SF:hite\"\x20FGCOLOR=\"black\">\n<H1>Host\x20Header\x20Required</H1>\n<HR>

SF:\n\n<FONT\x20FACE=\"Helvetica,Arial\"><B>\nDescription:\x20Your\x20brow

SF:ser\x20did\x20not\x20send\x20a\x20\"Host\"\x20HTTP\x20header\x20field\n

SF:and\x20therefore\x20the\x20virtual\x20host\x20being\x20requested\x20cou

SF:ld\x20not\x20be\x20determined\.\nTo\x20access\x20this\x20web\x20site\x2

SF:0correctly,\x20you\x20will\x20need\x20to\x20upgrade\x20to\x20a\x20brows

SF:er\nthat\x20supports\x20the\x20HTTP\x20\"Host\"\x20header\x20field\.\n<

SF:/B></FONT>\n<HR>\n</BODY>\n")%r(HTTPOptions,2ED,"HTTP/1\.0\x20400\x20Ho

SF:st\x20Header\x20Required\r\nDate:\x20Tue,\x2017\x20Dec\x202024\x2008:02

SF::09\x20GMT\r\nVia:\x20http/1\.1\x20inbom5-edge-bx-009\.ts\.apple\.com\x

SF:20\(acdn/14454\.1\)\r\nCache-Control:\x20no-store\r\nContent-Type:\x20t

SF:ext/html\r\nContent-Language:\x20en\r\nX-Cache:\x20none\r\nCDNUUID:\x20

SF:5a5fb615-9da6-4d16-b115-e6f58374cf4e-4424932431\r\nContent-Length:\x204

SF:47\r\n\r\n<HTML>\n<HEAD>\n<TITLE>Host\x20Header\x20Required</TITLE>\n</

SF:HEAD>\n\n<BODY\x20BGCOLOR=\"white\"\x20FGCOLOR=\"black\">\n<H1>Host\x20

SF:Header\x20Required</H1>\n<HR>\n\n<FONT\x20FACE=\"Helvetica,Arial\"><B>\

SF:nDescription:\x20Your\x20browser\x20did\x20not\x20send\x20a\x20\"Host\"

SF:\x20HTTP\x20header\x20field\nand\x20therefore\x20the\x20virtual\x20host

SF:\x20being\x20requested\x20could\x20not\x20be\x20determined\.\nTo\x20acc

SF:ess\x20this\x20web\x20site\x20correctly,\x20you\x20will\x20need\x20to\x

SF:20upgrade\x20to\x20a\x20browser\nthat\x20supports\x20the\x20HTTP\x20\"H

SF:ost\"\x20header\x20field\.\n</B></FONT>\n<HR>\n</BODY>\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 35.31 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- No Web Application Firewall (WAF) detected.

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://amrita.edu

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://amrita.edu

[+] The site https://amrita.edu is behind AWS Elastic Load Balancer (Amazon) WAF.

[~] Number of requests: 2

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Date: Tue, 17 Dec 2024 08:00:50 GMT

Content-Type: text/html; charset=UTF-8

Content-Length: 50224

Connection: keep-alive

link: <https://www.amrita.edu/wp-json/>; rel="https://api.w.org/", <https://www.amrita.edu/wp-json/wp/v2/pages/3108>; rel="alternate"; title="JSON"; type="application/json", <https://www.amrita.edu/>; rel=shortlink

vary: Accept-Encoding

server: LiteSpeed

access-control-allow-origin: \*

access-control-allow-methods: PUT, GET, POST, OPTIONS

access-control-allow-headers: origin, x-requested-with, content-type

x-litespeed-cache: hit

content-encoding: gzip

[!] Missing Security Headers:

- Content-Security-Policy

- Strict-Transport-Security

- X-Frame-Options

- X-XSS-Protection

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:00 EST

Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 9.55% done; ETC: 03:01 (0:00:38 remaining)

Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 10.00% done; ETC: 03:01 (0:00:36 remaining)

Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 13.30% done; ETC: 03:01 (0:00:26 remaining)

Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 17.05% done; ETC: 03:01 (0:00:24 remaining)

Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan

Connect Scan Timing: About 17.50% done; ETC: 03:01 (0:00:24 remaining)

Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 50.00% done; ETC: 03:01 (0:00:23 remaining)

Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 50.00% done; ETC: 03:01 (0:00:23 remaining)

Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 50.00% done; ETC: 03:01 (0:00:24 remaining)

Nmap scan report for amrita.edu (76.223.83.62)

Host is up (0.078s latency).

Other addresses for amrita.edu (not scanned): 75.2.112.164

rDNS record for 76.223.83.62: a5acf5b2eb6a55835.awsglobalaccelerator.com

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http LiteSpeed

443/tcp open ssl/https awselb/2.0

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.91%I=7%D=12/17%Time=67612FC3%P=x86\_64-pc-linux-gnu%r(Get

SF:Request,6BD,"HTTP/1\.1\x20404\x20Not\x20Found\r\nDate:\x20Tue,\x2017\x2

SF:0Dec\x202024\x2008:01:09\x20GMT\r\nContent-Type:\x20text/html\r\nConten

SF:t-Length:\x201249\r\nConnection:\x20close\r\ncache-control:\x20private,

SF:\x20no-cache,\x20max-age=0\r\npragma:\x20no-cache\r\nserver:\x20LiteSpe

SF:ed\r\naccess-control-allow-origin:\x20https://amrita\.edu\x20https://we

SF:bfiles\.amrita\.edu\x20http://amrita\.edu\x20https://www\.amrita\.edu\x

SF:20http://www\.amrita\.edu\r\naccess-control-allow-methods:\x20PUT,\x20G

SF:ET,\x20POST,\x20OPTIONS\r\naccess-control-allow-headers:\x20origin,\x20

SF:x-requested-with,\x20content-type\r\n\r\n<!DOCTYPE\x20html>\n<html\x20s

SF:tyle=\"height:100%\">\n<head>\n<meta\x20name=\"viewport\"\x20content=\"

