Sri Lanka Institute of Information Technology

IE2062

Web Security

Bug Bounty Report I

Submitted by:

Student Registration Number	Student Name
IT21197550	Nihila Premakanthan

Date of Submission: 28.05.2023

Acknowledgement

I would like to express my special thanks to our mentor Ms. Chethana Liyanapathirana and Dr. Lakmal Rupansighe for their time and efforts she provided throughout the course, and for the Web Security lecture panel for guiding us through this semester and for helping us by giving examples, guidelines, and advice about the project. Your useful advice and suggestions were really helpful to me during the project's completion. In this aspect, I am eternally grateful to you.

Executive Summary

This report aims to provide an overview of the vulnerability identified in a particular domain. The bug bounty platform called Hackerone was used for this purpose. This report analyses the domain of Tide (https://www.tide.co/).

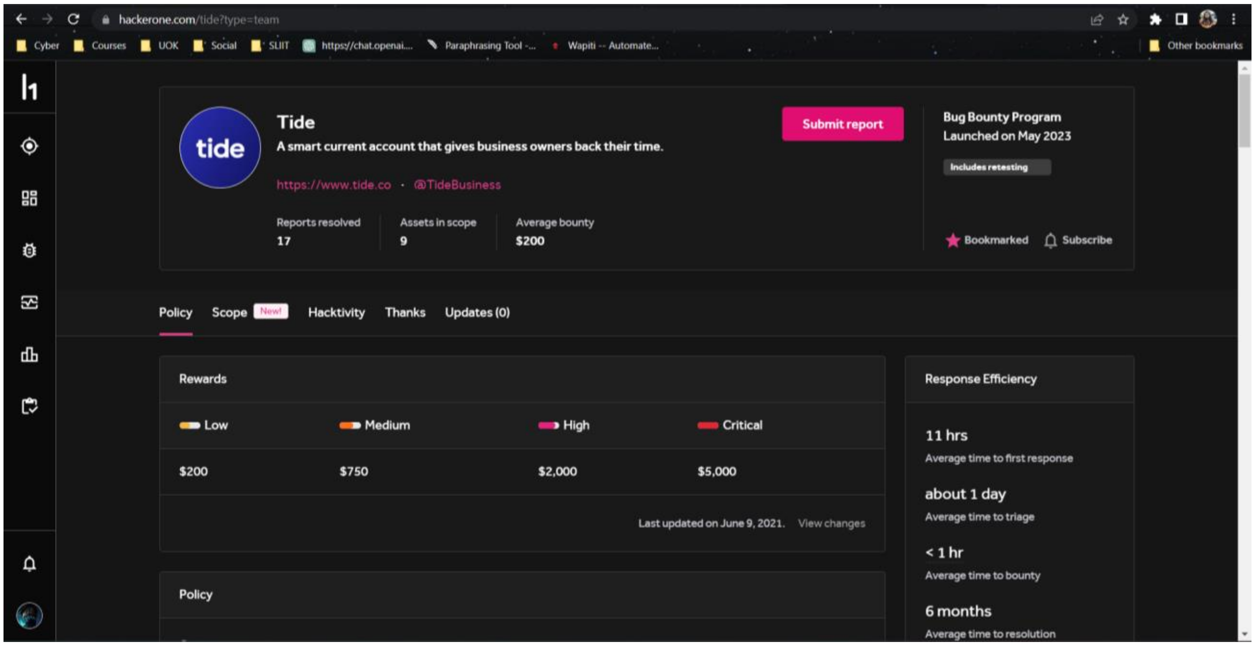
This report uses different tools to gather information detect vulnerabilities and perform penetration testing. The tool name Netsparker and Owasp Zap was mainly used to identify the vulnerability. Further this report provides the vulnerability title, vulnerability description, Affected Components, Impact Assessment, Steps to reproduce the vulnerability, proof of concept and the proposed mitigation.

By including these comprehensive details for each vulnerability, the report provides a comprehensive overview of the security weaknesses present within the system and offers actionable insights for remediation and improvement.

Contents

Introduction

Affected URL: https://www.tide.co/



Tide

A smart current account that gives business owners back their time.

https://www.tide.co · @TideBusiness

Reports resolved 17 | Assets in scope 9 | Average bounty $200

Bug Bounty Program
Launched on May 2023

Includes retesting

Rewards

Low	Medium	High	Critical
$200	$750	$2,000	$5,000

Last updated on June 9, 2021.

Response Efficiency

11 hrs
Average time to first response

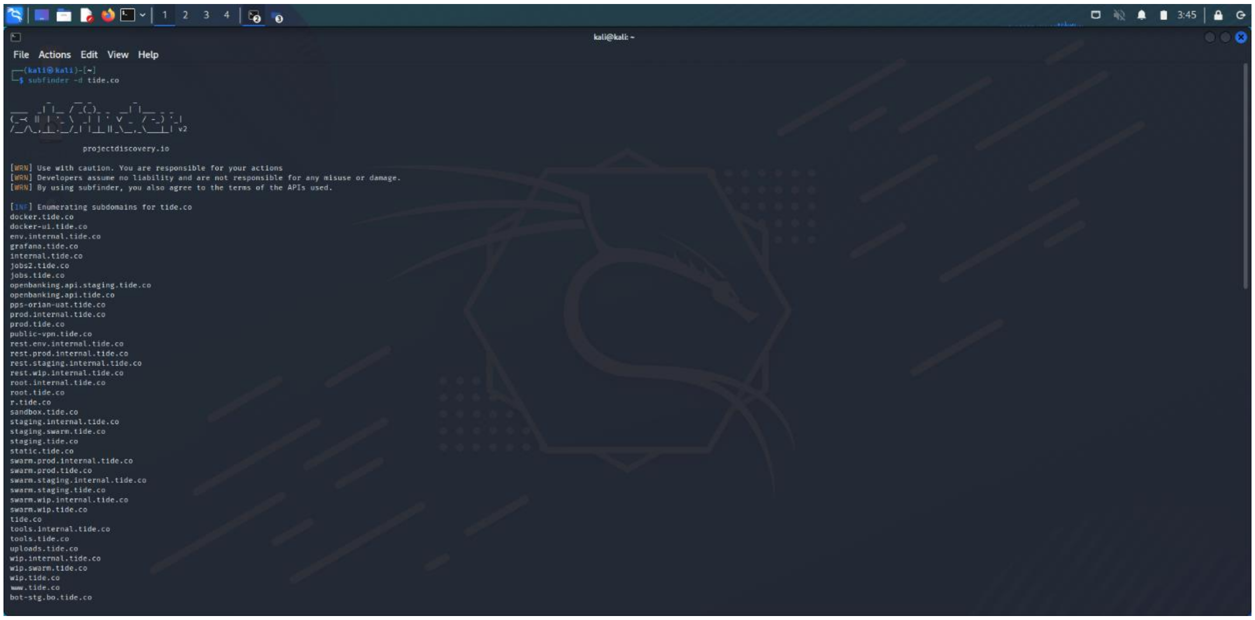
about 1 day
Average time to triage

< 1 hr
Average time to bounty

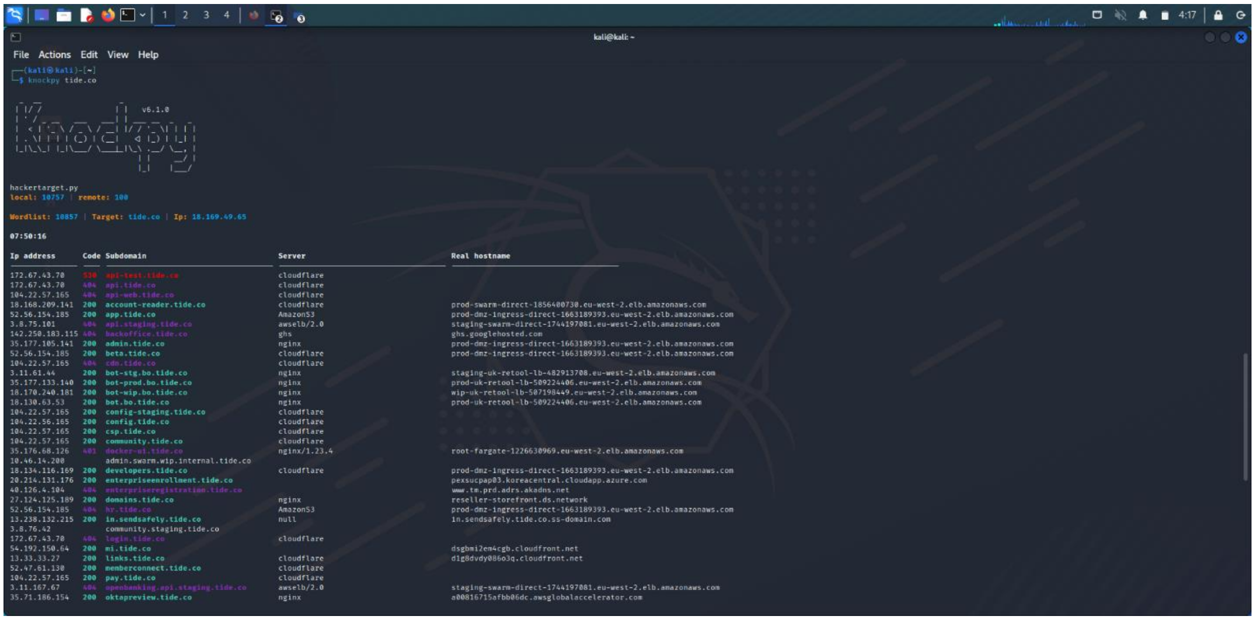
6 months
Average time to resolution

Policy

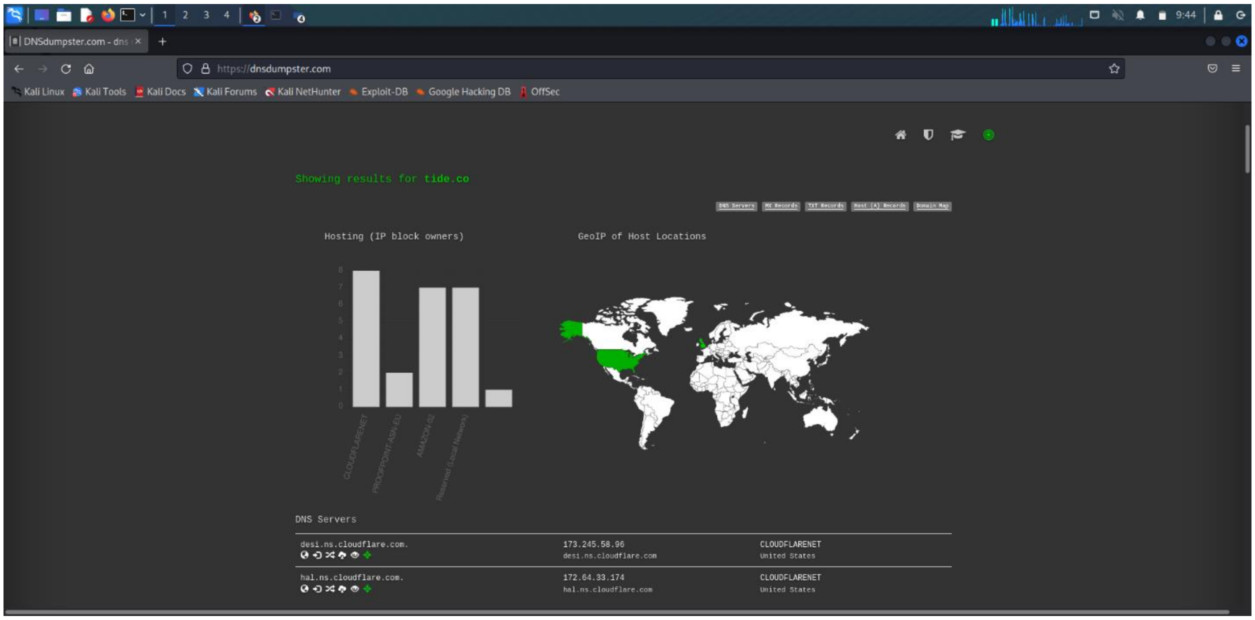
Information gathering



```
┌──(kali㉿kali)-[~]
└─$ subfinder -d tide.co

               __    _____           __         
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /    
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/ v2

                projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.

[INF] Enumerating subdomains for tide.co
docker.tide.co
docker-ui.tide.co
env.internal.tide.co
grafana.tide.co
internal.tide.co
jobs2.tide.co
jobs.tide.co
openbanking.api.staging.tide.co
openbanking.api.tide.co
pps-orian-uat.tide.co
prod.internal.tide.co
prod.tide.co
public-vpn.tide.co
rest.env.internal.tide.co
rest.prod.internal.tide.co
rest.staging.internal.tide.co
rest.wip.internal.tide.co
root.internal.tide.co
root.tide.co
r.tide.co
sandbox.tide.co
staging.internal.tide.co
staging.swarm.tide.co
staging.tide.co
static.tide.co
swarm.prod.internal.tide.co
swarm.prod.tide.co
swarm.staging.internal.tide.co
swarm.staging.tide.co
swarm.wip.internal.tide.co
swarm.wip.tide.co
tide.co
tools.internal.tide.co
tools.tide.co
uploads.tide.co
wip.internal.tide.co
wip.swarm.tide.co
wip.tide.co
www.tide.co
bot-stg.bo.tide.co
```



