Sri Lanka Institute of Information Technology

2024

Web Security - IE2062

Assignment

Year 2, Semester 2

IT22562074
JAYARATHNA K.P.G.C.M
Y2.S2.WE.CS.01
MALABE CAMPUS

Contents

Acknowledgement

I would like to express my gratitude to MS. CHETHANA LIYANAPATHIRANA for their guidance and support throughout the duration of this Web Security(IE2062) module assignment. Their expertise and insightful feedback have been instrumental in shaping my understanding of the subject matter. Additionally, I extend my appreciation to my classmates for their collaboration and exchange of ideas, which enriched my learning experience.

Assessment Objectives

The security assessment of the https://www.binance.com for the second year second semester Web Security Module. The purpose of this assessment is to discover the vulnerabilities in the target domain and to indicate the subsequent risk level for the vulnerabilities

protects us from doing Bug Bounty hunting for real-world web applications. By using these resources, you may learn a lot about penetration testing tools and how to utilize them these web audit reports give an excellent understanding of how to handle cybersecurity professional skills.

Introduction

This bug bounty report encapsulates a meticulous exploration into the cybersecurity landscape of Binance Cryptocurrency Exchange, one of the preeminent blockchain ecosystems and cryptocurrency infrastructure providers globally. With an unwavering commitment to fortifying online security measures, this endeavor delves deep into identifying and mitigating potential vulnerabilities within Binance's web applications, adhering closely to the specified scope and rules outlined by the company and Bugcrowd platform.

This report explores the cybersecurity landscape of Binance Cryptocurrency Exchange, a leading blockchain ecosystem and cryptocurrency infrastructure provider. The program aims to identify and mitigate potential vulnerabilities within Binance's web applications, adhering to the company's and Bugcrowd platform's guidelines. The report uses passive and active information gathering techniques to uncover potential vulnerabilities. The report provides a detailed account of the methodologies used, findings, and recommendations, detailing passive reconnaissance methods and active scanning techniques. It also explains the OWASP Top 10 vulnerabilities and provides mitigation strategies tailored to Binance's unique security landscape. The report aims to strengthen Binance's digital infrastructure and uphold user trust.

OWASP Top 10 Security Risks and Vulnerabilities

According to the Sucuri Guides, The Open Web Application Security Project (OWASP) is an online community that creates web application security papers, techniques, documentation, tools, and technologies. The OWASP has determined the top ten most significant threats to online application security. Successful Bug Bounty hunting requires an understanding of these dangers and taking steps to mitigate them. [1]

Fig 01

- Broken access control
    - According to OWASP data, broken access control is now the most often listed vulnerability in apps. Putting in place access control measures, turning off directory listing, keeping track of failures, and utilizing 2FA or MFA is all part of prevention.

- Cryptographic failures
    - Cryptographic Failures, previously known as Sensitive Data Exposure, refer to cryptographic failures causing sensitive data exposure and system compromise. To minimize this risk, identify sensitive data, encrypt data, use proper key management, and disable caching.

- Injection
    - Injection vulnerabilities involve attackers providing untrusted data to a program, leading to unintentional commands and changes in program execution. Common forms include SQL, NoSQL, OS, and LDAP injections. Preventing injections involves input validation checks, [2]rejecting suspicious data, and controlling database login permissions.

- Insecure design
    - Insecure Design is a new category in 2021, focusing on risks related to design and architectural flaws. It represents weaknesses in control design, lacking business risk profiling. Prevention involves AppSec teams, threat modeling, and integration tests. [2]

- Security misconfiguration
    - Security misconfiguration is a common vulnerability on the OWASP list, affecting applications with unpatched flaws, missing security hardening, unnecessary features, default accounts, or overly descriptive error messages. Preventing misconfiguration involves removing unused features, updating configurations, installing patches, and automating verification processes.

- Vulnerable and outdated components
    - The risk category "Using Components with Known Vulnerabilities" has increased from ninth to top, referring to web application security risks. This includes exploitation of sknown vulnerabilities in components, such as libraries and frameworks, and the failure to update them.

- Identification and authentication failures

- The risk category of "Broken Authentication" has dropped due to standardized frameworks. Attackers can compromise user identities through passwords, keys, or session tokens. Preventing this is possible through 2FA, strong password policies, and secure session management.

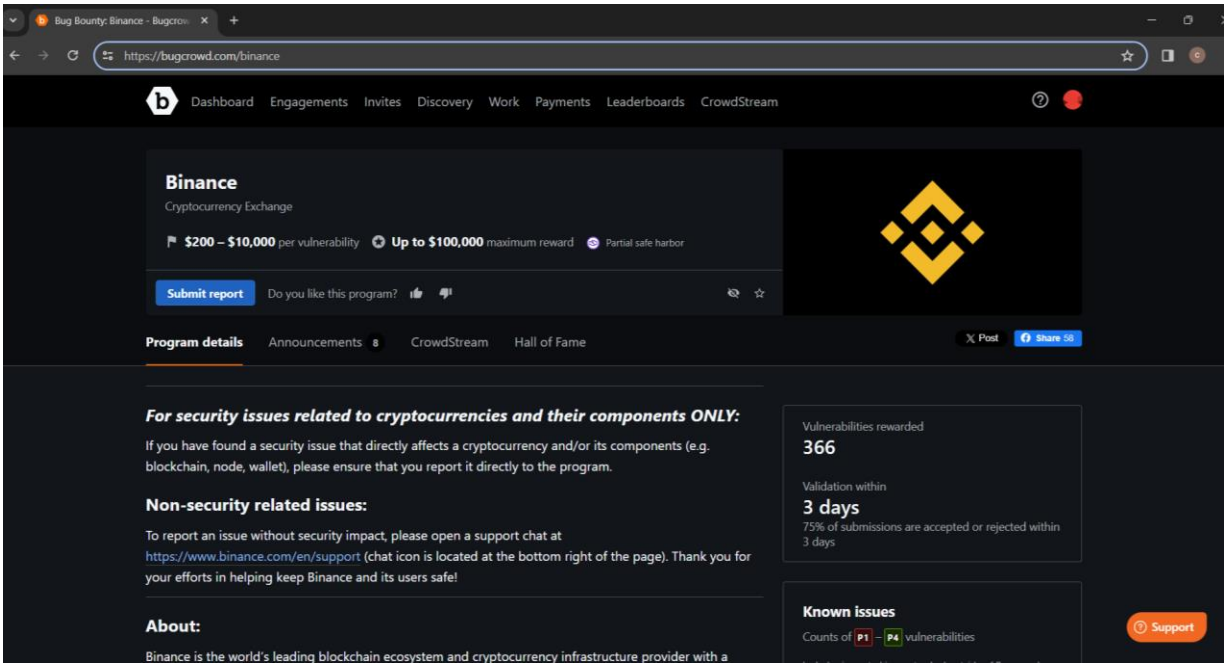
- Software and data integrity failures
  - The OWASP Top 10 has added a new category for Software and Data Integrity Failures, focusing on risks related to software updates, critical data, and insecure CI/CD pipelines.

- Security logging and monitoring failures
  - Insufficient logging and monitoring of security incidents can lead to data breaches and advanced persistent threat attacks. Proper logging, monitoring, and incident response are essential to prevent these risks, ensuring visibility, incident reporting, and digital forensics. [2]

- Server-side request forgery
  - Server-Side Request Forgery (SSRF) is a top security vulnerability, requiring attackers to bypass firewalls and VPNs. OWASP recommends prevention practices like disabling redirections and sanitizing input data.

Because cybercrime is growing daily, online security is essential for corporations and industries that rely on the internet. Attackers are always coming up with new ways to take advantage of online applications. Attackers also focus on making money as they hone their talents. Ransomware assaults are particularly common these days because of this. Web applications must thus include protection in order to ward against this kind of cybercrime.

We need to focus on these types of vulnerabilities according to the scope and rules provided by Binance Cryptocurrency Exchange company and the Bugcrowd platform.


Bug Bounty: Binance - Bugcrow
https://bugcrowd.com/binance
Dashboard
Engagements
Invites
Discovery
Work
Payments
Leaderboards
CrowdStream
Binance
Cryptocurrency Exchange
$200 – $10,000 per vulnerability
Up to $100,000 maximum reward
Partial safe harbor
Submit report
Do you like this program?
Program details
Announcements 8
CrowdStream
Hall of Fame
Post
Share 58
For security issues related to cryptocurrencies and their components ONLY:
If you have found a security issue that directly affects a cryptocurrency and/or its components (e.g. blockchain, node, wallet), please ensure that you report it directly to the program.
Non-security related issues:
To report an issue without security impact, please open a support chat at https://www.binance.com/en/support (chat icon is located at the bottom right of the page). Thank you for your efforts in helping keep Binance and its users safe!
About:
Binance is the world's leading blockchain ecosystem and cryptocurrency infrastructure provider with a
Vulnerabilities rewarded
366
Validation within
3 days
75% of submissions are accepted or rejected within 3 days
Known issues
Counts of P1 – P4 vulnerabilities
Support

About:

With the largest digital asset exchange by trading volume among its financial product suite, Binance is the world's top blockchain ecosystem and cryptocurrency infrastructure provider.

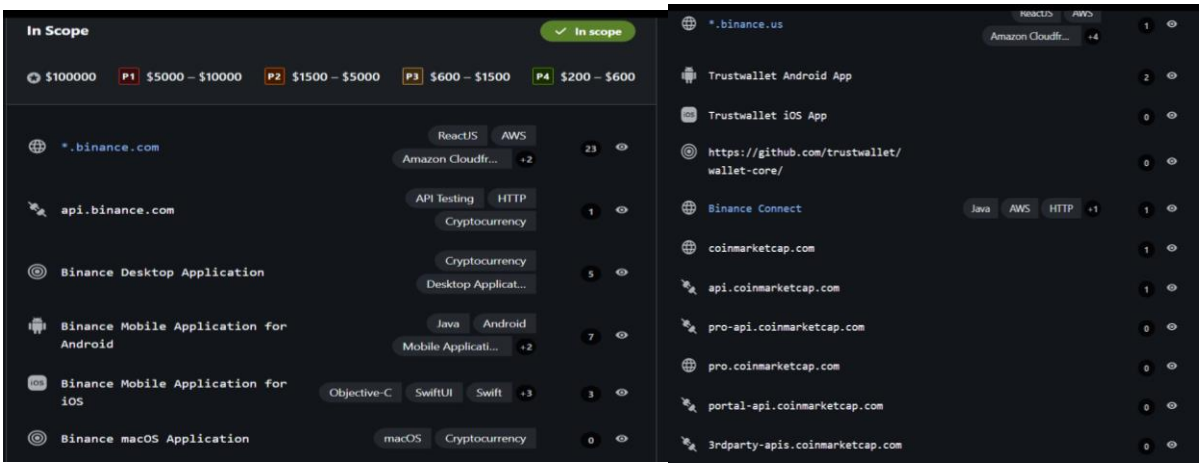
With millions of users worldwide, Binance's platform is trusted and committed to giving individuals more financial freedom by offering access to a wide range of financial instruments over an expanding global network at the lowest rates in the industry.

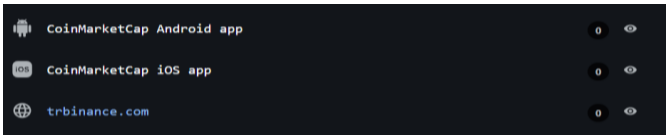
Being the blockchain ecosystem's infrastructure supplier is Binance's goal. Currently, Binance is a worldwide blockchain ecosystem that includes investment and incubation programs, research, instructional materials, infrastructure solutions, trading services, social good and philanthropic activities, and more. CoinMarketCap, Trust Wallet, and other partners are part of the Binance ecosystem.

The scope of the security audit according to "https://bugcrowd.com/binance "is as follows,

In Scope [3]

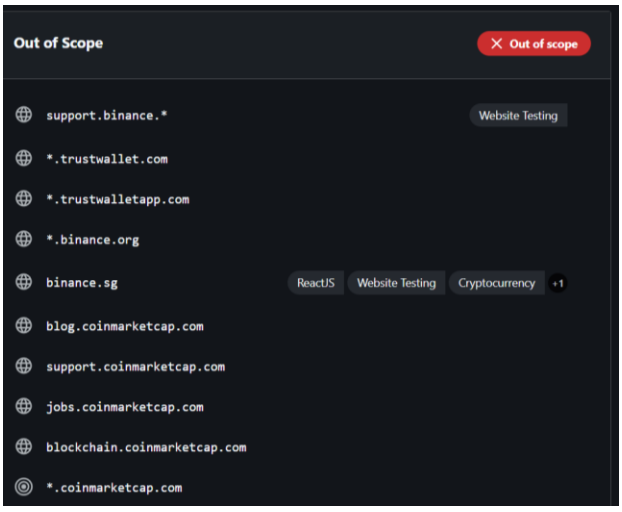
- *.binance.com
- api.binance.com
- Binance Desktop Application
- Binance Mobile Application for Android
- Binance Mobile Application for iOS
- Binance macOS Application
- coinmarketcap.com
- api.coinmarketcap.com
- pro-api.coinmarketcap.com
- pro.coinmarketcap.com
- portal-api.coinmarketcap.com
- 3rdparty-apis.coinmarketcap.com
- CoinMarketCap Android app
- CoinMarketCap iOS app
- trbinance.com





Out Scope

- support.binance.*
- *.trustwallet.com
- *.trustwalletapp.com
- *.binance.org
- binance.sg
- Website Testing
- Cryptocurrency
- blog.coinmarketcap.com
- support.coinmarketcap.com
- jobs.coinmarketcap.com
- blockchain.coinmarketcap.com
- *.coinmarketcap.com



Target Information:

Primary Targets - Eligible for bounty from P4 and above [3]

- *.binance.com (with exceptions, refer to Secondary Targets)
- api.binance.com
- binance.us
- Binance Mobile Application for Android
- Binance Mobile Application for iOS
- Binance Desktop Application
- Binance macOS Application
- Binance Connec
- c2c.binance.comt
- trbinance.com

Secondary Targets - Eligible for bounty for P1 and P2. P3 and P4 will be points only

- academy.binance.com
- info.binance.com
- coinmarketcap.com
- api.coinmarketcap.com
- pro-api.coinmarketcap.com
- pro.coinmarketcap.com
- portal-api.coinmarketcap.com
- 3rdparty-apis.coinmarketcap.com
- CoinMarketCap Android app
- CoinMarketCap iOS app
- account.binance.com
- support.binance.com

- ✓ *.binance.com
- ✓ trbinance.com
- ✓ academy.binance.com
- ✓ info.binance.com
- ✓ coinmarketcap.com
- ✓ pro.coinmarketcap.com
- ✓ *.binance.us
- ✓ account.binance.com
- ✓ c2c.binance.com
- ✓ support.binance.com

These are the domains selected to perform this Bug Bounty hunting program.

Information gathering

Information gathering is crucial for building a strong foundation for a bug bounty-hunting program. It involves collecting critical details about the targeted web application, such as IP addresses, open ports, and protection methods. Perfect information gathering unlocks vulnerabilities and improves vulnerability scanning, as per All About Testing. [4]

formation gathering can indeed be divided into two main parts:

Passive Information Gathering:

Data collection methods like online databases, social media profiling, public records searches, and reconnaissance techniques are employed to gather information without directly interacting with the target or investigating systems. [4]

Active Information Gathering:

Active gathering involves actively engaging with target systems, using techniques like scanning networks, vulnerability assessments, port scans, and scripts, despite increased risk of detection or interference.

These are the information-gathering tools used to analyze the targeted web domain.and passive information collecting technologies are my first choice. due to the high noisy level of active information collecting. But we need active information gathering to analyze information about what is open ports are in our targeted system.

Passive information gathering tools

- Sublist3r
- nslookup
- whois
- whatweb
- whoislookup
- netcarft
- wayback machine

Active information gathering tools

- nmap
- recon-ng
- sodan

Passive information gathering tools

Sublist3r

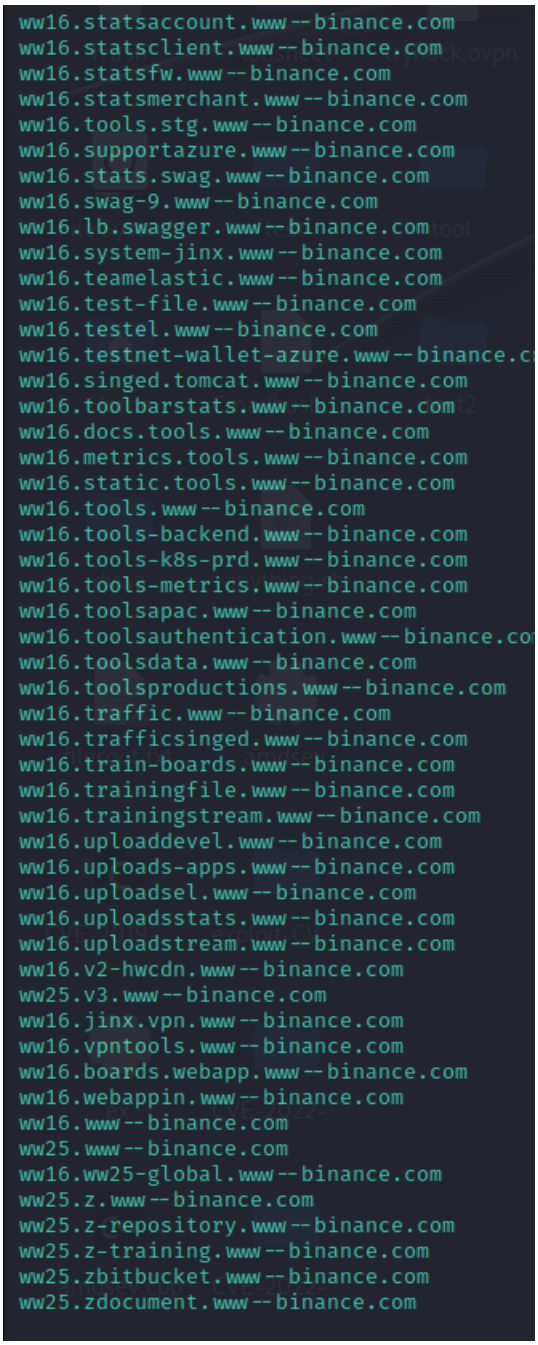
Sublist3r is a subdomain enumeration tool. That means this is a tool to identify the unique subdomains associated with the target domain. Because of this tool, we can gather more information about subdomains [5]

```
ww16.train.boards.www--binance.com
ww16.boards.www--binance.com
ww16.boardsconfluence.www--binance.com
ww16.lb.cert.www--binance.com
ww16.cert-file.www--binance.com
ww16.9.chd.www--binance.com
ww16.chef-hwcdn.www--binance.com
ww16.client-tools.www--binance.com
ww16.clienthwcdn.www--binance.com
ww16.s.cloudfront.www--binance.com
ww16.container.www--binance.com
ww16.container-s.www--binance.com
ww16.hwcdn.controller.www--binance.com
ww16.controller.www--binance.com
ww16.cvscdn.www--binance.com
ww16.dashboardlb.www--binance.com
ww16.dev-file.www--binance.com
ww16.paywall.devel.www--binance.com
ww16.v3.devel.www--binance.com
ww16.devel.www--binance.com
ww16.devel-active.www--binance.com
ww16.devel-admins.www--binance.com
ww16.devel-disabled.www--binance.com
ww16.develget.www--binance.com
ww16.developmentlb.www--binance.com
ww16.develpage.www--binance.com
ww16.hwcdn.docs.www--binance.com
ww16.singed.docs.www--binance.com
ww16.docs-singed.www--binance.com
ww16.lb.docsapi.www--binance.com
ww16.internals.ebs.www--binance.com
ww16.beta.elastic.www--binance.com
ww16.ssl.elastic.www--binance.com
ww16.stats.elastic.www--binance.com
ww16.elastic.www--binance.com
ww16.elastic-docs.www--binance.com
ww16.elastic-jinx.www--binance.com
ww16.elastic-skins.www--binance.com
ww16.elasticcloud.www--binance.com
ww16.elasticnautilus.www--binance.com
ww16.europefile.www--binance.com
ww16.europewestdevel.www--binance.com
ww16.opsstream.events.www--binance.com
ww16.ext9.www--binance.com
ww16.customer.file.www--binance.com
ww16.internal.file.www--binance.com
ww16.file.www--binance.com
ww16.filecloud.www--binance.com
ww16.filephp.www--binance.com
ww16.azure.frontpage.www--binance.com
ww16.apps.get.www--binance.com
ww16.get-lb.www--binance.com
```

```
themis.binance.com
vstream.binance.com
prebinance.com
www———binance.com
www——binance.com
www--binance.com
ww16.uploads.9.www--binance.com
ww16.9.www--binance.com
ww16.elastic.acc.www--binance.com
ww16.acccdn.www--binance.com
ww16.accounting-stats.www--binance.com
ww16.accounts.www--binance.com
ww16.confluence.admin.www--binance.com
ww16.demo.admin.www--binance.com
ww16.devel.admin.www--binance.com
ww16.prd.admin.www--binance.com
ww16.profile.admin.www--binance.com
ww16.support.admin.www--binance.com
ww16.swag.admin.www--binance.com
ww16.admin.www--binance.com
ww16.admin-apache.www--binance.com
ww16.admin-restricted.www--binance.com
ww16.adminapplications.www--binance.com
ww16.adminsinternals.www--binance.com
ww16.api-singed.www--binance.com
ww16.apidocs-elastic.www--binance.com
ww16.s.applications.www--binance.com
ww16.apps.www--binance.com
ww16.appsvpn.www--binance.com
ww16.lb.auth.www--binance.com
ww16.authorization-singed.www--binance.com
ww16.documentation.azure.www--binance.com
ww16.repository.azure.www--binance.com
ww16.azure.www--binance.com
ww16.azure-chd.www--binance.com
ww16.azure-ctl.www--binance.com
ww16.azuredev.www--binance.com
ww16.azureglobal.www--binance.com
ww16.beta-apps.www--binance.com
ww16.app.boards.www--binance.com
ww16.profiles.boards.www--binance.com
ww16.rpcww16.boards.www--binance.com
ww16.train.boards.www--binance.com
ww16.boards.www--binance.com
ww16.boardsconfluence.www--binance.com
ww16.lb.cert.www--binance.com
ww16.cert-file.www--binance.com
ww16.9.chd.www--binance.com
ww16.chef-hwcdn.www--binance.com
ww16.client-tools.www--binance.com
ww16.clienthwcdn.www--binance.com
ww16.s.cloudfront.www--binance.com
```

```
ww16.lb-mirror.www--binance.com
ww16.lb-oid.www--binance.com
ww16.lb-s3.www--binance.com
ww16.lb-stg.www--binance.com
ww16.lbadm.www--binance.com
ww16.lbemail.www--binance.com
ww16.lbhistory.www--binance.com
ww16.legacyboards.www--binance.com
ww16.login-tools.www--binance.com
ww16.logins.www--binance.com
ww16.loginstream.www--binance.com
ww16.elastic.mail.www--binance.com
ww16.manage-boards.www--binance.com
ww16.management-admin.www--binance.com
ww16.management-tools.www--binance.com
ww16.market9.www--binance.com
ww16.marketing-boards.www--binance.com
ww16.marketsinged.www--binance.com
ww16.9.merchant.www--binance.com
ww16.file.merchant.www--binance.com
ww16.hwcdn.metric.www--binance.com
ww16.mgmt-tools.www--binance.com
ww16.mirror-s.www--binance.com
ww25.z.mobile.www--binance.com
ww16.mobileclient-9.www--binance.com
ww16.mobileclient-stats.www--binance.com
ww16.nautilus-hwcdn.www--binance.com
ww16.node-devel.www--binance.com
ww16.northamericastream.www--binance.com
ww16.oid-apps.www--binance.com
ww16.old-jinx.www--binance.com
ww16.stats.ops.www--binance.com
ww16.client.opsstream.www--binance.com
ww16.engine.opsstream.www--binance.com
ww16.origin.opsstream.www--binance.com
ww16.team.opsstream.www--binance.com
ww16.opsstream.www--binance.com
ww16.opsstream-account.www--binance.com
ww16.opsstream-email.www--binance.com
ww16.opsstreamanalytics.www--binance.com
ww16.opsstreamdemo.www--binance.com
ww16.opsstreamdocument.www--binance.com
ww16.opsstreamhwcdn.www--binance.com
ww16.opsstreammail.www--binance.com
ww16.opsstreampartner.www--binance.com
ww16.orglb.www--binance.com
ww16.origin.www--binance.com
ww16.originelastic.www--binance.com
ww16.originin.www--binance.com
ww16.origins.www--binance.com
ww16.paymenthwcdn.www--binance.com
ww16.opsstream.paywall.www--binance.com
```

```
ww16.elastic-jinx.www--binance.com
ww16.elastic-skins.www--binance.com
ww16.elasticcloud.www--binance.com
ww16.elasticnautilus.www--binance.com
ww16.europefile.www--binance.com
ww16.europewestdevel.www--binance.com
ww16.opsstream.events.www--binance.com
ww16.ext9.www--binance.com
ww16.customer.file.www--binance.com
ww16.internal.file.www--binance.com
ww16.file.www--binance.com
ww16.filecloud.www--binance.com
ww16.filephp.www--binance.com
ww16.azure.frontpage.www--binance.com
ww16.apps.get.www--binance.com
ww16.get-lb.www--binance.com
ww16.getfile.www--binance.com
ww16.getter-singed.www--binance.com
ww16.githubazure.www--binance.com
ww16.globalelastic.www--binance.com
ww16.gw.www--binance.com
ww16.hw-jinx.www--binance.com
ww16.fw.hwcdn.www--binance.com
ww16.promo.hwcdn.www--binance.com
ww16.repository.hwcdn.www--binance.com
ww16.support.hwcdn.www--binance.com
ww16.tomcat.hwcdn.www--binance.com
ww16.hwcdn.www--binance.com
ww16.hwcdncontainer.www--binance.com
ww16.hwcdnopsstream.www--binance.com
ww16.hwcdnportal.www--binance.com
ww16.hwcdnw3.www--binance.com
ww16.hwtrain.www--binance.com
ww16.iad-elastic.www--binance.com
ww16.iadstream.www--binance.com
ww16.ids-admin.www--binance.com
ww16.ids-jinx.www--binance.com
ww16.app.internals.www--binance.com
ww16.documents.internals.www--binance.com
ww16.login.internals.www--binance.com
ww16.swag.internals.www--binance.com
ww16.webapp.internals.www--binance.com
ww16.internals.www--binance.com
ww16.internals-asana.www--binance.com
ww16.internals-dataseed4.www--binance.com
ww16.internals-elastic.www--binance.com
ww16.internalsadministrators.www--binance.com
ww16.internalsgist.www--binance.com
ww16.api.jinx.www--binance.com
ww16.profiles.jinx.www--binance.com
ww16.raw.jinx.www--binance.com
ww16.testing.jinx.www--binance.com
```



After the scan, the Sublist3r tool found 343 unique subdomains related to the main domain (binance.com).

Nslookup

Nslookup is perfect DNS enumeration.That means this is a tool for gathering information about the Domain Name System (DNS) of the targeted system. Nslookup tool help to find out the information related to DNS record names, IP addresses of a target, DNS domain names, and the MX records for the domain or the NS servers of the domain.