SF:width=device-width,\x20initial-scale=1,\x20shrink-to-fit=no\">\n<title>

SF:\x20404\x20Not\x20Found\r\n</title><style>@media\x20\(prefers-color-sch

SF:eme:dark\){body{background-color:#000!important}}</style></head>\n<body

SF:\x20style=\"color:\x20#444;\x20margin:0;font:\x20normal\x2014px/20px\x2

SF:0Arial,\x20Helvetica,\x20sans-serif;\x20height:100%;\x20background-colo

SF:r:\x20#fff;\">\n<div\x20style=\"height:auto;\x20min-heig")%r(HTTPOption

SF:s,6BD,"HTTP/1\.1\x20404\x20Not\x20Found\r\nDate:\x20Tue,\x2017\x20Dec\x

SF:202024\x2008:01:09\x20GMT\r\nContent-Type:\x20text/html\r\nContent-Leng

SF:th:\x201249\r\nConnection:\x20close\r\ncache-control:\x20private,\x20no

SF:-cache,\x20max-age=0\r\npragma:\x20no-cache\r\nserver:\x20LiteSpeed\r\n

SF:access-control-allow-origin:\x20https://amrita\.edu\x20https://webfiles

SF:\.amrita\.edu\x20http://amrita\.edu\x20https://www\.amrita\.edu\x20http

SF:://www\.amrita\.edu\r\naccess-control-allow-methods:\x20PUT,\x20GET,\x2

SF:0POST,\x20OPTIONS\r\naccess-control-allow-headers:\x20origin,\x20x-requ

SF:ested-with,\x20content-type\r\n\r\n<!DOCTYPE\x20html>\n<html\x20style=\

SF:"height:100%\">\n<head>\n<meta\x20name=\"viewport\"\x20content=\"width=

SF:device-width,\x20initial-scale=1,\x20shrink-to-fit=no\">\n<title>\x2040

SF:4\x20Not\x20Found\r\n</title><style>@media\x20\(prefers-color-scheme:da

SF:rk\){body{background-color:#000!important}}</style></head>\n<body\x20st

SF:yle=\"color:\x20#444;\x20margin:0;font:\x20normal\x2014px/20px\x20Arial

SF:,\x20Helvetica,\x20sans-serif;\x20height:100%;\x20background-color:\x20

SF:#fff;\">\n<div\x20style=\"height:auto;\x20min-heig");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port443-TCP:V=7.91%T=SSL%I=7%D=12/17%Time=67612FCA%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,AB7,"HTTP/1\.1\x20301\x20Moved\x20Permanently\r\nDate:\x

SF:20Tue,\x2017\x20Dec\x202024\x2008:01:15\x20GMT\r\nContent-Type:\x20text

SF:/html;\x20charset=UTF-8\r\nContent-Length:\x200\r\nConnection:\x20close

SF:\r\nset-cookie:\x20utm\_source=deleted;\x20expires=Thu,\x2001\x20Jan\x20

SF:1970\x2000:00:01\x20GMT;\x20Max-Age=0;\x20path=/;\x20domain=\.amritaedu

SF:-prod-1859494013\.ap-south-1\.elb\.amazonaws\.com\r\nset-cookie:\x20utm

SF:\_medium=deleted;\x20expires=Thu,\x2001\x20Jan\x201970\x2000:00:01\x20GM

SF:T;\x20Max-Age=0;\x20path=/;\x20domain=\.amritaedu-prod-1859494013\.ap-s

SF:outh-1\.elb\.amazonaws\.com\r\nset-cookie:\x20utm\_term=deleted;\x20expi

SF:res=Thu,\x2001\x20Jan\x201970\x2000:00:01\x20GMT;\x20Max-Age=0;\x20path

SF:=/;\x20domain=\.amritaedu-prod-1859494013\.ap-south-1\.elb\.amazonaws\.

SF:com\r\nset-cookie:\x20utm\_content=deleted;\x20expires=Thu,\x2001\x20Jan

SF:\x201970\x2000:00:01\x20GMT;\x20Max-Age=0;\x20path=/;\x20domain=\.amrit

SF:aedu-prod-1859494013\.ap-south-1\.elb\.amazonaws\.com\r\nset-cookie:\x2

SF:0utm\_campaign=deleted;\x20expires=Thu,\x2001\x20Jan\x201970\x2000:00:01

SF:\x20GMT;\x20Max-Age=0;\x20path=/;\x20domain=\.amritaedu-prod-1859494013

SF:\.ap-south-1\.e")%r(HTTPOptions,4000,"HTTP/1\.1\x20200\x20OK\r\nDate:\x

SF:20Tue,\x2017\x20Dec\x202024\x2008:01:18\x20GMT\r\nContent-Type:\x20text

SF:/html;\x20charset=UTF-8\r\nConnection:\x20close\r\nset-cookie:\x20utm\_s

SF:ource=deleted;\x20expires=Thu,\x2001\x20Jan\x201970\x2000:00:01\x20GMT;

SF:\x20Max-Age=0;\x20path=/;\x20domain=\.amritaedu-prod-1859494013\.ap-sou

SF:th-1\.elb\.amazonaws\.com\r\nset-cookie:\x20utm\_medium=deleted;\x20expi

SF:res=Thu,\x2001\x20Jan\x201970\x2000:00:01\x20GMT;\x20Max-Age=0;\x20path

SF:=/;\x20domain=\.amritaedu-prod-1859494013\.ap-south-1\.elb\.amazonaws\.

SF:com\r\nset-cookie:\x20utm\_term=deleted;\x20expires=Thu,\x2001\x20Jan\x2

SF:01970\x2000:00:01\x20GMT;\x20Max-Age=0;\x20path=/;\x20domain=\.amritaed

SF:u-prod-1859494013\.ap-south-1\.elb\.amazonaws\.com\r\nset-cookie:\x20ut

SF:m\_content=deleted;\x20expires=Thu,\x2001\x20Jan\x201970\x2000:00:01\x20

SF:GMT;\x20Max-Age=0;\x20path=/;\x20domain=\.amritaedu-prod-1859494013\.ap

SF:-south-1\.elb\.amazonaws\.com\r\nset-cookie:\x20utm\_campaign=deleted;\x

SF:20expires=Thu,\x2001\x20Jan\x201970\x2000:00:01\x20GMT;\x20Max-Age=0;\x

SF:20path=/;\x20domain=\.amritaedu-prod-1859494013\.ap-south-1\.elb\.amazo

SF:naws\.com\r\nset-cookie:\x20gcli");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 43.69 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- Missing security headers: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, X-XSS-Protection.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://groww.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://groww.com

[+] Generic Detection results:

[-] No WAF detected by the generic detection

[~] Number of requests: 7

[+] Checking HTTP Headers...

Error checking headers: HTTPSConnectionPool(host='groww.com', port=443): Max retries exceeded with url: / (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE\_VERIFY\_FAILED] certificate verify failed: self signed certificate (\_ssl.c:1123)')))

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:00 EST

Nmap scan report for groww.com (36.55.232.2)

Host is up (0.45s latency).

rDNS record for 36.55.232.2: usv0280.mfro-sv.net

Not shown: 964 filtered ports, 33 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp ProFTPD or KnFTPD

80/tcp open http Apache httpd

443/tcp open ssl/ssl Apache httpd (SSL-only mode)

Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 64.06 seconds

[+] Checking for outdated CMS...

Error checking CMS: HTTPSConnectionPool(host='groww.com', port=443): Max retries exceeded with url: / (Caused by SSLError(SSLCertVerificationError(1, '[SSL: CERTIFICATE\_VERIFY\_FAILED] certificate verify failed: self signed certificate (\_ssl.c:1123)')))

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- No Web Application Firewall (WAF) detected.