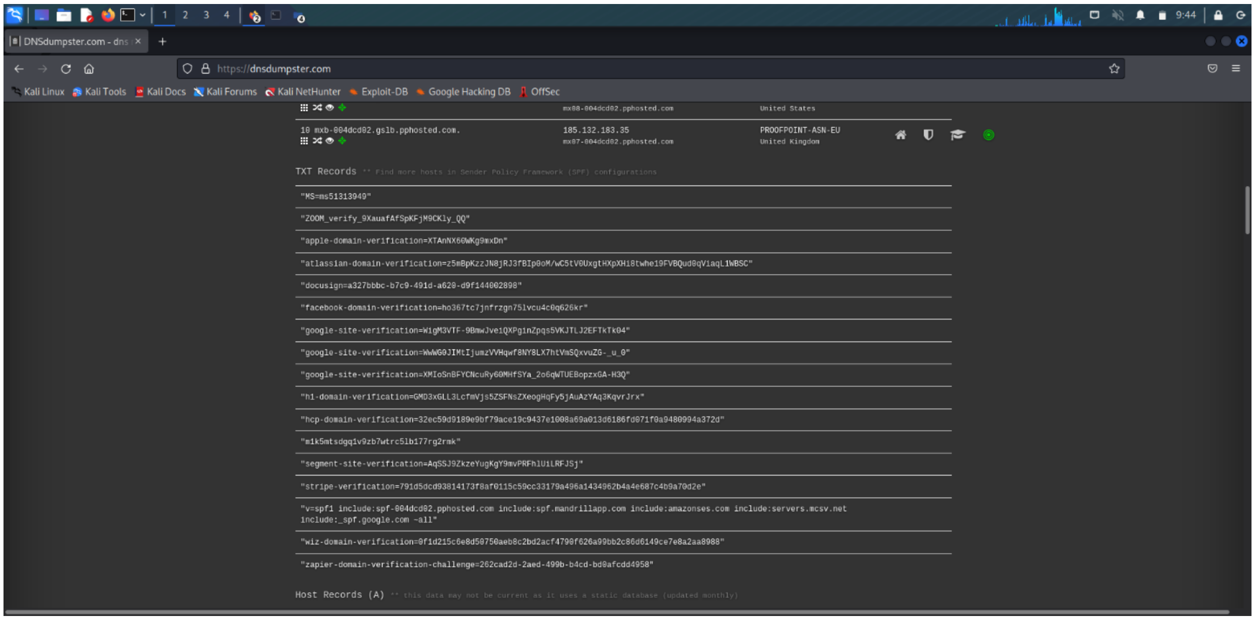
```
┌──(kali㉿kali)-[~]
└─$ knockpy tide.co

  _  __             _
 | |/ /            | |   v6.1.0
 | ' / _ __   ___   ___| | ___ __  _   _
 |  < | '_ \ / _ \ / __| |/ / '_ \| | | |
 | . \| | | | (_) | (__|   <| |_) | |_| |
 |_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                            | |     __/ |
                            |_|    |___/

hackertarget.py
local: 10757 | remote: 100

Wordlist: 10857 | Target: tide.co | Ip: 18.169.49.65

07:50:16

Ip address      Code Subdomain                             Server          Real hostname
_______________ ____ _____________________________________ _______________ __________________________________________________________

172.67.43.70    530  api-test.tide.co                      cloudflare
172.67.43.70    404  api.tide.co                           cloudflare
104.22.57.165   404  api-web.tide.co                       cloudflare
18.168.209.141  200  account-reader.tide.co                cloudflare      prod-swarm-direct-1856400730.eu-west-2.elb.amazonaws.com
52.56.154.185   200  app.tide.co                           AmazonS3        prod-dmz-ingress-direct-1663189393.eu-west-2.elb.amazonaws.com
3.8.75.101      404  api.staging.tide.co                   awselb/2.0      staging-swarm-direct-1744197081.eu-west-2.elb.amazonaws.com
142.250.183.115 404  backoffice.tide.co                    ghs             ghs.googlehosted.com
35.177.105.141  200  admin.tide.co                         nginx           prod-dmz-ingress-direct-1663189393.eu-west-2.elb.amazonaws.com
52.56.154.185   200  beta.tide.co                          cloudflare      prod-dmz-ingress-direct-1663189393.eu-west-2.elb.amazonaws.com
104.22.57.165   404  cdn.tide.co                           cloudflare
3.11.61.44      200  bot-stg.bo.tide.co                    nginx           staging-uk-retool-lb-482913708.eu-west-2.elb.amazonaws.com
35.177.133.140  200  bot-prod.bo.tide.co                   nginx           prod-uk-retool-lb-509224406.eu-west-2.elb.amazonaws.com
18.170.240.181  200  bot-wip.bo.tide.co                    nginx           wip-uk-retool-lb-507198449.eu-west-2.elb.amazonaws.com
18.130.63.53    200  bot.bo.tide.co                        nginx           prod-uk-retool-lb-509224406.eu-west-2.elb.amazonaws.com
104.22.57.165   200  config-staging.tide.co                cloudflare
104.22.56.165   200  config.tide.co                        cloudflare
104.22.57.165   200  csp.tide.co                           cloudflare
104.22.57.165   200  community.tide.co                     cloudflare
35.176.68.126   401  docker-ui.tide.co                     nginx/1.23.4    root-fargate-1226630969.eu-west-2.elb.amazonaws.com
10.46.14.200         admin.swarm.wip.internal.tide.co
18.134.116.169  200  developers.tide.co                    cloudflare      prod-dmz-ingress-direct-1663189393.eu-west-2.elb.amazonaws.com
20.214.131.176  200  enterpriseenrollment.tide.co                          pexsucpap03.koreacentral.cloudapp.azure.com
40.126.4.104    404  enterpriseregistration.tide.co                        www.tm.prd.adrs.akadns.net
27.124.125.189  200  domains.tide.co                       nginx           reseller-storefront.ds.network
52.56.154.185   404  hr.tide.co                            AmazonS3        prod-dmz-ingress-direct-1663189393.eu-west-2.elb.amazonaws.com
13.238.132.215  200  in.sendsafely.tide.co                 null            in.sendsafely.tide.co.ss-domain.com
3.8.76.42            community.staging.tide.co
172.67.43.70    404  login.tide.co                         cloudflare
54.192.150.64   200  mi.tide.co                                            dsgbmi2em4cgb.cloudfront.net
13.33.33.27     200  links.tide.co                         cloudflare      d1g8dvdy086o3q.cloudfront.net
52.47.61.130    200  memberconnect.tide.co                 cloudflare
104.22.57.165   200  pay.tide.co                           cloudflare
3.11.167.67     404  openbanking.api.staging.tide.co       awselb/2.0      staging-swarm-direct-1744197081.eu-west-2.elb.amazonaws.com
35.71.186.154   200  oktapreview.tide.co                   nginx           a00816715afbb06dc.awsglobalaccelerator.com
```



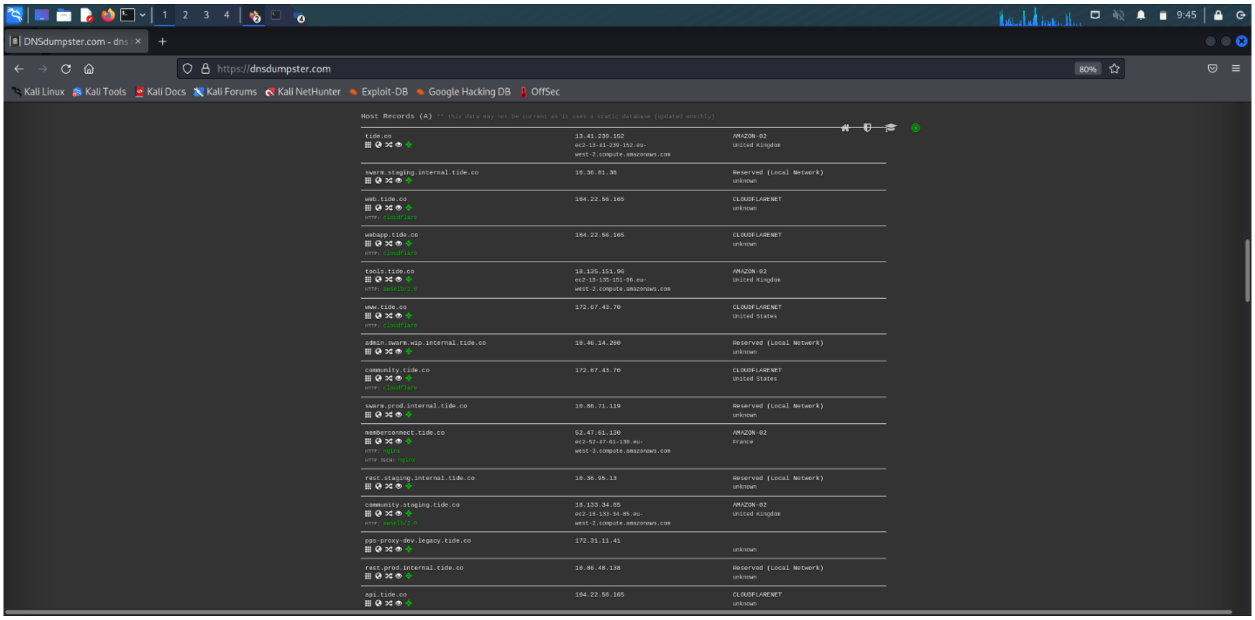
Showing results for tide.co

DNS Servers

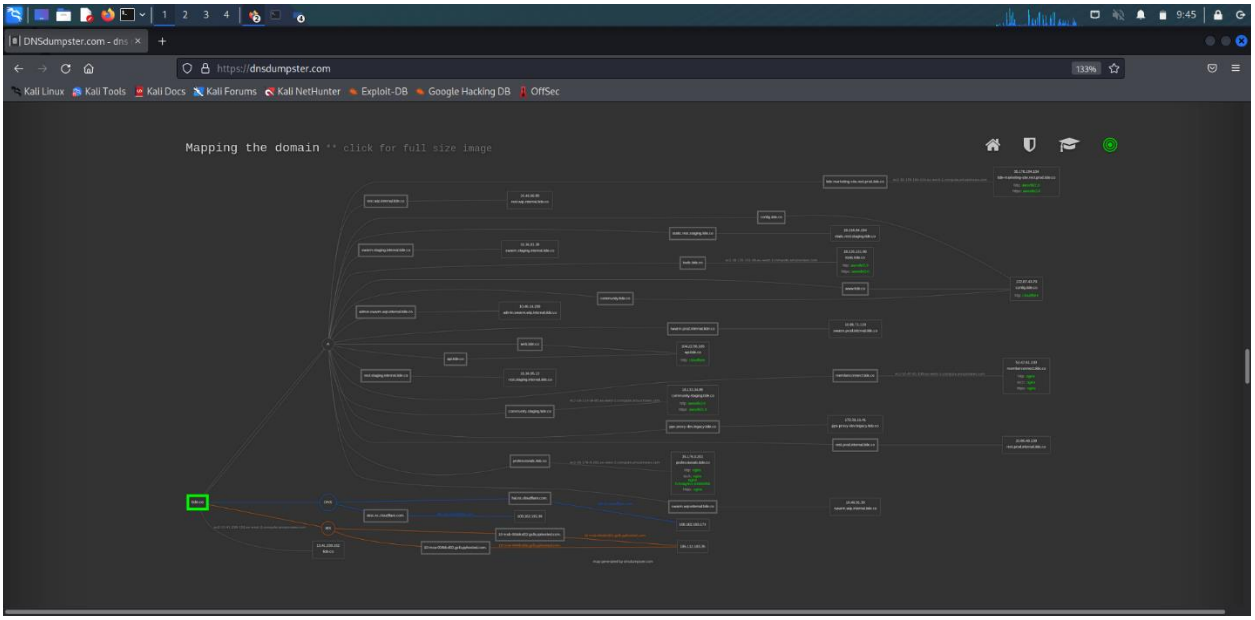
desi.ns.cloudflare.com.	173.245.58.96 desi.ns.cloudflare.com	CLOUDFLARENET United States
hal.ns.cloudflare.com.	172.64.33.174 hal.ns.cloudflare.com	CLOUDFLARENET United States

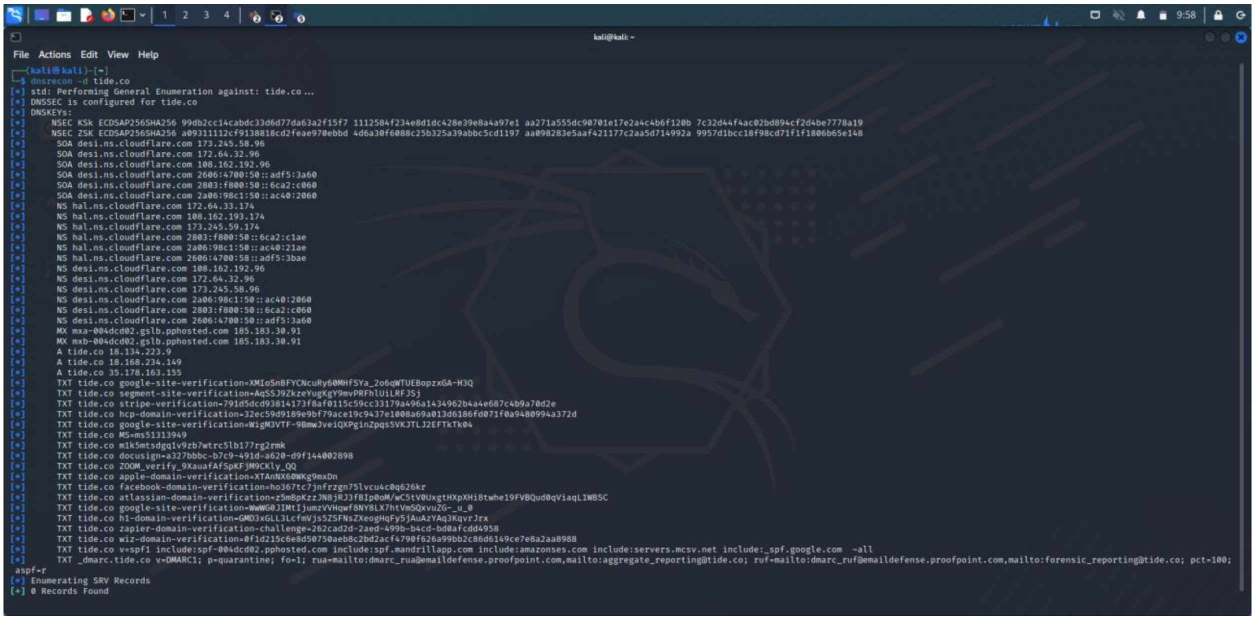


```
                                     mx08-004dcd02.pphosted.com        United States

10 mxb-004dcd02.gslb.pphosted.com.   185.132.183.35                    PROOFPOINT-ASN-EU
                                     mx07-004dcd02.pphosted.com        United Kingdom

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"MS=ms51313949"
"ZOOM_verify_9XauafAfSpKFjM9CKly_QQ"
"apple-domain-verification=XTAnNX60WKg9mxDn"
"atlassian-domain-verification=z5mBpKzzJN8jRJ3fBIp0oM/wC5tV0UxgtHXpXHi8twhe19FVBQud0qViaqL1WBSC"
"docusign=a327bbbc-b7c9-491d-a620-d9f144002898"
"facebook-domain-verification=ho367tc7jnfrzgn75lvcu4c0q626kr"
"google-site-verification=WigM3VTF-9BmwJve1QXPginZpqs5VKJTLJ2EFTkTk04"
"google-site-verification=WwWG0JIMtIjumzVVHqwf8NY8LX7htVmSQxvuZG-_u_0"
"google-site-verification=XMIoSnBFYCNcuRy60MHfSYa_2o6qWTUEBopzxGA-H3Q"
"h1-domain-verification=GMD3xGLL3LcfmVjs5ZSFNsZXeogHqFy5jAuAzYAq3KqvrJrx"
"hcp-domain-verification=32ec59d9189e9bf79ace19c9437e1008a69a013d6186fd071f0a9480994a372d"
"m1k5mtsdgq1v9zb7wtrc5lb177rg2rmk"
"segment-site-verification=AqSSJ9ZkzeYugKgY9mvPRFhlUiLRFJSj"
"stripe-verification=791d5dcd93814173f8af0115c59cc33179a496a1434962b4a4e687c4b9a70d2e"
"v=spf1 include:spf-004dcd02.pphosted.com include:spf.mandrillapp.com include:amazonses.com include:servers.mcsv.net
include:_spf.google.com ~all"
"wiz-domain-verification=0f1d215c6e8d50750aeb8c2bd2acf4790f626a99bb2c86d6149ce7e8a2aa8988"
"zapier-domain-verification-challenge=262cad2d-2aed-499b-b4cd-bd0afcdd4958"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)
```