Gather information about the IP address of the hostname.

```
┌──(root㉿kali)-[/home/kali]
└─# nslookup binance.com
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
Name:   binance.com
Address: 52.192.247.165
Name:   binance.com
Address: 35.74.171.132
Name:   binance.com
Address: 57.181.163.233
```

Gather information about the mail exchange (MX) records.

```
┌──(root㉿kali)-[/home/kali]
└─# nslookup -type=MX binance.com
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
binance.com     mail exchanger = 10 aspmx2.googlemail.com.
binance.com     mail exchanger = 5 alt2.aspmx.l.google.com.
binance.com     mail exchanger = 1 aspmx.l.google.com.
binance.com     mail exchanger = 10 aspmx3.googlemail.com.
binance.com     mail exchanger = 5 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
```

Gather information about the nameserver (NS) records.

```
┌──(root㉿kali)-[/home/kali]
└─# nslookup -type=NS binance.com

Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
binance.com     nameserver = ns-1319.awsdns-36.org.
binance.com     nameserver = ns-1701.awsdns-20.co.uk.
binance.com     nameserver = ns-234.awsdns-29.com.
binance.com     nameserver = ns-735.awsdns-27.net.

Authoritative answers can be found from:
ns-234.awsdns-29.com    internet address = 205.251.192.234
ns-735.awsdns-27.net    internet address = 205.251.194.223
ns-1319.awsdns-36.org   internet address = 205.251.197.39
ns-1701.awsdns-20.co.uk internet address = 205.251.198.165
ns-234.awsdns-29.com    has AAAA address 2600:9000:5300:ea00::1
ns-735.awsdns-27.net    has AAAA address 2600:9000:5302:df00::1
ns-1319.awsdns-36.org   has AAAA address 2600:9000:5305:2700::1
ns-1701.awsdns-20.co.uk has AAAA address 2600:9000:5306:a500::1
```

Gather information about the “start of authority” (SOA) records. That means we can get details about the domain or region, like the administrator's email address, how long the server should wait between refreshes, and the very last time the domain was modified.

```
┌──(root㉿kali)-[/home/kali]
└─# nslookup -type=SOA binance.com

Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
binance.com
        origin = ns-735.awsdns-27.net
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400

Authoritative answers can be found from:
```

“Any” keyword can use gather all the above information using only one command. So, I use that command to gather information on the in-scope domains.

```
┌──(root㉿kali)-[/home/kali]
└─# nslookup -type=ANY binance.com

Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
binance.com
        origin = ns-735.awsdns-27.net
        mail addr = awsdns-hostmaster.amazon.com
        serial = 1
        refresh = 7200
        retry = 900
        expire = 1209600
        minimum = 86400
binance.com     nameserver = ns-1701.awsdns-20.co.uk.
binance.com     nameserver = ns-735.awsdns-27.net.
binance.com     nameserver = ns-234.awsdns-29.com.
binance.com     nameserver = ns-1319.awsdns-36.org.

Authoritative answers can be found from:
```

Whois

Whois command gathers information related to targeted domain unknown and distant hosts, server information, network details, and any more details. This command also has a lot of filtering options and uses that “whois --help” command to grant filtering techniques

```
┌──(root㉿kali)-[/home/kali]
└─# whois binance.com
   Domain Name: BINANCE.COM
   Registry Domain ID: 2110253554_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2020-06-12T17:09:03Z
   Creation Date: 2017-04-01T16:48:33Z
   Registry Expiry Date: 2025-04-01T16:48:33Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS-1319.AWSDNS-36.ORG
   Name Server: NS-1701.AWSDNS-20.CO.UK
   Name Server: NS-234.AWSDNS-29.COM
   Name Server: NS-735.AWSDNS-27.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-04-09T18:09:28Z <<<

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

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
```

```
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: binance.com
Registry Domain ID: 2110253554_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-12-09T17:10:41+0000
Creation Date: 2017-04-01T16:48:33+0000
Registrar Registration Expiration Date: 2025-04-01T16:48:33+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: DNStination Inc.
Registrant Street: 3450 Sacramento Street, Suite 405
Registrant City: San Francisco
Registrant State/Province: CA
Registrant Postal Code: 94118
Registrant Country: US
Registrant Phone: +1.4155319335
Registrant Phone Ext:
Registrant Fax: +1.4155319336
Registrant Fax Ext:
Registrant Email: admin@dnstinations.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: DNStination Inc.
Admin Street: 3450 Sacramento Street, Suite 405
Admin City: San Francisco
Admin State/Province: CA
Admin Postal Code: 94118
Admin Country: US
Admin Phone: +1.4155319335
Admin Phone Ext:
Admin Fax: +1.4155319336
Admin Fax Ext:
```

```
Admin Fax Ext:
Admin Email: admin@dnstinations.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: DNStination Inc.
Tech Street: 3450 Sacramento Street, Suite 405
Tech City: San Francisco
Tech State/Province: CA
Tech Postal Code: 94118
Tech Country: US
Tech Phone: +1.4155319335
Tech Phone Ext:
Tech Fax: +1.4155319336
Tech Fax Ext:
Tech Email: admin@dnstinations.com
Name Server: ns-735.awsdns-27.net
Name Server: ns-234.awsdns-29.com
Name Server: ns-1319.awsdns-36.org
Name Server: ns-1701.awsdns-20.co.uk
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-04-09T18:09:39+0000 <<<

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

If you wish to contact this domain's Registrant, Administrative, or Technical
contact, and such email address is not visible above, you may do so via our web
form, pursuant to ICANN's Temporary Specification. To verify that you are not a
robot, please enter your email address to receive a link to a page that
facilitates email communication with the relevant contact(s).

Web-based WHOIS:
  https://domains.markmonitor.com/whois

If you have a legitimate interest in viewing the non-public WHOIS details, send
your request and the reasons for your request to whoisrequest@markmonitor.com
and specify the domain name in the subject line. We will review that request and
may ask for supporting documentation and explanation.

The data in MarkMonitor's WHOIS database is provided for information purposes,
and to assist persons in obtaining information about or related to a domain
name's registration record. While MarkMonitor believes the data to be accurate,
the data is provided "as is" with no guarantee or warranties regarding its
accuracy.

By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
```

```
By submitting a WHOIS query, you agree that you will use this data only for
lawful purposes and that, under no circumstances will you use this data to:
  (1) allow, enable, or otherwise support the transmission by email, telephone,
or facsimile of mass, unsolicited, commercial advertising, or spam; or
  (2) enable high volume, automated, or electronic processes that send queries,
data, or email to MarkMonitor (or its systems) or the domain name contacts (or
its systems).

MarkMonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
```

Whatweb

According to Kali Linux, "WhatWeb identifies websites. It recognizes web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices." This tool is very powerful because we can capture a lot of details using this Whatweb tool. Specially, we can gather information about what type of protection mechanism is used that the targeted domain to protect their web application. But the output information is not sorted well.So, we can use filtering options to gather information in a sorted way.

Gather information about www.binance.com in a sorted way with filtering methods.

- Scan "binance.com " with verbose plugin descriptions (./whatweb -v binance.com)
- An aggressive scan of "binance.com " detects the exact version of WordPress (./whatweb -a 3" binance.com ")

```
┌──(root㉿kali)-[/home/kali]
└─# whatweb -v -a 3 binance.com
WhatWeb report for http://binance.com
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 35.74.171.132
Country   : UNITED STATES, US

Summary   : HTTPServer[awselb/2.0], RedirectLocation[https://www.binance.com:443/]

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

        String       : awselb/2.0 (from server string)

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

        String       : https://www.binance.com:443/ (from location)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Server: awselb/2.0
        Date: Tue, 09 Apr 2024 18:30:32 GMT
        Content-Type: text/html
        Content-Length: 134
        Connection: close
        Location: https://www.binance.com:443/

WhatWeb report for https://www.binance.com/
Status    : 302 Found
Title     : <None>
IP        : 52.84.150.48
Country   : UNITED STATES, US

Summary   : HTTPServer[Tengine], RedirectLocation[https://www.binance.com/en], Strict-Transport-Security[max-age=31536000; includeSubdomains], Tengine-Web-Server, UncommonHeaders[x-gateway,x-trace-id,x-traefik-duration,x-content-type-options,referrer-policy,x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 c036ebfd4f49d40799f1a252f4bef276.cloudfront.net (CloudFront)], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]

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

        String       : Tengine (from server string)

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

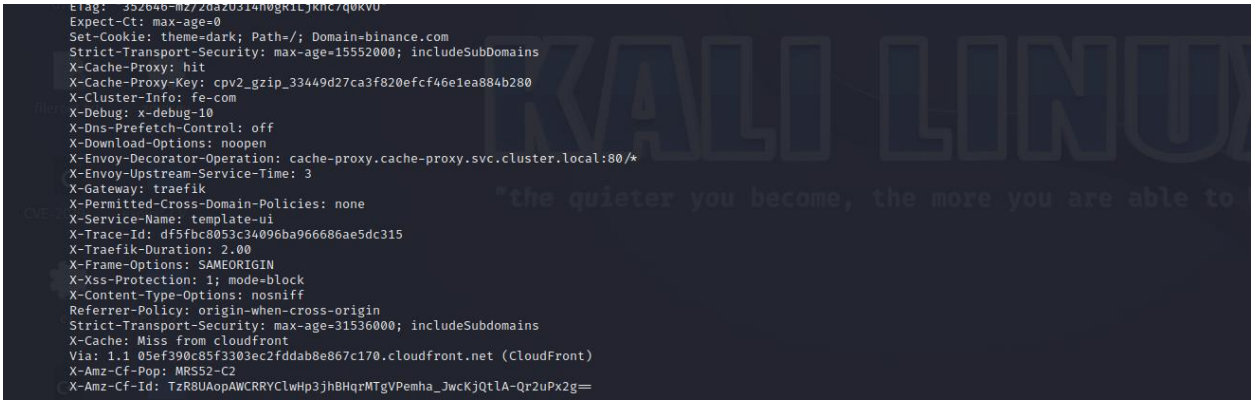
```
        302

        String       : https://www.binance.com/en (from location)

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

        String       : max-age=31536000; includeSubdomains

[ Tengine-Web-Server ]
        Tengine is a web server originated by Taobao, the largest
        e-commerce website in Asia. It is based on the popular
        Nginx HTTP server.

        Website      : http://tengine.taobao.org/

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

        String       : x-gateway,x-trace-id,x-traefik-duration,x-content-type-options,referrer-policy,x-amz-cf-pop,x-amz-cf-id (from headers)

[ Via-Proxy ]
        This plugin extracts the proxy server details from the Via
        param of the HTTP header.

        String       : 1.1 c036ebfd4f49d40799f1a252f4bef276.cloudfront.net (CloudFront)

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

        String       : SAMEORIGIN

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

        String       : 1; mode=block

HTTP Headers:
        HTTP/1.1 302 Moved Temporarily
        Content-Type: text/html; charset=utf-8
```


HTTP Headers:
HTTP/1.1 302 Moved Temporarily
Content-Type: text/html; charset=utf-8
Content-Length: 49
Connection: close
Date: Tue, 09 Apr 2024 18:29:21 GMT
Server: Tengine
Location: https://www.binance.com/en
X-Gateway: traefik
X-Trace-Id: 3c06d88f94714c2f9e5d9d6af07a412b
X-Traefik-Duration: 0.00
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: origin-when-cross-origin
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Cache: Hit from cloudfront
Via: 1.1 c036ebfd4f49d40799f1a252f4bef276.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: HHS52-C2
X-Amz-Cf-Id: 27atdjXIv6eTcFE6SAPoqThy7brcS0Z0zVbtDlRNTiqiRsC9gp8M3A==
Age: 74
WhatWeb report for https://www.binance.com/en
Status : 200 OK
Title : <None>
IP : 52.84.150.48
Country : UNITED STATES, US
Summary : Cookies[theme], Email[949d37812f604f039041170b5601fa1a@o529943.ingest.sentry.io,b2a@1.1.2.js,common@1.3.217.min.js,data@1.3.217.min.js,extension@1.3.217.min.js,footer@1.3.217.min.js,header@1.3.217.min.js,http@1.15.80.js,styles@1.3.217.css,themis@0.0.32.js,track@0.1.97.js,utils@1.3.217.min.js,uuid@9.0.0.js,vendor@1.3.217.min.js], Frame, Google-Analytics[Universal][UA-162512367-1], HTML5, HTTPServer[Tengine], Open-Graph-Protocol[website], Script[application/javascript,application/json,application/ld+json], Strict-Transport-Security[max-age=15552000; includeSubDomains, max-age=31536000; includeSubdomains], Tengine-Web-Server, UncommonHeaders[content-security-policy,expect-ct,x-cache-proxy,x-cache-proxy-key,x-cluster-info,x-debug,x-dns-prefetch-control,x-download-options,x-envoy-decorator-operation,x-envoy-upstream-service-time,x-gateway,x-permitted-cross-domain-policies,x-service-name,x-trace-id,x-traefik-duration,x-content-type-options,referrer-policy,x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 05ef390c85f3303ec2fddab8e867c170.cloudfront.net (CloudFront)], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]
Detected Plugins:
[Cookies]
Display the names of cookies in the HTTP headers. The values are not returned to save on space.
String : theme
[Email]
Extract email addresses. Find valid email address and syntactically invalid email addresses from mailto: link tags. We match syntactically invalid links containing mailto: to catch anti-spam email addresses, eg. bob at gmail.com. This uses the simplified email regular expression from http://www.regular-expressions.info/email.html for valid


String : 949d37812f604f039041170b5601fa1a@o529943.ingest.sentry.io,b2a@1.1.2.js,common@1.3.217.min.js,data@1.3.217.min.js,extension@1.3.217.min.js,footer@1.3.217.min.js,header@1.3.217.min.js,http@1.15.80.js,styles@1.3.217.css,themis@0.0.32.js,track@0.1.97.js,utils@1.3.217.min.js,uuid@9.0.0.js,vendor@1.3.217.min.js
[Frame]
This plugin detects instances of frame and iframe HTML elements.
[Google-Analytics]
This plugin identifies the Google Analytics account.
Version : Universal
Account : UA-162512367-1
Website : http://www.google.com/analytics/
[HTML5]
HTML version 5, detected by the doctype declaration
[HTTPServer]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.
String : Tengine (from server string)
[Open-Graph-Protocol]
The Open Graph protocol enables you to integrate your Web pages into the social graph. It is currently designed for Web pages representing profiles of real-world things . things like movies, sports teams, celebrities, and restaurants. Including Open Graph tags on your Web page, makes your page equivalent to a Facebook Page.
Version : website
[Script]
This plugin detects instances of script HTML elements and returns the script language/type.
String : application/javascript,application/json,application/ld+json
[Strict-Transport-Security]
Strict-Transport-Security is an HTTP header that restricts a web browser from accessing a website without the security of the HTTPS protocol.
String : max-age=15552000; includeSubDomains, max-age=31536000; includeSubdomains
[Tengine-Web-Server]

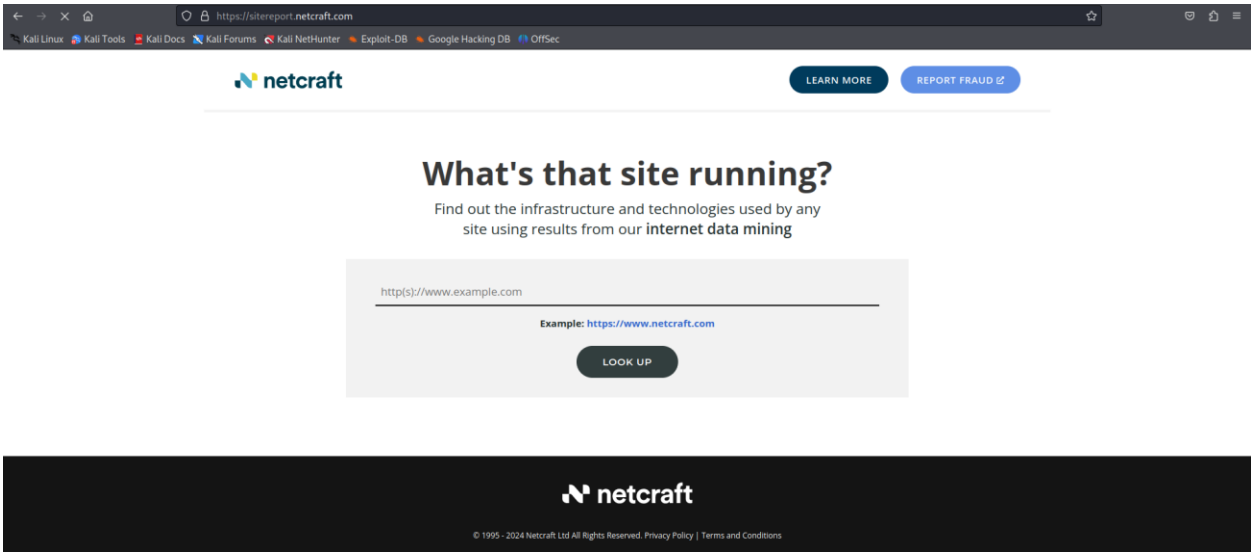

Nginx HTTP server.
Website : http://tengine.taobao.org/
[UncommonHeaders]
Uncommon HTTP server headers. The blacklist includes all the standard headers and many non standard but common ones. Interesting but fairly common headers should have their own plugins, eg. x-powered-by, server and x-aspnet-version. Info about headers can be found at www.http-stats.com
String : content-security-policy,expect-ct,x-cache-proxy,x-cache-proxy-key,x-cluster-info,x-debug,x-dns-prefetch-control,x-download-options,x-envoy-decorator-operation,x-envoy-upstream-service-time,x-gateway,x-permitted-cross-domain-policies,x-service-name,x-trace-id,x-traefik-duration,x-content-type-options,referrer-policy,x-amz-cf-pop,x-amz-cf-id (from headers)
[Via-Proxy]
This plugin extracts the proxy server details from the Via param of the HTTP header.
String : 1.1 05ef390c85f3303ec2fddab8e867c170.cloudfront.net (CloudFront)
[X-Frame-Options]
This plugin retrieves the X-Frame-Options value from the HTTP header. - More Info: http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx
String : SAMEORIGIN
[X-XSS-Protection]
This plugin retrieves the X-XSS-Protection value from the HTTP header. - More Info: http://msdn.microsoft.com/en-us/library/cc288472%28VS.85%29.aspx
String : 1; mode=block


HTTP Headers:
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 547197
Connection: close
Date: Tue, 09 Apr 2024 18:30:41 GMT
Server: Tengine
Cache-Control: max-age=0, must-revalidate
Content-Encoding: gzip
Content-Security-Policy: connect-src 'self' *.google.ad *.google.ae *.google.al *.google.am *.google.as *.google.at *.google.az *.google.ba *.google.be *.google.bf *.google.bg *.google.bi *.google.bj *.google.bs *.google.bt *.google.by *.google.ca *.google.cat *.google.cd *.google.cf *.google.cg *.google.ch *.google.ci *.google.cl *.google.cm *.google.cn *.google.co.ao *.google.co.bw *.google.co.ck *.google.co.cr *.google.co.id *.google.co.il *.google.co.in *.google.co.jp *.google.co.ke *.google.co.kr *.google.co.ls *.google.co.ma *.google.co.mz *.google.co.nz *.google.co.th *.google.co.tz *.google.co.ug *.google.co.uk *.google.co.uz *.google.co.ve *.google.co.vi *.google.co.za *.google.co.zm *.google.co.zw *.google.com *.google.com.af *.google.com.ag *.google.com.ar *.google.com.au *.google.com.bd *.google.com.bh *.google.com.bn *.google.com.bo *.google.com.br *.google.com.bz *.google.com.co *.google.com.cu *.google.com.cy *.google.com.do *.google.com.ec *.google.com.eg *.google.com.et *.google.com.fj *.google.com.gh *.google.com.gi *.google.com.gt *.google.com.hk *.google.com.jm *.google.com.kh *.google.com.kw *.google.com.lb *.google.com.ly *.google.com.mm *.google.com.mt *.google.com.mx *.google.com.my *.google.com.na *.google.com.ng *.google.com.ni *.google.com.np *.google.com.om *.google.com.pa *.google.com.pe *.google.com.pg *.google.com.ph *.google.com.pk *.google.com.pr *.google.com.py *.google.com.qa *.google.com.sa *.google.com.sb *.google.com.sg *.google.com.sl *.google.com.sv *.google.com.tj *.google.com.tr *.google.com.tw *.google.com.ua *.google.com.uy *.google.com.vc *.google.com.vn *.google.cv *.google.cz *.google.de *.google.dj *.google.dk *.google.dm *.google.dz *.google.ee *.google.es *.google.fi *.google.fm *.google.fr *.google.ga *.google.ge *.google.gg *.google.gl *.google.gm *.google.gr *.google.gy *.google.hn *.google.hr *.google.ht *.google.hu *.google.ie *.google.im *.google.iq *.google.is *.google.it *.google.je *.google.jo *.google.kg *.google.ki *.google.kz *.google.la *.google.li *.google.lk *.google.lt *.google.lu *.google.lv *.google.md *.google.me *.google.mg *.google.mk *.google.ml *.google.mn *.google.mu *.google.mv *.google.mw *.google.ne *.google.nl *.google.no *.google.nr *.google.nu *.google.pl *.google.pn *.google.ps *.google.pt *.google.ro *.google.rs *.google.ru *.google.rw *.google.sc *.google.se *.google.sh *.google.si *.google.sk *.google.sm *.google.sn *.google.so *.google.sr *.google.st *.google.td *.google.tg *.google.tl *.google.tm *.google.tn *.google.to *.google.tt *.google.vu *.google.ws https://*.agora.io:* https://*.binance.com https://*.edge.agora.io:* https://*.edge.sd-rtn.com:* https://*.litix.io https://*.s3-accelerate.amazonaws.com https://*.saasexch.cc https://*.saasexch.co https://*.saasexch.com https://*.sd-rtn.com:* https://*.sentry.io https://*.wistia.com https://accounts.google.com https://analytics.google.com https://api.saasexch.com https://api.saasexch.com/baqi/thwnis/api/ https://api.smartling.com https://bat.bing.com https://bin.bnbstatic.com https://cdn.cookielaw.org https://data-collect.toolsfdg.net https://embedwistia-a.akamaihd.net https://fcmregistrations.googleapis.com https://firebaseinstallations.googleapis.com https://frontend-m.binance.cloud https://geolocation.onetrust.com https://googleads.g.doubleclick.net https://log.bntrace.com https://logan-log.binance.gg https://obseu.segreencolumn.com https://privacyportal-bn.my.onetrust.com https://public-1306379396.file.myqcloud.com https://public.bnbstatic.com https://report.binance.gg https://sensors.binance.cloud https://static-file-1306379396.file.myqcloud.com https://stats.g.doubleclick.net https://upload-bnbstatic-com.s3.ap-northeast-1.amazonaws.com https://www.google-analytics.com https://www.google.com https://www.googletagmanager.com wss://*.agora.io:* wss://*.binance.com wss://*.edge.agora.io:* wss://*.edge.sd-rtn.com:* wss://*.sd-rtn.com:* wss://*.yshyqxx.com wss://bstream.binance.com:9443 wss://bstream.yshyqxx.com:443 wss://chat-wss.yshyqxx.com wss://haodesk.binance.im wss://margin-stream.binance.com:443 wss://margin-stream.yshyqxx.com:443 wss://nbstream.binance.com wss://nbstream.yshyqxx.com wss://nbstream.yshyqxx.com:443 wss://stream.binance.com wss://stream.yshyqxx.com:443; default-src 'self' https://*.saasexch.cc https://*.saasexch.co https://*.saasexch.com https://*.wistia.com https://*.wistia.net https://bin.bnbstatic.com https://public-1306379396.file.myqcloud.com https://public.bnbstatic.com https://static-file-1306379396.file.myqcloud.com; font-src 'self' data: https://*.saasexch.cc https://*.saasexch.co https://*.saasexch.com https://*.wistia.com https://accounts.google.com https://api.smartling.com https://at.alicdn.com https://bin.bnbstatic.com https://fonts.gstatic.com https://public-1306379396.file.myqcloud.com https://public.bnbstatic.com https://static-file-1306379396.file.myqcloud.com; frame-src 'self' bnc: https://*.saasexch.cc https://*.saasexch.co https://*.saasexch.com https://accounts.google.com https://accounts.google.com/ https://api.smartling.com https://bid.g.doubleclick.net https://fast.wistia.com https://fast.wistia.net https://optimize.google.com https://www.google.com; style-src 'self' 'unsafe-inline' blob: https://*.saasexch.cc https://*.saasexch.co https://*.saasexch.com https://accounts.google.com https://api.smartling.com https://bin.bnbstatic.com https://fast.wistia.com https://fonts.googleapis.com https://optimize.google.com https://public-1306379396.file.myqcloud.com https://public.bnbstatic.com https://static-file-1306379396.file.myqcloud.com; object-src 'none'; script-src 'nonce-20073258-5c6f-4212-868c-df311aaf5dfa' 'self' 'unsafe-inline' blob: bnc: data: https://*.saasexch.cc https://*.saasexch.co https://*.saasexch.com https://*.wistia.com https://*.wistia.net https://accounts.binance.com https://accounts.google.com https://accounts.google.com/gsi/client https://api.smartling.com https://apis.google.com/js/api:client.js https://appleid.cdn-apple.com https://bat.bing.com https://bin.bnbstatic.com https://cdn.cookielaw.org https://euob.segreencolumn.com https://geolocation.onetrust.com https://googleads.g.doubleclick.net https://log.bntrace.com https://maps.googleapis.com https://obseu.segreencolumn.com https://optimize.google.com https://privacyportal-bn.my.onetrust.com https://public-1306379396.file.myqcloud.com https://public.bnbstatic.com https://src.litix.io https://static-file-1306379396.file.myqcloud.com https://www.google-analytics.com https://www.google.com https://www.googleadservices.com https://www.googleanalytics.com https://www.googleoptimize.com https://www.googletagmanager.com https://www.gstatic.com; media-src 'self' blob: https://*.saasexch.cc https://*.saasexch.co https://*.saasexch.com https://*.wistia.com https://*.wistia.net https://accounts.google.com https://api.smartling.com https://bin.bnbstatic.com https://binance.com https://embedwistia-a.akamaihd.net https://fast.wistia.net https://public-1306379396.file.myqcloud.com https://public.bnbstatic.com https://static-file-1306379396.file.myqcloud.com https://upload-bnbstatic-com.s3.ap-northeast-1.amazonaws.com; base-uri 'self'; img-src 'self' blob: data: https://*.saasexch.cc https://*.saasexch.co https://*.saasexch.com https://*.wistia.com https://*.wistia.net https://accounts.google.com https://analytics.twitter.com https://api.smartling.com https://bat.bing.com https://bin.bnbstatic.com https://cdn.cookielaw.org https://embedwistia-a.akamaihd.net https://geolocation.onetrust.com https://googleads.g.doubleclick.net https://obseu.segreencolumn.com https://optimize.google.com https://privacyportal-bn.my.onetrust.com https://public-1259603563.file.myqcloud.com https://public-1306379396.file.myqcloud.com https://public.bnbstatic.com https://public.nftstatic.com https://sensors.binance.cloud https://static-file-1259603563.file.myqcloud.com https://static-file-1306379396.file.myqcloud.com https://static.devfdg.net https://t.co https://upload-bnbstatic-com.s3.ap-northeast-1.amazonaws.com https://www.facebook.com https://www.google-analytics.com https://www.google.com https://www.googletagmanager.com
ETag: "352646-mz/2dazU314h0gRiljknc7q0kVU"
Expect-Ct: max-age=0
Set-Cookie: theme=dark; Path=/; Domain=binance.com
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Cache-Proxy: hit


ETag: "352646-mz/2dazU314h0gRiljknc7q0kVU"
Expect-Ct: max-age=0
Set-Cookie: theme=dark; Path=/; Domain=binance.com
Strict-Transport-Security: max-age=15552000; includeSubDomains
X-Cache-Proxy: hit
X-Cache-Proxy-Key: cpv2_gzip_33449d27ca3f820efcf46e1ea884b280
X-Cluster-Info: fe-com
X-Debug: x-debug-10
X-Dns-Prefetch-Control: off
X-Download-Options: noopen
X-Envoy-Decorator-Operation: cache-proxy.cache-proxy.svc.cluster.local:80/*
X-Envoy-Upstream-Service-Time: 3
X-Gateway: traefik
X-Permitted-Cross-Domain-Policies: none
X-Service-Name: template-ui
X-Trace-Id: df5fbc8053c34096ba966686ae5dc315
X-Traefik-Duration: 2.00
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referrer-Policy: origin-when-cross-origin
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Cache: Miss from cloudfront
Via: 1.1 05ef390c85f3303ec2fddab8e867c170.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: MRS52-C2
X-Amz-Cf-Id: TzR8UAopAWCRRYClwHp3jhBHqrMTgVPemha_JwcKjQtlA-Qr2uPx2g==

Netcraft

Netcraft is a cybersecurity company offering tools and services to analyze and protect against online threats, including the Netcraft Web Server Survey, for both professionals and website owners.



This is the Netcraft tool's main user interface. To obtain the details from this tool, we need to enter the domain name.

Site report for http://binance.com

Gather details about the Network and Background of the targeted domain.

Background

Site title	Binance - Cryptocurrency Exchange for Bitcoin, Ethereum & Altcoins	**Date first seen**	November 2014
Site rank	34456	**Primary language**	English
Description	Binance cryptocurrency exchange - We operate the worlds biggest bitcoin exchange and altcoin crypto exchange in the world by volume		

Network

Site	http://binance.com	**Domain**	binance.com
Netblock Owner	Amazon Data Services Japan	**Nameserver**	ns-735.awsdns-27.net
Hosting company	Amazon - Asia Pacific (Tokyo) datacenter	**Domain registrar**	markmonitor.com
Hosting country	jp	**Nameserver organisation**	whois.markmonitor.com
IPv4 address	52.192.247.165 (VirusTotal)	**Organisation**	DNStination Inc., 3450 Sacramento Street, Suite 405, San Francisco, 94118, United States
IPv4 autonomous systems	AS16509	**DNS admin**	awsdns-hostmaster@amazon.com
IPv6 address	Not Present	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	Not Present	**DNS Security Extensions**	Unknown
Reverse DNS	ec2-52-192-247-165.ap-northeast-1.compute.amazonaws.com		

- Gather information regarded to IP Delegation of the targeted domain.

IP delegation

IPv4 address (52.192.247.165)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 52.0.0.0-52.255.255.255	United States	NET52	American Registry for Internet Numbers
↳ 52.192.0.0-52.223.191.255	United States	AT-88-Z	Amazon Technologies Inc.
↳ 52.192.0.0-52.193.255.255	Japan	AMAZON-NRT	Amazon Data Services Japan
↳ 52.192.247.165	Japan	AMAZON-NRT	Amazon Data Services Japan

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
▸ Amazon Data Services J...	52.68.48.32	Linux	awselb/2.0	19-Mar-2024
▸ Amazon Data Services J...	35.72.205.82	Linux	awselb/2.0	15-Mar-2024
▸ Amazon Data Services J...	52.68.48.32	Linux	awselb/2.0	14-Mar-2024
▸ Amazon Data Services J...	35.72.205.82	Linux	awselb/2.0	13-Mar-2024
▸ Amazon Data Services J...	52.197.246.6	Linux	awselb/2.0	12-Mar-2024
Amazon Technologies Inc. 410 Terry Ave N. Seattle WA US 98109	54.178.165.246	Linux	awselb/2.0	10-Mar-2024
	57.180.115.161	Linux	awselb/2.0	18-Feb-2024
▸ Amazon Data Services J...	54.92.46.150	Linux	awselb/2.0	17-Feb-2024
▸ Amazon.com, Inc. Amazo...	57.180.115.161	Linux	awselb/2.0	16-Feb-2024
▸ Amazon Data Services J...	54.92.66.34	Linux	awselb/2.0	15-Feb-2024

Sender Policy Framework

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

Qualifier	Mechanism	Argument
+ (Pass)	include	_spf.google.com
- (Fail)	all	

DMARC

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

Raw DMARC record:

```
v=DMARC1;                          p=quarantine;                          rua=mailto:binance@rua.netcraft.com,mailto:dmarc@binance.com;
ruf=mailto:binance@ruf.netcraft.com,mailto:dmarc@binance.com;
```

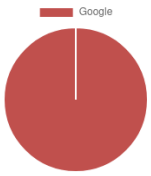
Tag	Field	Value
p=quarantine	Requested handling policy	Quarantine: emails that fail the DMARC mechanism check should be treated by Mail Receivers as suspicious. Depending on the capabilities of the Mail Receiver, this can mean "place into spam folder", "scrutinize with additional intensity", and/or "flag as suspicious".
rua=mailto:binance@rua.netcraft.com,mailto:dmarc@binance.com	Reporting URI(s) for aggregate data	binance@rua.netcraft.com, dmarc@binance.com
ruf=mailto:binance@ruf.netcraft.com,mailto:dmarc@binance.com	Reporting URI(s) for failure data	binance@ruf.netcraft.com, dmarc@binance.com

Web Trackers

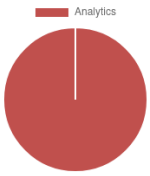
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics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

2 known trackers were identified.

Companies



Categories



Company	Primary Category	Tracker	Popular Sites with this Tracker
Google	Analytics	Google Analytics	www.interia.pl, www.bleepingcomputer.com, www.ikea.com
		Googletagmanager	www.chess.com, www.speedtest.net, www.ilovepdf.com

- Gather the information about Site Technology.

Site Technology (fetched 31 days ago)

Cloud & PaaS

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service.

Technology	Description	Popular sites using this technology
Amazon Web Services - EC2	Cloud computing service (Elastic Compute Cloud)	www.duolingo.com, onlyfans.com, arco.freshservice.com
Amazon Web Services - CloudFront	Amazon Content Delivery Network	www.primevideo.com, base-contacts.aftral.com

Network

Any network related service or technology.

Technology	Description	Popular sites using this technology
Amazon Web Services - Route 53	Cloud based Domain Name System (DNS) servie	

HTTP Accelerator

A web accelerator is a proxy server that reduces web site access times.

Technology	Description	Popular sites using this technology
Envoy	Open source proxy	www.ebay.com, www.pinterest.com, www.nytimes.com

Server-Side

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

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	
Tengine Web Server	*No description*	www.bilibili.com, space.bilibili.com, es.aliexpress.com

Client-Side

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

Technology	Description	Popular sites using this technology
Local Storage	*No description*	
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	

Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

Technology	Description	Popular sites using this technology
Google Tag Manager	*No description*	www.coingecko.com, www.chess.com, www.hmhco.com
Google Hosted Libraries	Google API to retrieve JavaScript libraries	www.roblox.com, www.google.com, www.qwant.com
D3.js Visualisation Library	*No description*	www.tumblr.com, www.javatpoint.com, www.ubereats.com
AJAX	*No description*	www.amazon.com, www.amazon.de, accounts.google.com

Technology	Description	Popular sites using this technology
Currency EUR	*No description*	www.boursorama.com, www.etsy.com, www.essig-oel.de

Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
Cloudfront	*No description*	www.amazon.es, www.espn.com, www.amazon.co.uk

Character Encoding

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

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

HTTP Compression

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

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.virustotal.com, www.amazon.in, www.amazon.ca

Web Browser Targeting

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

Technology	Description	Popular sites using this technology
Expect Certificate Transparency Header	Enforce Certificate Transparency requirements	www.mercadolibre.com.ar, www.nk.ca, www.mercadolivre.com.br
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	www.linkedin.com, www.instagram.com, mail.google.com
Strict-Transport-Security (including subdomains)	*No description*	www.startpage.com, support.microsoft.com, support.google.com
Content Security Policy	Detect and mitigate attacks in the browser	www.bbc.co.uk, teams.microsoft.com, twitter.com
X-Content-Type-Options	Browser MIME type sniffing is disabled	mail-redir.mention.com
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	
Referrer Policy	Restrict referrer information included in subsequent requests	www.notion.so, www.bbc.com, mail.proton.me
X-XSS-Protection Block	Block pages on which cross-site scripting is detected	

Doctype

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

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

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	

CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.twitch.tv, www.binance.com, www.netflix.com
CSS Media Query	*No description*	www.imdb.com, www.arco.co.uk, www.paypal.com
Embedded	Styles defined within a webpage	www.aliexpress.com, www.xvideos.com, www.amazon.fr

Doctype

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

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

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	

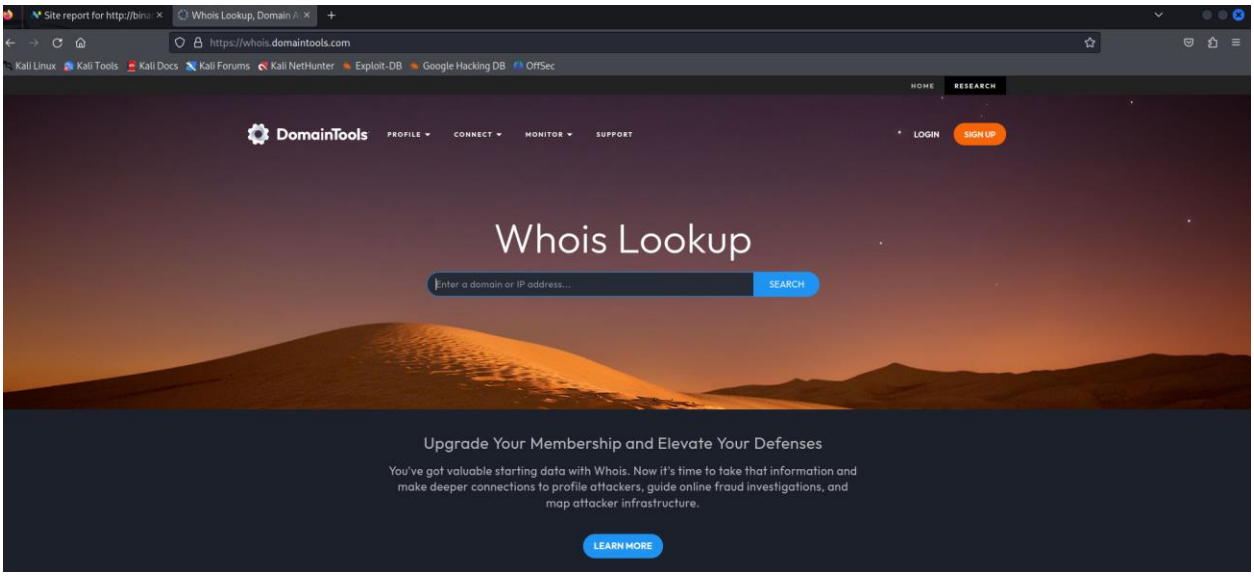
CSS Usage

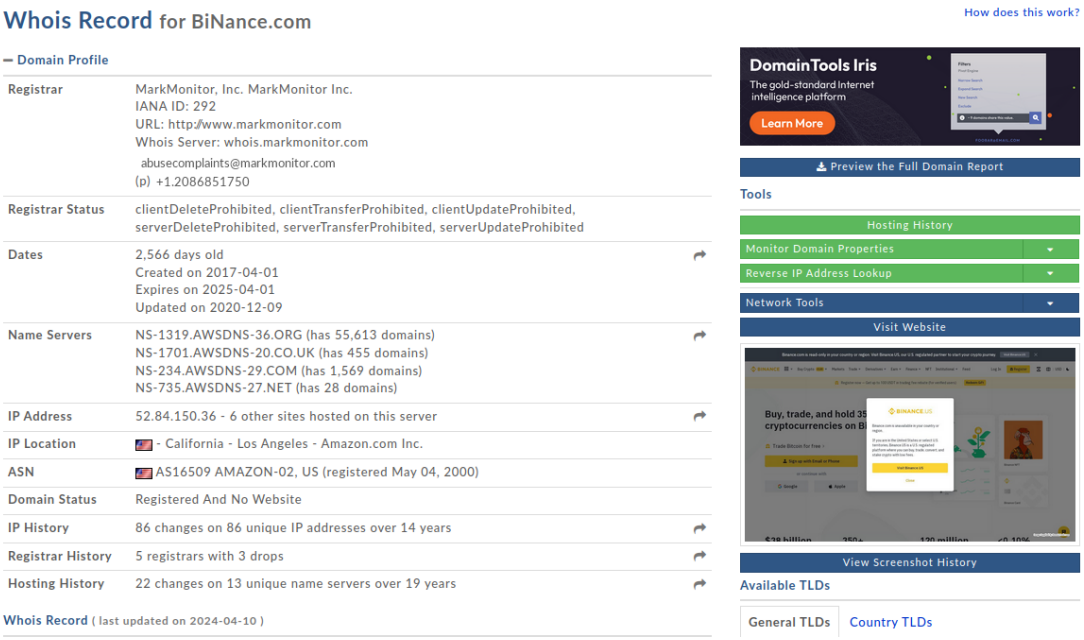
Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.twitch.tv, www.binance.com, www.netflix.com
CSS Media Query	*No description*	www.imdb.com, www.arco.co.uk, www.paypal.com
Embedded	Styles defined within a webpage	www.aliexpress.com, www.xvideos.com, www.amazon.fr

Whois Lookup

WHOIS lookup tools provide domain registration details, owner's name, contact information, and expiration dates, aiding in verifying ownership, investigating website issues, and contacting domain owners.





Whois Record (last updated on 2024-04-10)

```
Domain Name: binance.com
Registry Domain ID:
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2020-12-09T17:10:41+00:00
        2020-06-12
Creation Date: 2017-04-01T16:48:33+00:00
        2017-04-01
Registrar Registration Expiration Date: 2025-04-01T16:48:33+00:00
        2025-04-01
Registrar: MarkMonitor, Inc.
        MarkMonitor Inc.
Sponsoring Registrar IANA ID: 292
Registrar Abuse Contact Email:  abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Status:
        clientDeleteProhibited
        clientTransferProhibited
        clientUpdateProhibited
        serverDeleteProhibited
        serverTransferProhibited
        serverUpdateProhibited
Registry Registrant ID:
Registrant Name: REDACTED FOR PRIVACY (DT)
Registrant Organization: DNStination Inc.
Registrant Street: 3450 Sacramento Street, Suite 405
Registrant City: San Francisco
Registrant State/Province: CA
Registrant Postal Code: 94118
Registrant Country: US
Registrant Phone: +1.4155319335
Registrant Phone Ext:
Registrant Fax: +1.4155319336
Registrant Fax Ext:
Registrant Email:  admin@dnstinations.com
Registry Admin ID:
Admin Name: REDACTED FOR PRIVACY (DT)
Admin Organization: DNStination Inc.
Admin Street: 3450 Sacramento Street, Suite 405
Admin City: San Francisco
Admin State/Province: CA
Admin Postal Code: 94118
Admin Country: US
Admin Phone: REDACTED FOR PRIVACY (DT)
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY (DT)
Admin Fax Ext:
Admin Email:  admin@dnstinations.com
Registry Tech ID:
Tech Name: REDACTED FOR PRIVACY (DT)
Tech Organization: DNStination Inc.
Tech Street: 3450 Sacramento Street, Suite 405
Tech City: San Francisco
Tech State/Province: CA
Tech Postal Code: 94118
Tech Country: US
Tech Phone: REDACTED FOR PRIVACY (DT)
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY (DT)
Tech Fax Ext:
Tech Email:  admin@dnstinations.com
Registry Billing ID:
Billing Name:
Billing Organization:
Billing Street:
Billing City:
Billing State/Province:
Billing Postal Code:
Billing Country:
Billing Phone:
Billing Phone Ext:
Billing Fax:
Billing Fax Ext:
Billing Email:
Nameservers:
        ns-1319.awsdns-36.org
        ns-1701.awsdns-20.co.uk
        ns-234.awsdns-29.com
        ns-735.awsdns-27.net
Registry ID: 2110253554_DOMAIN_COM-VRSN
DNSSEC: unsigned
```

General TLDs | **Country TLDs**

The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)

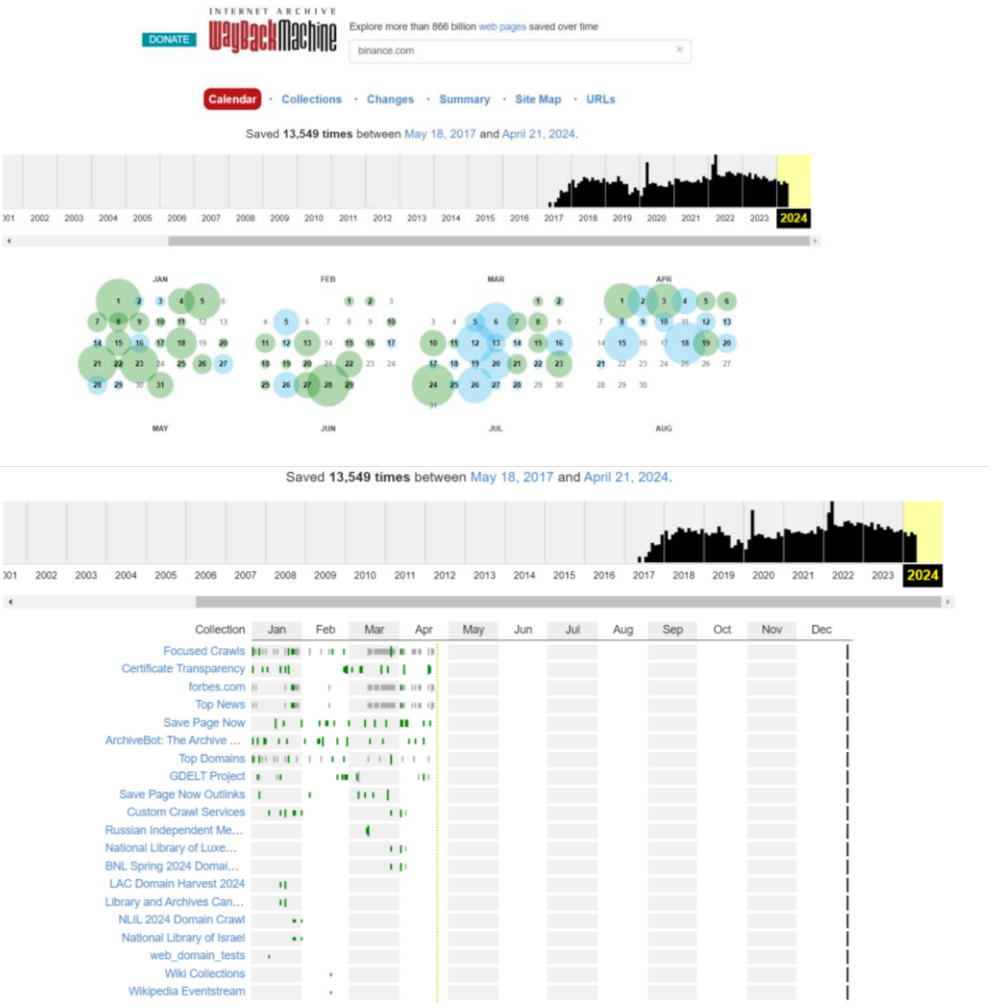
- Taken domain.
- Available domain.
- Deleted previously owned domain.

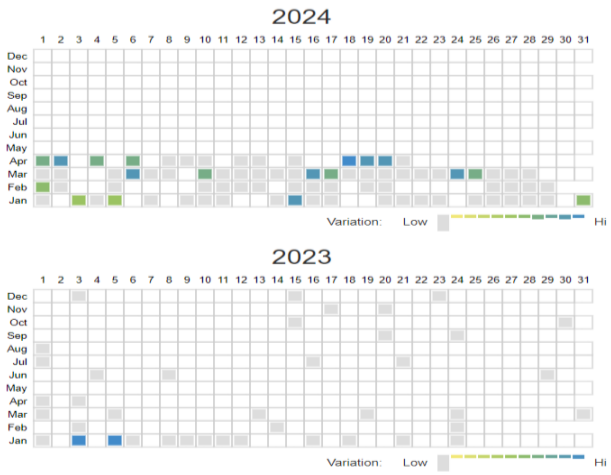
BiNance.com	View Whois
BiNance.org	View Whois
BiNance.info	View Whois
BiNance.biz	View Whois
BiNance.us	View Whois

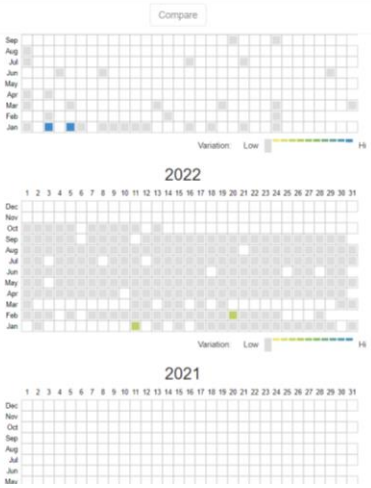
Wayback machine

Website link - https://web.archive.org/web

This tool is invaluable for finding archived versions of websites. It can be used to access historical snapshots of web pages, which can be useful for various purposes such as retrieving old content, investigating past versions of a site, or verifying changes over time.







This approach yields some fascinating data, which makes it quite beneficial for information collecting. Examples include:

• Sensitive data;

• Old, forgotten endpoints;

• Interesting JS files

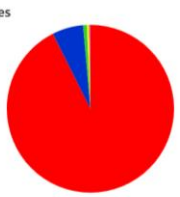
Summary on MIME-types Count

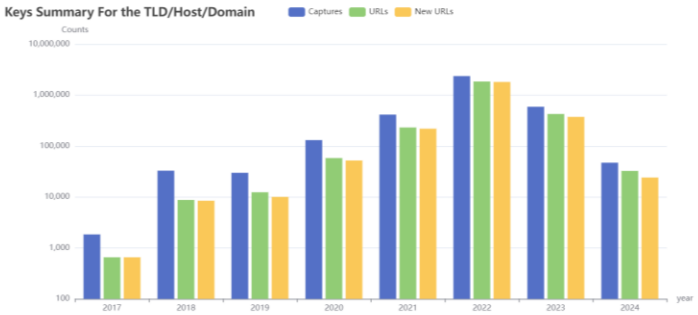
Quick search on MIME-types...

<< < 1 2 > >>

	Captures	Unique URLs
text/html	3,334,650	2,439,125
application/json	215,903	30,694
application/xml	26,430	11,289
application/xhtml+xml	12,782	10,498
image/png	4,487	779
image/jpeg	2,942	267
application/javascript	1,456	380
image/svg+xml	1,090	56
text/plain	1,058	140
text/css	529	182

Explore binance.com URLs





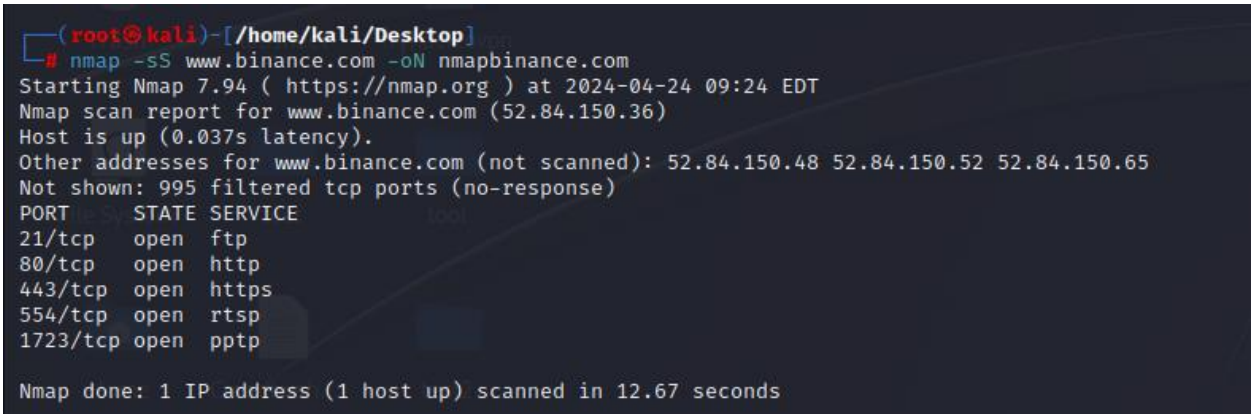
Moreover URLS

URL ↑	MIME Type	From	To	Captures	Duplicates	Uniques
http://binance.com/$BINAX	text/html	Dec 23, 2021	Dec 23, 2021	2	1	1
http://binance.com/&esheet=52722894&newsitemid=20220518005291&lan=en-US&anchor=Binance.com&index=14&md5=6b47ae79bbb8a3b4ea1b64e90b8370bd	text/html	May 18, 2022	May 18, 2022	2	1	1
http://binance.com/)	warc/revisit	Dec 2, 2023	Dec 2, 2023	1	0	1
http://binance.com/*/999/3mBinanceLabs	text/html	Jan 18, 2023	Jan 18, 2023	2	1	1
http://binance.com/ Подробнее	text/html	Jan 21, 2023	Jan 21, 2023	2	0	2
http://binance.com/../5908700f092e4807bd48c03a5bbe8258	text/html	Jul 27, 2021	Jul 27, 2021	1	0	1
http://binance.com/../6498a2181910495eb14152cf5da39188	text/html	Sep 4, 2022	Sep 4, 2022	1	0	1
http://binance.com/.us	text/html	Jun 23, 2021	Jun 23, 2021	1	0	1
http://binance.com/123445	text/html	Jul 21, 2021	Jul 21, 2021	1	0	1
http://binance.com/391497354	text/html	Jul 5, 2022	Jul 5, 2022	1	0	1
http://binance.com/?	text/html	Jan 7, 2023	Jan 7, 2023	2	0	2
http://binance.com/?/=16788521	text/html	Oct 31, 2020	May 7, 2023	6	2	4
http://binance.com/?1369628	text/html	Nov 11, 2021	Feb 5, 2023	3	0	3
http://binance.com/?=16349875	text/html	Jan 19, 2022	Jan 19, 2022	2	0	2
http://binance.com/?=16967708	text/html	Feb 15, 2020	Mar 3, 2020	2	0	2
http://binance.com/?=51995506	text/html	Feb 12, 2021	Feb 12, 2021	2	0	2
http://binance.com/?=ref567657	warc/revisit	Nov 1, 2020	Nov 1, 2020	2	0	2
http://binance.com/?amp	text/html	Aug 19, 2022	Aug 31, 2022	3	0	3
http://binance.com/?fbclid=IwAR1NcHEKchdf_bjHqYEITqJKV-98gPreTwV3NKa6BYtAaiLcj-LjS_I2I4s	text/html	Nov 14, 2022	Nov 14, 2022	1	0	1
http://binance.com/?fbclid=IwAR1TE0A1tqQOW8h4NoRtaqChJlg-QPXyODSO3R66TYeWc9ImxG_P_2RMmD0	text/html	Nov 12, 2020	Nov 12, 2020	2	0	2
http://binance.com/?id=y9JMX-NjQO	text/html	Sep 2, 2021	Sep 2, 2021	2	0	2
http://binance.com/?liquid?coinhako?kucoin?bitfinex	text/html	Nov 15, 2022	Nov 15, 2022	2	0	2
http://binance.com/?m	text/html	Oct 12, 2022	Oct 12, 2022	2	0	2

Active information gathering tools

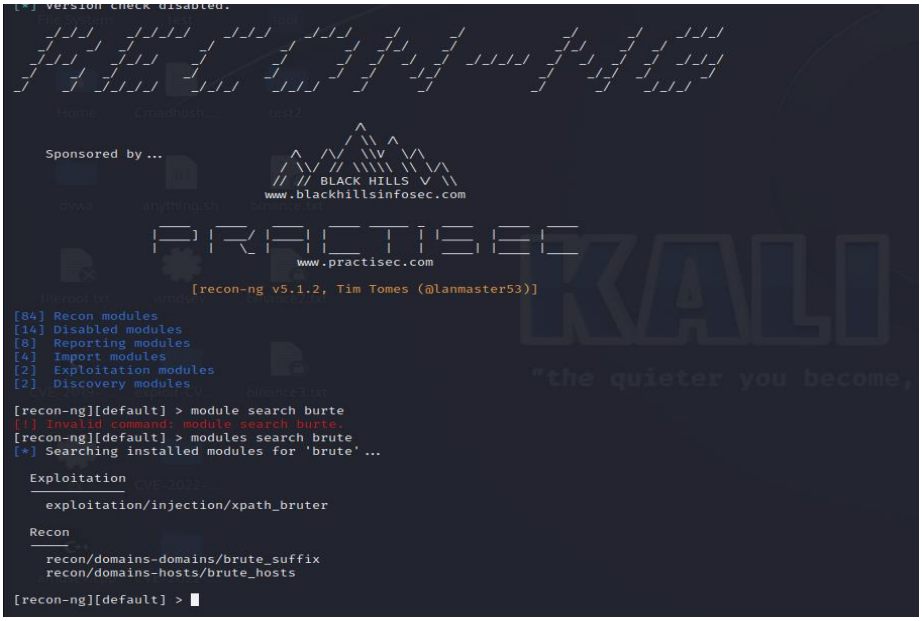
Nmap

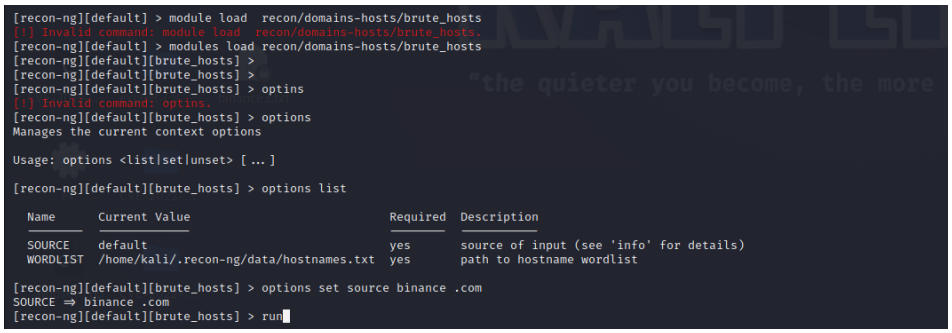
Nmap is a tool that can be used to determine the status of ports, whether the host is up and running, and a host of other helpful information. The targeted domain's vulnerabilities can also be scanned using the Nmap tool. However, at this point, my only purpose for using this tool is to learn whether any ports are open, closed, or filtered. Thus, to obtain information about the open port of the targeted domains, run a SYN scan using the Nmap tool.



Recon -ng Tool

Recon-ng is a robust security tool used by professionals and bug bounty hunters to gather information about target systems, simplifying intelligence gathering during security assessments and penetration testing engagements.

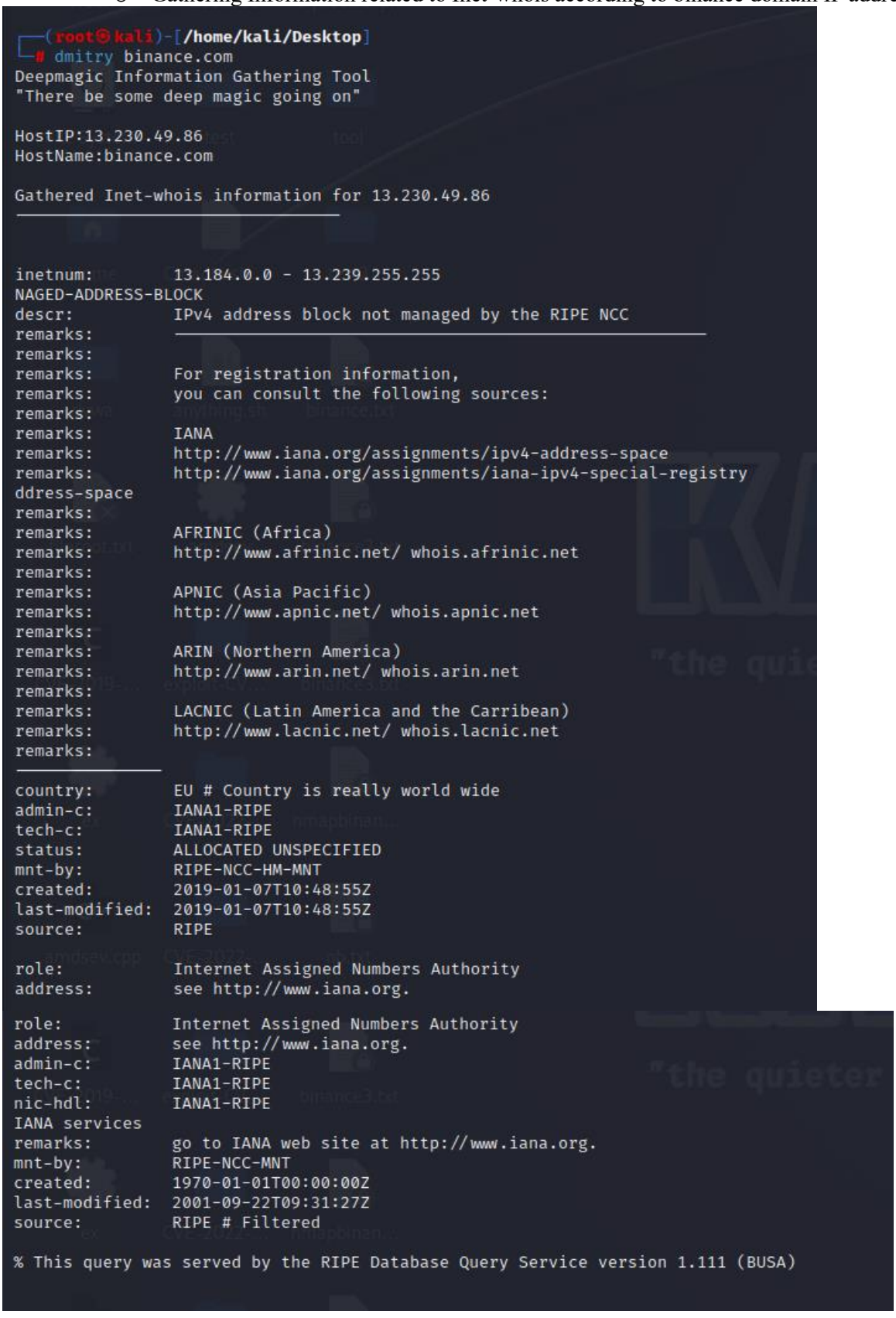

[*] Version check disabled.
Sponsored by ...
www.blackhillsinfosec.com
www.practisec.com
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[84] Recon modules
[14] Disabled modules
[8] Reporting modules
[4] Import modules
[2] Exploitation modules
[2] Discovery modules
[recon-ng][default] > module search burte
[!] Invalid command: module search burte.
[recon-ng][default] > modules search brute
[*] Searching installed modules for 'brute' ...
Exploitation
exploitation/injection/xpath_bruter
Recon
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts
[recon-ng][default] >


[recon-ng][default] > module load recon/domains-hosts/brute_hosts
[!] Invalid command: module load recon/domains-hosts/brute_hosts.
[recon-ng][default] > modules load recon/domains-hosts/brute_hosts
[recon-ng][default][brute_hosts] >
[recon-ng][default][brute_hosts] >
[recon-ng][default][brute_hosts] > optins
[!] Invalid command: optins.
[recon-ng][default][brute_hosts] > options
Manages the current context options
Usage: options <list|set|unset> [...]
[recon-ng][default][brute_hosts] > options list
Name Current Value Required Description
SOURCE default yes source of input (see 'info' for details)
WORDLIST /home/kali/.recon-ng/data/hostnames.txt yes path to hostname wordlist
[recon-ng][default][brute_hosts] > options set source binance .com
SOURCE => binance .com
[recon-ng][default][brute_hosts] > run

Dmitry

Dmitry is an assortment of data collection tools. This makes the tool a package or combination of tools. We can obtain information about Netcraft, open ports, and Whois lookup web tool details by using this tool. Dmitry is an active information gathering tool since it collects data about open ports.

- Gathering Information related to Inet-whois according to binance domain IP address.