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://asus.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://asus.com

[+] The site https://asus.com is behind Edgecast (Verizon Digital Media) WAF.

[~] Number of requests: 2

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Content-Encoding: gzip

Content-Type: text/html

Date: Tue, 17 Dec 2024 08:00:24 GMT

IP: 152.58.239.189

Reference: 785191569241817261112798922937975584293

Server: ECD (tir/CD11)

URL: https://www.asus.com/

uuid: 785191569241817261112798922937975584293

X-ACL-AUD: 403

X-ACL-PROD: 403

X-Akamai-Device-Characteristics: desktop

x-log-country: IN

x-vmg-version: v7.18.4

Content-Length: 60409

[!] Missing Security Headers:

- Content-Security-Policy

- Strict-Transport-Security

- X-Frame-Options

- X-XSS-Protection

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:00 EST

Nmap scan report for asus.com (103.10.4.227)

Host is up (0.31s latency).

Not shown: 994 closed ports

PORT STATE SERVICE VERSION

25/tcp filtered smtp

80/tcp open upnp Microsoft IIS httpd

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

443/tcp open ssl/https

445/tcp filtered microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 81.36 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- Missing security headers: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, X-XSS-Protection.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://pinapple.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://pinapple.com

[+] Generic Detection results:

[-] No WAF detected by the generic detection

[~] Number of requests: 7

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Server: openresty/1.27.1.1

Date: Tue, 17 Dec 2024 08:02:20 GMT

Content-Type: text/html

Content-Length: 6419

Last-Modified: Thu, 14 Nov 2024 16:40:11 GMT

Connection: keep-alive

ETag: "673627eb-1913"

Strict-Transport-Security: max-age=63072000

Accept-Ranges: bytes

[!] Missing Security Headers:

- Content-Security-Policy

- X-Frame-Options

- X-XSS-Protection

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:02 EST

Nmap scan report for pinapple.com (192.64.151.235)

Host is up (0.35s latency).

Not shown: 997 filtered ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)

80/tcp open http OpenResty web app server 1.27.1.1

443/tcp open ssl/http OpenResty web app server 1.27.1.1

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 46.08 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- No Web Application Firewall (WAF) detected.

- Missing security headers: Content-Security-Policy, X-Frame-Options, X-XSS-Protection.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://ksrtc.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( W00f! )

\ \_\_\_\_/

,, \_\_ 404 Hack Not Found

|`-.\_\_ / / \_\_ \_\_

/" \_/ /\_/ \ \ / /

\*===\* / \ \\_/ / 405 Not Allowed

/ )\_\_// \ /

/| / /---` 403 Forbidden

\\/` \ | / \_ \

`\ /\_\\\_ 502 Bad Gateway / / \ \ 500 Internal Error

`\_\_\_\_\_``-` /\_/ \\_\

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://ksrtc.com

[+] Generic Detection results:

[-] No WAF detected by the generic detection

[~] Number of requests: 7

[+] Checking HTTP Headers...

Security Headers:

------------------------------

server: openresty/1.13.6.1

date: Tue, 17 Dec 2024 08:05:10 GMT

content-type: application/octet-stream, text/html

content-length: 100

[!] Missing Security Headers:

- Content-Security-Policy

- Strict-Transport-Security

- X-Frame-Options

- X-XSS-Protection

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:05 EST

Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 50.00% done; ETC: 03:06 (0:00:31 remaining)

Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 50.00% done; ETC: 03:06 (0:00:33 remaining)

Nmap scan report for ksrtc.com (72.14.178.174)

Host is up (0.35s latency).

Other addresses for ksrtc.com (not scanned): 45.33.30.197 45.33.18.44 72.14.185.43 173.255.194.134 45.33.2.79 45.79.19.196 96.126.123.244 45.33.23.183 198.58.118.167 45.56.79.23 45.33.20.235

rDNS record for 72.14.178.174: li40-174.members.linode.com

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http-proxy (bad gateway)

443/tcp open ssl/https openresty/1.13.6.1

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.91%I=7%D=12/17%Time=676130D0%P=x86\_64-pc-linux-gnu%r(Get

SF:Request,14B,"HTTP/1\.1\x20404\x20Not\x20Found\r\nserver:\x20openresty/1

SF:\.13\.6\.1\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x2008:05:37\x20GMT\r\n

SF:content-type:\x20text/html\r\ncontent-length:\x20175\r\nconnection:\x20

SF:close\r\n\r\n<html>\r\n<head><title>404\x20Not\x20Found</title></head>\

SF:r\n<body\x20bgcolor=\"white\">\r\n<center><h1>404\x20Not\x20Found</h1><

SF:/center>\r\n<hr><center>openresty/1\.13\.6\.1</center>\r\n</body>\r\n</

SF:html>\r\n")%r(HTTPOptions,14B,"HTTP/1\.1\x20404\x20Not\x20Found\r\nserv

SF:er:\x20openresty/1\.13\.6\.1\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x200

SF:8:05:38\x20GMT\r\ncontent-type:\x20text/html\r\ncontent-length:\x20175\

SF:r\nconnection:\x20close\r\n\r\n<html>\r\n<head><title>404\x20Not\x20Fou

SF:nd</title></head>\r\n<body\x20bgcolor=\"white\">\r\n<center><h1>404\x20

SF:Not\x20Found</h1></center>\r\n<hr><center>openresty/1\.13\.6\.1</center

SF:>\r\n</body>\r\n</html>\r\n")%r(RTSPRequest,E1,"HTTP/1\.1\x20502\x20Bad

SF:\x20Gateway\r\ncontent-length:\x20107\r\ncache-control:\x20no-cache\r\n

SF:content-type:\x20text/html\r\nconnection:\x20close\r\n\r\n<html><body><

SF:h1>502\x20Bad\x20Gateway</h1>\nThe\x20server\x20returned\x20an\x20inval

SF:id\x20or\x20incomplete\x20response\.\n</body></html>\n")%r(FourOhFourRe

SF:quest,14B,"HTTP/1\.1\x20404\x20Not\x20Found\r\nserver:\x20openresty/1\.

