

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	6
Assessment Objectives	6
Introduction	7
OWASP Top 10 Security Risks and Vulnerabilities	8
About:	12
Target Information:	14
Information gathering	15
Passive Information Gathering:	15
Active Information Gathering:	15
Passive information gathering tools	16
Sublist3r	16
Nslookup	20
Whois	21
Whatweb	25
Netcraft	29
Whois Lookup	34
Wayback machine.....	36
Active information gathering tools	39
Nmap.....	39
Recon -ng Tool.....	39
Dmitry.....	41
Shodan	44
Planning and Analysis	46
Vulnerability Detection	47
Legion.....	47
Nikto.....	49
Wapiti	50
UniScan	52
Netsparker	57
Vulnerability Details	59
Impact.....	59
Actions to Take.....	59

mitigation	60
Sub domain 02	61
Legion.....	61
Nikto.....	61
Wapiti	63
Netsparker	64
Vulnerability Details	65
Impact.....	65
Actions to Take.....	65
mitigation	65
Sub domain 03	66
Legion.....	66
Wapiti	68
Sub domain 04	70
Legion.....	70
Nikto.....	70
Wapiti	72
Netsparker	73
Vulnerability Details	76
Impact.....	76
Mitigation	77
Sub domain 05	78
Legion	78
Nikto	78
Netspaker	79
Vulnerability Details	82
Impact.....	82
Actions to Take.....	82
mitigation	83
Sub domain 06	84
Legion	84
Nikto	84
Wapiti	85

Sub domain 07	87
Legion.....	87
Nikto.....	87
Wapiti	89
Sub domain 08	91
Legion.....	91
Nikto.....	91
Wapiti	92
Sub domain 09	94
Legion.....	94
Nikto.....	94
Wapiti	95
Sub domain 10	97
Legion.....	97
Nikto.....	97
Wapiti	99
Identified weaknesses in the target domain	101
Missing X-Frame-Options Header:.....	101
Vulnerability:	101
Attack:.....	101
Missing X-Content-Type-Options Header:.....	101
Vulnerability:	101
Attack:.....	101
SSRF (Server-Side Request Forgery):	101
Vulnerability:	101
Attack:.....	101
Content-Encoding Header Vulnerability:.....	102
Vulnerability:	102
Attack:.....	102
Missing Content Security Policy (CSP):	102
Vulnerability:	102
Attack:.....	102

Uncommon Headers (x-traefik-route, x-envoy-decorator-operation, x-envoy-upstream-service-time):	102
Vulnerability:	102
Attack:.....	102
Insecure Cookie Attributes:.....	103
Vulnerability:	103
Attack:.....	103
Missing Security Headers (X-XSS-Protection, Strict-Transport-Security):.....	103
Vulnerability:	103
Attack:.....	103
mitigation strategies for the vulnerabilities identified:	104
Missing X-Frame-Options Header:.....	104
Missing X-Content-Type-Options Header:	104
SSRF (Server-Side Request Forgery):	104
Content-Encoding Header Vulnerability:.....	104
Missing Content Security Policy (CSP):	104
Uncommon Headers (x-traefik-route, x-envoy-decorator-operation, x-envoy-upstream-service-time):	104
Insecure Cookie Attributes:.....	105
Missing Security Headers (X-XSS-Protection, Strict-Transport-Security):	105
References	106

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]