```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# dmitry binance.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:13.230.49.86
HostName:binance.com

Gathered Inet-whois information for 13.230.49.86
---------------------------------


inetnum:        13.184.0.0 - 13.239.255.255
NAGED-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
ddress-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:
---------------
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:        2019-01-07T10:48:55Z
last-modified:  2019-01-07T10:48:55Z
source:         RIPE

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
created:        1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:31:27Z
source:         RIPE # Filtered

% This query was served by the RIPE Database Query Service version 1.111 (BUSA)
```

```
Gathered Inic-whois information for binance.com
---------------------------------
   Domain Name: BINANCE.COM
   Registry Domain ID: 2110253554_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2020-06-12T17:09:03Z
   Creation Date: 2017-04-01T16:48:33Z
   Registry Expiry Date: 2025-04-01T16:48:33Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
tDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
bited
   Name Server: NS-1319.AWSDNS-36.ORG
   Name Server: NS-1701.AWSDNS-20.CO.UK
   Name Server: NS-234.AWSDNS-29.COM
   Name Server: NS-735.AWSDNS-27.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-04-24T13:38:46Z <<<
```

- Gathering Information related to Netcraft according to binance domain.

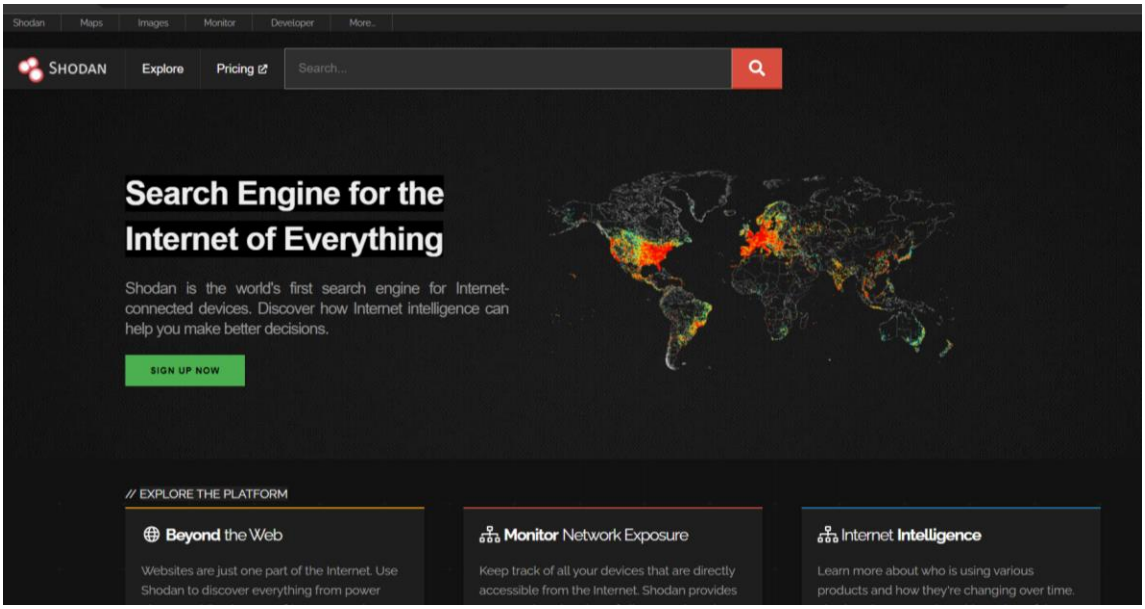
```
Gathered Netcraft information for binance.com
---------------------------------

Retrieving Netcraft.com information for binance.com
Netcraft.com Information gathered

Gathered Subdomain information for binance.com
---------------------------------
Searching Google.com:80 ...
HostName:www.binance.com
HostIP:52.84.150.48
HostName:launchpad.binance.com
HostIP:18.155.68.89
HostName:pool.binance.com
HostIP:13.33.30.124
HostName:accounts.binance.com
HostIP:13.33.88.22
HostName:margin-stream.binance.com
HostIP:54.64.46.210
HostName:data.binance.com
HostIP:13.113.223.241
HostName:fstream-auth.binance.com
HostIP:13.230.49.86
HostName:counts.binance.com
HostIP:54.249.159.43
HostName:p2p.binance.com
HostIP:108.157.254.73
HostName:api.binance.com
HostIP:108.158.2.107
HostName:pay.binance.com
HostIP:52.84.150.48
HostName:academy.binance.com
HostIP:18.155.68.31
Searching Altavista.com:80 ...
Found 12 possible subdomain(s) for host binance.com, Searched 0 pages containing 0 results
```

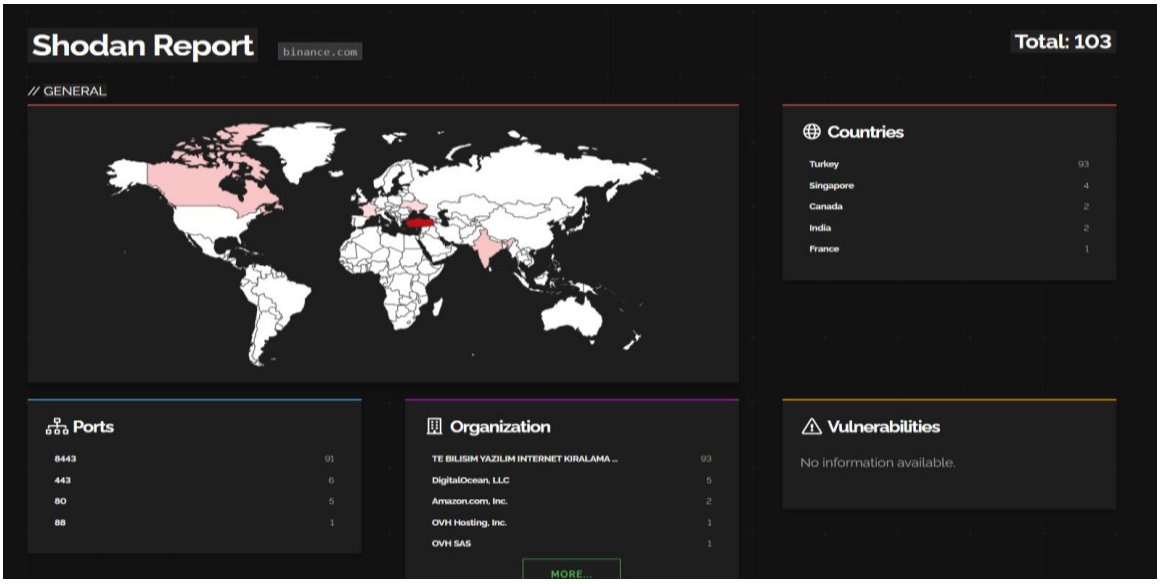
- Gathering Information related to E-mail and state of TCP port according to binance domain.

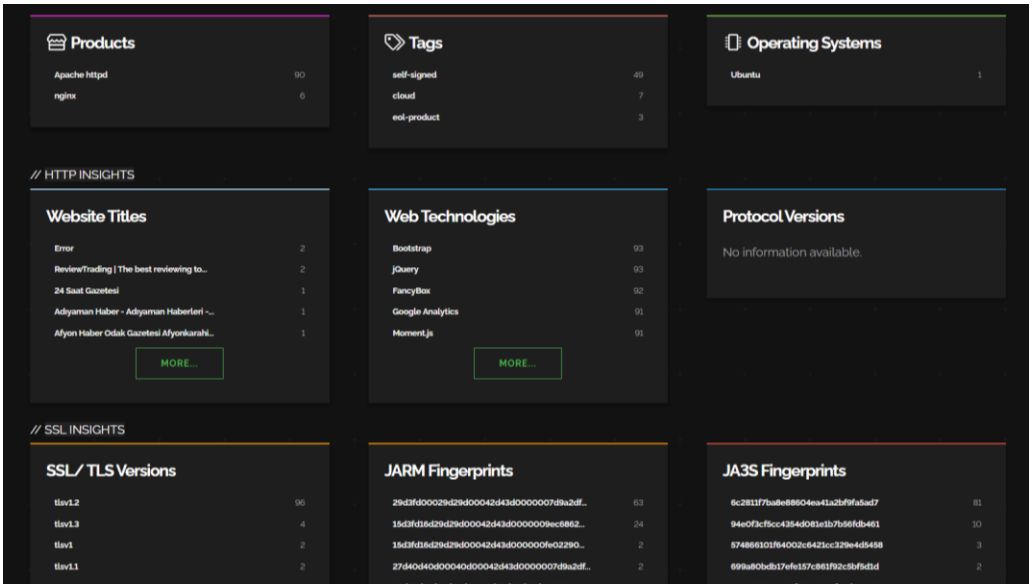
```
Gathered E-Mail information for binance.com
---------------------------------
Searching Google.com:80 ...
Searching Altavista.com:80 ...
Found 0 E-Mail(s) for host binance.com, Searched 0 pages containing 0 results

Gathered TCP Port information for 13.113.223.241
---------------------------------

 Port            State

21/tcp           open
80/tcp           open

Portscan Finished: Scanned 150 ports, 0 ports were in state closed


All scans completed, exiting
```

Shodan

Shodan is a powerful tool for internet device analysis, but its use should be ethically and responsibly, ensuring proper authorization for unauthorized scanning or exploitation.







These are the Passive and Active tools I use to gather information about the www.binance.com domain

Planning and Analysis

After the information gathering period, we must examine those specifics to determine our next steps of focus. Since vulnerability detection is a time-consuming process and can be done in a targeted manner with a plan, the planning stage is very important. As a result, we can save time and carry out vulnerability detection very effectively.

So, following the information collection process, the data can be categorized based on technical specifications, including those of the Web server, application server, and database server. Additionally, the information targeted at running the vulnerability scan is the status of the ports and the HTTP security measures.

- Technical Details
    - Web server
        - CloudFront server
            - trbinance.com
            - info.binance.com
            - c2c.binance.com
        - Tengine server
            - trbinance.com
            - info.binance.com
            - account.binance.com
            - c2c.binance.com
            - coinmarketcap.com
            - pro.coinmarketcap.com
        - Nginx server
            - *.binance.com
            - info.binance.com
- Gathering information about the Domain Name System (DNS) of the targeted system in Nslookup report
- Open ports details are in the Nmap scan report done in the information gathering stage. ➢
- HTTP security details are in the Wahtweb scan report done in the information gathering stage.

Next, choose the tools for vulnerability scanning based on the data that has been gathered, and schedule the vulnerability scanning process based on the specifics of the information analysis.

Vulnerability Detection

Vulnerability detection is a crucial stage in Bug Bounty assessment, identifying weaknesses in software, hardware, networks, or systems that could be exploited by attackers to compromise an organization's security.

There are two techniques for detecting vulnerabilities: automated and manual scanning. Automated scanning checks for vulnerabilities in all system subdomains, while manual scanning filters the scanning process. While automated scanning is simple, it takes time, making manual scanning a more productive approach for identifying vulnerabilities. Both methods are widely available and can be used to scan system vulnerabilities.

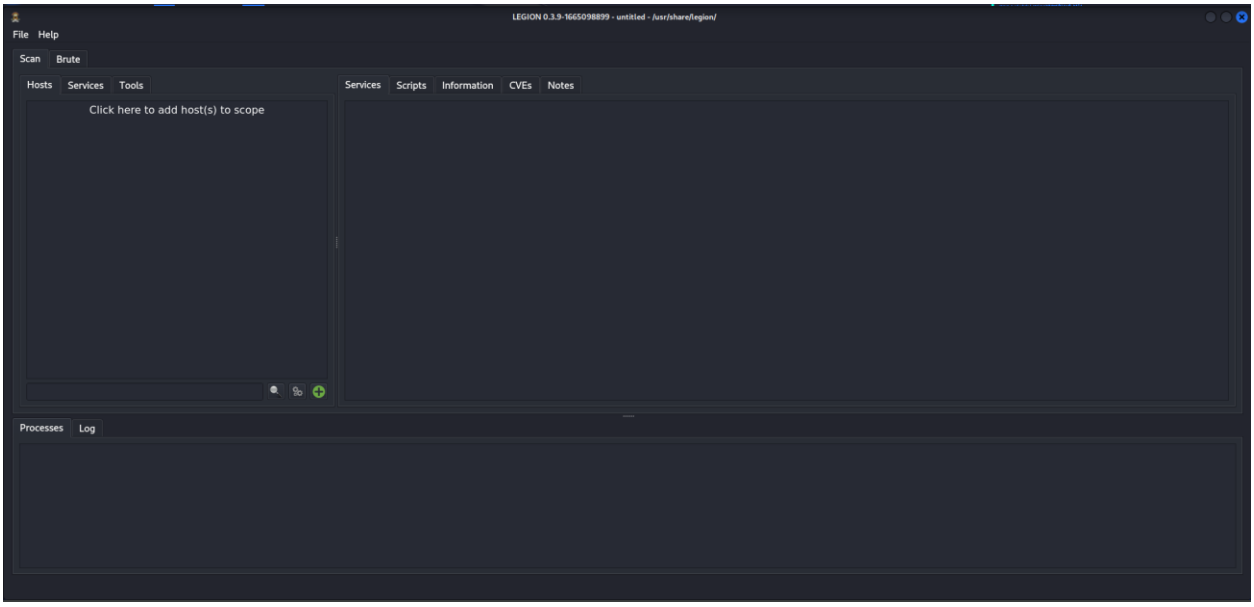
So, detecting those vulnerabilities can be done using the Vulnerability Detection tools.

- ✓ Legion
- ✓ Nikto
- ✓ Nmap
- ✓ Arachni
- ✓ Uniscan
- ✓ Netsparker
- ✓ Nessus
- ✓ Owasp Zap

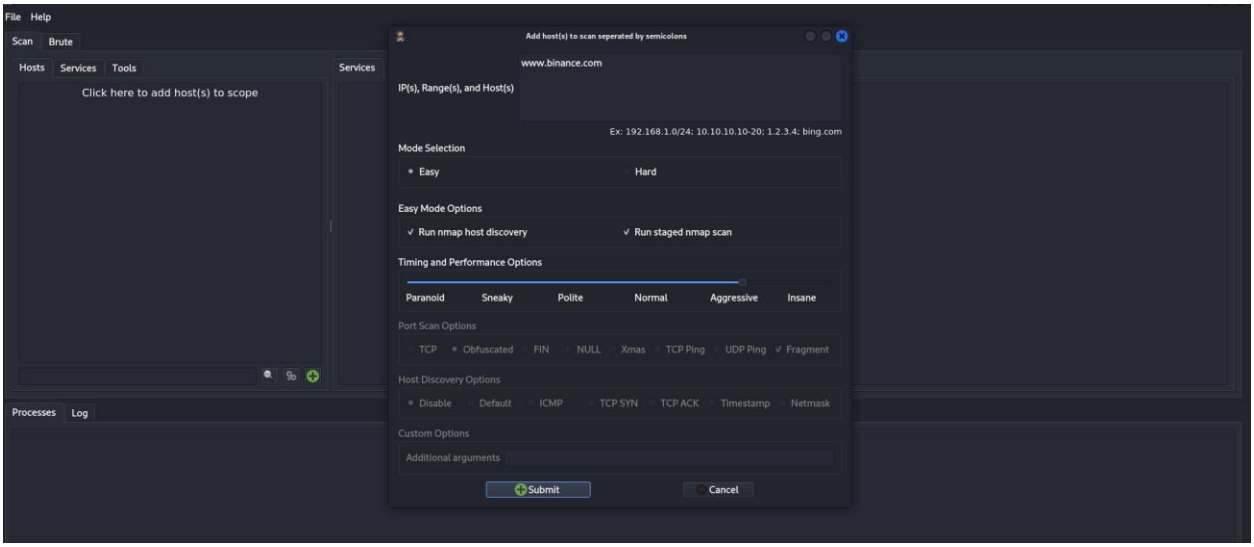
I choose that the most suitable vulnerability detection tool according to the gathered information and the usability of those tools. Because some of those tools are not freeware

Legion

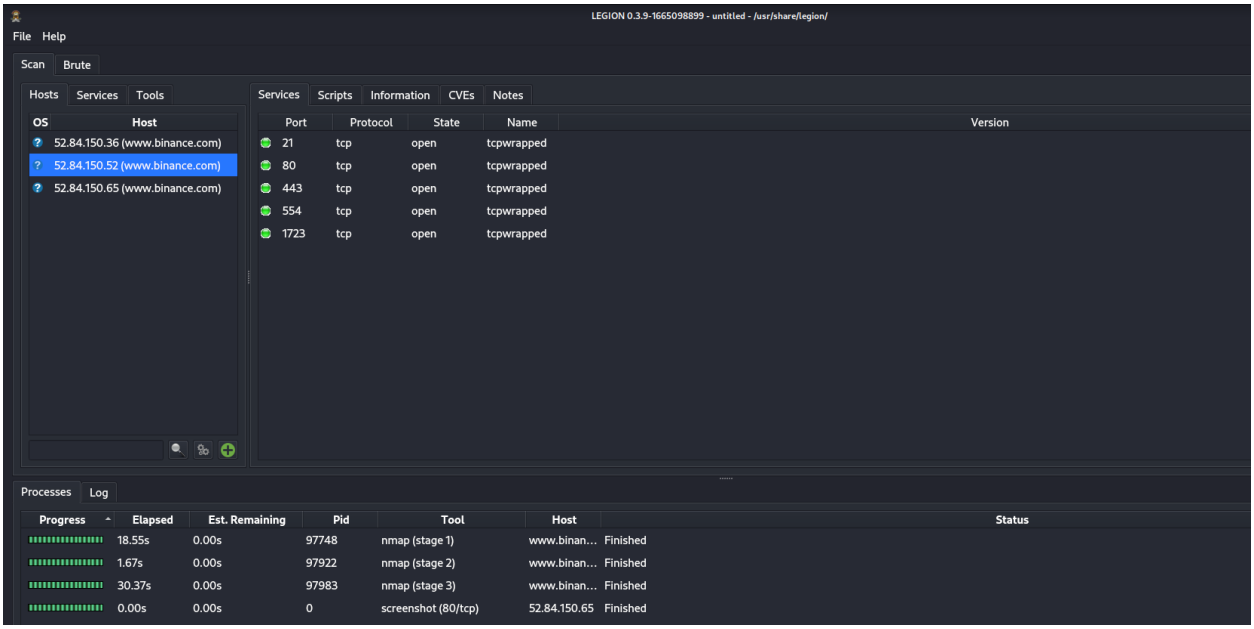
Legion is an open-source tool for detecting network vulnerabilities that can be used to find devices connected to a network, gather relevant data about systems that are being targeted, and identify exploits for specific systems. This tool combines several vulnerability detection tools into one. The Legion tool makes use of Nmap, Whatweb, sslyzer, vulnerabilities, SMBenum, and Shodan tools, among others. Therefore, Nmap and other tools are not required to find vulnerabilities in the system that is being targeted.



This is the dashboard of the Legion tool. Using the green plus button we can do any type of customization to scan vulnerabilities and provide relevant subdomain links to this tool.



The automated scan tool is chosen for a quick and efficient scan of targeted domains, allowing for easy identification of targeted systems using IP addresses or hostnames. It also offers Nmap customization methods, requiring submission for scanning results.



Port scanning also gives the same result given through the Nmap scanning done in the information gathering stage. Because that is the same tool used in this scan. Port 21(FTP), Port 554(RTSP), Port 1723(PPTP), Port 80(HTTP), Port 443 (HTTPS) are the open port in the targeted domain. Port 80 can use to exploit vulnerabilities. Because that port is not a protected HTTP port.

Nikto

Nikto is an open-source web server scanner that tests web servers for over 6700 dangerous files, outdated versions, and version-specific problems. It is used by security professionals and system administrators to assess server security and identify vulnerabilities. Nikto can be downloaded from its official website or security-focused Linux distributions, but should be used responsibly and with permission.

Therefore, in order to obtain the scan result of the Nikto tool, we now require the open ports scan details that were gathered during the information gathering stage using the Nmap tool. I check every open port used in each of the targeted subdomains based on the findings of the Nmap scan. Thus, we can use the Nikto tool's "-h" and "-p" commands to input the port address and hostname, respectively.

- Scan result of the www.binance.com using open port 80

- Missing X-Frame-Options Header: The anti-clickjacking X-Frame-Options header is not present. This means the website might be vulnerable to clickjacking attacks where an attacker could embed the website within a malicious frame to trick users into performing unintended actions.

- Missing X-Content-Type-Options Header: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. This might lead to MIME-sniffing attacks where an attacker could manipulate how content is interpreted by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities.

Wapiti

Wapiti is an open-source web application vulnerability scanner developed in Python that identifies security vulnerabilities in web applications through black-box testing. It performs this testing from the outside, allowing it to test both internal and external-facing web applications. Wapiti crawls through the target web application, identifying various parameters and entry points, and performs various types of scans to detect vulnerabilities. Users can customize the scanning process by specifying the types of vulnerabilities to search for and configuring options like crawling depth and thread number. After completing the scan, Wapiti generates reports detailing the discovered vulnerabilities, helping developers and security teams prioritize and address issues effectively. Its command-line interface makes it suitable for integration into automated testing processes and scripting. Wapiti is platform-independent and can be run on various operating systems.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ wapiti -u https://www.binance.com/

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Saving scan state, please wait ...

 Note
 ========
This scan has been saved in the file /home/kali/.wapiti/scans/www.binance.com_folder_21ddbbec.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe
Problem with local wapp database.
Downloading from the web ...

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set

[*] Launching module cookieflags

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=5bwc39 for results, please wait ...

[*] Launching module redirect
```

```
[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=5bwc39 for results, please wait ...

[*] Launching module redirect

[*] Launching module blindsql

[*] Launching module permanentxss

Report
 ------
A report has been generated in the file /home/kali/.wapiti/generated_report
Open /home/kali/.wapiti/generated_report/www.binance.com_04252024_1803.html with a browser to see this report.
```

- Missing Content Security Policy (CSP):

  Vulnerability:

  CSP is not set which means the website may be vulnerable to various types of attacks such as cross-site scripting (XSS) and data injection.