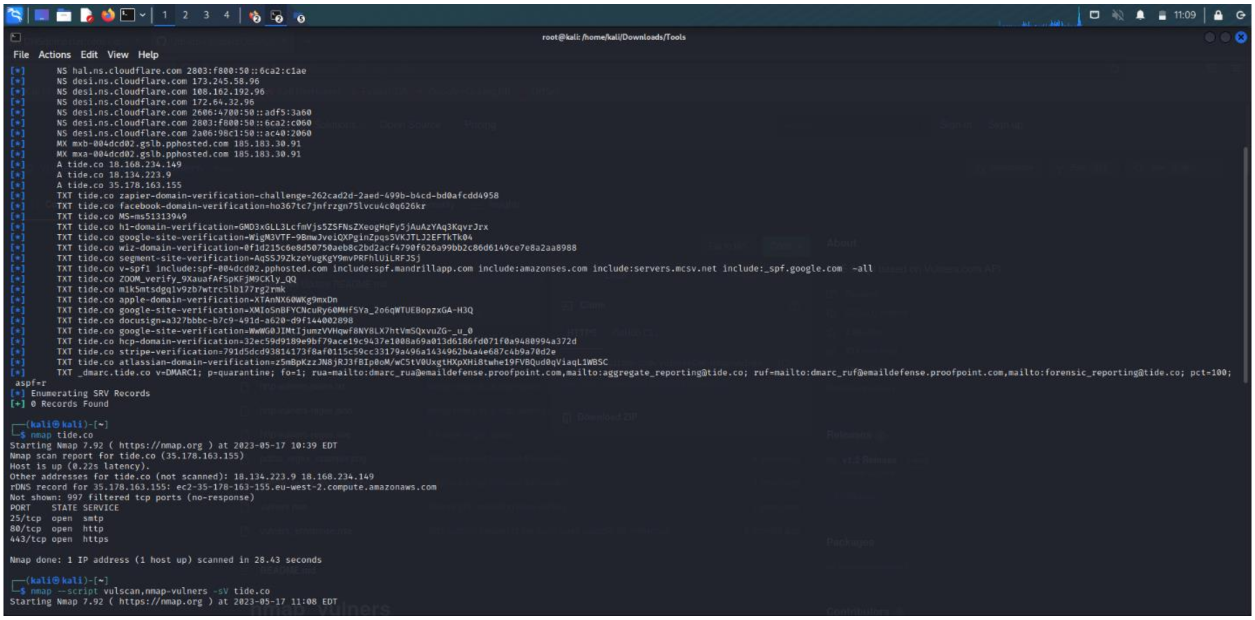


```
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

tide.co                            13.41.239.152                      AMAZON-02
                                   ec2-13-41-239-152.eu-              United Kingdom
                                   west-2.compute.amazonaws.com

swarm.staging.internal.tide.co     10.36.81.38                        Reserved (Local Network)
                                                                      unknown

web.tide.co                        104.22.56.165                      CLOUDFLARENET
                                                                      unknown
HTTP: cloudflare

webapp.tide.co                     104.22.56.165                      CLOUDFLARENET
                                                                      unknown
HTTP: cloudflare

tools.tide.co                      18.135.151.96                      AMAZON-02
                                   ec2-18-135-151-96.eu-              United Kingdom
HTTP: awselb/2.0                   west-2.compute.amazonaws.com

www.tide.co                        172.67.43.70                       CLOUDFLARENET
                                                                      United States
HTTP: cloudflare

admin.swarm.wip.internal.tide.co   10.46.14.200                       Reserved (Local Network)
                                                                      unknown

community.tide.co                  172.67.43.70                       CLOUDFLARENET
                                                                      United States
HTTP: cloudflare

swarm.prod.internal.tide.co        10.86.71.119                       Reserved (Local Network)
                                                                      unknown

memberconnect.tide.co              52.47.61.130                       AMAZON-02
                                   ec2-52-47-61-130.eu-               France
HTTP: nginx                        west-3.compute.amazonaws.com
HTTP TECH: nginx

rest.staging.internal.tide.co      10.36.95.13                        Reserved (Local Network)
                                                                      unknown

community.staging.tide.co          18.133.34.85                       AMAZON-02
                                   ec2-18-133-34-85.eu-               United Kingdom
HTTP: awselb/2.0                   west-2.compute.amazonaws.com

pps-proxy-dev.legacy.tide.co       172.31.11.41
                                                                      unknown

rest.prod.internal.tide.co         10.86.48.138                       Reserved (Local Network)
                                                                      unknown

api.tide.co                        104.22.56.165                      CLOUDFLARENET
                                                                      unknown
```

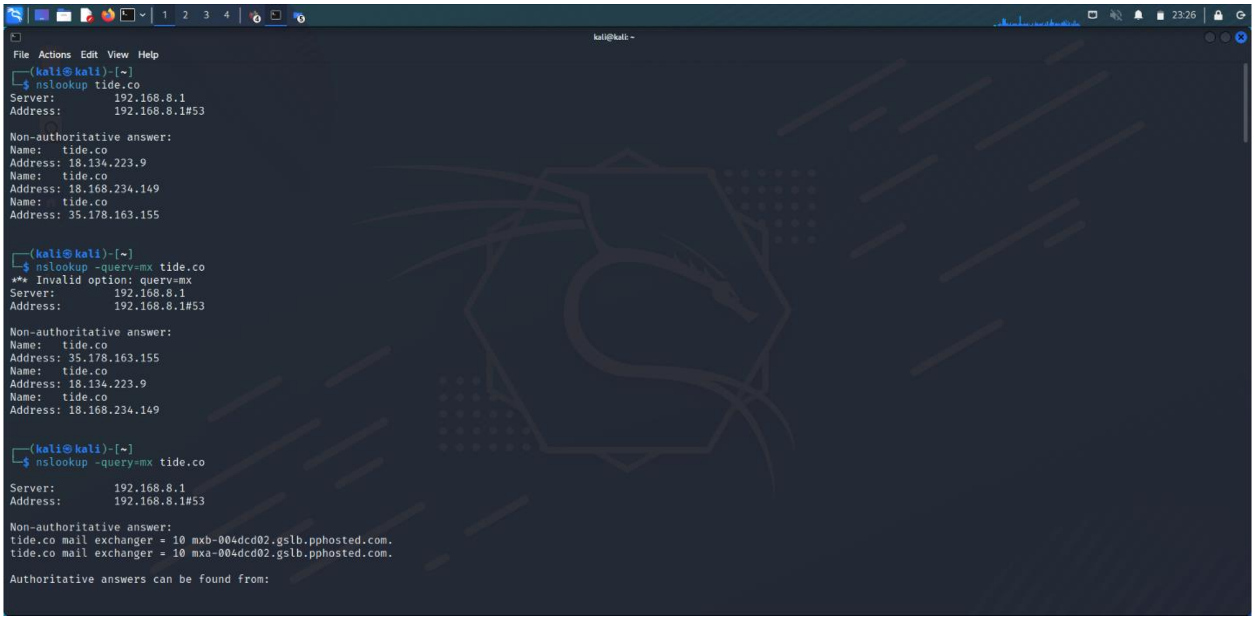




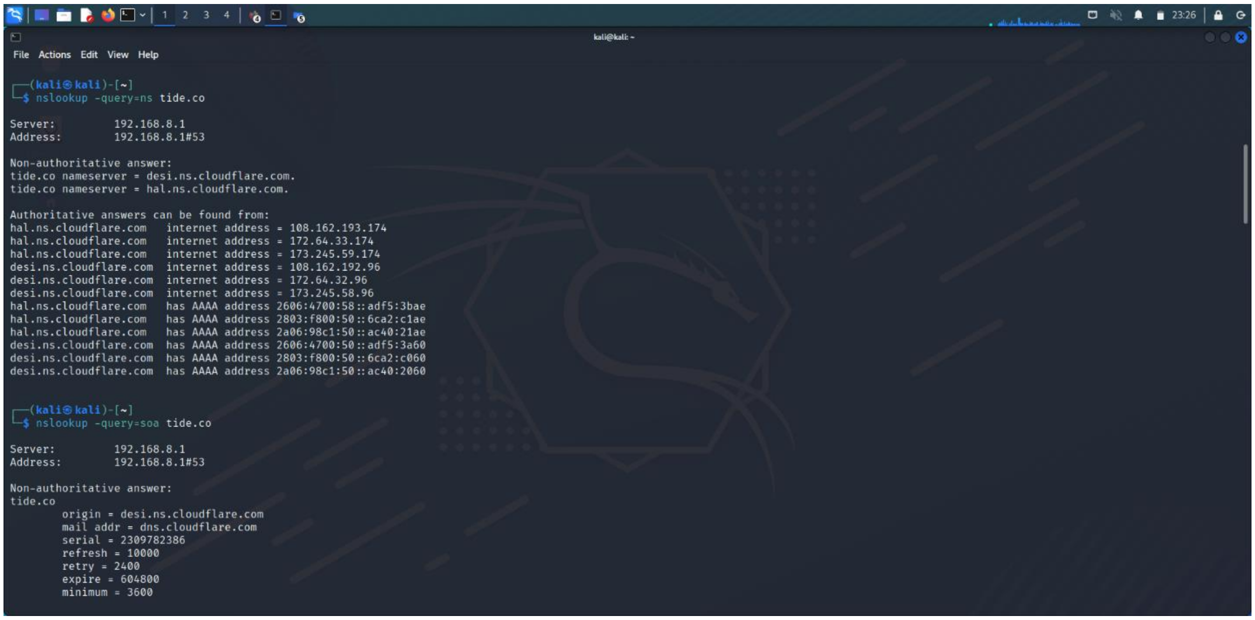
```
┌──(kali㉿kali)-[~]
└─$ dnsrecon -d tide.co
[*] std: Performing General Enumeration against: tide.co ...
[*] DNSSEC is configured for tide.co
[*] DNSKEYs:
[*]     NSEC KSk ECDSAP256SHA256 99db2cc14cabdc33d6d77da63a2f15f7 1112584f234e8d1dc428e39e8a4a97e1 aa271a555dc90701e17e2a4c4b6f120b 7c32d44f4ac02bd894cf2d4be7778a19
[*]     NSEC ZSK ECDSAP256SHA256 a09311112cf9138818cd2feae970ebbd 4d6a30f6088c25b325a39abbc5cd1197 aa098283e5aaf421177c2aa5d714992a 9957d1bcc18f98cd71f1f1806b65e148
[*]      SOA desi.ns.cloudflare.com 173.245.58.96
[*]      SOA desi.ns.cloudflare.com 172.64.32.96
[*]      SOA desi.ns.cloudflare.com 108.162.192.96
[*]      SOA desi.ns.cloudflare.com 2606:4700:50::adf5:3a60
[*]      SOA desi.ns.cloudflare.com 2803:f800:50::6ca2:c060
[*]      SOA desi.ns.cloudflare.com 2a06:98c1:50::ac40:2060
[*]      NS hal.ns.cloudflare.com 172.64.33.174
[*]      NS hal.ns.cloudflare.com 108.162.193.174
[*]      NS hal.ns.cloudflare.com 173.245.59.174
[*]      NS hal.ns.cloudflare.com 2803:f800:50::6ca2:c1ae
[*]      NS hal.ns.cloudflare.com 2a06:98c1:50::ac40:21ae
[*]      NS hal.ns.cloudflare.com 2606:4700:58::adf5:3bae
[*]      NS desi.ns.cloudflare.com 108.162.192.96
[*]      NS desi.ns.cloudflare.com 172.64.32.96
[*]      NS desi.ns.cloudflare.com 173.245.58.96
[*]      NS desi.ns.cloudflare.com 2a06:98c1:50::ac40:2060
[*]      NS desi.ns.cloudflare.com 2803:f800:50::6ca2:c060
[*]      NS desi.ns.cloudflare.com 2606:4700:50::adf5:3a60
[*]      MX mxa-004dcd02.gslb.pphosted.com 185.183.30.91
[*]      MX mxb-004dcd02.gslb.pphosted.com 185.183.30.91
[*]      A tide.co 18.134.223.9
[*]      A tide.co 18.168.234.149
[*]      A tide.co 35.178.163.155
[*]      TXT tide.co google-site-verification=XMIoSnBFYCNcuRy60MHfSYa_2o6qWTUEBopzxGA-H3Q
[*]      TXT tide.co segment-site-verification=AqSSJ9ZkzeYugKgY9mvPRFhlUiLRFJSj
[*]      TXT tide.co stripe-verification=791d5dcd93814173f8af0115c59cc33179a496a1434962b4a4e687c4b9a70d2e
[*]      TXT tide.co hcp-domain-verification=32ec59d9189e9bf79ace19c9437e1008a69a013d6186fd071f0a9480994a372d
[*]      TXT tide.co google-site-verification=WigM3VTF-9BmwJveiQXPginZpqs5VKJTLJ2EFTkTk04
[*]      TXT tide.co MS=ms51313949
[*]      TXT tide.co m1k5mtsdgq1v9zb7wtrc5lb177rg2rmk
[*]      TXT tide.co docusign=a327bbbc-b7c9-491d-a620-d9f144002898
[*]      TXT tide.co ZOOM_verify_9XauafAfSpKFjM9CKly_QQ
[*]      TXT tide.co apple-domain-verification=XTAnNX60WKg9mxDn
[*]      TXT tide.co facebook-domain-verification=ho367tc7jnfrzgn75lvcu4c0q626kr
[*]      TXT tide.co atlassian-domain-verification=z5mBpKzzJN8jRJ3fBIp0oM/wC5tV0UxgtHXpXHi8twhe19FVBQud0qViaqL1WBSC
[*]      TXT tide.co google-site-verification=WwWG0JIMtIjumzVVHqwf8NY8LX7htVmSQxvuZG-_u_0
[*]      TXT tide.co h1-domain-verification=GMD3xGLL3LcfmVjs5ZSFNsZXeogHqFy5jAuAzYAq3KqvrJrx
[*]      TXT tide.co zapier-domain-verification-challenge=262cad2d-2aed-499b-b4cd-bd0afcdd4958
[*]      TXT tide.co wiz-domain-verification=0f1d215c6e8d50750aeb8c2bd2acf4790f626a99bb2c86d6149ce7e8a2aa8988
[*]      TXT tide.co v=spf1 include:spf-004dcd02.pphosted.com include:spf.mandrillapp.com include:amazonses.com include:servers.mcsv.net include:_spf.google.com  ~all
[*]      TXT _dmarc.tide.co v=DMARC1; p=quarantine; fo=1; rua=mailto:dmarc_rua@emaildefense.proofpoint.com,mailto:aggregate_reporting@tide.co; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com,mailto:forensic_reporting@tide.co; pct=100;
 aspf=r
[*] Enumerating SRV Records
[+] 0 Records Found
```