SF:13\.6\.1\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x2008:05:40\x20GMT\r\nco

SF:ntent-type:\x20text/html\r\ncontent-length:\x20175\r\nconnection:\x20cl

SF:ose\r\n\r\n<html>\r\n<head><title>404\x20Not\x20Found</title></head>\r\

SF:n<body\x20bgcolor=\"white\">\r\n<center><h1>404\x20Not\x20Found</h1></c

SF:enter>\r\n<hr><center>openresty/1\.13\.6\.1</center>\r\n</body>\r\n</ht

SF:ml>\r\n")%r(Help,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-leng

SF:th:\x2090\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nCont

SF:ent-Type:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1

SF:>\nYour\x20browser\x20sent\x20an\x20invalid\x20request\.\n</body></html

SF:>\n")%r(SSLSessionReq,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent

SF:-length:\x2090\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\

SF:nContent-Type:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20reques

SF:t</h1>\nYour\x20browser\x20sent\x20an\x20invalid\x20request\.\n</body><

SF:/html>\n");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port443-TCP:V=7.91%T=SSL%I=7%D=12/17%Time=676130DA%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,14B,"HTTP/1\.1\x20404\x20Not\x20Found\r\nserver:\x20open

SF:resty/1\.13\.6\.1\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x2008:05:47\x20

SF:GMT\r\ncontent-type:\x20text/html\r\ncontent-length:\x20175\r\nconnecti

SF:on:\x20close\r\n\r\n<html>\r\n<head><title>404\x20Not\x20Found</title><

SF:/head>\r\n<body\x20bgcolor=\"white\">\r\n<center><h1>404\x20Not\x20Foun

SF:d</h1></center>\r\n<hr><center>openresty/1\.13\.6\.1</center>\r\n</body

SF:>\r\n</html>\r\n")%r(HTTPOptions,14B,"HTTP/1\.1\x20404\x20Not\x20Found\

SF:r\nserver:\x20openresty/1\.13\.6\.1\r\ndate:\x20Tue,\x2017\x20Dec\x2020

SF:24\x2008:05:48\x20GMT\r\ncontent-type:\x20text/html\r\ncontent-length:\

SF:x20175\r\nconnection:\x20close\r\n\r\n<html>\r\n<head><title>404\x20Not

SF:\x20Found</title></head>\r\n<body\x20bgcolor=\"white\">\r\n<center><h1>

SF:404\x20Not\x20Found</h1></center>\r\n<hr><center>openresty/1\.13\.6\.1<

SF:/center>\r\n</body>\r\n</html>\r\n")%r(FourOhFourRequest,14B,"HTTP/1\.1

SF:\x20404\x20Not\x20Found\r\nserver:\x20openresty/1\.13\.6\.1\r\ndate:\x2

SF:0Tue,\x2017\x20Dec\x202024\x2008:05:50\x20GMT\r\ncontent-type:\x20text/

SF:html\r\ncontent-length:\x20175\r\nconnection:\x20close\r\n\r\n<html>\r\

SF:n<head><title>404\x20Not\x20Found</title></head>\r\n<body\x20bgcolor=\"

SF:white\">\r\n<center><h1>404\x20Not\x20Found</h1></center>\r\n<hr><cente

SF:r>openresty/1\.13\.6\.1</center>\r\n</body>\r\n</html>\r\n")%r(tor-vers

SF:ions,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x2090\r\

SF:nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-Type:\x2

SF:0text/html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYour\x20b

SF:rowser\x20sent\x20an\x20invalid\x20request\.\n</body></html>\n")%r(RTSP

SF:Request,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x2090

SF:\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-Type:

SF:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYour\x

SF:20browser\x20sent\x20an\x20invalid\x20request\.\n</body></html>\n")%r(R

SF:PCCheck,CF,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-length:\x2090

SF:\r\nCache-Control:\x20no-cache\r\nConnection:\x20close\r\nContent-Type:

SF:\x20text/html\r\n\r\n<html><body><h1>400\x20Bad\x20request</h1>\nYour\x

SF:20browser\x20sent\x20an\x20invalid\x20request\.\n</body></html>\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 89.68 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- No Web Application Firewall (WAF) detected.

- Missing security headers: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, X-XSS-Protection.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://pubg.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://pubg.com

[+] The site https://pubg.com is behind Cloudfront (Amazon) WAF.

[~] Number of requests: 2

[+] Checking HTTP Headers...

Security Headers:

------------------------------

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

Transfer-Encoding: chunked

Connection: keep-alive

Date: Tue, 17 Dec 2024 08:07:29 GMT

Set-Cookie: i18n\_redirected=en; Max-Age=31536000; Path=/; SameSite=Lax

ETag: "1138c7-3ZZZCHThBV6snNE+P9z51+xyguw"

Accept-Ranges: none

Content-Encoding: gzip

Vary: Accept-Encoding

X-Cache: Miss from cloudfront

Via: 1.1 9f4cce6859e22bfe7ef1809523b01cb6.cloudfront.net (CloudFront)

X-Amz-Cf-Pop: MAA51-C1

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

X-Amz-Cf-Id: jIjIAlHmzwwEjKU\_iGV06fPF-UhbSW8Z81XMgfQ8SSQHJDpAFoMFnA==

[!] Missing Security Headers:

- Content-Security-Policy

- Strict-Transport-Security

- X-Frame-Options

- X-XSS-Protection

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:07 EST

Nmap scan report for pubg.com (52.84.150.63)

Host is up (0.076s latency).

Other addresses for pubg.com (not scanned): 52.84.150.55 52.84.150.59 52.84.150.60

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http Amazon CloudFront httpd

443/tcp open ssl/http Amazon CloudFront httpd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 24.50 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- Missing security headers: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, X-XSS-Protection.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://bgmi.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://bgmi.com

[+] The site https://bgmi.com is behind ModSecurity (SpiderLabs) WAF.

[~] Number of requests: 2

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Date: Tue, 17 Dec 2024 08:07:40 GMT

Server: Apache

Content-Length: 226

Keep-Alive: timeout=5, max=75

Connection: Keep-Alive

Content-Type: text/html; charset=iso-8859-1

[!] Missing Security Headers:

- Content-Security-Policy

- Strict-Transport-Security

- X-Frame-Options

- X-XSS-Protection

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:07 EST

Nmap scan report for bgmi.com (192.185.26.253)

Host is up (0.31s latency).

rDNS record for 192.185.26.253: 192-185-26-253.unifiedlayer.com

Not shown: 980 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp Pure-FTPd

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

25/tcp filtered smtp

26/tcp open smtp Exim smtpd 4.96.2

53/tcp open domain ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)

80/tcp open http Apache httpd

110/tcp open pop3 Dovecot pop3d

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

143/tcp open imap Dovecot imapd

161/tcp filtered snmp

443/tcp open ssl/http Apache httpd

445/tcp filtered microsoft-ds

465/tcp open ssl/smtp Exim smtpd 4.96.2

587/tcp open smtp Exim smtpd 4.96.2

993/tcp open ssl/imap Dovecot imapd

995/tcp open ssl/pop3 Dovecot pop3d

1688/tcp filtered nsjtp-data

2222/tcp open ssh OpenSSH 7.4 (protocol 2.0)

3306/tcp open mysql MySQL 5.7.23-23

Service Info: Host: testarossa.websitewelcome.com; OS: Linux; CPE: cpe:/o:redhat:enterprise\_linux:7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 34.23 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- Missing security headers: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, X-XSS-Protection.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://reliance.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( W00f! )

\ \_\_\_\_/

,, \_\_ 404 Hack Not Found

|`-.\_\_ / / \_\_ \_\_

/" \_/ /\_/ \ \ / /

\*===\* / \ \\_/ / 405 Not Allowed

/ )\_\_// \ /

/| / /---` 403 Forbidden

\\/` \ | / \_ \

`\ /\_\\\_ 502 Bad Gateway / / \ \ 500 Internal Error

`\_\_\_\_\_``-` /\_/ \\_\

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://reliance.com

[+] The site https://reliance.com is behind Cloudflare (Cloudflare Inc.) WAF.