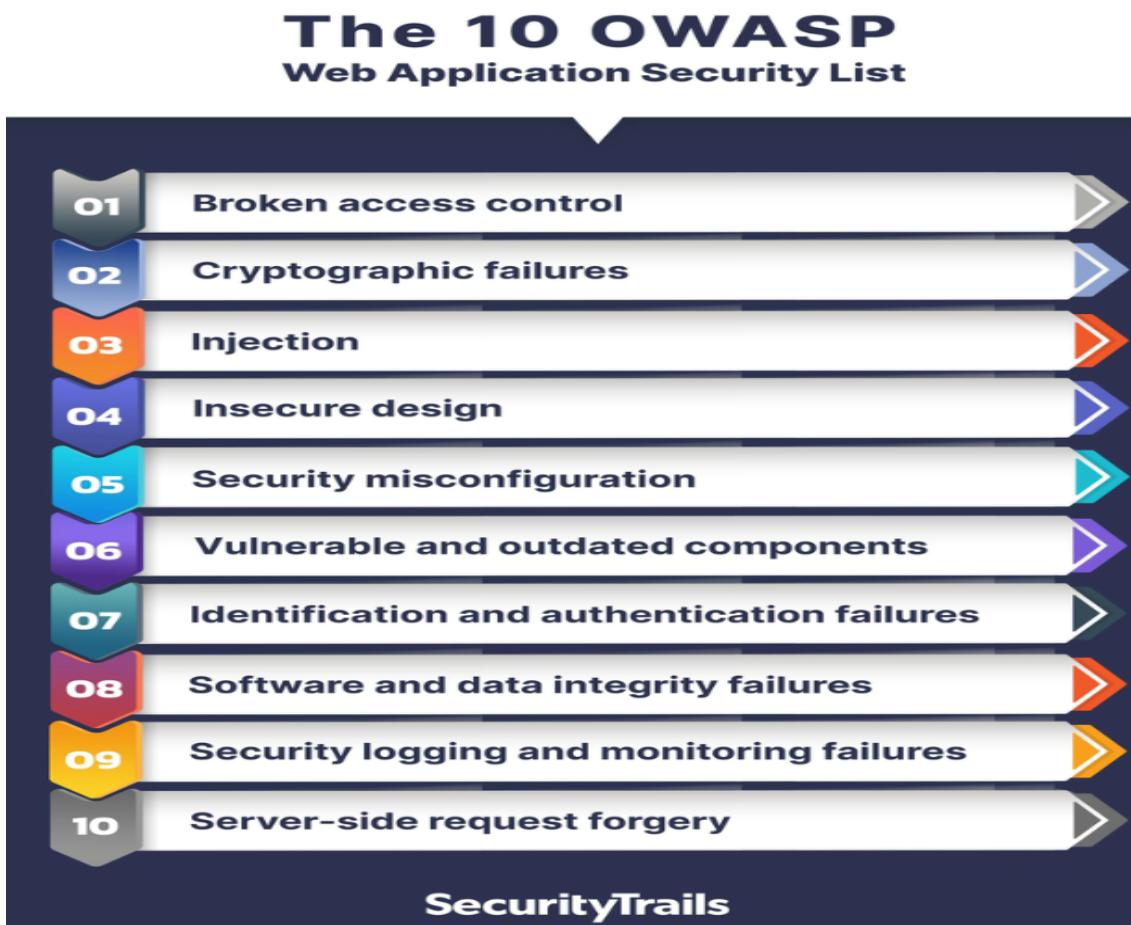


Fig 01

- 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 known 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 - Bugcrowd

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 X Post Share 56

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.

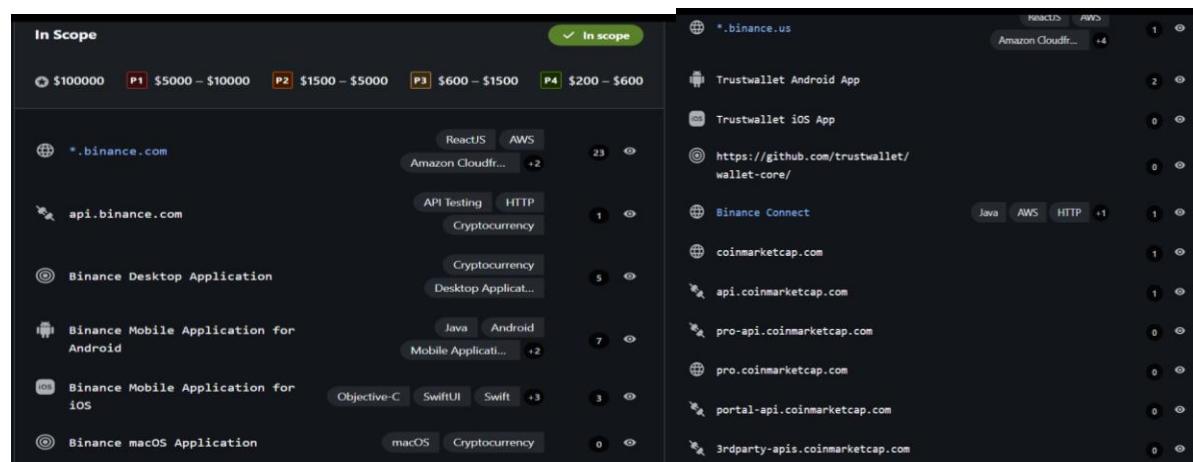
With millions of users worldwide, Binance's platform is trusted and committed to giving individuals more financial freedom by offering access to a wide range of financial instruments over an expanding global network at the lowest rates in the industry.