  Attack:

  A malicious attacker could exploit this vulnerability by injecting and executing malicious scripts on the web page, potentially leading to theft of sensitive information or hijacking of user sessions.

- Missing Security Headers (X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, Strict-Transport-Security):

  Vulnerability:

These security headers are not set, leaving the website vulnerable to attacks such as clickjacking, XSS, MIME type sniffing, and protocol downgrade attacks.

Attack:

Attackers could exploit these missing headers to perform various attacks, including clickjacking attacks where the website is embedded within a malicious frame, XSS attacks where malicious scripts are injected and executed in users' browsers, and protocol downgrade attacks where secure connections are downgraded to insecure ones.

- SSRF (Server-Side Request Forgery):

  Vulnerability:

  The scan detected a potential SSRF vulnerability, indicating that the website may be susceptible to allowing attackers to make unauthorized requests from the server.

  Attack:

  An attacker could exploit SSRF to access internal resources, bypass firewalls, or perform reconnaissance on internal network infrastructure. This could lead to unauthorized data access or further exploitation of internal systems.

The scan also launched various other modules such as exec, file, sql, xss, redirect, blindsql, and permanentxss, which indicate potential areas of vulnerability such as command injection, file inclusion, SQL injection, cross-site scripting, open redirect, blind SQL injection, and persistent XSS. Each of these vulnerabilities could be exploited by attackers to gain unauthorized access or perform malicious actions on the website.

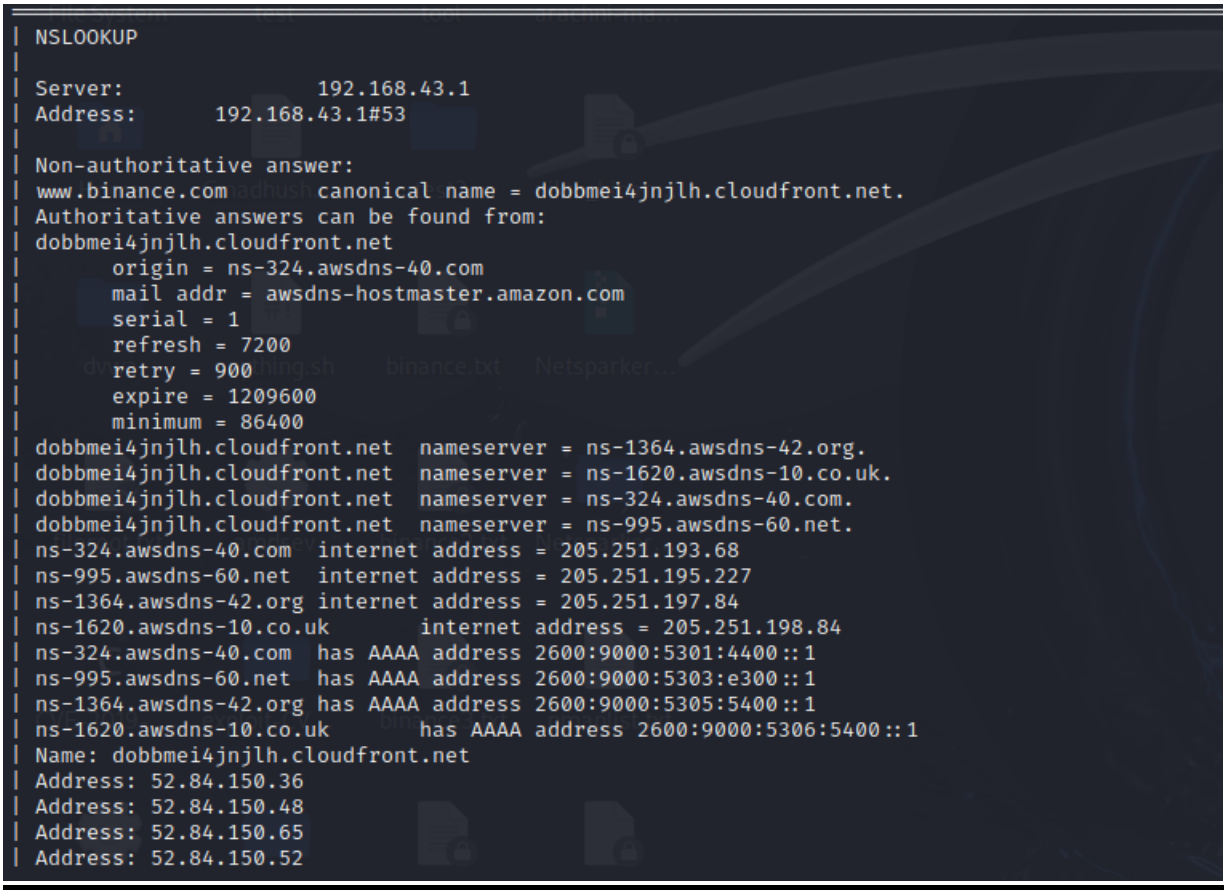
UniScan

Uniscan is another web vulnerability scanner, similar to Nikto but with some differences in features and capabilities. It's designed to identify various types of vulnerabilities in web applications, including SQL injection, XSS (Cross-Site Scripting), LFI (Local File Inclusion), and RCE (Remote Code Execution), among others.

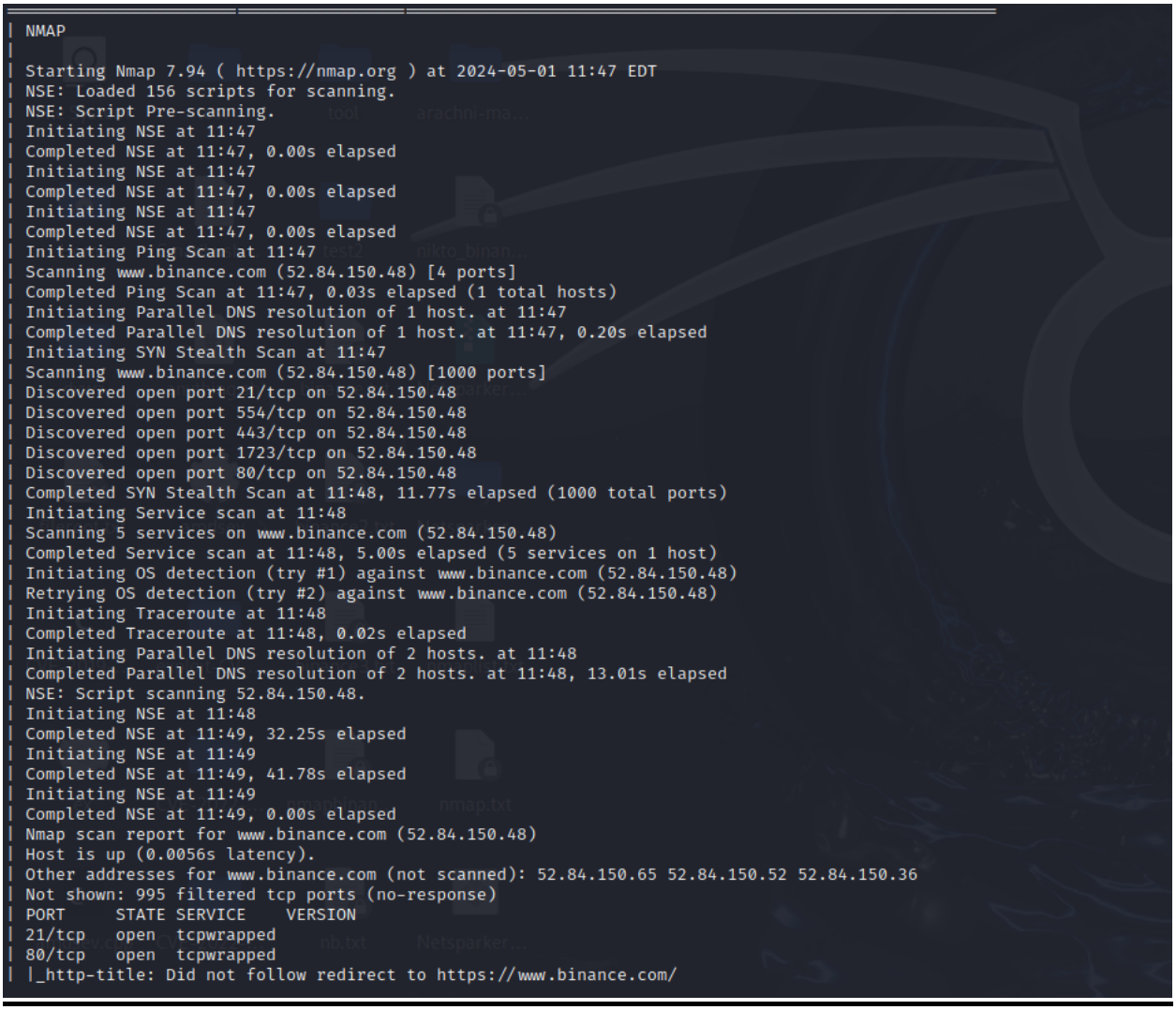
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# uniscan -bwedsj -u https://www.binance.com/
###################################
# Uniscan project                 #
# http://uniscan.sourceforge.net/ #
###################################
V. 6.3


Going to background with pid: [40987]
Scan date: 1-5-2024 11:47:14

┌──(root㉿kali)-[/home/kali/Desktop]
└─# ============================================================================
| Domain: https://www.binance.com/
| IP: 52.84.150.65
============================================================================
============================================================================
| PING

| PING dobbmei4jnjlh.cloudfront.net (52.84.150.48) 56(84) bytes of data.
| 64 bytes from 52.84.150.48 (52.84.150.48): icmp_seq=1 ttl=242 time=158 ms
| 64 bytes from 52.84.150.48 (52.84.150.48): icmp_seq=2 ttl=242 time=1007 ms
| 64 bytes from 52.84.150.48 (52.84.150.48): icmp_seq=3 ttl=242 time=151 ms
| 64 bytes from 52.84.150.48 (52.84.150.48): icmp_seq=4 ttl=242 time=207 ms

| --- dobbmei4jnjlh.cloudfront.net ping statistics ---
| 4 packets transmitted, 4 received, 0% packet loss, time 3015ms
| rtt min/avg/max/mdev = 151.146/380.710/1006.620/362.015 ms, pipe 2
============================================================================
| TRACEROUTE

| traceroute to www.binance.com (52.84.150.65), 30 hops max, 60 byte packets
|  1  10.0.2.2 (10.0.2.2)  1.940 ms  1.764 ms  1.696 ms
|  2  * * *
|  3  * * *
|  4  * * *
|  5  * * *
|  6  * * *
|  7  * * *
|  8  * * *
|  9  * * *
| 10  * * *
| 11  * * *
| 12  * * *
| 13  * * *
| 14  * * *
| 15  * * *
| 16  * * *
```

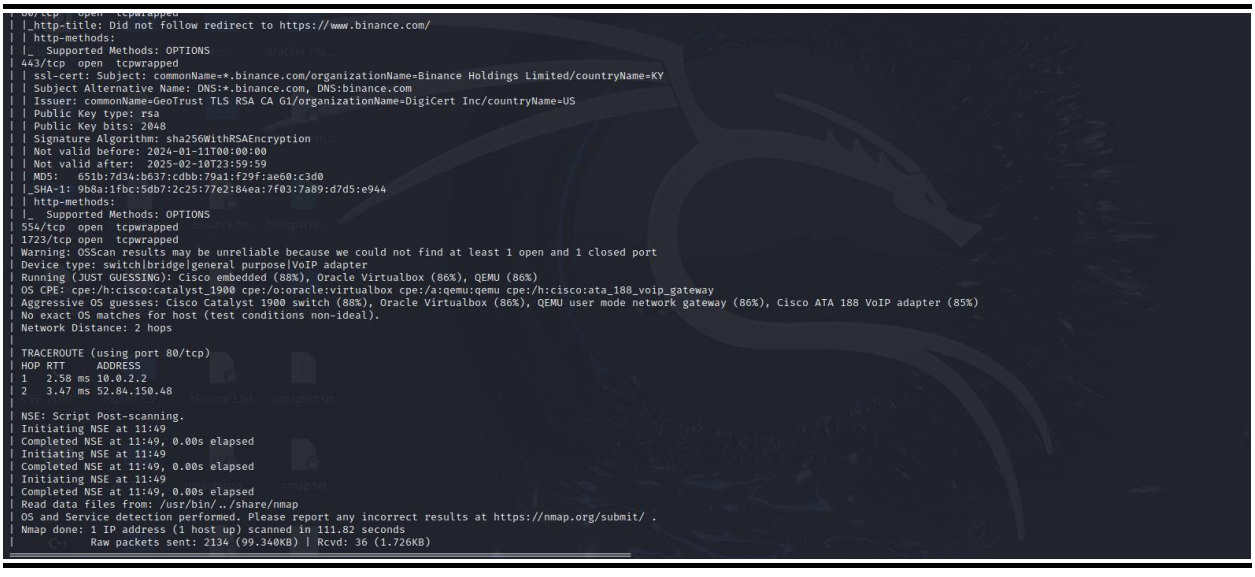
```
| 16  * * *
| 17  * * *
| 18  * * *
| 19  * * *
| 20  * * *
| 21  * * *
| 22  * * *
| 23  * * *
| 24  * * *
| 25  * * *
| 26  * * *
| 27  * * *
| 28  * * *
| 29  * * *
| 30  * * *
```

Uniscan nosslooup report



Uniscan nmap report





File check reort and static test report

```
File check:


Timthumb < 1.33 vulnerability:


Backup Files:
[+] CODE: 302 URL: https://www.binance.com/a~


Blind SQL Injection:


Local File Include:


PHP CGI Argument Injection:


Remote Command Execution:


Remote File Include:


SQL Injection:


Cross-Site Scripting (XSS):


Web Shell Finder:
```

```
Static tests:
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.1 Loaded.


Local File Include:


Remote Command Execution:


Remote File Include:
[+] CODE: 200 URL: https://www.binance.com/robots.txt
```

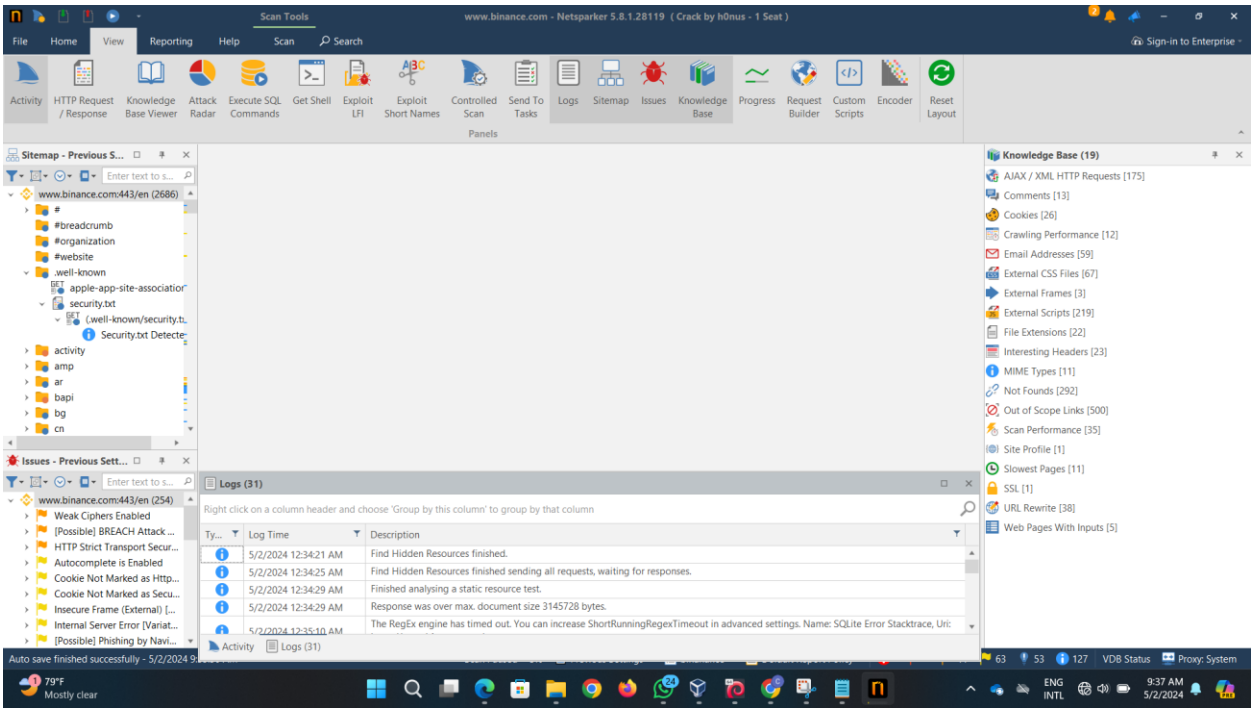
```
Check robots.txt:
[+] User-agent: Baiduspider
[+] User-agent: Bingbot
[+] User-agent: DuckDuckBot
[+] User-agent: Slurp
[+] User-agent: Googlebot
[+] Allow: /
[+] Disallow: */activity/challenge-competition/
[+] Disallow: */activity/collect-and-win/
[+] Disallow: */activity/referral-entry/
[+] Disallow: *fbclid=
[+] Disallow: */collected/undefined
[+] Disallow: */advertiserDetail
[+] Disallow: */funding-history
[+] Disallow: */trading-rules
[+] Disallow: */comments
[+] Disallow: */feed/search
[+] Disallow: */version.web
[+] Disallow: */loan/data/
[+] Disallow: */markets/spot-FIAT/
[+] Disallow: */markets/spot-USDT/
[+] Disallow: */OTC-Trading/
[+] Disallow: */amp/
[+] Disallow: */backtest/
[+] Disallow: */buy-sell-crypto/referral/
[+] Disallow: */chart-webview/
[+] Disallow: */chat/
[+] Disallow: */complaint-form/
[+] Disallow: */compliance-confirm/
[+] Disallow: */convert-modal-ui/
[+] Disallow: */customindicator/
[+] Disallow: */delivery/
[+] Disallow: */crypto/recurring/
[+] Disallow: */deposit/result/order-v3/
[+] Disallow: */my/
[+]
[+] Disallow: /ar-AE*
[+] Disallow: */buy-sell-crypto/buy-sell/result/buy/
[+] Disallow: */buy-sell-crypto/buy-sell/result/sell/
[+] Disallow: */survey/
[+] Disallow: */mp-cms/app/
[+] Disallow: */kyc-ui/
[+] Disallow: */sitemap_.xml
[+] Disallow: */my/user-support/feedback/
[+] Disallow: */fiat/deposit/result/order
[+] Disallow: */bapi/
```

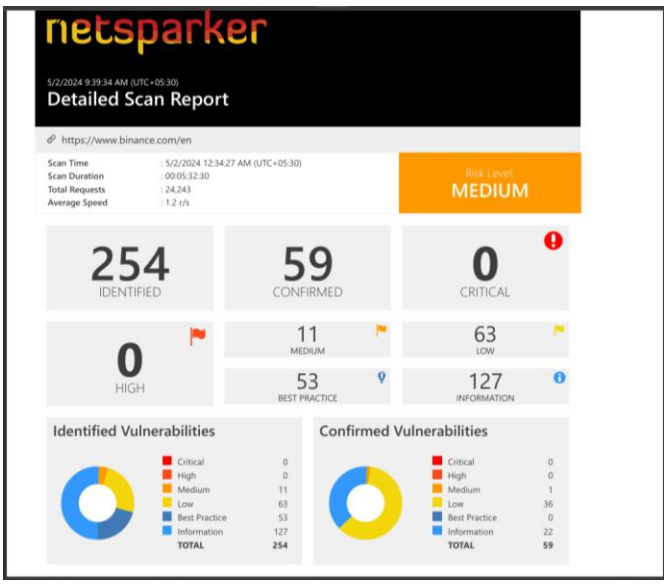
this is the scan result we can get from this tool. So, there are no vulnerabilities captured by this tool. But Nmap and other scan results are important to find vulnerabilities in the targeted system.

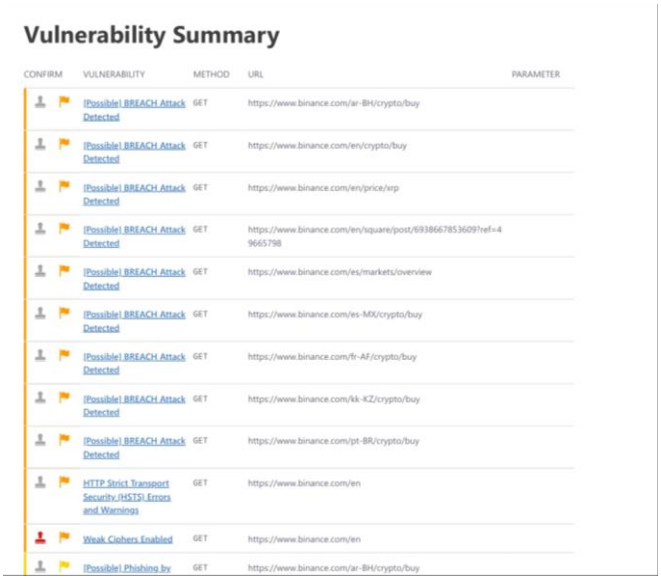
Netsparker

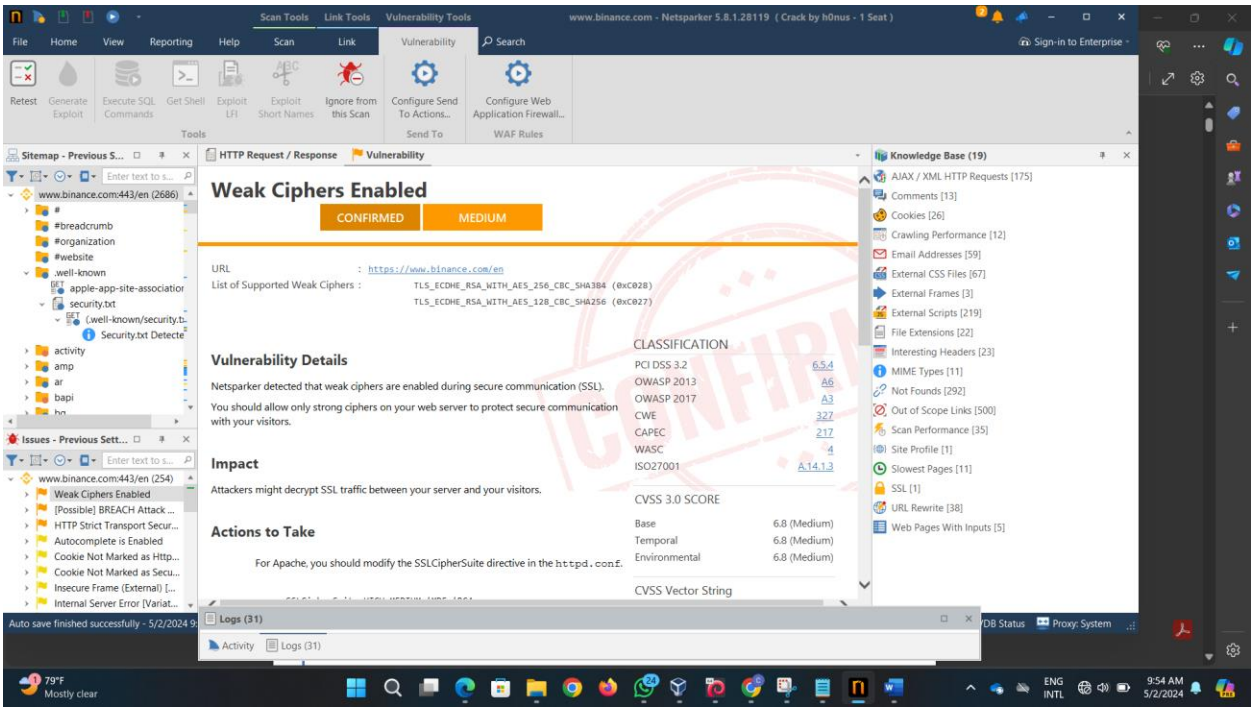
Netsparker is a web application security scanner developed by Netsparker Ltd. It's designed to automatically identify security vulnerabilities in web applications. It works by scanning web applications, analyzing their structure and behavior, and then detecting potential security issues such as SQL injection, cross-site scripting (XSS), and other common vulnerabilities.

Netsparker typically provides a user-friendly interface for configuring scans, reviewing scan results, and generating detailed reports. It's often used by security professionals, penetration testers, and developers to identify and remediate security flaws in web applications before they can be exploited by attackers.




netsparker
5/2/2024 9:39:34 AM (UTC+05:30)
Detailed Scan Report
https://www.binance.com/en
Scan Time : 5/2/2024 12:34:27 AM (UTC+05:30)
Scan Duration : 00:05:32:30
Total Requests : 24,243
Average Speed : 1.2 r/s
Risk Level:
MEDIUM
254
IDENTIFIED
59
CONFIRMED
0
CRITICAL
0
HIGH
11
MEDIUM
63
LOW
53
BEST PRACTICE
127
INFORMATION
Identified Vulnerabilities
Critical 0
High 0
Medium 11
Low 63
Best Practice 53
Information 127
TOTAL 254
Confirmed Vulnerabilities
Critical 0
High 0
Medium 1
Low 36
Best Practice 0
Information 22
TOTAL 59


Vulnerability Summary
CONFIRM
VULNERABILITY
METHOD
URL
PARAMETER
[Possible] BREACH Attack Detected GET https://www.binance.com/ar-BH/crypto/buy
[Possible] BREACH Attack Detected GET https://www.binance.com/en/crypto/buy
[Possible] BREACH Attack Detected GET https://www.binance.com/en/price/xrp
[Possible] BREACH Attack Detected GET https://www.binance.com/en/square/post/6938667853609?ref=49665798
[Possible] BREACH Attack Detected GET https://www.binance.com/es/markets/overview
[Possible] BREACH Attack Detected GET https://www.binance.com/es-MX/crypto/buy
[Possible] BREACH Attack Detected GET https://www.binance.com/fr-AF/crypto/buy
[Possible] BREACH Attack Detected GET https://www.binance.com/kk-KZ/crypto/buy
[Possible] BREACH Attack Detected GET https://www.binance.com/pt-BR/crypto/buy
HTTP Strict Transport Security (HSTS) Errors and Warnings GET https://www.binance.com/en
Weak Ciphers Enabled GET https://www.binance.com/en
[Possible] Phishing by GET https://www.binance.com/ar-BH/crypto/buy



Risk type : Medium

URL : https://www.binance.com/

Vulnerability Details

- Netsparker detected that weak ciphers are enabled during secure communication (SSL). You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

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

Actions to Take

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

   SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

2. Lighttpd:
   3.ssl.honor-cipher-order = "enable"

   ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"

4. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the**

registry, you should back up any valued data on your computer.

a. Click Start, click Run, type regedt32 or type regedit, and then click OK.
b. In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
c. Set "Enabled" DWORD to "0x0" for the following registry keys:

SCHANNEL\Ciphers\DES	56/56
SCHANNEL\Ciphers\RC4	64/128
SCHANNEL\Ciphers\RC4	40/128
SCHANNEL\Ciphers\RC2	56/128
SCHANNEL\Ciphers\RC2	40/128
SCHANNEL\Ciphers\NULL	
SCHANNEL\Hashes\MD5	

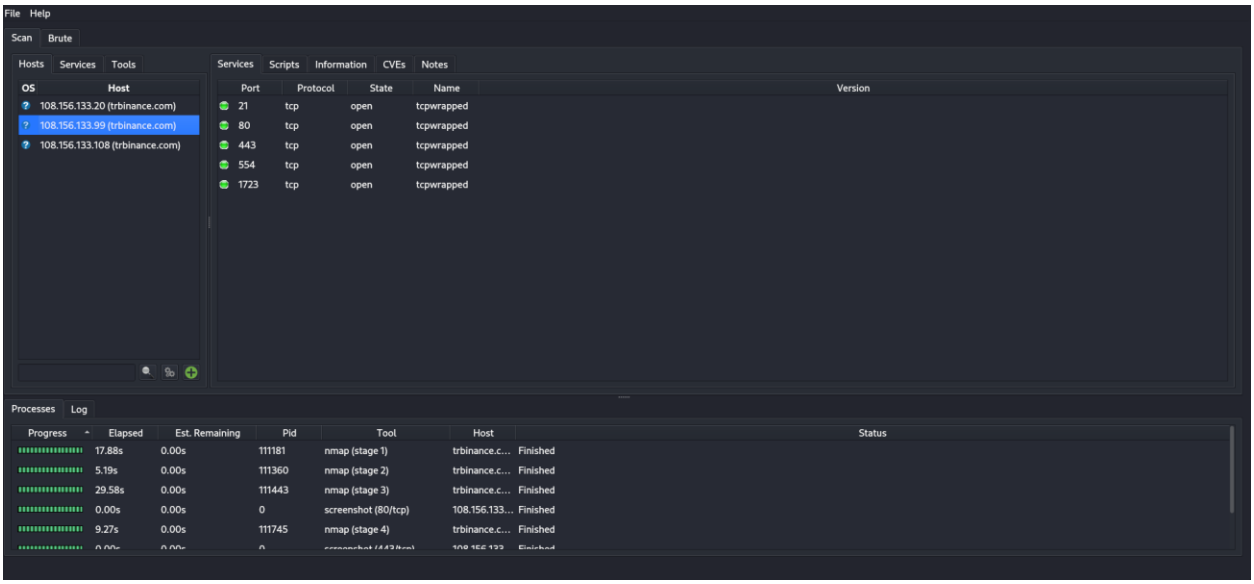
mitigation

- Configure your web server to disallow using weak ciphers.

Sub domain 02

Target sub domain : https://www.trbinance.com/

Legion



Nikto

- Missing X-Frame-Options Header:
    - Vulnerability:
        - The X-Frame-Options header is not present, leaving the website vulnerable to clickjacking attacks.
    - Attack:
        - Attackers could embed the website within a malicious frame to trick users into performing unintended actions, such as clicking on hidden elements or submitting sensitive information.

- Missing Strict-Transport-Security Header:
  - Vulnerability:
    - The Strict-Transport-Security header is not defined, which could expose users to risks related to protocol downgrade attacks.
  - Attack:
    - Attackers could attempt to downgrade secure HTTPS connections to insecure HTTP connections, making users susceptible to various forms of attacks, including man-in-the-middle attacks.

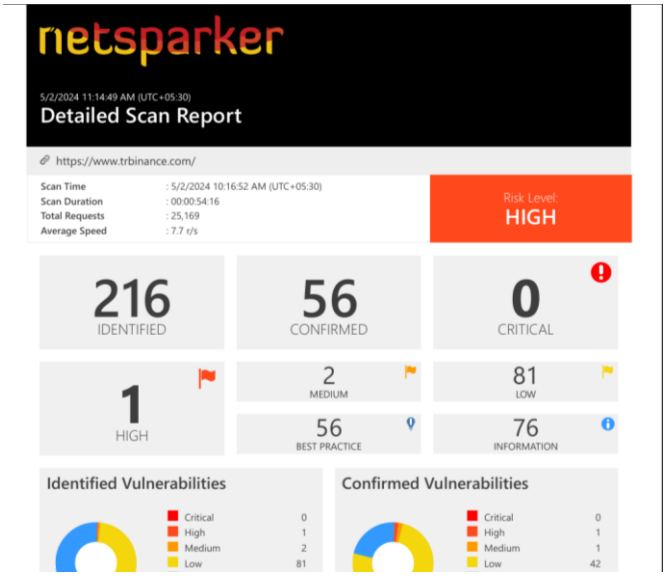
- Missing X-Content-Type-Options Header:
  - Vulnerability:
    - The X-Content-Type-Options header is not set, allowing potential content-type sniffing attacks.
  - Attack:
    - Attackers could exploit this vulnerability to force the browser to interpret certain files as executable content, leading to XSS or other attacks.

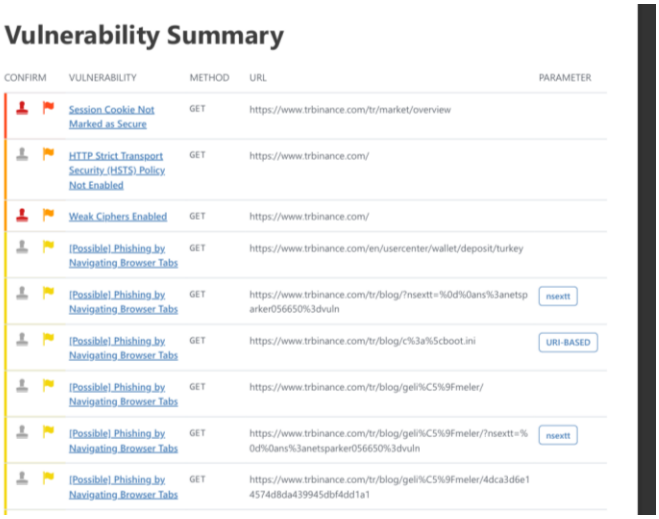
- Content-Encoding Header Vulnerability:
  - Vulnerability:
    - The Content-Encoding header is set to "deflate," which may indicate vulnerability to the BREACH attack.
  - Attack:
    - BREACH is a cryptographic attack that can be used to extract sensitive information, such as authentication tokens or other secrets, from encrypted web traffic.

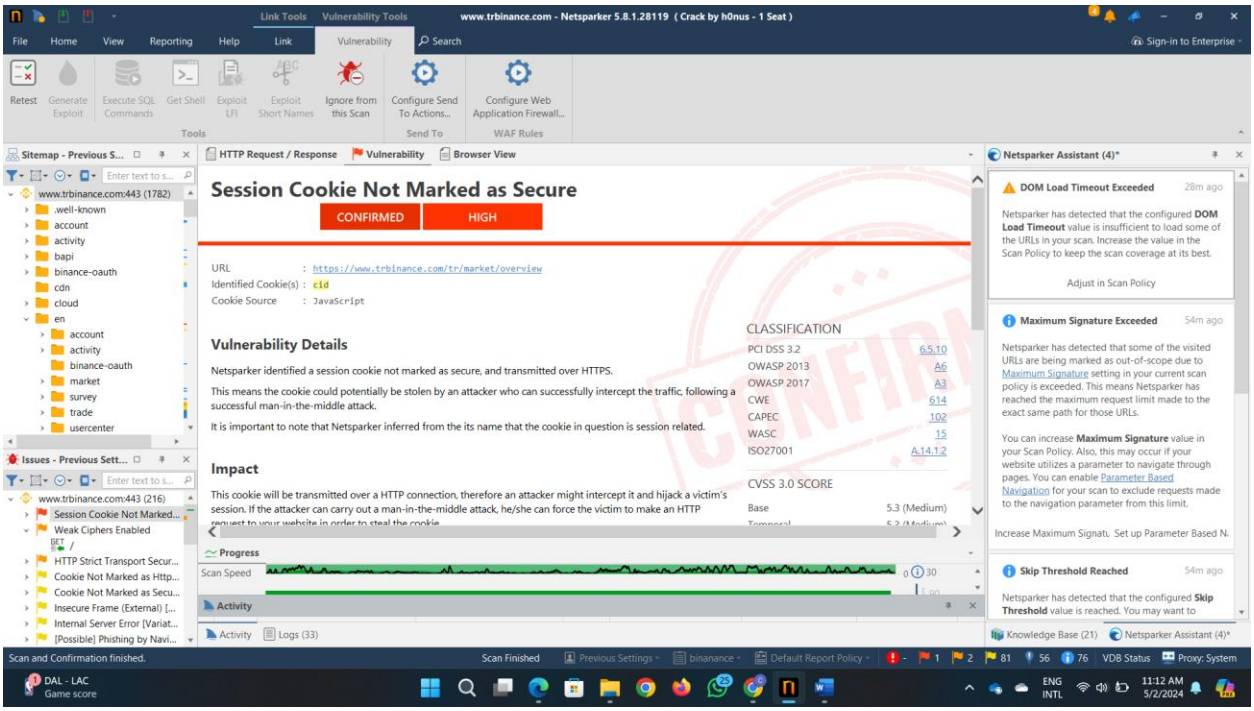
Wapiti

- Potential SSRF (Server-Side Request Forgery) Vulnerability:
  - Vulnerability:
    - The scan detected a potential SSRF vulnerability, indicating that the website may be susceptible to allowing attackers to make unauthorized requests from the server.
  - Attack:
    - An attacker could exploit SSRF to access internal resources, bypass firewalls, or perform reconnaissance on internal network infrastructure, leading to unauthorized data access or further exploitation of internal systems.

Netsparker


netsparker
5/2/2024 11:14:49 AM (UTC+05:30)
Detailed Scan Report
https://www.trbinance.com/
Scan Time : 5/2/2024 10:16:52 AM (UTC+05:30)
Scan Duration : 00:00:54:16
Total Requests : 25,169
Average Speed : 7.7 r/s
Risk Level:
HIGH
216
IDENTIFIED
56
CONFIRMED
0
CRITICAL
1
HIGH
2
MEDIUM
81
LOW
56
BEST PRACTICE
76
INFORMATION
Identified Vulnerabilities
Critical 0
High 1
Medium 2
Low 81
Confirmed Vulnerabilities
Critical 0
High 1
Medium 1
Low 42


Vulnerability Summary
CONFIRM
VULNERABILITY
METHOD
URL
PARAMETER
Session Cookie Not Marked as Secure
GET
https://www.trbinance.com/tr/market/overview
HTTP Strict Transport Security (HSTS) Policy Not Enabled
GET
https://www.trbinance.com/
Weak Ciphers Enabled
GET
https://www.trbinance.com/
[Possible] Phishing by Navigating Browser Tabs
GET
https://www.trbinance.com/en/usercenter/wallet/deposit/turkey
[Possible] Phishing by Navigating Browser Tabs
GET
https://www.trbinance.com/tr/blog/?nsextt=%0d%0ans%3anetsparker056650%3dvuln
nsextt
[Possible] Phishing by Navigating Browser Tabs
GET
https://www.trbinance.com/tr/blog/c%3a%5cboot.ini
URI-BASED
[Possible] Phishing by Navigating Browser Tabs
GET
https://www.trbinance.com/tr/blog/geli%C5%9Fmeler/
[Possible] Phishing by Navigating Browser Tabs
GET
https://www.trbinance.com/tr/blog/geli%C5%9Fmeler/?nsextt=%0d%0ans%3anetsparker056650%3dvuln
nsextt
[Possible] Phishing by Navigating Browser Tabs
GET
https://www.trbinance.com/tr/blog/geli%C5%9Fmeler/4dca3d6e14574d8da439945dbf4dd1a1



Vulnerability Details

- Netsparker identified a session cookie not marked as secure, and transmitted over HTTPS.
- This means the cookie could potentially be stolen by an attacker who can successfully intercept the traffic, following a successful man-in-the-middle attack.
- It is important to note that Netsparker inferred from the its name that the cookie in question is session related.

Impact

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

Actions to Take

- Mark all cookies used within the application as secure. *(If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.)*

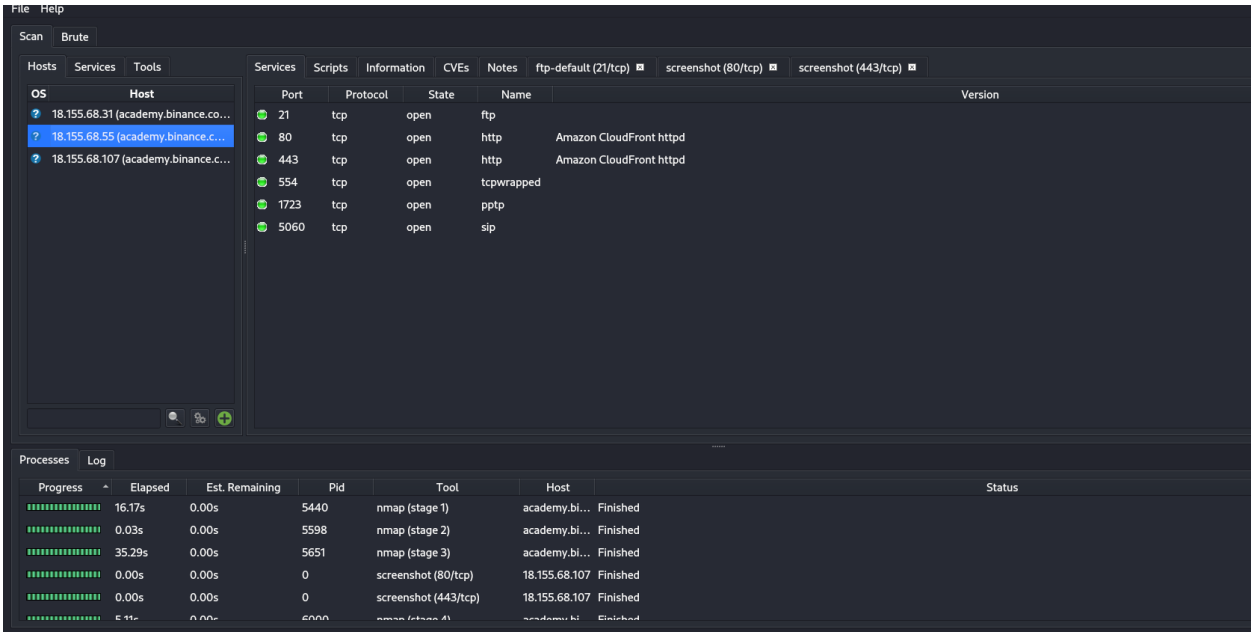
mitigation

- Mark all cookies used within the application as secure.

Sub domain 03

Target sub domain : https://academy.binance.com/en

Legion



- ✓ **Nikto**

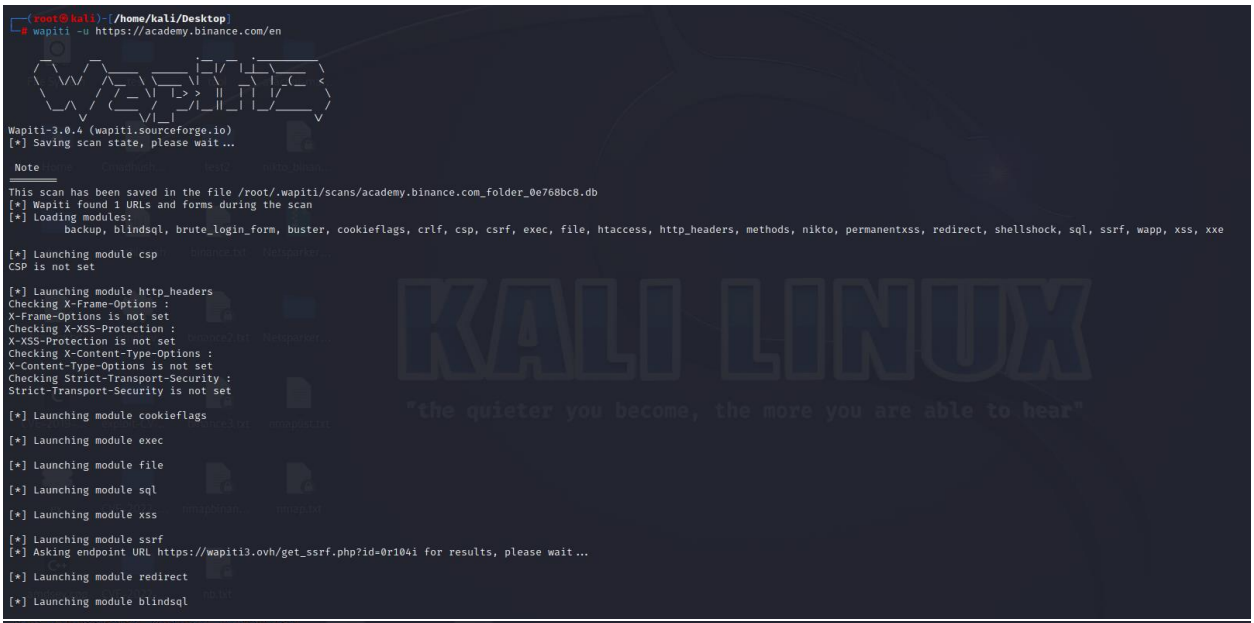
- Missing X-Frame-Options Header:
  - Vulnerability:
    - The anti-clickjacking X-Frame-Options header is not present, leaving the website vulnerable to clickjacking attacks.
  - Attack:
    - Attackers can create a malicious frame on their website, causing users to perform unintended actions like clicking on hidden buttons or links.

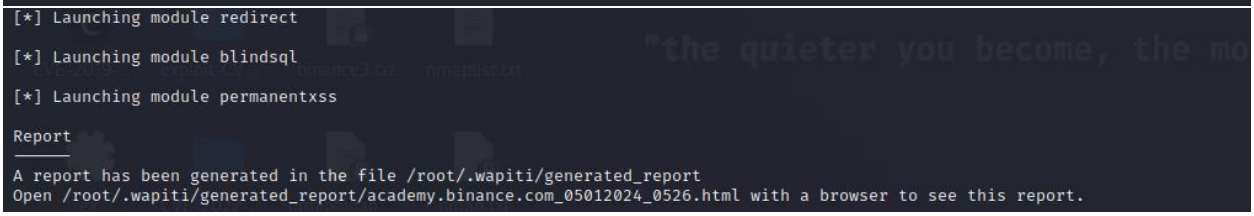
- Missing Strict-Transport-Security Header:
  - Vulnerability:
    - The site uses TLS (HTTPS), but the Strict-Transport-Security (HSTS) header is not defined, leaving it vulnerable to protocol downgrade attacks.
  - Attackers:
    - can intercept and modify requests, converting secure HTTPS connections to insecure ones, potentially exposing sensitive data to interception or manipulation.

- Missing X-Content-Type-Options Header:
  - Vulnerability:
    - The X-Content-Type-Options header is not set, potentially allowing the browser to render content in a different fashion to the MIME type, which could lead to MIME-sniffing attacks.
  - Attack:
    - Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

- Content-Encoding Header Vulnerability:
  - Vulnerability:
    - The Content-Encoding header is set to "deflate," which may indicate vulnerability to the BREACH attack.
  - Attack:
    - BREACH is a cryptographic attack that can be used to extract sensitive information, such as authentication tokens or other secrets, from encrypted web traffic.

Wapiti





- Missing Content Security Policy (CSP):
  - Vulnerability:
    - CSP is not set, which means the website may be vulnerable to various attacks such as cross-site scripting (XSS) and data injection.
  - Attack:
    - A malicious attacker could exploit this vulnerability by injecting and executing malicious scripts on the web page, potentially leading to theft of sensitive information or hijacking of user sessions.

- Missing Security Headers (X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, Strict-Transport-Security):
  - Vulnerability:
    - These security headers are not set, leaving the website vulnerable to attacks such as clickjacking, XSS, MIME type sniffing, and protocol downgrade attacks.
  - Attack:

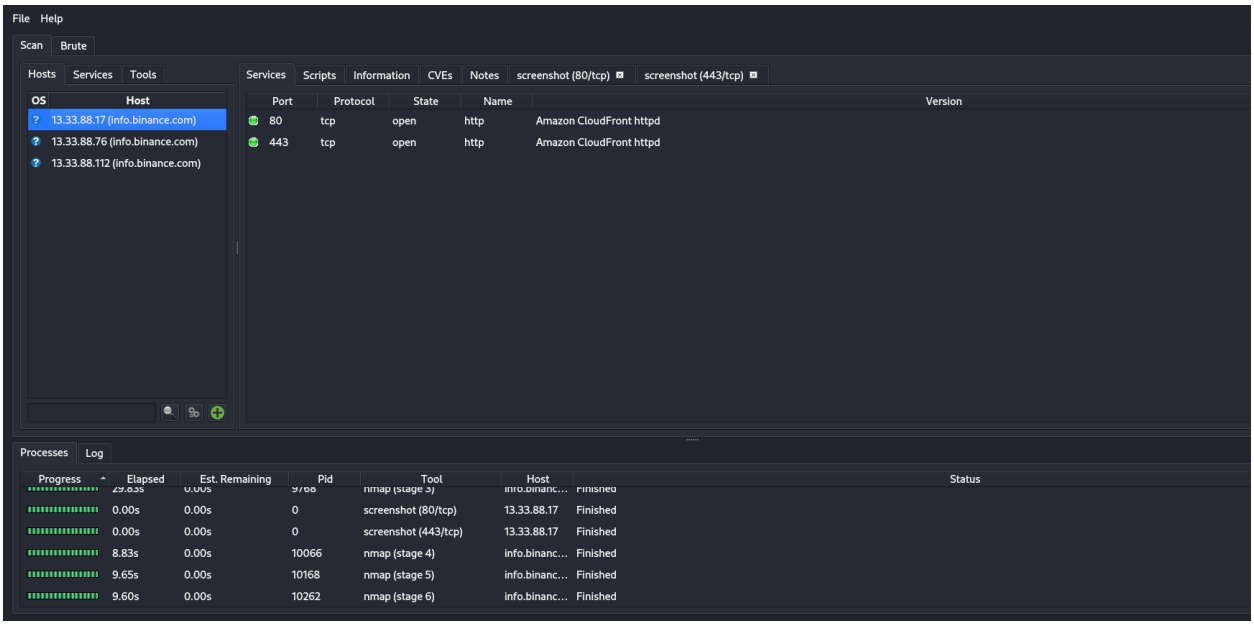
        - Missing headers can be exploited by attackers for various attacks, including clickjacking, XSS, and protocol downgrade, where websites are embedded in malicious frames.

- Potential SSRF (Server-Side Request Forgery) Vulnerability:
    - Vulnerability:
        - The scan detected a potential SSRF vulnerability, indicating that the website may be susceptible to allowing attackers to make unauthorized requests from the server.
    - Attack:
        - An SSRF attack can allow an attacker to access internal resources, bypass firewalls, and perform reconnaissance, potentially leading to unauthorized data access or further system exploitation.

Sub domain 04

Target sub domain : https://www.binance.com/en/price

Legion



Nikto

- Insecure Cookie Attributes:
    - Vulnerability:

        - Cookies such as "theme" are created without the secure and httponly flags, making them vulnerable to interception and manipulation.
    - Attack:
        - Attackers could intercept these cookies over insecure channels, potentially leading to session hijacking or other attacks

- content-Encoding Header Vulnerability:
    - Vulnerability:
        - The Content-Encoding header is set to "deflate," which may indicate vulnerability to the BREACH attack.
    - Attack:
        - BREACH is a cryptographic attack that can be used to extract sensitive information, such as authentication tokens or other secrets, from encrypted web traffic.

Wapiti

- Missing X-Frame-Options Header:
  - Vulnerability:
    - The X-Frame-Options header is not set, which leaves the website vulnerable to clickjacking attacks.
  - Attack:
    - Attackers could embed the website within a malicious frame to trick users into performing unintended actions, such as clicking on hidden elements or submitting sensitive information.