[~] Number of requests: 2

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Date: Tue, 17 Dec 2024 08:09:45 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

X-Powered-By: PHP/8.3.13

Link: <https://reliance.com/wp-json/>; rel="https://api.w.org/", <https://reliance.com/wp-json/wp/v2/pages/6>; rel="alternate"; title="JSON"; type="application/json", <https://reliance.com/>; rel=shortlink

CF-Cache-Status: DYNAMIC

Server: cloudflare

CF-RAY: 8f356ebf2f6006bb-MAA

Content-Encoding: gzip

[!] Missing Security Headers:

- Content-Security-Policy

- Strict-Transport-Security

- X-Frame-Options

- X-XSS-Protection

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:09 EST

Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 50.00% done; ETC: 03:10 (0:00:12 remaining)

Nmap scan report for reliance.com (104.18.40.242)

Host is up (0.075s latency).

Other addresses for reliance.com (not scanned): 2606:4700:83b3:bf9a:9dd:40a:fece:43f0 172.64.147.14

Not shown: 996 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http Cloudflare http proxy

443/tcp open ssl/http Cloudflare http proxy

8080/tcp open http Cloudflare http proxy

8443/tcp open ssl/http Cloudflare http proxy

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 49.29 seconds

[+] Checking for outdated CMS...

CMS Detected: WordPress 6.7.1

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- Missing security headers: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, X-XSS-Protection.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

- Detected CMS: WordPress 6.7.1 (check for vulnerabilities).

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://netbeans.com

Starting Website Scan...

========================================

[+] Detecting WAF...

ERROR:wafw00f:Something went wrong HTTPSConnectionPool(host='netbeans.com', port=443): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7ff98931d190>: Failed to establish a new connection: [Errno -3] Temporary failure in name resolution'))

ERROR:wafw00f:Site netbeans.com appears to be down

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://netbeans.com

[+] Checking HTTP Headers...

Error checking headers: HTTPSConnectionPool(host='netbeans.com', port=443): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7fd0bf926a30>: Failed to establish a new connection: [Errno -3] Temporary failure in name resolution'))

[+] Scanning open ports...

Failed to resolve "netbeans.com".

WARNING: No targets were specified, so 0 hosts scanned.

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:08 EST

Nmap done: 0 IP addresses (0 hosts up) scanned in 11.98 seconds

[+] Checking for outdated CMS...

Error checking CMS: HTTPSConnectionPool(host='netbeans.com', port=443): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7fd0bf926b50>: Failed to establish a new connection: [Errno -3] Temporary failure in name resolution'))

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- No HTTPS detected; using HTTP only.

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://visualstudio.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://visualstudio.com

[+] The site https://visualstudio.com is behind Kona SiteDefender (Akamai) WAF.

[~] Number of requests: 2

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Server: nginx

Content-Type: text/html; charset=UTF-8

x-powered-by: WP Engine

Link: <https://visualstudio.microsoft.com/>; rel=shortlink

X-Cacheable: SHORT

X-Cache-Group: normal

Access-Control-Allow-Origin: https://cdn-assets-prod.s3.amazonaws.com

Content-Security-Policy: upgrade-insecure-requests, script-src 'self' 'unsafe-inline' 'unsafe-eval' https:

X-Content-Type-Options: nosniff, nosniff

X-XSS-Protection: 1; mode=block, 1; mode=block

Feature-Policy: geolocation 'none'; midi 'none'; sync-xhr 'none'; microphone 'none'; camera 'none'; magnetometer 'none'; gyroscope 'none'; speaker 'self'; fullscreen 'self'; payment 'none', geolocation 'none'; midi 'none'; sync-xhr 'none'; microphone 'none'; camera 'none'; magnetometer 'none'; gyroscope 'none'; fullscreen 'self' https://www.youtube.com https://mediastream.microsoft.com; payment 'none'

Content-Encoding: gzip

Content-Length: 61413

Cache-Control: must-revalidate, max-age=600

Date: Tue, 17 Dec 2024 08:09:07 GMT

Connection: keep-alive

Vary: Accept-Encoding

X-Frame-Options: SAMEORIGIN

Referrer-Policy: no-referrer-when-downgrade

Strict-Transport-Security: max-age=15768000 ; includeSubDomains ; preload

[+] All important security headers are present.

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:09 EST

Nmap scan report for visualstudio.com (13.107.42.18)

Host is up (0.11s latency).

Not shown: 997 filtered ports

PORT STATE SERVICE VERSION

53/tcp closed domain

80/tcp open upnp Microsoft IIS httpd

443/tcp open ssl/https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 33.90 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website is relatively safe with no critical issues detected.

[+] Keep monitoring and maintaining security configurations.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://android.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( Woof! )

\ \_\_\_\_/ )

,, ) (\_

.-. - \_\_\_\_\_\_\_ ( |\_\_|

()``; |==|\_\_\_\_\_\_\_) .)|\_\_|

/ (' /|\ ( |\_\_|

( / ) / | \ . |\_\_|

\(\_)\_)) / | \ |\_\_|

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://android.com

[+] Generic Detection results:

[-] No WAF detected by the generic detection

[~] Number of requests: 7

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Accept-Ranges: bytes

Vary: Accept-Encoding

Content-Encoding: gzip

Content-Type: text/html

Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://csp.withgoogle.com/csp/uxe-owners-acl/android

Cross-Origin-Opener-Policy-Report-Only: same-origin; report-to="uxe-owners-acl/android"

Report-To: {"group":"uxe-owners-acl/android","max\_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/uxe-owners-acl/android"}]}

Date: Tue, 17 Dec 2024 08:09:29 GMT

Expires: Tue, 17 Dec 2024 08:09:29 GMT

Cache-Control: private, max-age=3000

Last-Modified: Tue, 17 Dec 2024 05:58:00 GMT

X-Content-Type-Options: nosniff

Server: sffe

X-XSS-Protection: 0

Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

Transfer-Encoding: chunked

[!] Missing Security Headers:

- Content-Security-Policy

- Strict-Transport-Security

- X-Frame-Options

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:09 EST

Nmap scan report for android.com (142.250.205.228)

Host is up (0.066s latency).