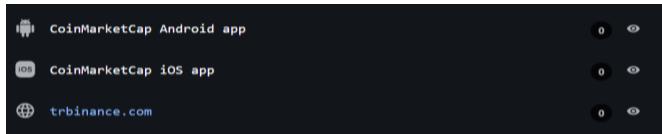
Being the blockchain ecosystem's infrastructure supplier is Binance's goal. Currently, Binance is a worldwide blockchain ecosystem that includes investment and incubation programs, research, instructional materials, infrastructure solutions, trading services, social good and philanthropic activities, 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

Out of Scope X Out of scope

Website	Category
support.binance.*	Website Testing
*.trustwallet.com	
*.trustwalletapp.com	
*.binance.org	
binance.sg	ReactJS Website Testing Cryptocurrency +1
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 Conne
- 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]

Information 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]

```
(kali㉿kali)-[~/Desktop/tool/Sublist3r]
$ python3 sublist3r.py -d binance.com

File System
└── test
    └── subdomains
        └── binance.com
            └── www.binance.com
                └── academy.binance.com
                    └── accounts.binance.com
                        └── api.binance.com
                            └── api.binance.com
                                └── app.binance.com
                                    └── c2c.binance.com
                                        └── c2c-admin.binance.com
                                            └── cloud.binance.com
                                                └── developers.binance.com
                                                    └── download.binance.com
                                                        └── fapi.binance.com
                                                            └── help.binance.com
                                                                └── labs.binance.com
                                                                    └── launchpad.binance.com
                                                                        └── merchant.binance.com
                                                                            └── nft.binance.com
                                                                                └── opstream.binance.com
                                                                                    └── oracle.binance.com
                                                                                        └── p2p.binance.com
                                                                                            └── pay.binance.com
                                                                                                └── pool.binance.com
                                                                                                    └── research.binance.com
                                                                                                        └── status.binance.com
                                                                                                            └── support.binance.com
                                                                                                                └── themis.binance.com

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for binance.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..      test2
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 343
www.binance.com
academy.binance.com
accounts.binance.com
api.binance.com      amdsev
api.binance.com
app.binance.com
c2c.binance.com
c2c-admin.binance.com
cloud.binance.com
developers.binance.com
download.binance.com
fapi.binance.com
help.binance.com
labs.binance.com
launchpad.binance.com
merchant.binance.com
nft.binance.com
opstream.binance.com
oracle.binance.com
p2p.binance.com
pay.binance.com
pool.binance.com
research.binance.com
status.binance.com
support.binance.com
themis.binance.com
```

```
ww16.train.boards.www--binance.com
ww16.boards.www--binance.com tryhack.ovpn
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.hwdn.controller.www--binance.com
ww16.controller.www--binance.com
ww16.csvcdn.www--binance.com
ww16.dashboardlb.www--binance.com test2
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.developepage.www--binance.com
ww16.hwdn.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.europewestfile.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
```

```
THE Actions Edit View Help
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 test2
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.admininternals.www--binance.com
ww16.apisinged.www--binance.com
ww16.apidocs-elastc.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.lbhstory.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.hwdn.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-hwdn.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.opsstreamhwdn.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.europofile.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 test2  
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.hwdn.www--binance.com  
ww16.promo.hwdn.www--binance.com  
ww16.repository.hwdn.www--binance.com  
ww16.support.hwdn.www--binance.com  
ww16.tomcat.hwdn.www--binance.com  
ww16.hwdn。www--binance.com  
ww16.hwdncontainer.www--binance.com  
ww16.hwdnopsstream.www--binance.com  
ww16.hwdnportal.www--binance.com  
ww16.hwdnw3.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-database4.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
```

```
ww16.statsaccount.www--binance.com  
ww16.statsclient.www--binance.com  
ww16.statsfw.www--binance.com  
ww16.statsmerchant.www--binance.com  
ww16.tools.stg.www--binance.com  
ww16.supportazure.www--binance.com  
ww16.stats.swag.www--binance.com  
ww16.swag-9.www--binance.com  
ww16.lb.swagger.www--binance.comtool  
ww16.system-jinx.www--binance.com  
ww16.teamelastic.www--binance.com  
ww16.test-file.www--binance.com  
ww16.testel.www--binance.com  
ww16.testnet-wallet-azure.www--binance.co  
ww16.singed.tomcat.www--binance.com  
ww16.toolbarstats.www--binance.comt2  
ww16.docs.tools.www--binance.com  
ww16.metrics.tools.www--binance.com  
ww16.static.tools.www--binance.com  
ww16.tools.www--binance.com  
ww16.tools-backend.www--binance.com  
ww16.tools-k8s-prd.www--binance.com  
ww16.tools-metrics.www--binance.com  
ww16.toolsapac.www--binance.com  
ww16.toolsauthentication.www--binance.co  
ww16.toolsdata。www--binance.com  
ww16.toolsproductions.www--binance.com  
ww16.traffic.www--binance.com  
ww16.trafficsinged.www--binance.com  
ww16.train-boards.www--binance.com  
ww16.trainingfile.www--binance.com  
ww16.trainingstream.www--binance.com  
ww16.uploaddevel.www--binance.com  
ww16.uploads-apps.www--binance.com  
ww16.uploadsel.www--binance.com  
ww16.uploadsstats.www--binance.com  
ww16.uploadstream.www--binance.com  
ww16.v2-hwcdn.www--binance.com  
ww25.v3.www--binance.com  
ww16.jinx.vpn.www--binance.com  
ww16.vpntools.www--binance.com  
ww16.boards.webapp.www--binance.com  
ww16.webappin.www--binance.com  
ww16.www--binance.com  
ww25.www--binance.com  
ww16.ww25-global.www--binance.com  
ww25.z.www--binance.com  
ww25.z-repository.www--binance.com  
ww25.z-training.www--binance.com  
ww25.zbitbucket.www--binance.com  
ww25.zdocument.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]# 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]# 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]# 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]~[~/tryhackme]
# 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]~[~/tryhackme]
# 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] tryhackovern
# 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: DNSstation 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 st2  
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.