File Actions Edit View Help
root@kali: /home/kali/Downloads/Tools

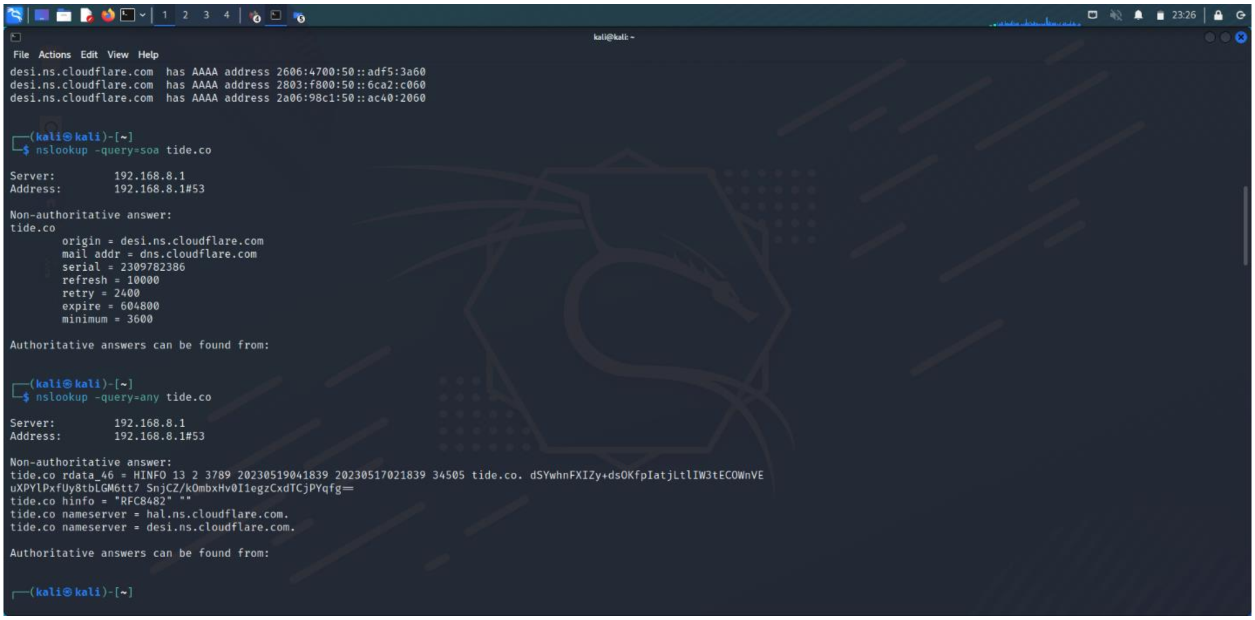
```
[*]       NS hal.ns.cloudflare.com 2803:f800:50::6ca2:c1ae
[*]       NS desi.ns.cloudflare.com 173.245.58.96
[*]       NS desi.ns.cloudflare.com 108.162.192.96
[*]       NS desi.ns.cloudflare.com 172.64.32.96
[*]       NS desi.ns.cloudflare.com 2606:4700:50::adf5:3a60
[*]       NS desi.ns.cloudflare.com 2803:f800:50::6ca2:c060
[*]       NS desi.ns.cloudflare.com 2a06:98c1:50::ac40:2060
[*]       MX mxb-004dcd02.gslb.pphosted.com 185.183.30.91
[*]       MX mxa-004dcd02.gslb.pphosted.com 185.183.30.91
[*]       A tide.co 18.168.234.149
[*]       A tide.co 18.134.223.9
[*]       A tide.co 35.178.163.155
[*]       TXT tide.co zapier-domain-verification-challenge=262cad2d-2aed-499b-b4cd-bd0afcdd4958
[*]       TXT tide.co facebook-domain-verification=ho367tc7jnfrzgn75lvcu4c0q626kr
[*]       TXT tide.co MS=ms51313949
[*]       TXT tide.co h1-domain-verification-GMD3xGLL3LcfmVjs5ZSFNsZXeogHqFy5jAuAzYAq3KqvrJrx
[*]       TXT tide.co google-site-verification-WigM3VTF-9BmwJveiQXPginZpqs5VKJTLJ2EFTkTk04
[*]       TXT tide.co wiz-domain-verification-0f1d215c6e8d50750aeb8c2bd2acf4790f626a99bb2c86d6149ce7e8a2aa8988
[*]       TXT tide.co segment-site-verification-AqSSJ9ZkzeYugKgY9mvPRFhlUiLRFJSj
[*]       TXT tide.co v-spf1 include:spf-004dcd02.pphosted.com include:spf.mandrillapp.com include:amazonses.com include:servers.mcsv.net include:_spf.google.com  ~all
[*]       TXT tide.co ZOOM_verify_9XauafAfSpKFjM9CKly_QQ
[*]       TXT tide.co m1k5mtsdgq1v9zb7wtrc5lb177rg2rmk
[*]       TXT tide.co apple-domain-verification-XTAnNX60WKg9mxDn
[*]       TXT tide.co google-site-verification-XMIoSnBFYCNcuRy60MHfSYa_2o6qWTUEBopzxGA-H3Q
[*]       TXT tide.co docusign-a327bbbc-b7c9-491d-a620-d9f144002898
[*]       TXT tide.co google-site-verification=WwWG0JIMtIjumzVVHqwf8NY8LX7htVmSQxvuZG-_u_0
[*]       TXT tide.co hcp-domain-verification=32ec59d9189e9bf79ace19c9437e1008a69a013d6186fd071f0a9480994a372d
[*]       TXT tide.co stripe-verification=791d5dcd93814173f8af0115c59cc33179a496a1434962b4a4e687c4b9a70d2e
[*]       TXT tide.co atlassian-domain-verification=z5mBpKzzJN8jRJ3fBIp0oM/wC5tV0UxgtHXpXHi8twhe19FVBQud0qViaqL1WBSC
[*]       TXT _dmarc.tide.co v=DMARC1; p=quarantine; fo=1; rua=mailto:dmarc_rua@emaildefense.proofpoint.com,mailto:aggregate_reporting@tide.co; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com,mailto:forensic_reporting@tide.co; pct=100;
 aspf=r
[*] Enumerating SRV Records
[+] 0 Records Found

┌──(kali㉿kali)-[~]
└─$ nmap tide.co
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-17 10:39 EDT
Nmap scan report for tide.co (35.178.163.155)
Host is up (0.22s latency).
Other addresses for tide.co (not scanned): 18.134.223.9 18.168.234.149
rDNS record for 35.178.163.155: ec2-35-178-163-155.eu-west-2.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 28.43 seconds

┌──(kali㉿kali)-[~]
└─$ nmap --script vulscan,nmap-vulners -sV tide.co
Starting Nmap 7.92 ( https://nmap.org ) at 2023-05-17 11:08 EDT
```



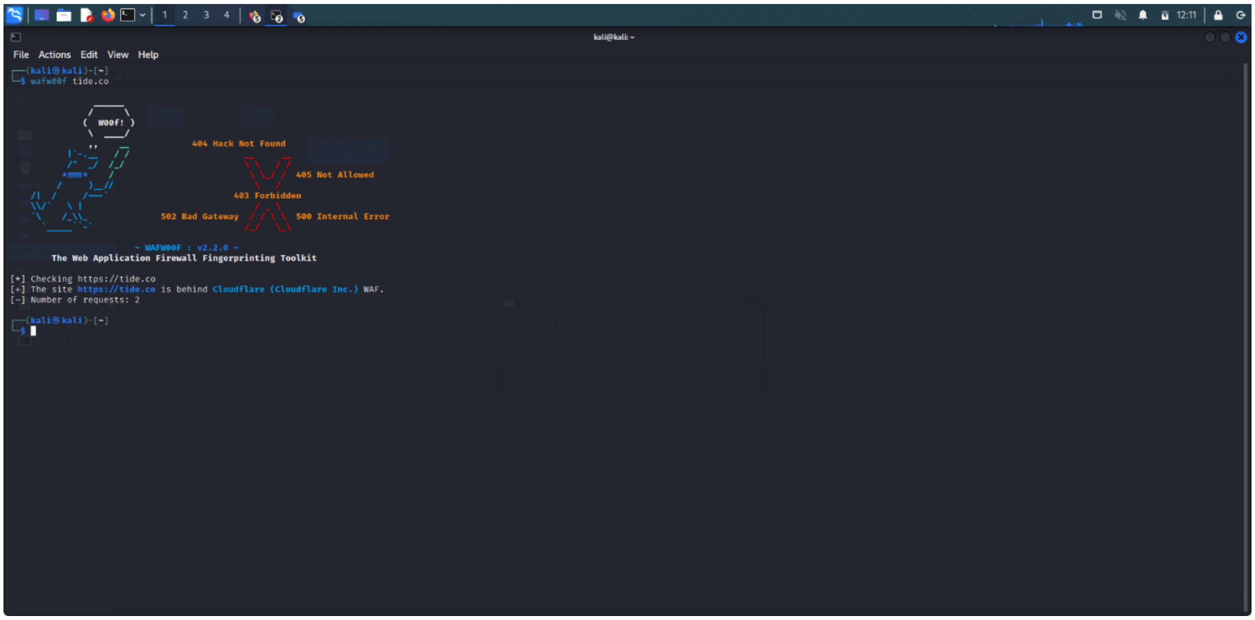
```
┌──(kali㉿kali)-[~]
└─$ nslookup tide.co
Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
Name:   tide.co
Address: 18.134.223.9
Name:   tide.co
Address: 18.168.234.149
Name:   tide.co
Address: 35.178.163.155


┌──(kali㉿kali)-[~]
└─$ nslookup -querv=mx tide.co
*** Invalid option: querv=mx
Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
Name:   tide.co
Address: 35.178.163.155
Name:   tide.co
Address: 18.134.223.9
Name:   tide.co
Address: 18.168.234.149


┌──(kali㉿kali)-[~]
└─$ nslookup -query=mx tide.co

Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
tide.co mail exchanger = 10 mxb-004dcd02.gslb.pphosted.com.
tide.co mail exchanger = 10 mxa-004dcd02.gslb.pphosted.com.

Authoritative answers can be found from:
```



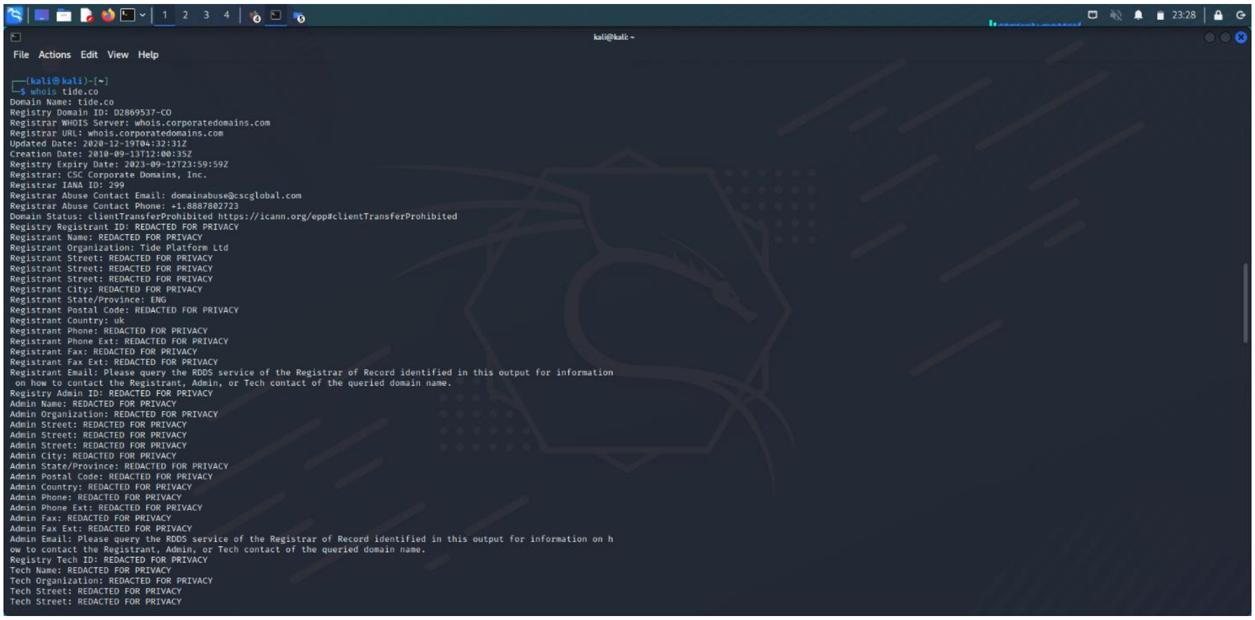
```
┌──(kali㉿kali)-[~]
└─$ nslookup -query=ns tide.co

Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
tide.co nameserver = desi.ns.cloudflare.com.
tide.co nameserver = hal.ns.cloudflare.com.

Authoritative answers can be found from:
hal.ns.cloudflare.com   internet address = 108.162.193.174
hal.ns.cloudflare.com   internet address = 172.64.33.174
hal.ns.cloudflare.com   internet address = 173.245.59.174
desi.ns.cloudflare.com  internet address = 108.162.192.96
desi.ns.cloudflare.com  internet address = 172.64.32.96
desi.ns.cloudflare.com  internet address = 173.245.58.96
hal.ns.cloudflare.com   has AAAA address 2606:4700:58::adf5:3bae
hal.ns.cloudflare.com   has AAAA address 2803:f800:50::6ca2:c1ae
hal.ns.cloudflare.com   has AAAA address 2a06:98c1:50::ac40:21ae
desi.ns.cloudflare.com  has AAAA address 2606:4700:50::adf5:3a60
desi.ns.cloudflare.com  has AAAA address 2803:f800:50::6ca2:c060
desi.ns.cloudflare.com  has AAAA address 2a06:98c1:50::ac40:2060


┌──(kali㉿kali)-[~]
└─$ nslookup -query=soa tide.co

Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
tide.co
        origin = desi.ns.cloudflare.com
        mail addr = dns.cloudflare.com
        serial = 2309782386
        refresh = 10000
        retry = 2400
        expire = 604800
        minimum = 3600
```