Other addresses for android.com (not scanned): 2404:6800:4007:82d::2004

rDNS record for 142.250.205.228: maa05s28-in-f4.1e100.net

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http gws

443/tcp open ssl/https gws

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.91%I=7%D=12/17%Time=676131C6%P=x86\_64-pc-linux-gnu%r(Get

SF:Request,3188,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Tue,\x2017\x20Dec\x202

SF:024\x2008:09:43\x20GMT\r\nExpires:\x20-1\r\nCache-Control:\x20private,\

SF:x20max-age=0\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-1\r\nCo

SF:ntent-Security-Policy-Report-Only:\x20object-src\x20'none';base-uri\x20

SF:'self';script-src\x20'nonce-vhZxkgrOClqSGK8TDiS7ug'\x20'strict-dynamic'

SF:\x20'report-sample'\x20'unsafe-eval'\x20'unsafe-inline'\x20https:\x20ht

SF:tp:;report-uri\x20https://csp\.withgoogle\.com/csp/gws/other-hp\r\nP3P:

SF:\x20CP=\"This\x20is\x20not\x20a\x20P3P\x20policy!\x20See\x20g\.co/p3phe

SF:lp\x20for\x20more\x20info\.\"\r\nServer:\x20gws\r\nX-XSS-Protection:\x2

SF:00\r\nX-Frame-Options:\x20SAMEORIGIN\r\nSet-Cookie:\x20AEC=AZ6Zc-WA4JUg

SF:SOqI2B4Ghnzd9JsCs1YJJUJvDNfci5Gp4cbUXxUptgfnVQ;\x20expires=Sun,\x2015-J

SF:un-2025\x2008:09:43\x20GMT;\x20path=/;\x20domain=\.google\.com;\x20Secu

SF:re;\x20HttpOnly;\x20SameSite=lax\r\nSet-Cookie:\x20NID=520=UBCjdjrlzIEi

SF:tgacM0X9huz3jIV8X5\_Ej77rAwV9WEAJCiUqm59Qc55IytXIYO3Pkv3IlqouZHLe6cUCOqt

SF:KyDBQsPeUHcsnLBvoSw\_W8s7KfL3C8BTarGOxxuAeZZfSYx-dNh7rNMx5BLmbt9L7zT2o-y

SF:wOS2SDuV74B2RBN0nvK4YyYW7Od")%r(HTTPOptions,6DC,"HTTP/1\.0\x20405\x20Me

SF:thod\x20Not\x20Allowed\r\nContent-Type:\x20text/html;\x20charset=UTF-8\

SF:r\nReferrer-Policy:\x20no-referrer\r\nContent-Length:\x201592\r\nDate:\

SF:x20Tue,\x2017\x20Dec\x202024\x2008:09:43\x20GMT\r\n\r\n<!DOCTYPE\x20htm

SF:l>\n<html\x20lang=en>\n\x20\x20<meta\x20charset=utf-8>\n\x20\x20<meta\x

SF:20name=viewport\x20content=\"initial-scale=1,\x20minimum-scale=1,\x20wi

SF:dth=device-width\">\n\x20\x20<title>Error\x20405\x20\(Method\x20Not\x20

SF:Allowed\)!!1</title>\n\x20\x20<style>\n\x20\x20\x20\x20\\*{margin:0;padd

SF:ing:0}html,code{font:15px/22px\x20arial,sans-serif}html{background:#fff

SF:;color:#222;padding:15px}body{margin:7%\x20auto\x200;max-width:390px;mi

SF:n-height:180px;padding:30px\x200\x2015px}\\*\x20>\x20body{background:url

SF:\(//www\.google\.com/images/errors/robot\.png\)\x20100%\x205px\x20no-re

SF:peat;padding-right:205px}p{margin:11px\x200\x2022px;overflow:hidden}ins

SF:{color:#777;text-decoration:none}a\x20img{border:0}@media\x20screen\x20

SF:and\x20\(max-width:772px\){body{background:none;margin-top:0;max-width:

SF:none;padding-right:0}}#logo{background:url\(//www\.google\.com/images/b

SF:randing");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port443-TCP:V=7.91%T=SSL%I=7%D=12/17%Time=676131CC%P=x86\_64-pc-linux-gn

SF:u%r(GetRequest,1378,"HTTP/1\.0\x20200\x20OK\r\nDate:\x20Tue,\x2017\x20D

SF:ec\x202024\x2008:09:49\x20GMT\r\nExpires:\x20-1\r\nCache-Control:\x20pr

SF:ivate,\x20max-age=0\r\nContent-Type:\x20text/html;\x20charset=ISO-8859-

SF:1\r\nContent-Security-Policy-Report-Only:\x20object-src\x20'none';base-

SF:uri\x20'self';script-src\x20'nonce-nuK1VAIuO2yzraC6bpWkHQ'\x20'strict-d

SF:ynamic'\x20'report-sample'\x20'unsafe-eval'\x20'unsafe-inline'\x20https

SF::\x20http:;report-uri\x20https://csp\.withgoogle\.com/csp/gws/other-hp\

SF:r\nAccept-CH:\x20Sec-CH-Prefers-Color-Scheme\r\nP3P:\x20CP=\"This\x20is

SF:\x20not\x20a\x20P3P\x20policy!\x20See\x20g\.co/p3phelp\x20for\x20more\x

SF:20info\.\"\r\nServer:\x20gws\r\nX-XSS-Protection:\x200\r\nX-Frame-Optio

SF:ns:\x20SAMEORIGIN\r\nSet-Cookie:\x20AEC=AZ6Zc-VmqUi56Xt0XN\_kOiRMPpVvHfN

SF:T82RuED2qMdptWIl-PBUX8ir-QS0;\x20expires=Sun,\x2015-Jun-2025\x2008:09:4

SF:9\x20GMT;\x20path=/;\x20domain=\.google\.com;\x20Secure;\x20HttpOnly;\x

SF:20SameSite=lax\r\nSet-Cookie:\x20NID=520=ZQCqqxMTmD28zINkc6fjdM3c6Gj-C5

SF:Ntoa6BwfLe96g13Tzrl7o5AvbMTOVjHNraNYbdCUD8reFizrAZl-3XnxU0XRXrd9cD4zAye

SF:aTYusiqpfcPWA8KaY-nCXq1FfYlv0wdyzN5zDTQ")%r(HTTPOptions,715,"HTTP/1\.0\

SF:x20405\x20Method\x20Not\x20Allowed\r\nContent-Type:\x20text/html;\x20ch

SF:arset=UTF-8\r\nReferrer-Policy:\x20no-referrer\r\nContent-Length:\x2015

SF:92\r\nDate:\x20Tue,\x2017\x20Dec\x202024\x2008:09:50\x20GMT\r\nAlt-Svc:

SF:\x20h3=\":443\";\x20ma=2592000,h3-29=\":443\";\x20ma=2592000\r\n\r\n<!D

SF:OCTYPE\x20html>\n<html\x20lang=en>\n\x20\x20<meta\x20charset=utf-8>\n\x

SF:20\x20<meta\x20name=viewport\x20content=\"initial-scale=1,\x20minimum-s

SF:cale=1,\x20width=device-width\">\n\x20\x20<title>Error\x20405\x20\(Meth

SF:od\x20Not\x20Allowed\)!!1</title>\n\x20\x20<style>\n\x20\x20\x20\x20\\*{

SF:margin:0;padding:0}html,code{font:15px/22px\x20arial,sans-serif}html{ba

SF:ckground:#fff;color:#222;padding:15px}body{margin:7%\x20auto\x200;max-w

SF:idth:390px;min-height:180px;padding:30px\x200\x2015px}\\*\x20>\x20body{b

SF:ackground:url\(//www\.google\.com/images/errors/robot\.png\)\x20100%\x2

SF:05px\x20no-repeat;padding-right:205px}p{margin:11px\x200\x2022px;overfl

SF:ow:hidden}ins{color:#777;text-decoration:none}a\x20img{border:0}@media\

SF:x20screen\x20and\x20\(max-width:772px\){body{background:none;margin-top

SF::0;max-width:none;padding-right");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 83.72 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- No Web Application Firewall (WAF) detected.

- Missing security headers: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

┌──(kali㉿kali)-[~]

└─$ python3 website\_scan.py

Enter the target website URL (e.g., https://example.com): https://cod.com

Starting Website Scan...

========================================

[+] Detecting WAF...

\_\_\_\_\_\_

/ \

( W00f! )

\ \_\_\_\_/

,, \_\_ 404 Hack Not Found

|`-.\_\_ / / \_\_ \_\_

/" \_/ /\_/ \ \ / /

\*===\* / \ \\_/ / 405 Not Allowed

/ )\_\_// \ /

/| / /---` 403 Forbidden

\\/` \ | / \_ \

`\ /\_\\\_ 502 Bad Gateway / / \ \ 500 Internal Error

`\_\_\_\_\_``-` /\_/ \\_\

~ WAFW00F : v2.1.0 ~

The Web Application Firewall Fingerprinting Toolkit

[\*] Checking https://cod.com

[+] Generic Detection results:

[-] No WAF detected by the generic detection

[~] Number of requests: 7

[+] Checking HTTP Headers...

Security Headers:

------------------------------

Date: Tue, 17 Dec 2024 08:08:47 GMT

Server: Apache

Upgrade: h2,h2c

Connection: Upgrade, Keep-Alive

X-Mod-Pagespeed: 1.11.33.2-0

Cache-Control: max-age=0, no-cache

Vary: Accept-Encoding,User-Agent

Content-Encoding: gzip

Keep-Alive: timeout=2, max=150

Transfer-Encoding: chunked

Content-Type: text/html;charset=UTF-8

[!] Missing Security Headers:

- Content-Security-Policy

- Strict-Transport-Security

- X-Frame-Options

- X-XSS-Protection

[+] Scanning open ports...

Starting Nmap 7.91 ( https://nmap.org ) at 2024-12-17 03:08 EST

Nmap scan report for cod.com (54.67.42.145)

Host is up (0.32s latency).

rDNS record for 54.67.42.145: ec2-54-67-42-145.us-west-1.compute.amazonaws.com

Not shown: 998 filtered ports

PORT STATE SERVICE VERSION

80/tcp open http

443/tcp open ssl/https

2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port80-TCP:V=7.91%I=7%D=12/17%Time=676131AA%P=x86\_64-pc-linux-gnu%r(Get

SF:Request,112,"HTTP/1\.1\x20404\x20Not\x20Found\r\ncontent-type:\x20text/

SF:plain\r\ncontent-length:\x200\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x20

SF:8:09:15\x20GMT\r\nx-frame-options:\x20SAMEORIGIN\r\nstrict-transport-se

SF:curity:\x20max-age=2592000\r\ncache-control:\x20private,\x20no-cache,\x

SF:20no-store,\x20max-age=0\r\nexpires:\x20Mon,\x2001\x20Jan\x201990\x200:

SF:00:00\x20GMT\r\n\r\n")%r(HTTPOptions,112,"HTTP/1\.1\x20404\x20Not\x20Fo

SF:und\r\ncontent-type:\x20text/plain\r\ncontent-length:\x200\r\ndate:\x20

SF:Tue,\x2017\x20Dec\x202024\x208:09:16\x20GMT\r\nx-frame-options:\x20SAME

SF:ORIGIN\r\nstrict-transport-security:\x20max-age=2592000\r\ncache-contro

SF:l:\x20private,\x20no-cache,\x20no-store,\x20max-age=0\r\nexpires:\x20Mo

SF:n,\x2001\x20Jan\x201990\x200:00:00\x20GMT\r\n\r\n")%r(RTSPRequest,112,"

SF:HTTP/1\.1\x20404\x20Not\x20Found\r\ncontent-type:\x20text/plain\r\ncont

SF:ent-length:\x200\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x208:09:17\x20GM

SF:T\r\nx-frame-options:\x20SAMEORIGIN\r\nstrict-transport-security:\x20ma

SF:x-age=2592000\r\ncache-control:\x20private,\x20no-cache,\x20no-store,\x

SF:20max-age=0\r\nexpires:\x20Mon,\x2001\x20Jan\x201990\x200:00:00\x20GMT\

SF:r\n\r\n")%r(FourOhFourRequest,112,"HTTP/1\.1\x20404\x20Not\x20Found\r\n

SF:content-type:\x20text/plain\r\ncontent-length:\x200\r\ndate:\x20Tue,\x2

SF:017\x20Dec\x202024\x208:09:23\x20GMT\r\nx-frame-options:\x20SAMEORIGIN\

SF:r\nstrict-transport-security:\x20max-age=2592000\r\ncache-control:\x20p

SF:rivate,\x20no-cache,\x20no-store,\x20max-age=0\r\nexpires:\x20Mon,\x200

SF:1\x20Jan\x201990\x200:00:00\x20GMT\r\n\r\n")%r(Help,112,"HTTP/1\.1\x204

SF:04\x20Not\x20Found\r\ncontent-type:\x20text/plain\r\ncontent-length:\x2

SF:00\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x208:09:44\x20GMT\r\nx-frame-o