- Missing X-XSS-Protection Header:
  - Vulnerability:
    - The X-XSS-Protection header is not set, which may expose the website to cross-site scripting (XSS) attacks.
  - Attack:

        - Attackers could inject malicious scripts into the website, potentially leading to the theft of user session cookies, manipulation of page content, or redirection to malicious websites.

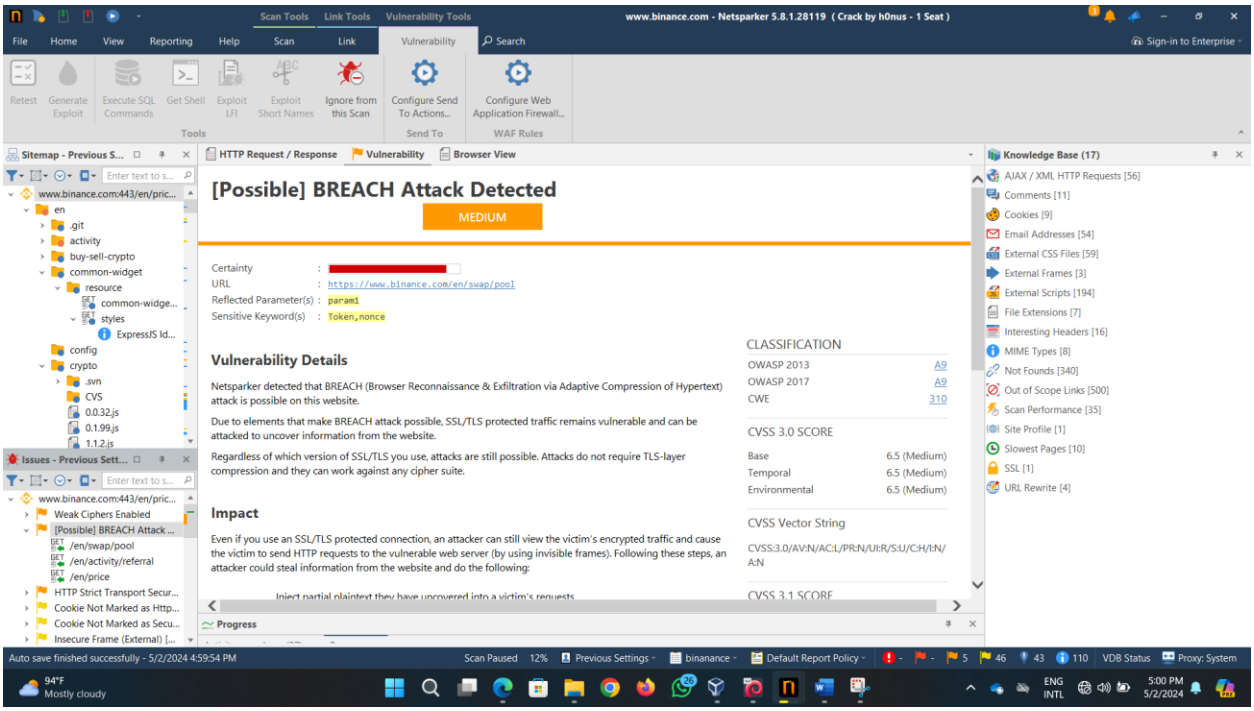
- Missing X-Content-Type-Options Header:
    - Vulnerability:
        - The X-Content-Type-Options header is not set, allowing potential content-type sniffing attacks.

    - Attack:
        - Attackers could exploit this vulnerability to force the browser to interpret certain files as executable content, leading to XSS or other attacks.

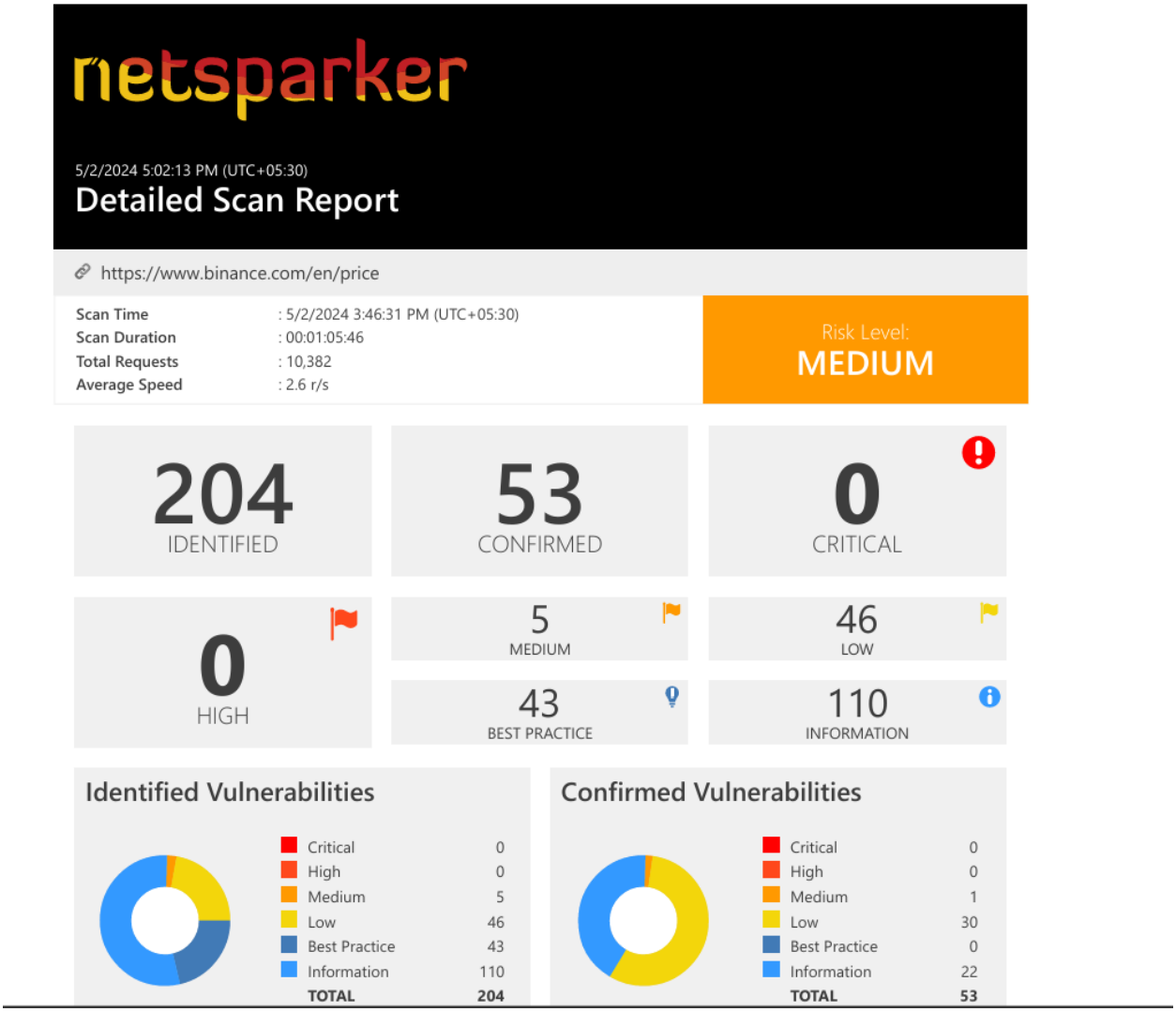
- Missing Strict-Transport-Security Header:
    - Vulnerability:
        - The Strict-Transport-Security header is not set, which could expose users to risks related to protocol downgrade attacks.

    - Attack:
        - Attackers could attempt to downgrade secure HTTPS connections to insecure HTTP connections, making users susceptible to various forms of attacks, including man-in-the-middle attacks.

Netsparker


www.binance.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
[Possible] BREACH Attack Detected
MEDIUM
Certainty :
URL : https://www.binance.com/en/swap/pool
Reflected Parameter(s) : param1
Sensitive Keyword(s) : Token,nonce
Vulnerability Details
Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.
Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.
Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.
Impact
Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:
CLASSIFICATION
OWASP 2013 A9
OWASP 2017 A9
CWE 310
CVSS 3.0 SCORE
Base 6.5 (Medium)
Temporal 6.5 (Medium)
Environmental 6.5 (Medium)
CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
CVSS 3.1 SCORE
Knowledge Base (17)
AJAX / XML HTTP Requests [56]
Comments [11]
Cookies [9]
Email Addresses [54]
External CSS Files [59]
External Frames [3]
External Scripts [194]
File Extensions [7]
Interesting Headers [16]
MIME Types [8]
Not Founds [340]
Out of Scope Links [500]
Scan Performance [35]
Site Profile [1]
Slowest Pages [10]
SSL [1]
URL Rewrite [4]

.


netsparker
5/2/2024 5:02:13 PM (UTC+05:30)
Detailed Scan Report
https://www.binance.com/en/price
Scan Time : 5/2/2024 3:46:31 PM (UTC+05:30)
Scan Duration : 00:01:05:46
Total Requests : 10,382
Average Speed : 2.6 r/s
Risk Level:
MEDIUM
204
IDENTIFIED
53
CONFIRMED
0
CRITICAL
0
HIGH
5
MEDIUM
46
LOW
43
BEST PRACTICE
110
INFORMATION
Identified Vulnerabilities
Critical 0
High 0
Medium 5
Low 46
Best Practice 43
Information 110
TOTAL 204
Confirmed Vulnerabilities
Critical 0
High 0
Medium 1
Low 30
Best Practice 0
Information 22
TOTAL 53

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] BREACH Attack Detected	GET	https://www.binance.com/en/activity/referral?utm_source=Lite_web_account	
	[Possible] BREACH Attack Detected	GET	https://www.binance.com/en/price?page=2	
	[Possible] BREACH Attack Detected	GET	https://www.binance.com/en/swap/pool	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://www.binance.com/en/price	
	Weak Ciphers Enabled	GET	https://www.binance.com/en/price	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.binance.com/en/binance-api	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.binance.com/en/crypto/buy	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.binance.com/en/support/announcement/binance-copy-trading-adds-new-usd%E2%93%A2-m-contracts-2024-03-19-7e8fa8f2c5214f788860e2b4f3e1a012	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.binance.com/en/support/announcement/binance-options-expands-options-writing-access-eligibility-23b9d38c76804aa7bf3786e0188c5c44	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.binance.com/en/support/announcement/binance-options-opens-applications-for-options-writing-access-ac3cf6a7bbff42be98e7f2538df496ae	

Vulnerability Details

- Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website.
- Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website.
- Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

- Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:
    - Inject partial plaintext they have uncovered into a victim's requests
    - Measure the size of encrypted traffic

Mitigation

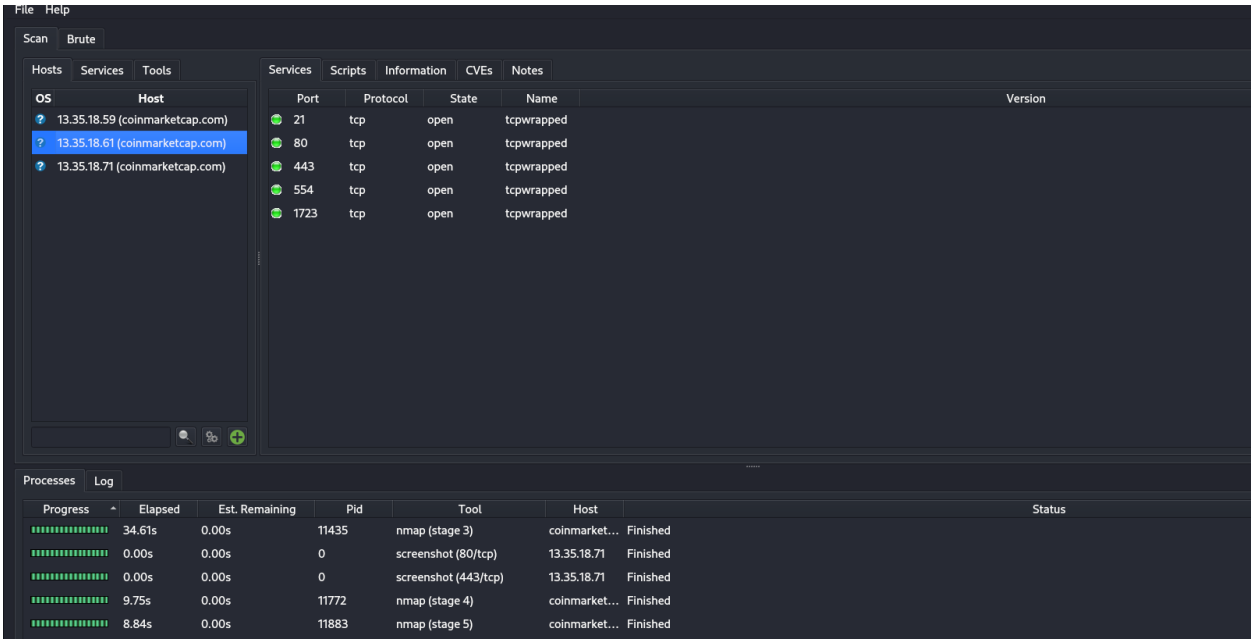
- Netsparker reported a Possible BREACH Attack issue because the target web page meets the following conditions that facilitate it:
    - Served from a server that uses HTTP-level compression (ie. gzip)
    - Reflects user-input in the HTTP response bodies
    - Contains sensitive information (such as a CSRF token) in HTTP response bodies
- To mitigate the issue, we recommend the following solutions:

1. If possible, disable HTTP level compression
2. Separate sensitive information from user input
3. Protect vulnerable pages with CSRF token. The SameSite Cookie attribute will mitigate this issue, because to exploit this issue an attacker forces the victim to visit a target website using invisible frames. With the SameSite cookie attribute added, cookies that belong to the target won't be sent with a request that does not include top level navigation.
4. Hide the length of the traffic by adding a random number of bytes to the responses.
5. Add in a rate limit, so that the page maximum is reached five times per minute.

Sub domain 05

Target sub domain: https://coinmarketcap.com/

Legion



Nikto

- Missing X-Content-Type-Options Header:
    - Vulnerability:
        - The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.

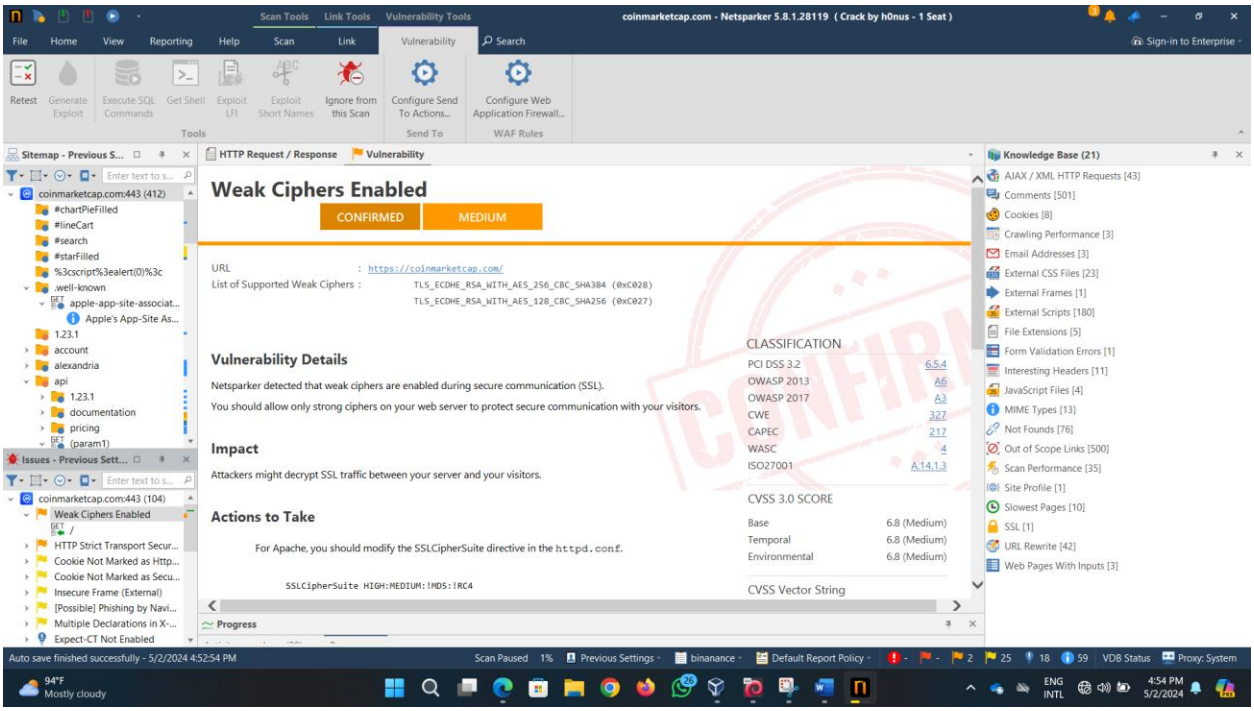
    - Attack:

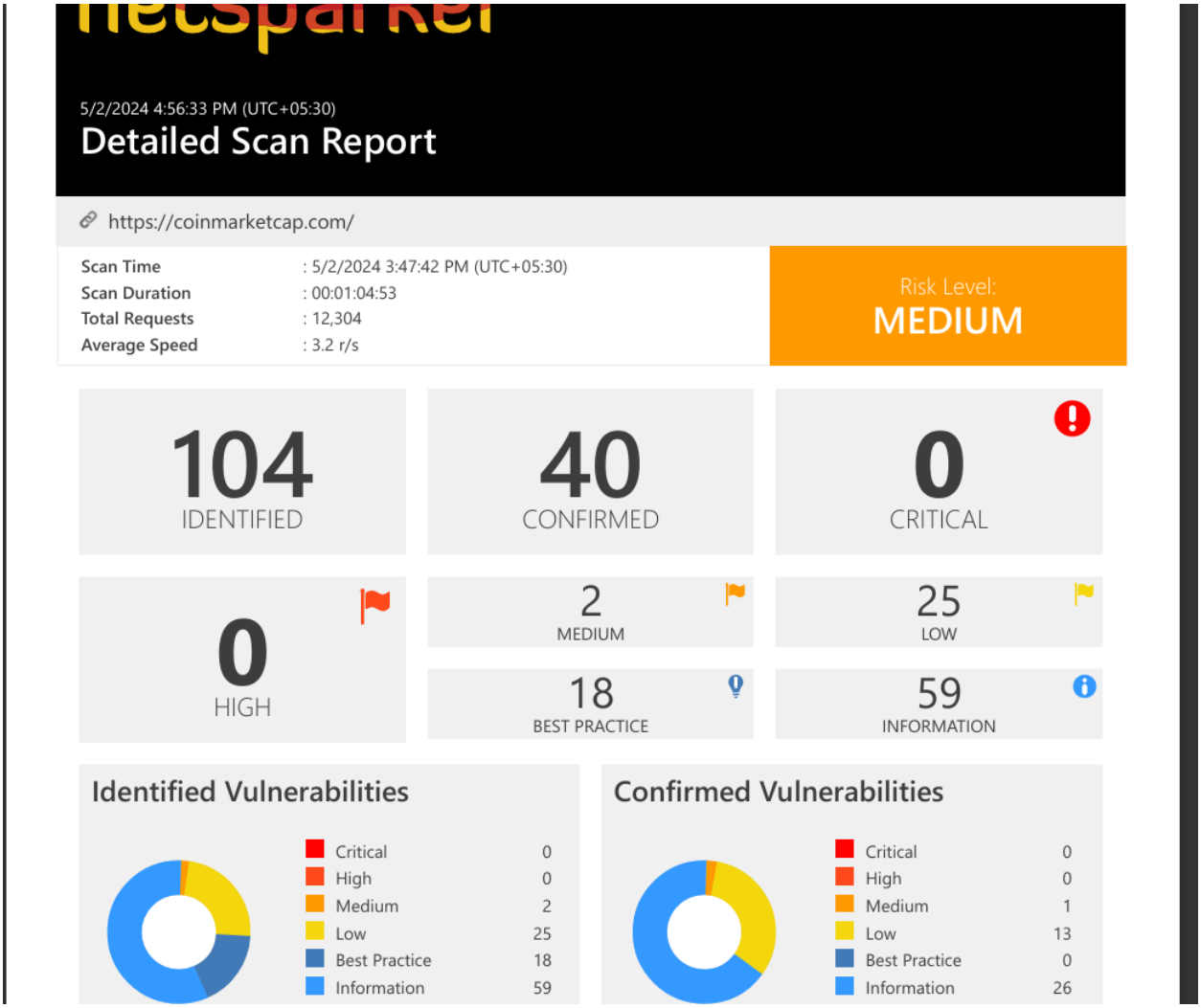
        - Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

- Content-Encoding Header Vulnerability:
    - Vulnerability:
        - The Content-Encoding header is set to "deflate," which may indicate vulnerability to the BREACH attack.

    - Attack:
        - BREACH is a cryptographic attack that can be used to extract sensitive information, such as authentication tokens or other secrets, from encrypted web traffic.

Netspaker


coinmarketcap.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
Weak Ciphers Enabled
CONFIRMED
MEDIUM
URL : https://coinmarketcap.com/
List of Supported Weak Ciphers : TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
Vulnerability Details
Netsparker detected that weak ciphers are enabled during secure communication (SSL).
You should allow only strong ciphers on your web server to protect secure communication with your visitors.
Impact
Attackers might decrypt SSL traffic between your server and your visitors.
Actions to Take
For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
CLASSIFICATION
PCI DSS 3.2 6.5.4
OWASP 2013 A6
OWASP 2017 A3
CWE 327
CAPEC 217
WASC 4
ISO27001 A14.1.3
CVSS 3.0 SCORE
Base 6.8 (Medium)
Temporal 6.8 (Medium)
Environmental 6.8 (Medium)
CVSS Vector String


5/2/2024 4:56:33 PM (UTC+05:30)
Detailed Scan Report
https://coinmarketcap.com/
Scan Time : 5/2/2024 3:47:42 PM (UTC+05:30)
Scan Duration : 00:01:04:53
Total Requests : 12,304
Average Speed : 3.2 r/s
Risk Level:
MEDIUM
104
IDENTIFIED
40
CONFIRMED
0
CRITICAL
0
HIGH
2
MEDIUM
25
LOW
18
BEST PRACTICE
59
INFORMATION
Identified Vulnerabilities
Critical 0
High 0
Medium 2
Low 25
Best Practice 18
Information 59
Confirmed Vulnerabilities
Critical 0
High 0
Medium 1
Low 13
Best Practice 0
Information 26

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://coinmarketcap.com/	
	Weak Ciphers Enabled	GET	https://coinmarketcap.com/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://coinmarketcap.com/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://coinmarketcap.com/community/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://coinmarketcap.com/community/articles/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://coinmarketcap.com/currencies/bitcoin/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://coinmarketcap.com/currencies/litecoin/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://coinmarketcap.com/da/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://coinmarketcap.com/dexscan/top-traders/all/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://coinmarketcap.com/dexscan/top-traders/c%3a%5cboot.ini	URI-BASED

Vulnerability Details

- Netsparker detected that weak ciphers are enabled during secure communication (SSL).
- You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

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

Actions to Take

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

   SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4

2. Lighttpd:
   3.ssl.honor-cipher-order = "enable"

ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"

4. For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

   a. Click Start, click Run, type regedt32 or type regedit, and then click OK.
   b. In Registry Editor, locate the following registry key: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders
   c. Set "Enabled" DWORD to "0x0" for the following registry keys:

SCHANNEL\Ciphers\DES	56/56
SCHANNEL\Ciphers\RC4	64/128
SCHANNEL\Ciphers\RC4	40/128
SCHANNEL\Ciphers\RC2	56/128
SCHANNEL\Ciphers\RC2	40/128
SCHANNEL\Ciphers\NULL	
SCHANNEL\Hashes\MD5	

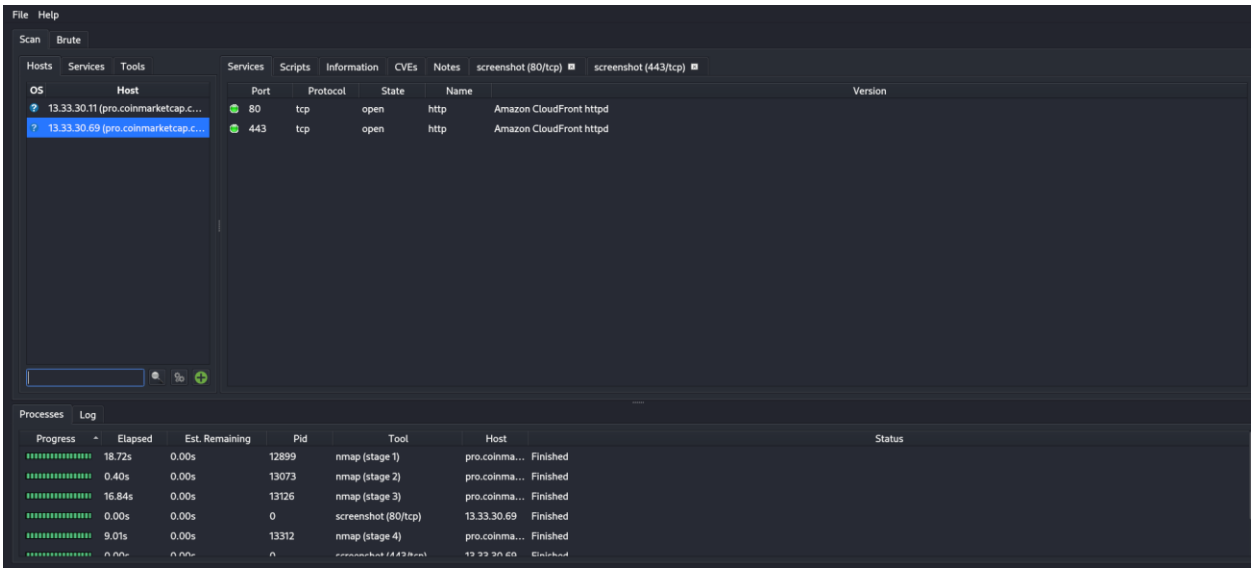
mitigation

- Configure your web server to disallow using weak ciphers

Sub domain 06

Target sub domain : https://pro.coinmarketcap.com/

Legion



Nikto

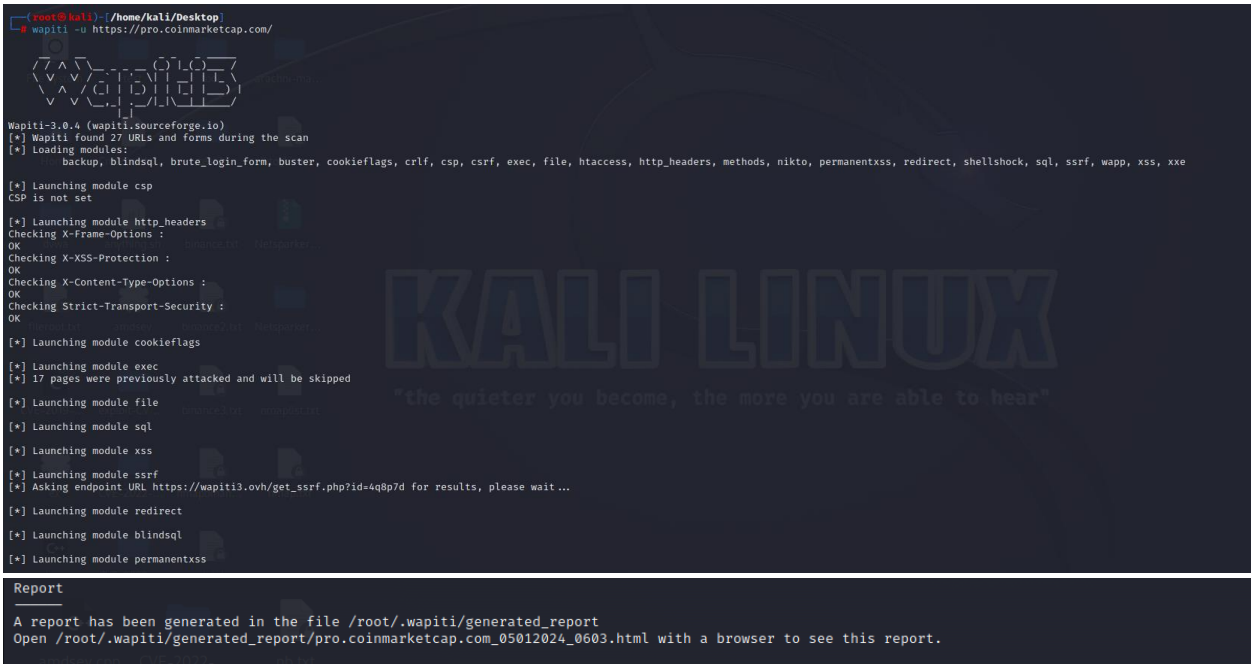
- Missing X-Content-Type-Options Header:
  - Vulnerability:
    - The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.
  - Attack:
    - Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

- Content-Encoding Header Vulnerability:
  - Vulnerability:

        - The Content-Encoding header is set to "deflate," which may indicate vulnerability to the BREACH attack.
    - Attack:
        - BREACH is a cryptographic attack that can be used to extract sensitive information, such as authentication tokens or other secrets, from encrypted web traffic.

- Uncommon Headers (x-traefik-route, x-envoy-decorator-operation, x-envoy-upstream-service-time):
    - Vulnerability:
        - Uncommon headers may indicate specific configurations or technologies used by the server, which could be targeted for exploitation if they reveal sensitive information.
    - Attack:
        - Attackers could leverage information from these headers to understand the server architecture or exploit known vulnerabilities associated with the technologies mentioned.

Wapiti

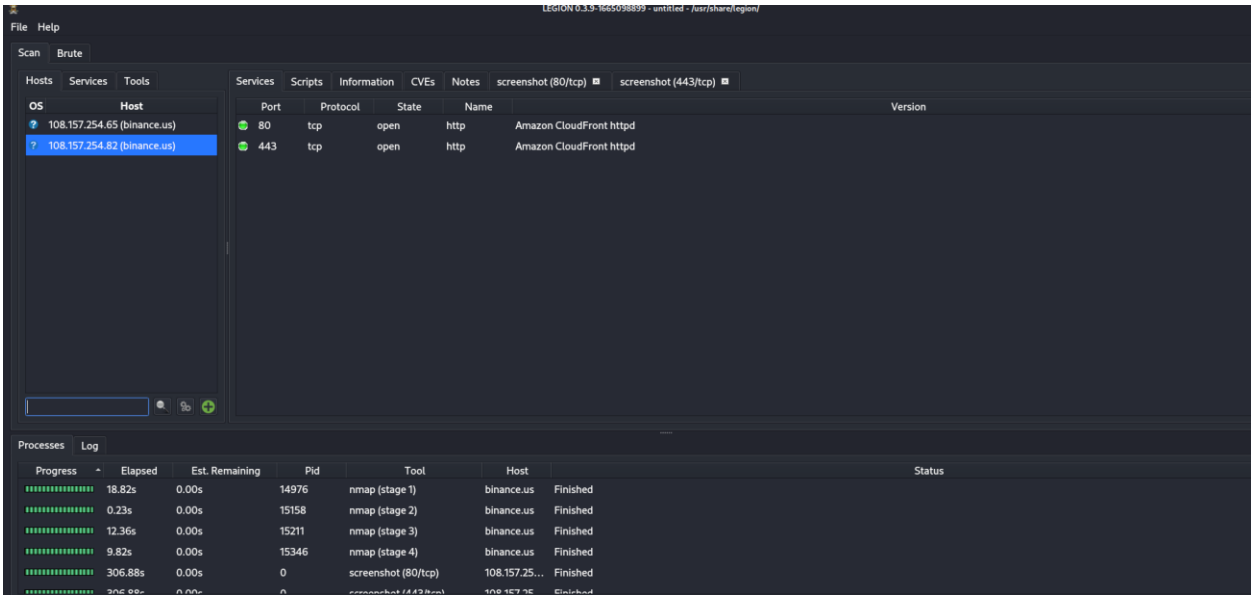


- Missing Content Security Policy (CSP):
    - Vulnerability:
        - The Content Security Policy (CSP) is not set, which may expose the website to various types of content injection attacks, such as XSS.
    - Attack:
        - Attackers could inject malicious scripts into the website's content, leading to cross-site scripting (XSS) attacks. This could allow them to steal sensitive information, manipulate the appearance of the page, or perform other malicious activities.

Sub domain 07

Target sub domain : https://www.binance.us/

Legion



Nikto

- Missing X-Frame-Options Header:
    - Vulnerability:
        - The anti-clickjacking X-Frame-Options header is not present, leaving the website vulnerable to clickjacking attacks.

    - Attack:

        - Attackers could embed the website within a malicious frame to trick users into performing unintended actions, such as clicking on hidden elements or submitting sensitive information.

- Missing Strict-Transport-Security Header:
    - Vulnerability:
        - The site does not define the Strict-Transport-Security HTTP header, which could expose users to risks related to protocol downgrade attacks.

    - Attack:
        - Attackers could attempt to downgrade secure HTTPS connections to insecure HTTP connections, making users susceptible to various forms of attacks, including man-in-the-middle attacks.

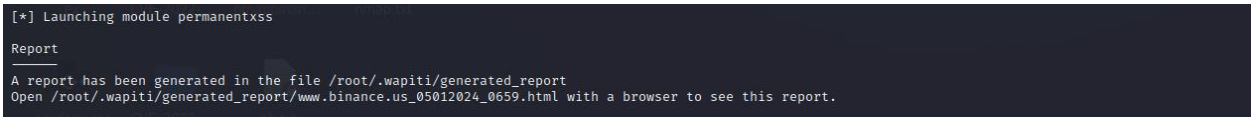
- Missing X-Content-Type-Options Header:
    - Vulnerability:
        - The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.

    - Attack:
        - Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

- Content-Encoding Header Vulnerability:
    - Vulnerability:
        - The Content-Encoding header is set to "deflate," which may indicate vulnerability to the BREACH attack.

    - Attack:
        - BREACH is a cryptographic attack that can be used to extract sensitive information, such as authentication tokens or other secrets, from encrypted web traffic.

Wapiti



- Missing X-Frame-Options Header:
  - Vulnerability:
    - The anti-clickjacking X-Frame-Options header is not present, leaving the website vulnerable to clickjacking attacks.
  - Attack:
    - Attackers could embed the website within a malicious frame to trick users into performing unintended actions, such as clicking on hidden elements or submitting sensitive information.

- Missing Strict-Transport-Security Header:
  - Vulnerability:
    - The site does not define the Strict-Transport-Security HTTP header, which could expose users to risks related to protocol downgrade attacks.
  - Attack:
    - Attackers could attempt to downgrade secure HTTPS connections to insecure HTTP connections, making users susceptible to various forms of attacks, including man-in-the-middle attacks.

- Missing X-Content-Type-Options Header:
  - Vulnerability:

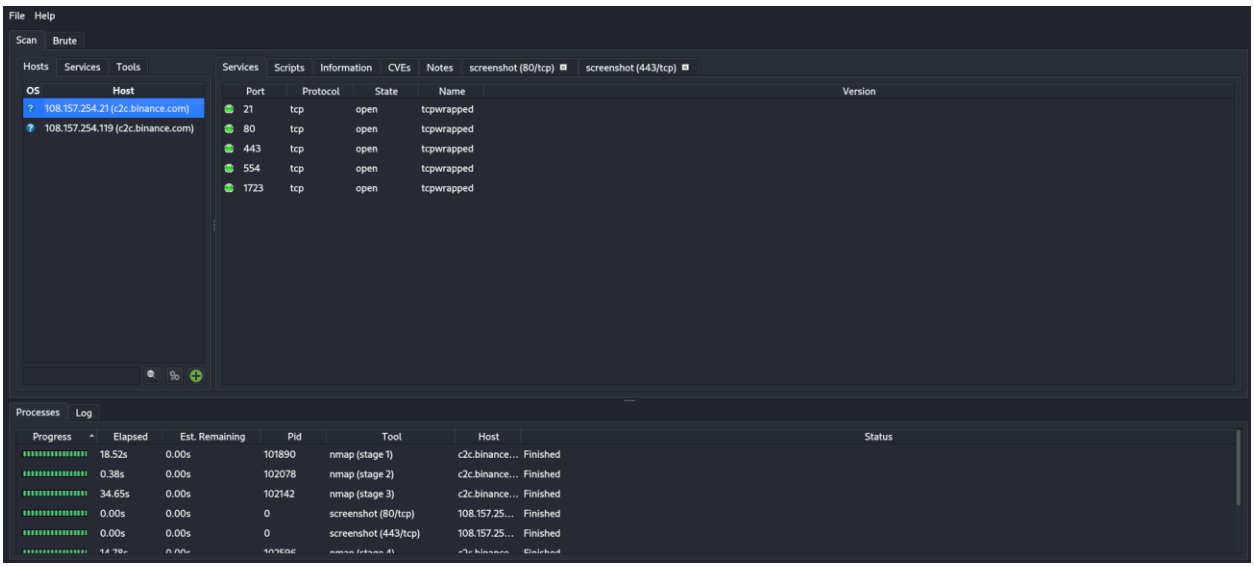
        - The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.
    - Attack:
        - Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