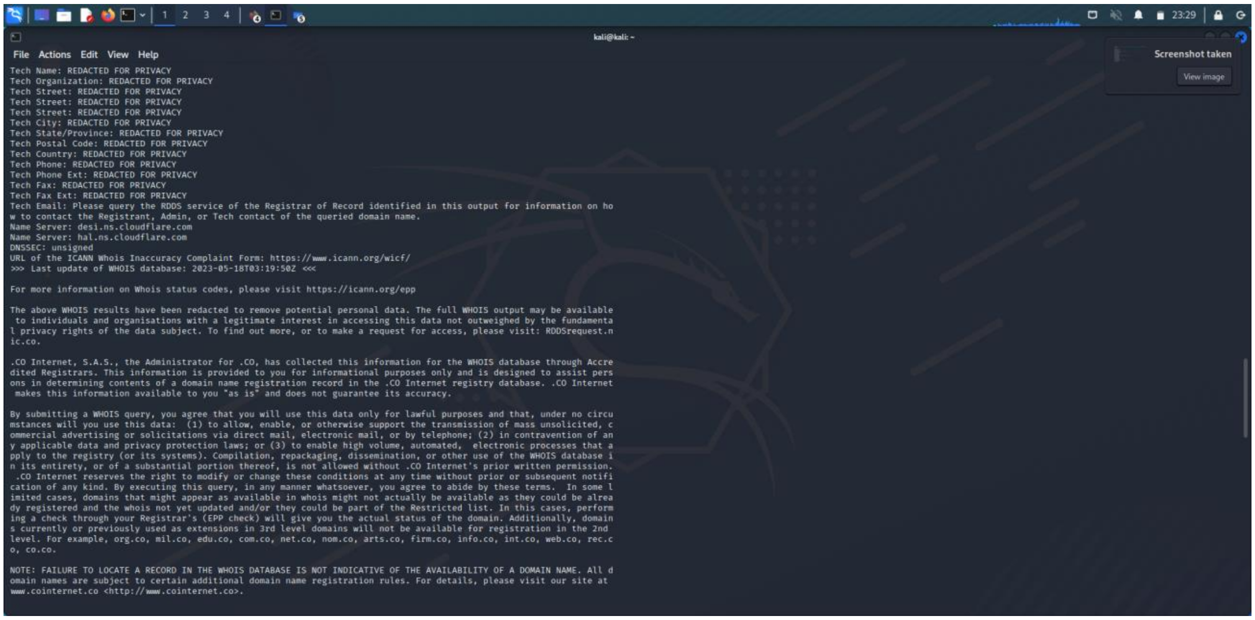
```
desi.ns.cloudflare.com  has AAAA address 2606:4700:50::adf5:3a60
desi.ns.cloudflare.com  has AAAA address 2803:f800:50::6ca2:c060
desi.ns.cloudflare.com  has AAAA address 2a06:98c1:50::ac40:2060


┌──(kali㉿kali)-[~]
└─$ nslookup -query=soa tide.co

Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
tide.co
        origin = desi.ns.cloudflare.com
        mail addr = dns.cloudflare.com
        serial = 2309782386
        refresh = 10000
        retry = 2400
        expire = 604800
        minimum = 3600

Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
└─$ nslookup -query=any tide.co

Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
tide.co rdata_46 = HINFO 13 2 3789 20230519041839 20230517021839 34505 tide.co. dSYwhnFXIZy+dsOKfpIatjLtlIW3tECOWnVE uXPYlPxfUy8tbLGM6tt7 SnjCZ/kOmbxHv0I1egzCxdTCjPYqfg==
tide.co hinfo = "RFC8482" ""
tide.co nameserver = hal.ns.cloudflare.com.
tide.co nameserver = desi.ns.cloudflare.com.

Authoritative answers can be found from:


┌──(kali㉿kali)-[~]
```



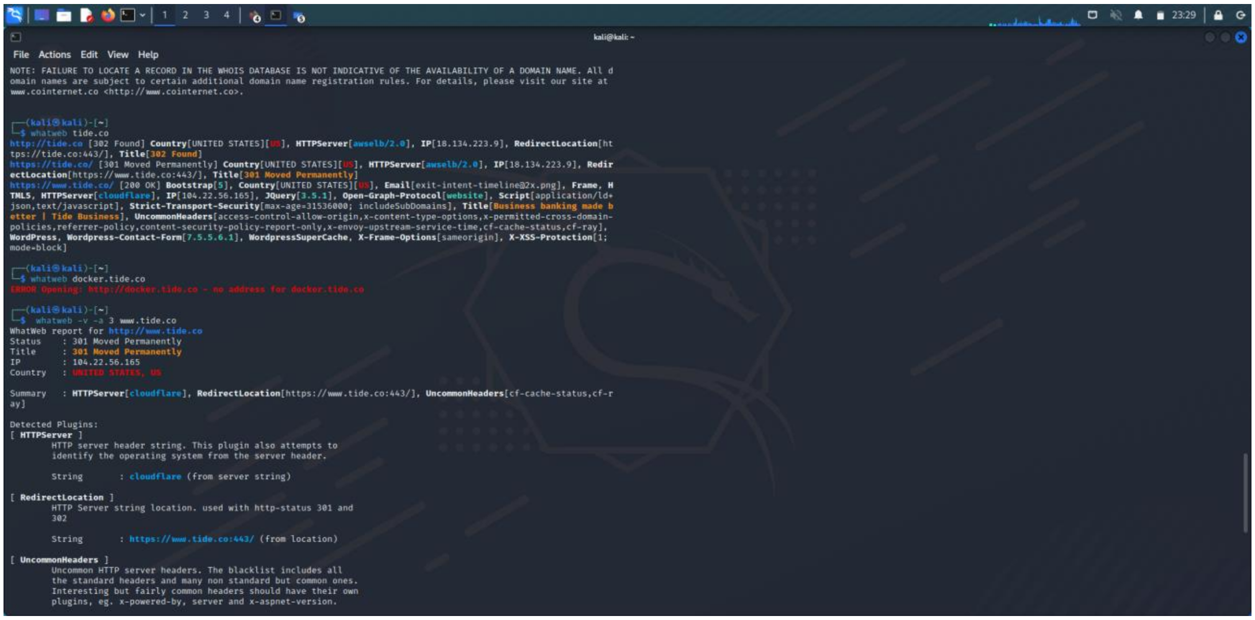
```
┌──(kali㉿kali)-[~]
└─$ wafw00f tide.co

                ______
               /      \
              (  W00f! )
               \  ____/
               ,,    __            404 Hack Not Found
           |`-.__   / /                      __     __
           /"  _/  /_/                       \ \   / /        405 Not Allowed
          *===*    /                          \ \_/ /
         /     )__//                           \   /
    /|  /     /---`                        403 Forbidden
    \\/`  \ |                                  / \
    `\    /_\\_                502 Bad Gateway / / \ \      500 Internal Error
      `_____``-`                               /_/   \_\

                        ~ WAFW00F : v2.2.0 ~
        The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://tide.co
[+] The site https://tide.co is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

┌──(kali㉿kali)-[~]
└─$ █
```



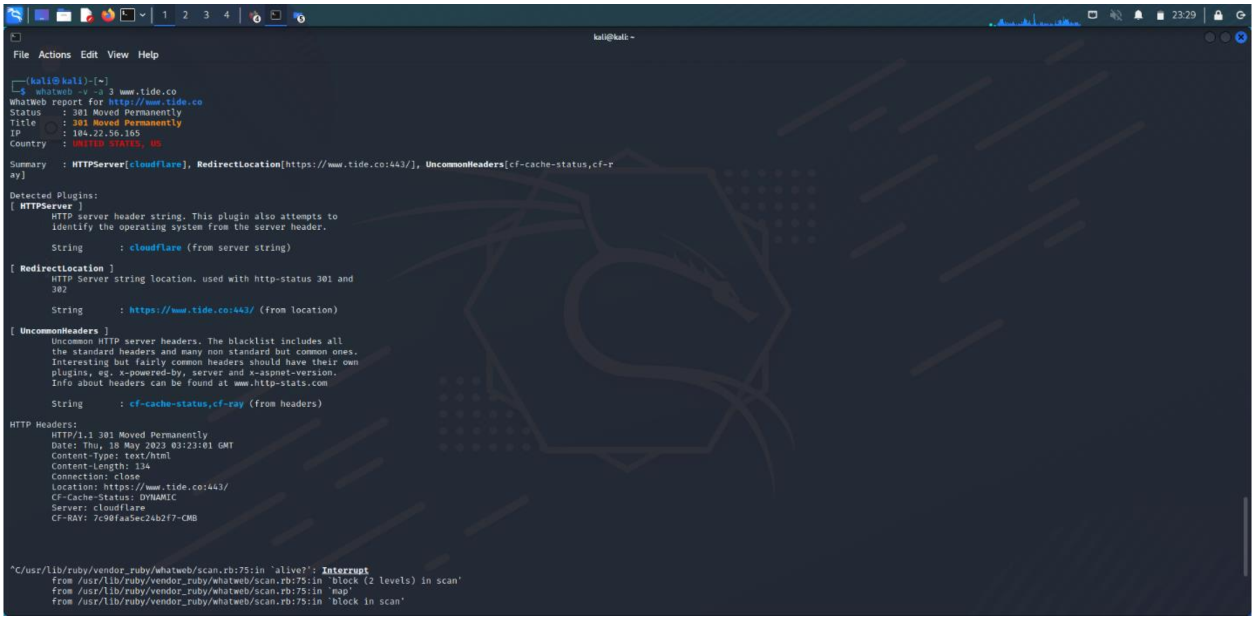
```
┌──(kali㉿kali)-[~]
└─$ whois tide.co
Domain Name: tide.co
Registry Domain ID: D2869537-CO
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: whois.corporatedomains.com
Updated Date: 2020-12-19T04:32:31Z
Creation Date: 2010-09-13T12:00:35Z
Registry Expiry Date: 2023-09-12T23:59:59Z
Registrar: CSC Corporate Domains, Inc.
Registrar IANA ID: 299
Registrar Abuse Contact Email: domainabuse@cscglobal.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Tide Platform Ltd
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: ENG
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: uk
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information
 on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on h
ow to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
```



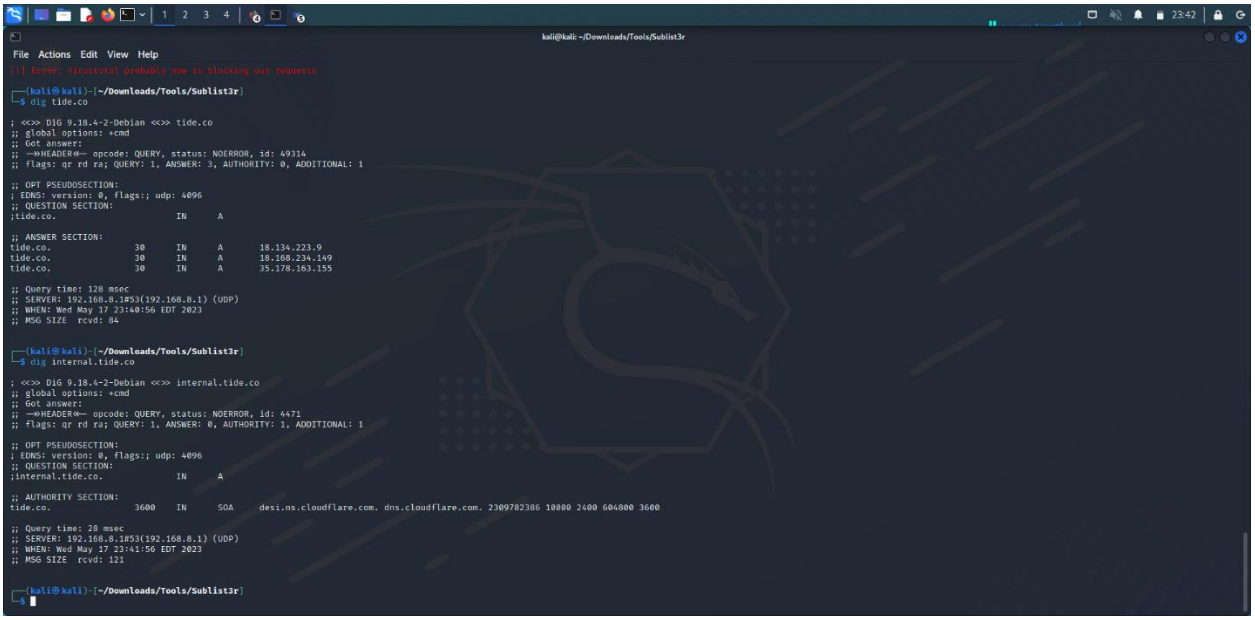
```
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on ho
w to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: desi.ns.cloudflare.com
Name Server: hal.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-05-18T03:19:50Z <<<

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

The above WHOIS results have been redacted to remove potential personal data. The full WHOIS output may be available
 to individuals and organisations with a legitimate interest in accessing this data not outweighed by the fundamenta
l privacy rights of the data subject. To find out more, or to make a request for access, please visit: RDDSrequest.n
ic.co.

.CO Internet, S.A.S., the Administrator for .CO, has collected this information for the WHOIS database through Accre
dited Registrars. This information is provided to you for informational purposes only and is designed to assist pers
ons in determining contents of a domain name registration record in the .CO Internet registry database. .CO Internet
 makes this information available to you "as is" and does not guarantee its accuracy.

By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circu
mstances will you use this data:  (1) to allow, enable, or otherwise support the transmission of mass unsolicited, c
ommercial advertising or solicitations via direct mail, electronic mail, or by telephone; (2) in contravention of an
y applicable data and privacy protection laws; or (3) to enable high volume, automated,  electronic processes that a
pply to the registry (or its systems). Compilation, repackaging, dissemination, or other use of the WHOIS database i
n its entirety, or of a substantial portion thereof, is not allowed without .CO Internet's prior written permission.
 .CO Internet reserves the right to modify or change these conditions at any time without prior or subsequent notifi
cation of any kind. By executing this query, in any manner whatsoever, you agree to abide by these terms.  In some l
imited cases, domains that might appear as available in whois might not actually be available as they could be alrea
dy registered and the whois not yet updated and/or they could be part of the Restricted list. In this cases, perform
ing a check through your Registrar's (EPP check) will give you the actual status of the domain. Additionally, domain
s currently or previously used as extensions in 3rd level domains will not be available for registration in the 2nd
level. For example, org.co, mil.co, edu.co, com.co, net.co, nom.co, arts.co, firm.co, info.co, int.co, web.co, rec.c
o, co.co.

NOTE: FAILURE TO LOCATE A RECORD IN THE WHOIS DATABASE IS NOT INDICATIVE OF THE AVAILABILITY OF A DOMAIN NAME. All d
omain names are subject to certain additional domain name registration rules. For details, please visit our site at
www.cointernet.co <http://www.cointernet.co>.
```