SF:ptions:\x20SAMEORIGIN\r\nstrict-transport-security:\x20max-age=2592000\

SF:r\ncache-control:\x20private,\x20no-cache,\x20no-store,\x20max-age=0\r\

SF:nexpires:\x20Mon,\x2001\x20Jan\x201990\x200:00:00\x20GMT\r\n\r\n")%r(SS

SF:LSessionReq,112,"HTTP/1\.1\x20404\x20Not\x20Found\r\ncontent-type:\x20t

SF:ext/plain\r\ncontent-length:\x200\r\ndate:\x20Tue,\x2017\x20Dec\x202024

SF:\x208:09:45\x20GMT\r\nx-frame-options:\x20SAMEORIGIN\r\nstrict-transpor

SF:t-security:\x20max-age=2592000\r\ncache-control:\x20private,\x20no-cach

SF:e,\x20no-store,\x20max-age=0\r\nexpires:\x20Mon,\x2001\x20Jan\x201990\x

SF:200:00:00\x20GMT\r\n\r\n");

==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============

SF-Port443-TCP:V=7.91%T=SSL%I=7%D=12/17%Time=676131BE%P=x86\_64-pc-linux-gn

SF:u%r(FourOhFourRequest,112,"HTTP/1\.1\x20404\x20Not\x20Found\r\ncontent-

SF:type:\x20text/plain\r\ncontent-length:\x200\r\ndate:\x20Tue,\x2017\x20D

SF:ec\x202024\x208:09:35\x20GMT\r\nx-frame-options:\x20SAMEORIGIN\r\nstric

SF:t-transport-security:\x20max-age=2592000\r\ncache-control:\x20private,\

SF:x20no-cache,\x20no-store,\x20max-age=0\r\nexpires:\x20Mon,\x2001\x20Jan

SF:\x201990\x200:00:00\x20GMT\r\n\r\n")%r(SSLSessionReq,112,"HTTP/1\.1\x20

SF:404\x20Not\x20Found\r\ncontent-type:\x20text/plain\r\ncontent-length:\x

SF:200\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x208:10:19\x20GMT\r\nx-frame-

SF:options:\x20SAMEORIGIN\r\nstrict-transport-security:\x20max-age=2592000

SF:\r\ncache-control:\x20private,\x20no-cache,\x20no-store,\x20max-age=0\r

SF:\nexpires:\x20Mon,\x2001\x20Jan\x201990\x200:00:00\x20GMT\r\n\r\n")%r(T

SF:erminalServerCookie,112,"HTTP/1\.1\x20404\x20Not\x20Found\r\ncontent-ty

SF:pe:\x20text/plain\r\ncontent-length:\x200\r\ndate:\x20Tue,\x2017\x20Dec

SF:\x202024\x208:10:20\x20GMT\r\nx-frame-options:\x20SAMEORIGIN\r\nstrict-

SF:transport-security:\x20max-age=2592000\r\ncache-control:\x20private,\x2

SF:0no-cache,\x20no-store,\x20max-age=0\r\nexpires:\x20Mon,\x2001\x20Jan\x

SF:201990\x200:00:00\x20GMT\r\n\r\n")%r(TLSSessionReq,112,"HTTP/1\.1\x2040

SF:4\x20Not\x20Found\r\ncontent-type:\x20text/plain\r\ncontent-length:\x20

SF:0\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x208:10:21\x20GMT\r\nx-frame-op

SF:tions:\x20SAMEORIGIN\r\nstrict-transport-security:\x20max-age=2592000\r

SF:\ncache-control:\x20private,\x20no-cache,\x20no-store,\x20max-age=0\r\n

SF:expires:\x20Mon,\x2001\x20Jan\x201990\x200:00:00\x20GMT\r\n\r\n")%r(Ker

SF:beros,112,"HTTP/1\.1\x20404\x20Not\x20Found\r\ncontent-type:\x20text/pl

SF:ain\r\ncontent-length:\x200\r\ndate:\x20Tue,\x2017\x20Dec\x202024\x208:

SF:10:22\x20GMT\r\nx-frame-options:\x20SAMEORIGIN\r\nstrict-transport-secu

SF:rity:\x20max-age=2592000\r\ncache-control:\x20private,\x20no-cache,\x20

SF:no-store,\x20max-age=0\r\nexpires:\x20Mon,\x2001\x20Jan\x201990\x200:00

SF::00\x20GMT\r\n\r\n")%r(LDAPSearchReq,112,"HTTP/1\.1\x20404\x20Not\x20Fo

SF:und\r\ncontent-type:\x20text/plain\r\ncontent-length:\x200\r\ndate:\x20

SF:Tue,\x2017\x20Dec\x202024\x208:10:40\x20GMT\r\nx-frame-options:\x20SAME

SF:ORIGIN\r\nstrict-transport-security:\x20max-age=2592000\r\ncache-contro

SF:l:\x20private,\x20no-cache,\x20no-store,\x20max-age=0\r\nexpires:\x20Mo

SF:n,\x2001\x20Jan\x201990\x200:00:00\x20GMT\r\n\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 178.45 seconds

[+] Checking for outdated CMS...

No CMS detected.

[+] Is the Website Safe?

------------------------------

Current Status: The website has vulnerabilities, making it not entirely safe.

[!] Issues Detected:

- No Web Application Firewall (WAF) detected.

- Missing security headers: Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, X-XSS-Protection.

- Missing critical security headers, making the site prone to attacks like XSS or clickjacking

[+] Next Steps:

- If this is your website, prioritize fixing the issues listed above.

- If it's a third-party website, avoid sharing sensitive data with it until these issues are resolved.

------------------------------

Scan Completed!

Website: https://example.com

WAF: No WAF detected

HTTPS: HTTPS (443) detected

CMS: No CMS detected

Missing Headers: Content-Security-Policy, X-Frame-Options

[!] Issues Detected:

No Web Application Firewall (WAF) detected

Missing security headers: Content-Security-Policy, X-Frame-Options

Website: https://google.com

WAF: WAF detected

HTTPS: HTTPS (443) detected

CMS: No CMS detected

Missing Headers: None

[+] No critical issues detected.

Website: https://wordpress.com

WAF: No WAF detected

HTTPS: HTTPS (443) detected

CMS: WordPress 6.3

Missing Headers: Strict-Transport-Security

[!] Issues Detected:

No Web Application Firewall (WAF) detected

Detected CMS: WordPress 6.3 (check for vulnerabilities)

Missing security headers: Strict-Transport-Security

Website: https://testphp.vulnweb.com

WAF: No WAF detected

HTTPS: HTTPS not detected

CMS: No CMS detected

Missing Headers: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security

[!] Issues Detected:

No Web Application Firewall (WAF) detected

No HTTPS detected

Missing security headers: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security

Website: https://github.com

WAF: WAF detected

HTTPS: HTTPS (443) detected

CMS: No CMS detected

Missing Headers: None

[+] No critical issues detected.