- Missing X-XSS-Protection Header:
    - Vulnerability:
        - The X-XSS-Protection header is not set, leaving the website susceptible to cross-site scripting (XSS) attacks.
    - Attack:
        - Attackers could inject malicious scripts into the website, leading to the execution of unauthorized code in users' browsers, potentially compromising their sensitive information.

Sub domain 08

Target sub domain : https://c2c.binance.com/en

Legion

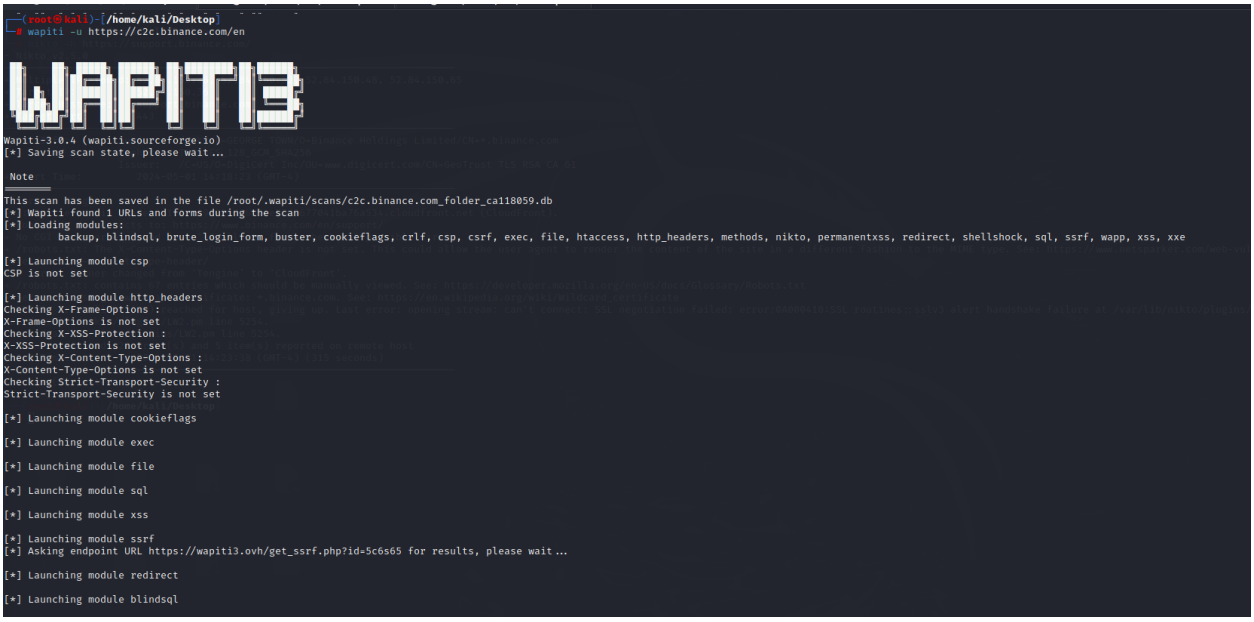


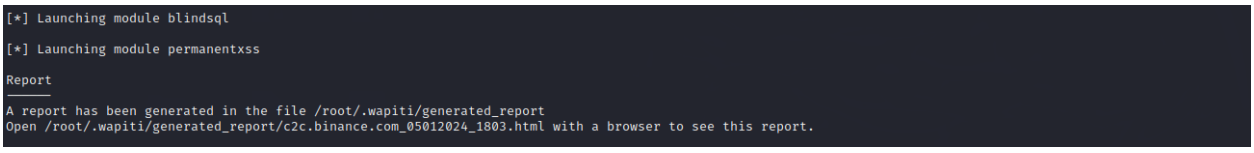
Nikto

- Missing X-Content-Type-Options Header:
  - Vulnerability:
    - The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.
  - Attack:
    - Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

- Content-Encoding Header Vulnerability:
    - Vulnerability:
        - The Content-Encoding header is set to "deflate," which may indicate vulnerability to the BREACH attack.
    - Attack:
        - BREACH is a cryptographic attack that can be used to extract sensitive information, such as authentication tokens or other secrets, from encrypted web traffic.
- Insecure Cookie Attributes:
    - Vulnerability:
        - Cookies such as "theme" are created without the secure and httponly flags, making them vulnerable to interception and manipulation.
    - Attack:
        - Attackers could intercept these cookies over insecure channels, potentially leading to session hijacking or other attacks

Wapiti





- Missing X-Frame-Options Header:
  - Vulnerability:
    - The anti-clickjacking X-Frame-Options header is not present, leaving the website vulnerable to clickjacking attacks.
  - Attack:
    - Attackers could embed the website within a malicious frame to trick users into performing unintended actions, such as clicking on hidden elements or submitting sensitive information.

- Missing Strict-Transport-Security Header:
  - Vulnerability:
    - The site does not define the Strict-Transport-Security HTTP header, which could expose users to risks related to protocol downgrade attacks.
  - Attack:
    - Attackers could attempt to downgrade secure HTTPS connections to insecure HTTP connections, making users susceptible to various forms of attacks, including man-in-the-middle attacks.

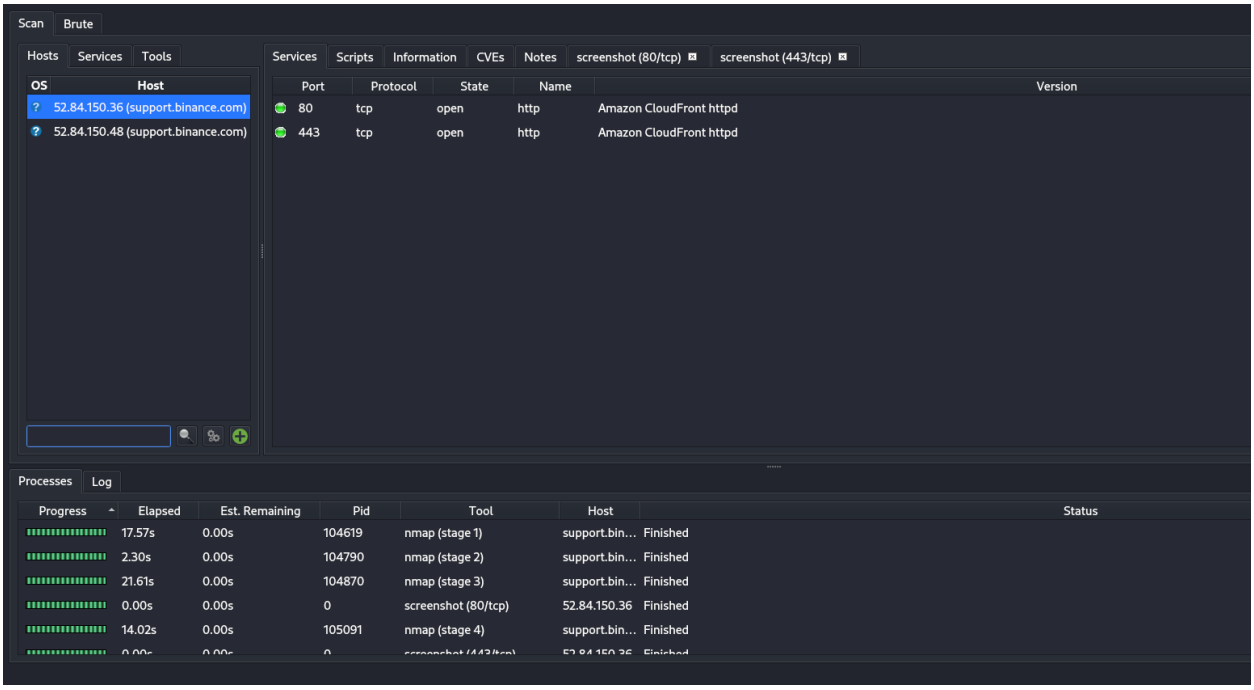
- Missing X-Content-Type-Options Header:
  - Vulnerability:
    - The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.
  - Attack:
    - Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

- Missing X-XSS-Protection Header:
  - Vulnerability:
    - The X-XSS-Protection header is not set, leaving the website susceptible to cross-site scripting (XSS) attacks.
  - Attack:
    - Attackers could inject malicious scripts into the website, leading to the execution of unauthorized code in users' browsers, potentially compromising their sensitive information.

Sub domain 09

Target sub domain : https://support.binance.com/

Legion

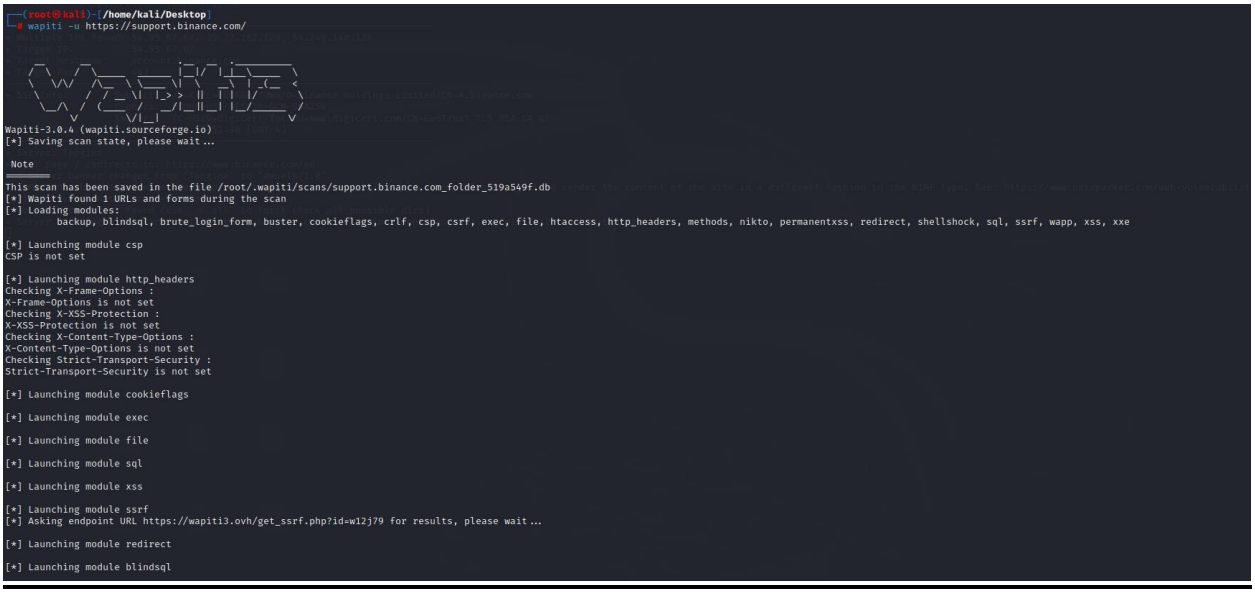


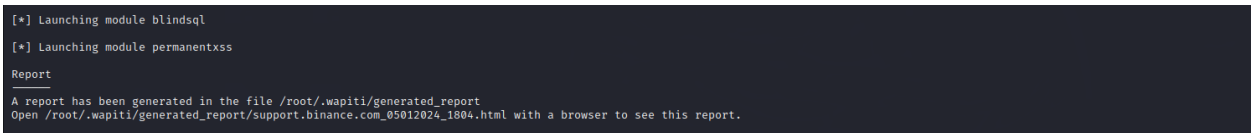
Nikto

- Missing X-Content-Type-Options Header:
  - Vulnerability:
    - The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.
  - Attack:

- Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

Wapiti





- Missing X-Frame-Options Header:
  - Vulnerability:
    - The anti-clickjacking X-Frame-Options header is not present, leaving the website vulnerable to clickjacking attacks.
  - Attack:
    - Attackers could embed the website within a malicious frame to trick users into performing unintended actions, such as clicking on hidden elements or submitting sensitive information.

- Missing Strict-Transport-Security Header:
  - Vulnerability:
    - The site does not define the Strict-Transport-Security HTTP header, which could expose users to risks related to protocol downgrade attacks.
  - Attack:
    - Attackers could attempt to downgrade secure HTTPS connections to insecure HTTP connections, making users susceptible to various forms of attacks, including man-in-the-middle attacks.

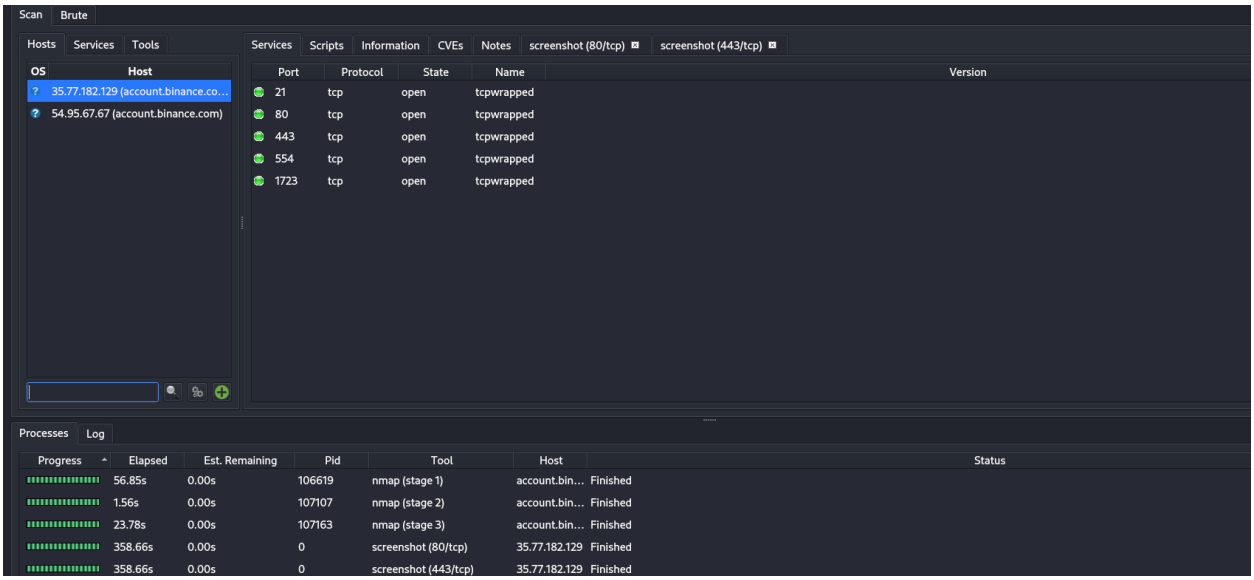
- Missing X-Content-Type-Options Header:
  - Vulnerability:
    - The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.
  - Attack:
    - Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

- Missing X-XSS-Protection Header:
  - Vulnerability:
    - The X-XSS-Protection header is not set, leaving the website susceptible to cross-site scripting (XSS) attacks.
  - Attack:
    - Attackers could inject malicious scripts into the website, leading to the execution of unauthorized code in users' browsers, potentially compromising their sensitive information.

Sub domain 10

Target sub domain: https://account.binance.com/

Legion



Nikto

- Missing X-Frame-Options Header:
    - Vulnerability:
        - The anti-clickjacking X-Frame-Options header is not present, leaving the website vulnerable to clickjacking attacks.
    - Attack:

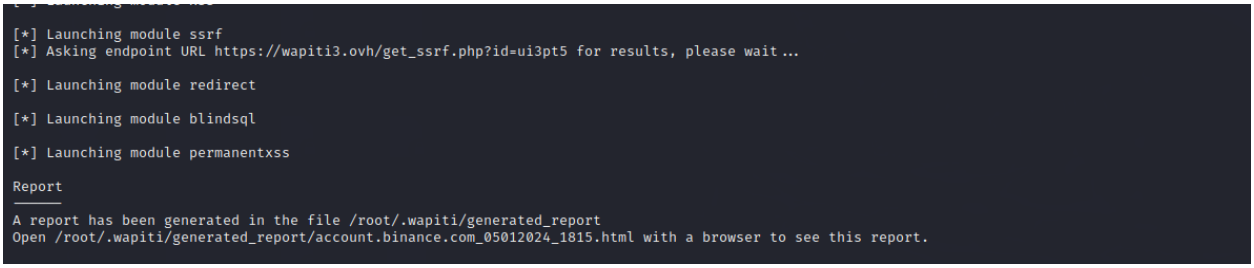
        - Attackers could embed the website within a malicious frame to trick users into performing unintended actions, such as clicking on hidden elements or submitting sensitive information.

- Missing Strict-Transport-Security Header:
    - Vulnerability:
        - The site does not define the Strict-Transport-Security HTTP header, which could expose users to risks related to protocol downgrade attacks.
    - Attack:
        - Attackers could attempt to downgrade secure HTTPS connections to insecure HTTP connections, making users susceptible to various forms of attacks, including man-in-the-middle attacks.

- Missing X-Content-Type-Options Header:
    - Vulnerability:
        - The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.
    - Attack:
        - Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

- Content-Encoding Header Vulnerability:
    - Vulnerability:
        - The Content-Encoding header is set to "deflate," which may indicate vulnerability to the BREACH attack.
    - Attack:
        - BREACH is a cryptographic attack that can be used to extract sensitive information, such as authentication tokens or other secrets, from encrypted web traffic.

Wapiti



- Missing X-Frame-Options Header:
  - Vulnerability:
    - The anti-clickjacking X-Frame-Options header is not present, leaving the website vulnerable to clickjacking attacks.
  - Attack:
    - Attackers could embed the website within a malicious frame to trick users into performing unintended actions, such as clicking on hidden elements or submitting sensitive information.

- Missing Strict-Transport-Security Header:
  - Vulnerability:
    - The site does not define the Strict-Transport-Security HTTP header, which could expose users to risks related to protocol downgrade attacks.
  - Attack:
    - Attackers could attempt to downgrade secure HTTPS connections to insecure HTTP connections, making users susceptible to various forms of attacks, including man-in-the-middle attacks.

- Missing X-Content-Type-Options Header:
  - Vulnerability:
    - The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.
  - Attack:
    - Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

- Missing X-XSS-Protection Header:
  - Vulnerability:
    - The X-XSS-Protection header is not set, leaving the website susceptible to cross-site scripting (XSS) attacks.
  - Attack:
    - Attackers could inject malicious scripts into the website, leading to the execution of unauthorized code in users' browsers, potentially compromising their sensitive information.

Identified weaknesses in the target domain

Missing X-Frame-Options Header:

Vulnerability:

- The anti-clickjacking X-Frame-Options header is not present, leaving the website vulnerable to clickjacking attacks.

Attack:

- Attackers could embed the website within a malicious frame to trick users into performing unintended actions, such as clicking on hidden elements or submitting sensitive information.

Missing X-Content-Type-Options Header:

Vulnerability:

- The X-Content-Type-Options header is not set, potentially allowing the user agent to render the content of the site in a different fashion to the MIME type.

Attack:

- Attackers could manipulate the content interpretation by the browser, potentially leading to cross-site scripting (XSS) vulnerabilities or other types of attacks.

SSRF (Server-Side Request Forgery):

Vulnerability:

- The scan detected a potential SSRF vulnerability, indicating that the website may be susceptible to allowing attackers to make unauthorized requests from the server.

Attack:

- An SSRF attack can allow an attacker to access internal resources, bypass firewalls, and perform reconnaissance, potentially leading to unauthorized data access or further system exploitation.

Content-Encoding Header Vulnerability:

Vulnerability:

- The Content-Encoding header is set to "deflate," which may indicate vulnerability to the BREACH attack.

Attack:

- BREACH is a cryptographic attack that can be used to extract sensitive information, such as authentication tokens or other secrets, from encrypted web traffic.

Missing Content Security Policy (CSP):

Vulnerability:

- The Content Security Policy (CSP) is not set, which may expose the website to various types of content injection attacks, such as XSS.

Attack:

- Attackers could inject malicious scripts into the website's content, leading to cross-site scripting (XSS) attacks. This could allow them to steal sensitive information, manipulate the appearance of the page, or perform other malicious activities.

Uncommon Headers (x-traefik-route, x-envoy-decorator-operation, x-envoy-upstream-service-time):

Vulnerability:

- Uncommon headers may indicate specific configurations or technologies used by the server, which could be targeted for exploitation if they reveal sensitive information.

Attack:

- Attackers could leverage information from these headers to understand the server architecture or exploit known vulnerabilities associated with the technologies mentioned.

Insecure Cookie Attributes:

Vulnerability:

- Cookies such as "theme" are created without the secure and httponly flags, making them vulnerable to interception and manipulation.

Attack:

- Attackers could intercept these cookies over insecure channels, potentially leading to session hijacking or other attacks

Missing Security Headers (X-XSS-Protection, Strict-Transport-Security):

Vulnerability:

These security headers are not set, leaving the website vulnerable to attacks such as clickjacking, XSS, MIME type sniffing, and protocol downgrade attacks.

Attack:

Attackers could exploit these missing headers to perform various attacks, including clickjacking attacks where the website is embedded within a malicious frame, XSS attacks where malicious scripts are injected and executed in users' browsers, and protocol downgrade attacks where secure connections are downgraded to insecure ones.

mitigation strategies for the vulnerabilities identified:

Missing X-Frame-Options Header:

- Add X-Frame-Options header with the value DENY or SAMEORIGIN to prevent your site from being embedded in frames on other domains.

Missing X-Content-Type-Options Header:

- Set the X-Content-Type-Options header to "nosniff" to prevent content-type sniffing attacks.

SSRF (Server-Side Request Forgery):

- Implement input validation and sanitization to prevent malicious URLs, whitelist allowed domains, and use DNS resolution to ensure valid and safe resource points.

Content-Encoding Header Vulnerability:

- To protect sensitive information, disable compression algorithms like "deflate" and implement additional security controls like data encryption, input validation, and rate limiting.

Missing Content Security Policy (CSP):

- Implement a strict Content Security Policy (CSP) to whitelist trusted content sources and scripts, using directives like default-src, script-src, and style-src to restrict resource loading.

Uncommon Headers (x-traefik-route, x-envoy-decorator-operation, x-envoy-upstream-service-time):

- To protect sensitive information, regularly review uncommon headers, configure web servers and reverse proxies to strip unnecessary ones, and use appropriate security headers to mitigate common attack vectors.

Insecure Cookie Attributes:

- Set the "secure" attribute on cookies to ensure secure HTTPS connections, and "httponly" to prevent client-side script access, reducing XSS attacks. Review all application-used cookies for appropriate attributes

Missing Security Headers (X-XSS-Protection, Strict-Transport-Security):

- To mitigate XSS attacks, add additional security headers in web server configuration or application code, and implement X-XSS-Protection header with 1 value and mode=block.

References

[1] E.-i.-C. H. N. S. Zeljka Zorz, "OWASP Top 10 2021: The most serious web application security risks," Help Net Security, 24 09 2021. [Online]. Available: https://www.helpnetsecurity.com/2021/09/24/owasp-top-10-2021/.

[2] O. Foundation, "OWASP Top Ten," [Online]. Available: https://owasp.org/www-project-top-ten/.

[3] "bugcrowd," [Online]. Available: https://bugcrowd.com/binance.

[4] S. Rahalkar, " Network Vulnerability Assessment," [Online]. Available: https://www.oreilly.com/library/view/network-vulnerability-assessment/9781788627252/7fdd1499-ecbd-4ae0-90db-9f7354105dfe.xhtml#:~:text=Passive%20information%20gathering%20is%20a,us%20with%20passive%20information%20gathering..

[5] "Sublist3r," [Online]. Available: https://www.kali.org/tools/sublist3r/.

[6] C. P. S. T. Ltd., "Cyber Hub Secure The Cloud Application Security (AppSec): Threats, Tools, and Techniques OWASP Top 10 Vulnerabilities," [Online]. Available: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-application-security-appsec/owasp-top-10-vulnerabilities/.