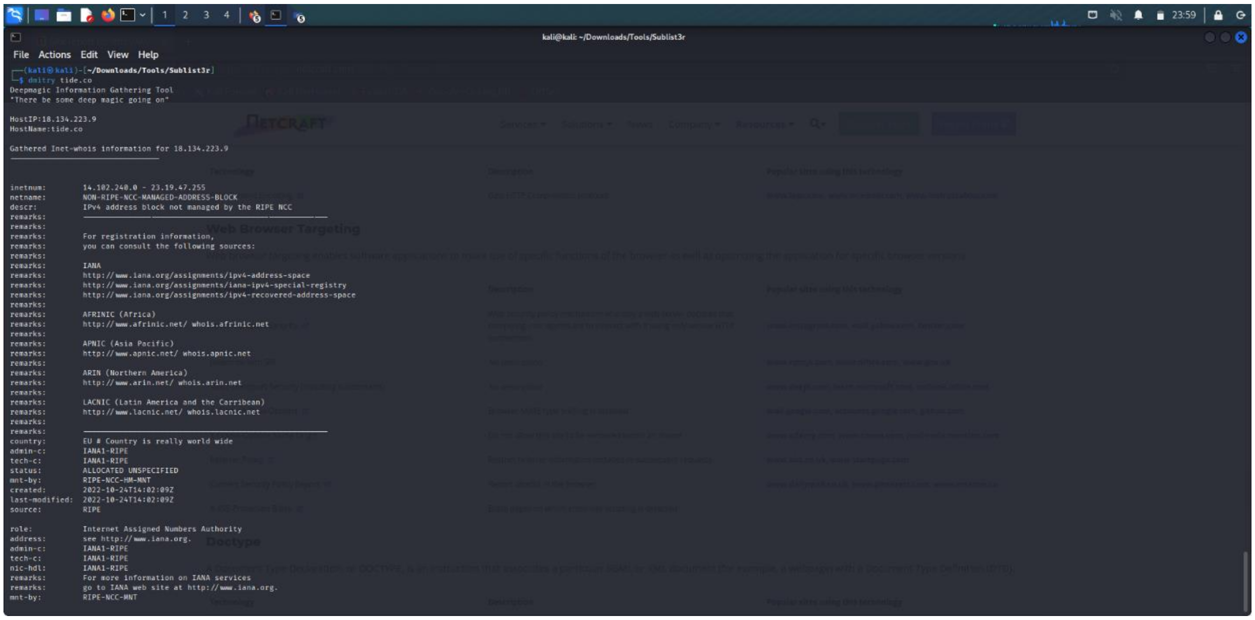
```
NOTE: FAILURE TO LOCATE A RECORD IN THE WHOIS DATABASE IS NOT INDICATIVE OF THE AVAILABILITY OF A DOMAIN NAME. All d
omain names are subject to certain additional domain name registration rules. For details, please visit our site at
www.cointernet.co <http://www.cointernet.co>.


┌──(kali㉿kali)-[~]
└─$ whatweb tide.co
http://tide.co [302 Found] Country[UNITED STATES][US], HTTPServer[awselb/2.0], IP[18.134.223.9], RedirectLocation[ht
tps://tide.co:443/], Title[302 Found]
https://tide.co/ [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[awselb/2.0], IP[18.134.223.9], Redir
ectLocation[https://www.tide.co:443/], Title[301 Moved Permanently]
https://www.tide.co/ [200 OK] Bootstrap[5], Country[UNITED STATES][US], Email[exit-intent-timeline@2x.png], Frame, H
TML5, HTTPServer[cloudflare], IP[104.22.56.165], JQuery[3.5.1], Open-Graph-Protocol[website], Script[application/ld+
json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[Business banking made b
etter | Tide Business], UncommonHeaders[access-control-allow-origin,x-content-type-options,x-permitted-cross-domain-
policies,referrer-policy,content-security-policy-report-only,x-envoy-upstream-service-time,cf-cache-status,cf-ray],
WordPress, Wordpress-Contact-Form[7.5.5.6.1], WordpressSuperCache, X-Frame-Options[sameorigin], X-XSS-Protection[1;
mode=block]

┌──(kali㉿kali)-[~]
└─$ whatweb docker.tide.co
ERROR Opening: http://docker.tide.co - no address for docker.tide.co

┌──(kali㉿kali)-[~]
└─$  whatweb -v -a 3 www.tide.co
WhatWeb report for http://www.tide.co
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 104.22.56.165
Country   : UNITED STATES, US

Summary   : HTTPServer[cloudflare], RedirectLocation[https://www.tide.co:443/], UncommonHeaders[cf-cache-status,cf-r
ay]

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

        String       : cloudflare (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://www.tide.co:443/ (from location)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
```



```
┌──(kali㉿kali)-[~]
└─$ whatweb -v -a 3 www.tide.co
WhatWeb report for http://www.tide.co
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 104.22.56.165
Country   : UNITED STATES, US

Summary   : HTTPServer[cloudflare], RedirectLocation[https://www.tide.co:443/], UncommonHeaders[cf-cache-status,cf-r
ay]

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

        String       : cloudflare (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://www.tide.co:443/ (from location)

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

        String       : cf-cache-status,cf-ray (from headers)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Date: Thu, 18 May 2023 03:23:01 GMT
        Content-Type: text/html
        Content-Length: 134
        Connection: close
        Location: https://www.tide.co:443/
        CF-Cache-Status: DYNAMIC
        Server: cloudflare
        CF-RAY: 7c90faa5ec24b2f7-CMB


^C/usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `alive?': Interrupt
        from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `block (2 levels) in scan'
        from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `map'
        from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `block in scan'
```

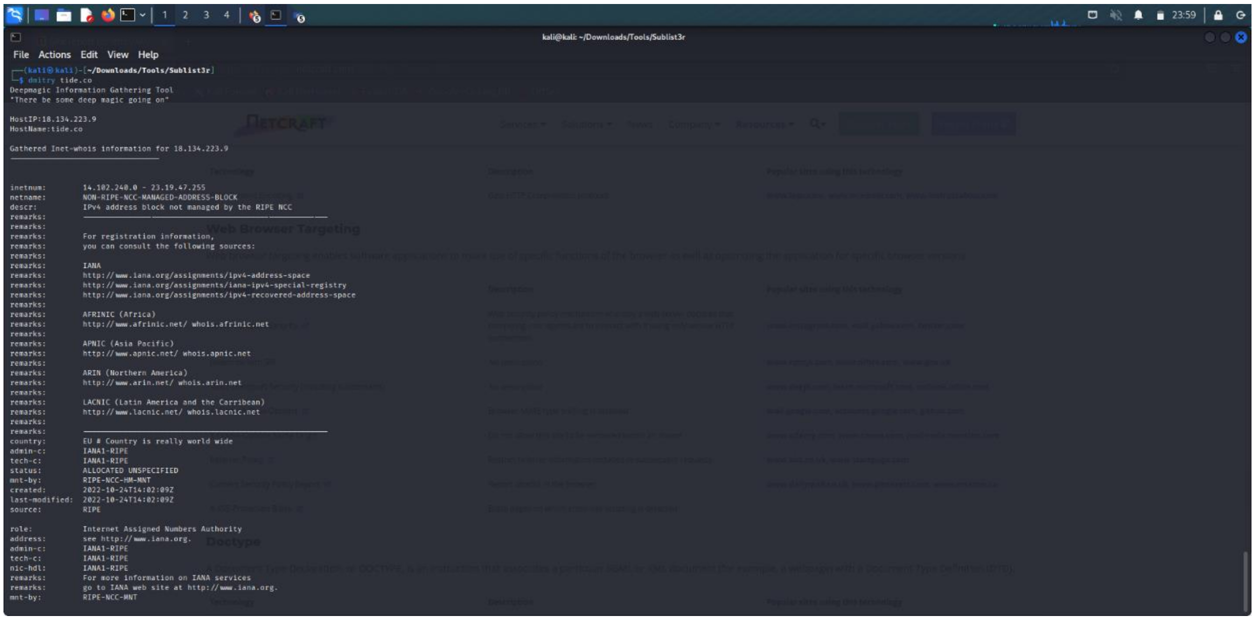

1 2 3 4
23:42
kali@kali: ~/Downloads/Tools/Sublist3r
File Actions Edit View Help

```
[!] Error: Virustotal probably now is blocking our requests

┌──(kali㉿kali)-[~/Downloads/Tools/Sublist3r]
└─$ dig tide.co

; <<>> DiG 9.18.4-2-Debian <<>> tide.co
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49314
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;tide.co.                       IN      A

;; ANSWER SECTION:
tide.co.                30      IN      A       18.134.223.9
tide.co.                30      IN      A       18.168.234.149
tide.co.                30      IN      A       35.178.163.155

;; Query time: 128 msec
;; SERVER: 192.168.8.1#53(192.168.8.1) (UDP)
;; WHEN: Wed May 17 23:40:56 EDT 2023
;; MSG SIZE  rcvd: 84


┌──(kali㉿kali)-[~/Downloads/Tools/Sublist3r]
└─$ dig internal.tide.co

; <<>> DiG 9.18.4-2-Debian <<>> internal.tide.co
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4471
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;internal.tide.co.              IN      A

;; AUTHORITY SECTION:
tide.co.                3600    IN      SOA     desi.ns.cloudflare.com. dns.cloudflare.com. 2309782386 10000 2400 604800 3600

;; Query time: 28 msec
;; SERVER: 192.168.8.1#53(192.168.8.1) (UDP)
;; WHEN: Wed May 17 23:41:56 EDT 2023
;; MSG SIZE  rcvd: 121


┌──(kali㉿kali)-[~/Downloads/Tools/Sublist3r]
└─$ 
```

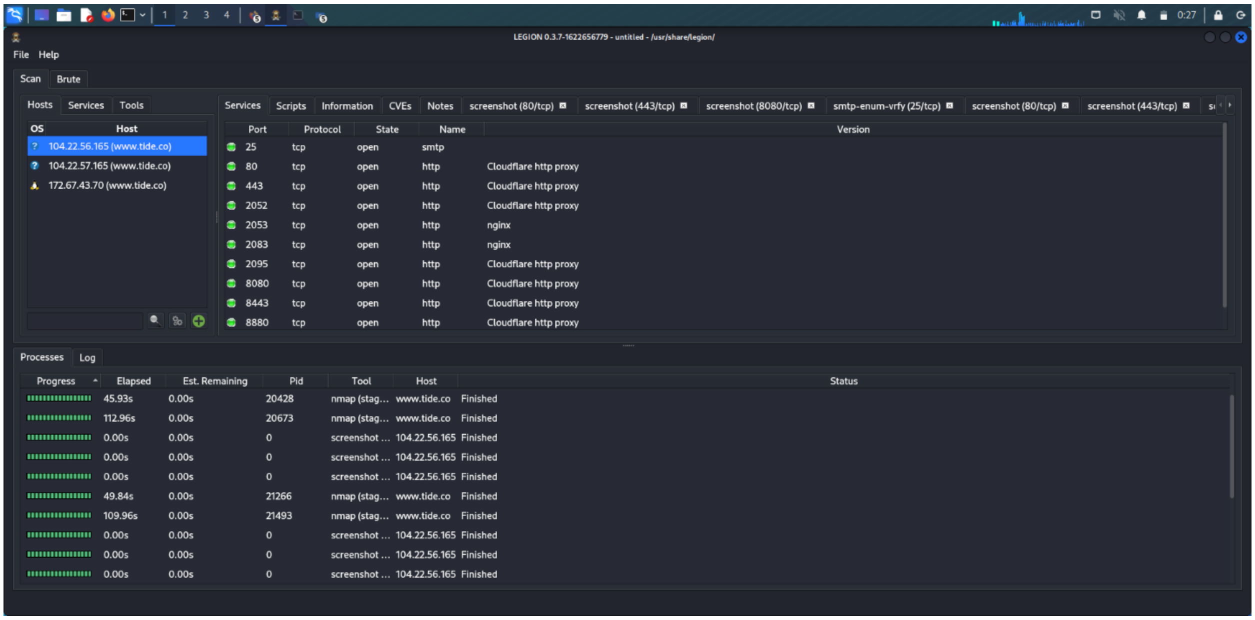


File Actions Edit View Help
kali@kali: ~/Downloads/Tools/Sublist3r

```
┌──(kali㉿kali)-[~/Downloads/Tools/Sublist3r]
└─$ dmitry tide.co
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:18.134.223.9
HostName:tide.co

Gathered Inet-whois information for 18.134.223.9
---------------------------------


inetnum:        14.102.240.0 - 23.19.47.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ------------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2022-10-24T14:02:09Z
last-modified:  2022-10-24T14:02:09Z
source:         RIPE

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
```



```
┌──(kali㉿kali)-[~/Downloads/Tools/Sublist3r]
└─$ dmitry tide.co
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:18.134.223.9
HostName:tide.co

Gathered Inet-whois information for 18.134.223.9
---------------------------------


inetnum:        14.102.240.0 - 23.19.47.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks:        ------------------------------------------------------
country:        EU # Country is really world wide
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
mnt-by:         RIPE-NCC-HM-MNT
created:        2022-10-24T14:02:09Z
last-modified:  2022-10-24T14:02:09Z
source:         RIPE

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
```



OS	Host
?	104.22.56.165 (www.tide.co)
?	104.22.57.165 (www.tide.co)
	172.67.43.70 (www.tide.co)

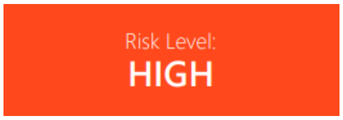
Port	Protocol	State	Name	Version
25	tcp	open	smtp	
80	tcp	open	http	Cloudflare http proxy
443	tcp	open	http	Cloudflare http proxy
2052	tcp	open	http	Cloudflare http proxy
2053	tcp	open	http	nginx
2083	tcp	open	http	nginx
2095	tcp	open	http	Cloudflare http proxy
8080	tcp	open	http	Cloudflare http proxy
8443	tcp	open	http	Cloudflare http proxy
8880	tcp	open	http	Cloudflare http proxy

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
	45.93s	0.00s	20428	nmap (stag…	www.tide.co	Finished
	112.96s	0.00s	20673	nmap (stag…	www.tide.co	Finished
	0.00s	0.00s	0	screenshot …	104.22.56.165	Finished
	0.00s	0.00s	0	screenshot …	104.22.56.165	Finished
	0.00s	0.00s	0	screenshot …	104.22.56.165	Finished
	49.84s	0.00s	21266	nmap (stag…	www.tide.co	Finished
	109.96s	0.00s	21493	nmap (stag…	www.tide.co	Finished
	0.00s	0.00s	0	screenshot …	104.22.56.165	Finished
	0.00s	0.00s	0	screenshot …	104.22.56.165	Finished
	0.00s	0.00s	0	screenshot …	104.22.56.165	Finished

Vulnerability Title

Out-of-date Version (WordPress)

Severity:



Risk Level:
HIGH

Vulnerability Description

An earlier or older version of the WordPress software, a well-known content management system (CMS) used for building and maintaining websites, is referred to as a "out-of-date" version of WordPress. Updates for WordPress are frequently released to enhance functionality, address security flaws, and add new features.

A WordPress version that has been out-of-date indicates that it has not been upgraded to the newest release. This may happen for a number of reasons, including a user's choice to delay or disregard updates or a lack of knowledge on the availability of new versions.

Affected Components

A website's various elements may be impacted by an outdated version of WordPress. The following are the primary factors that may be impacted:

- Security: The biggest worry about using an outdated WordPress version is the potential security flaws it might have. Because they are aware of the flaws in older versions, hackers and other bad guys aggressively target outdated software. By not updating WordPress, you put your website at risk for security breaches, malware infestations, unauthorized access, and other security problems.
- Plugins and Themes: The WordPress core software and numerous third-party developers' plugins and themes are made to function together effortlessly. However, as WordPress develops, it makes changes that necessitate the updating of plugin and theme creators' creations. It's possible that using an outdated WordPress version will cause plugin and theme compatibility problems. They might not work properly, produce mistakes, or even ruin the appearance and operation of the website.

- Performance and Stability: WordPress updates frequently come with performance enhancements, bug fixes, and optimizations. You could lose out on these improvements if you don't upgrade, which could impair the general functionality and stability of your website. The user experience may be negatively impacted by outdated versions' performance bottlenecks, slower loading times, and incompatibility with modern technology, which could perhaps turn visitors away.
- New Features: WordPress upgrades frequently include new features and functionality. These updates improve the CMS's functionality and give website owners more options for personalization, content management, and user interaction. You miss out on these new capabilities if you continue using an outdated version, which limits your capacity to take use of the most recent tools and developments in website construction and maintenance.

Impact Assessment

A website may have a number of effects from using an outdated version of WordPress. An evaluation of the probable effects is provided below:

- Security Vulnerabilities: They are exposed on your website while using an outdated WordPress version. Because they are aware of the flaws in older versions, hackers aggressively target outdated software. Exploiting these vulnerabilities might result in unwanted activity that harms your website and compromises user data, such as defacement, malware infections, unauthorized access, and data breaches.
- Increased Hacking Risk: Hackers who take advantage of known vulnerabilities to gain unauthorized access to websites frequently target outdated WordPress versions. Once they have access, hackers can alter your website, inject dangerous code, put in backdoors, or use it to spread spam or malware. This could harm your reputation, interfere with your internet presence, and possibly result in monetary loss or legal problems.
- Compatibility Problems: As WordPress develops, upgrades may bring about changes that necessitate the update of plugin and theme authors' creations for compatibility. When utilizing an outdated version of WordPress, errors, broken functionality, or even website crashes may occur due to compatibility problems with plugins and themes. This may have an adverse effect on user experience, negatively affect website performance, and make it more difficult to fix compatibility issues.

- Lack of New Features and Improvements: WordPress updates frequently include new features, enhancements, and optimizations that improve your website's usability, functionality, and performance. If you don't update, you may have less customization options, content management options, and user engagement tools available to you. If you aren't using the most recent WordPress capabilities, your website may suffer in comparison to rivals who do.
- Limited Resources and Support: The WordPress community, which consists of users, developers, and designers, actively promotes the platform by offering materials, guidance, and support. However, the most recent iterations of WordPress are the ones that receive the most community support. Your ability to access current support, documentation, tutorials, and troubleshooting tools may be hampered if you're using an outdated version. This may make it more difficult to fix problems, put new features into place, or keep up with industry best practices.

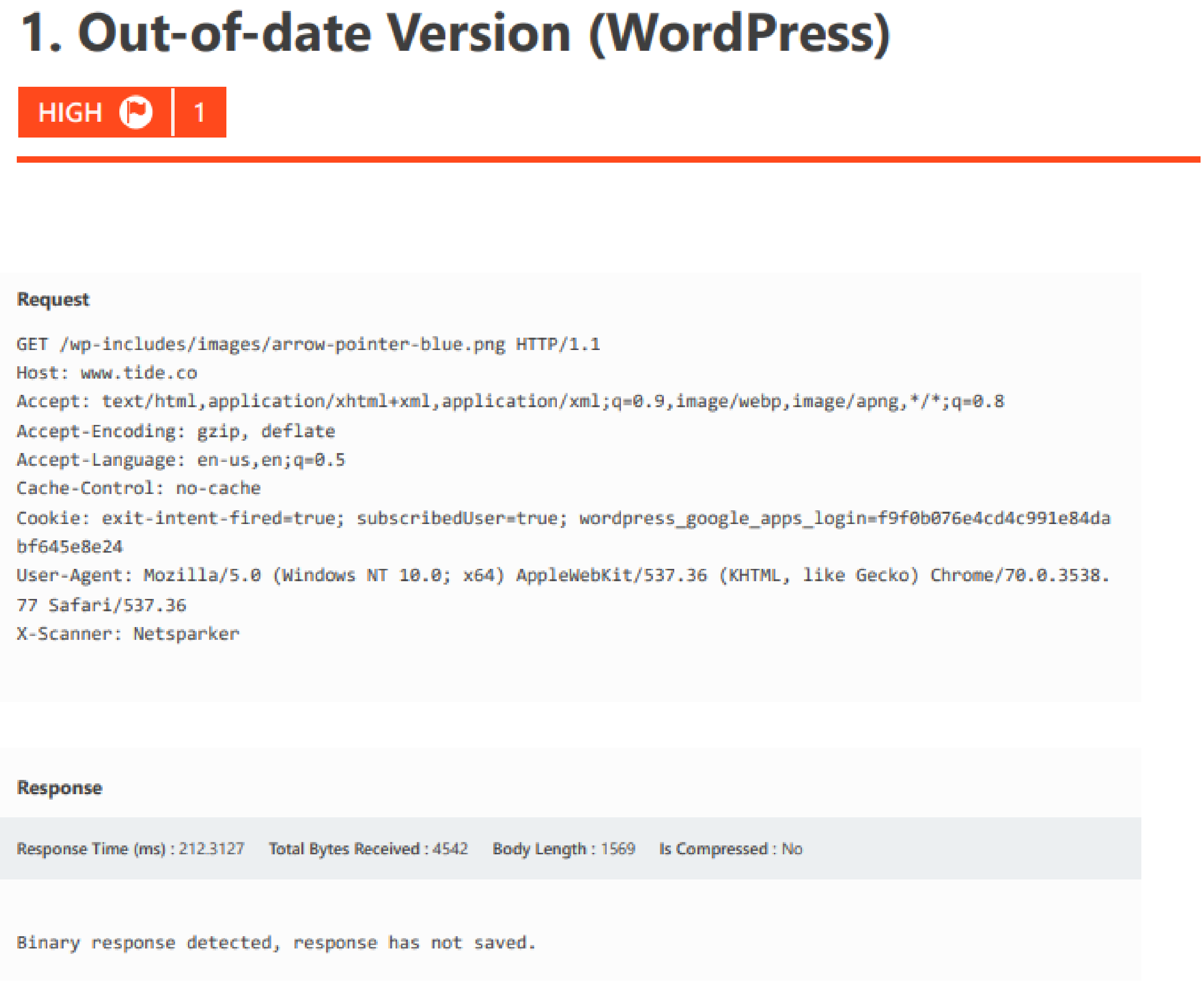
Steps to Reproduce

Normally, you would need to perform the following procedures in order to replicate an outdated version of WordPress:

- Installation: Rather than starting with the most recent version of WordPress, install an earlier version first. Previous versions of WordPress can be found on the official WordPress website or via reliable third parties.
- Decide on the Version: Choose the version of WordPress that you want to use from the list. Find the version's release number or date if you want to copy it.
- Get the WordPress package here: Find the installation package for the WordPress version you want to use and download it. To avoid downloading any corrupted or altered files, be sure you are doing it from a reliable source.
- Create a conducive environment: The installation of WordPress by setting up the environment. This normally entails installing PHP on your own machine or a hosting environment, together with a web server (such as Apache or Nginx), a database server (such as MySQL or MariaDB), and other software.
- Database Creation: To create a new database for your WordPress installation, go here. Usually, you may do this using the command line or the database management tool that your hosting provider offers.

- Extract and Upload Files: Downloaded WordPress packages can be extracted, then the files are uploaded to a web server or hosting environment. To move the files to the right location, you can use an FTP client or file manager that your hosting provider offers.
- Configuration: Input the URL of the location where you uploaded the files to access the WordPress installation through a web browser. To set up the database connection, enter site details, and create an administrative account, adhere to the on-screen instructions.
- Complete Installation: Keep through with the installation procedure until you have a WordPress website that is operational and using the older version you choose.

Proof of Concept



1. Out-of-date Version (WordPress)

HIGH | 1

Request

```
GET /wp-includes/images/arrow-pointer-blue.png HTTP/1.1
Host: www.tide.co
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: exit-intent-fired=true; subscribedUser=true; wordpress_google_apps_login=f9f0b076e4cd4c991e84da
bf645e8e24
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 212.3127   Total Bytes Received : 4542   Body Length : 1569   Is Compressed : No

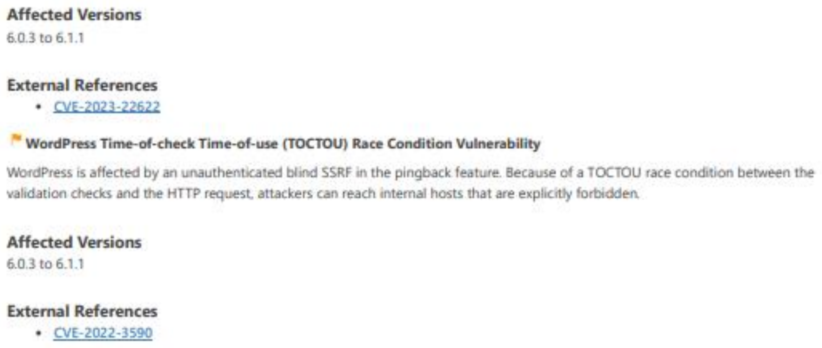
```
Binary response detected, response has not saved.
```

Proposed mitigation

The following steps are advised in order to reduce the hazards brought on by an outdated WordPress version:

- Updates on a regular basis: Keep WordPress installation current by swiftly implementing new updates and security patches. This guarantees that the most recent security upgrades are in place as well as the patching of identified vulnerabilities.
- Update installed plugins and themes frequently to make sure they are compatible with the newest release of WordPress. Security flaws can also be caused by exploiting vulnerabilities in plugins or themes.
- Monitoring Vulnerabilities: Keep up to date on any new security flaws impacting WordPress and any related plugins and themes. Keep an eye on security warnings and sign up for update notifications to stay on top of new dangers.
- Discard Unused Plugins and Themes: Discard any plugins or themes that are no longer being used by your WordPress installation. Inactive plugins and themes that still have security flaws could be dangerous.
- Strong Passwords and User Access Control: Ensure that all user accounts have strong passwords, and only allow people you can trust with administrator privileges. Apply the principle of least privilege, giving users only the access levels required for their particular responsibilities.
- Plugins for security: Take into account using trustworthy security plugins created especially for WordPress. These plugins can add further levels of security by firewalling, screening for malware, and preventing brute-force attacks.

External Reference



Affected Versions
6.0.3 to 6.1.1

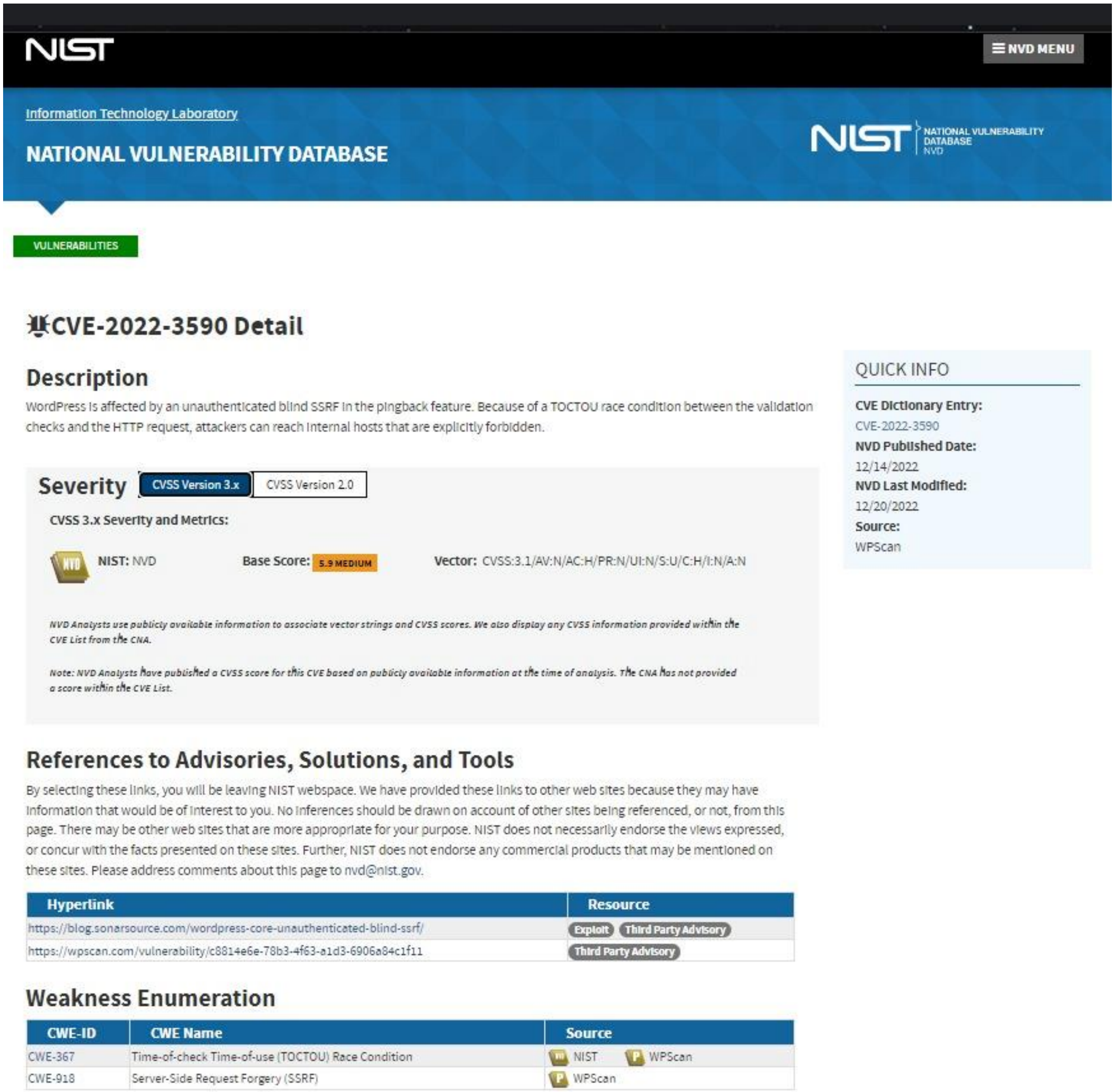
External References
- CVE-2023-22622

WordPress Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability

WordPress is affected by an unauthenticated blind SSRF in the pingback feature. Because of a TOCTOU race condition between the validation checks and the HTTP request, attackers can reach internal hosts that are explicitly forbidden.

Affected Versions
6.0.3 to 6.1.1

External References
- CVE-2022-3590


NIST
≡ NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NIST NATIONAL VULNERABILITY DATABASE NVD
VULNERABILITIES

CVE-2022-3590 Detail

Description

WordPress is affected by an unauthenticated blind SSRF in the pingback feature. Because of a TOCTOU race condition between the validation checks and the HTTP request, attackers can reach internal hosts that are explicitly forbidden.

Severity

CVSS Version 3.x
CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 5.9 MEDIUM **Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry:
CVE-2022-3590
NVD Published Date:
12/14/2022
NVD Last Modified:
12/20/2022
Source:
WPScan

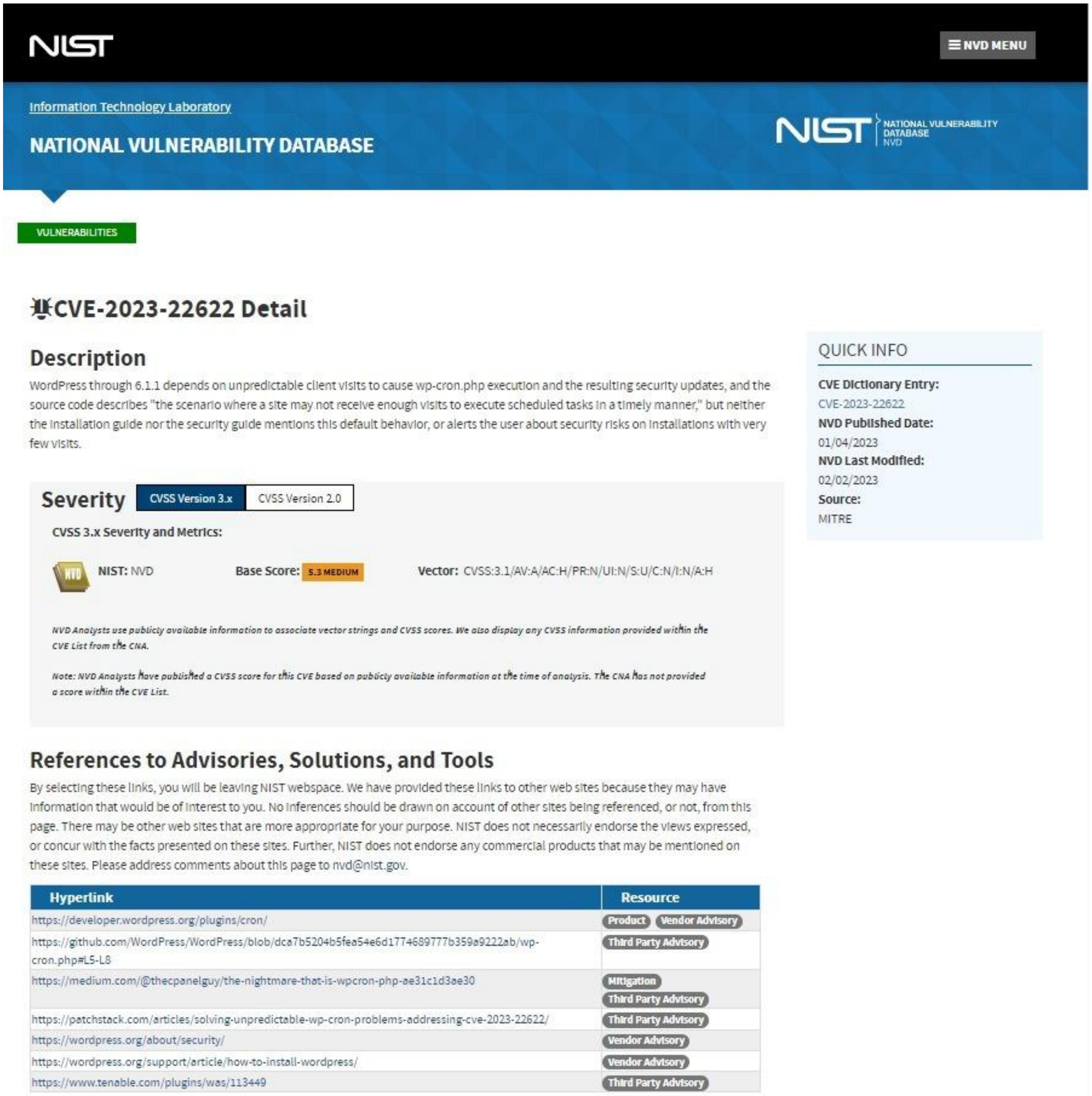
References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://blog.sonarsource.com/wordpress-core-unauthenticated-blind-ssrf/	Exploit Third Party Advisory
https://wpscan.com/vulnerability/c8814e6e-78b3-4f63-a1d3-6906a84c1f11	Third Party Advisory

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition	NIST WPScan
CWE-918	Server-Side Request Forgery (SSRF)	WPScan



NIST
☰ NVD MENU
Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD
VULNERABILITIES

CVE-2023-22622 Detail

Description

WordPress through 6.1.1 depends on unpredictable client visits to cause wp-cron.php execution and the resulting security updates, and the source code describes "the scenario where a site may not receive enough visits to execute scheduled tasks in a timely manner," but neither the installation guide nor the security guide mentions this default behavior, or alerts the user about security risks on installations with very few visits.

Severity

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** 5.3 MEDIUM **Vector:** CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

References to Advisories, Solutions, and Tools

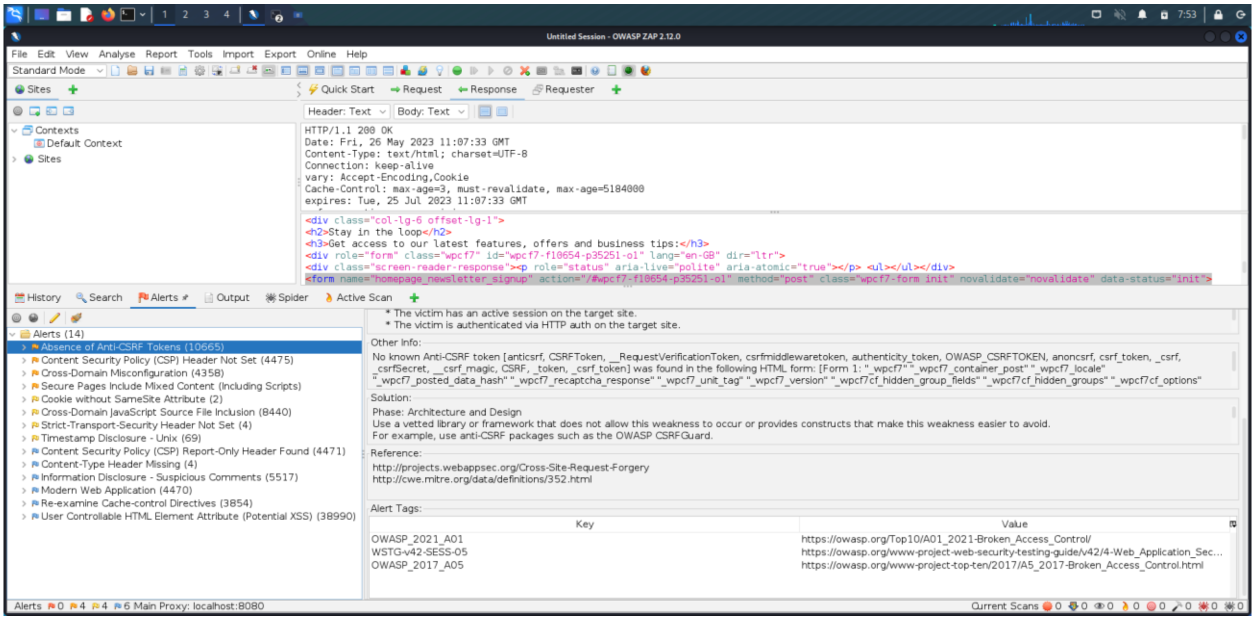
By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
https://developer.wordpress.org/plugins/cron/	Product Vendor Advisory
https://github.com/WordPress/WordPress/blob/dca7b5204b5fea54e6d1774689777b359a9222ab/wp-cron.php#L5-L8	Third Party Advisory
https://medium.com/@thecpanelguy/the-nightmare-that-is-wpcron-php-ae31c1d3ae30	Mitigation Third Party Advisory
https://patchstack.com/articles/solving-unpredictable-wp-cron-problems-addressing-cve-2023-22622/	Third Party Advisory
https://wordpress.org/about/security/	Vendor Advisory
https://wordpress.org/support/article/how-to-install-wordpress/	Vendor Advisory
https://www.tenable.com/plugins/was/113449	Third Party Advisory

QUICK INFO

CVE Dictionary Entry:
CVE-2023-22622
NVD Published Date:
01/04/2023
NVD Last Modified:
02/02/2023
Source:
MITRE

Some of the other vulnerabilities identified in the particular domain.



```
HTTP/1.1 200 OK
Date: Fri, 26 May 2023 11:07:33 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
vary: Accept-Encoding,Cookie
Cache-Control: max-age=3, must-revalidate, max-age=5184000
expires: Tue, 25 Jul 2023 11:07:33 GMT
```

```
<div class="col-lg-6 offset-lg-1">
<h2>Stay in the loop</h2>
<h3>Get access to our latest features, offers and business tips:</h3>
<div role="form" class="wpcf7" id="wpcf7-f10654-p35251-o1" lang="en-GB" dir="ltr">
<div class="screen-reader-response"><p role="status" aria-live="polite" aria-atomic="true"></p> <ul></ul></div>
<form name="homepage_newsletter_signup" action="/#wpcf7-f10654-p35251-o1" method="post" class="wpcf7-form init" novalidate="novalidate" data-status="init">
```

Alerts (14)
- Absence of Anti-CSRF Tokens (10665)
- Content Security Policy (CSP) Header Not Set (4475)
- Cross-Domain Misconfiguration (4358)
- Secure Pages Include Mixed Content (Including Scripts)
- Cookie without SameSite Attribute (2)
- Cross-Domain JavaScript Source File Inclusion (8440)
- Strict-Transport-Security Header Not Set (4)
- Timestamp Disclosure - Unix (69)
- Content Security Policy (CSP) Report-Only Header Found (4471)
- Content-Type Header Missing (4)
- Information Disclosure - Suspicious Comments (5517)
- Modern Web Application (4470)
- Re-examine Cache-control Directives (3854)
- User Controllable HTML Element Attribute (Potential XSS) (38990)

* The victim has an active session on the target site.
* The victim is authenticated via HTTP auth on the target site.

Other Info:

No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "_wpcf7" "_wpcf7_container_post" "_wpcf7_locale" "_wpcf7_posted_data_hash" "_wpcf7_recaptcha_response" "_wpcf7_unit_tag" "_wpcf7_version" "_wpcf7cf_hidden_group_fields" "_wpcf7cf_hidden_groups" "_wpcf7cf_options"

Solution:

Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Reference:

http://projects.webappsec.org/Cross-Site-Request-Forgery
http://cwe.mitre.org/data/definitions/352.html

Alert Tags:

Key	Value
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/
WSTG-v42-SESS-05	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Sec...
OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html

Alerts 0 4 4 6 Main Proxy: localhost:8080

Current Scans 0 0 0 0 0 0 0 0