```
[root@kali]# /home/kali
# whatweb binance.com
http://binance.com [301 Moved Permanently] Country[UNITED STATES][en], HTTPServer[nginx/2.4], IP[35.76.171.122], RedirectLocation[https://www.binance.com/en/], Title[301 Moved Permanently]
https://www.binance.com [302 Found] Country[UNITED STATES][en], HTTPServer[Tengine], IP[52.84.150.48], RedirectLocation[https://www.binance.com/en/], Strict-Transport-Security[max-age=1536000; 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 59953d425efb321e28a3ea2f7886740.cloudfront.net [CloudFront]], X-Frame-Options[SAMEORIGIN], X-KSS-Protection[; mode-block]
https://www.binance.com [200 OK] Cookies[theme], Country[UNITED STATES][en], Email[940d3781f694c839941770b560ff1a80529942], Ingest-sentry.io-b2a91..2.js, commonjs_3.217.min.js, extensionjs_3.217.min.js, footerjs_1.3.217.min.js, headerjs_1.3.217.min.js, https0.15.89.js, stylejs_3.217.css, themeis0.0.12.js, track08.1.97.js, util08.0.0.js, vendor08.0.0.js, vendor08.1.97.js, Frame, Google-Analytics[Universal][UA-102512267-1], HTML5, HTTPServer[Tengine], IP[52.84.150.48], Open-Graph-Protocol[website], Script[application/javascript,application/json,application/javascript], Strict-Transport-Security[max-age=1536000; 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,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 d746738e11aa2150666bd5157a78e.cloudfront.net [CloudFront]], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[; mode-block]
[root@kali]# /home/kali
# whatweb api.binance.com
http://api.binance.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][en], HTTPServer[CloudFront], IP[108.158.2.107], RedirectLocation[https://api.binance.com/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 91632d5983c87fa33cb45fcbbaf8.cloudfront.net [CloudFront]]
https://api.binance.com [200 OK] Access-Control-Allow-Methods[GET, HEAD, OPTIONS], Content-Security-Policy[default-src 'self'], Country[UNITED STATES][en], HTML5, HTTPServer[nginx], IP[108.158.2.107], Strict-Transport-Security[max-age=1536000; includeSubdomains, strict-set-on], Title[301 Moved Permanently], UncommonHeaders[x-content-type-options,content-security-policy,x-permitted-cross-domain-policies,content-security-policy,x-envoy-decorator-operation,x-traefik-route,x-envoy-upstream-service-time,x-cache-proxy,x-cache-proxy-key,x-envoy-decorator-operation,x-permitted-cross-domain-policies,content-security-policy,x-content-type-options,referrer-policy,x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 643f7754e4426e5f006f0a89899efc.cloudfront.net [CloudFront]], X-Frame-Options[SAMEORIGIN], X-KSS-Protection[; mode-block], nginx
[root@kali]# /home/kali
# whatweb coinmarketcap.com
http://coinmarketcap.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][en], HTTPServer[CloudFront], IP[13.35.18.48], RedirectLocation[https://coinmarketcap.com/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 f28347a3148f4f8af1d98375689073c.cloudfront.net [CloudFront]]
https://coinmarketcap.com [200 OK] Content-Language[en], Country[UNITED STATES][en], HTML5, HTTPServer[Tengine], IP[13.35.18.48], Open-Graph-Protocol[website], Script[application/javascript,application/json,application/javascript], Tengine-Web-Server, Title[Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap], UncommonHeaders[x-traefik-route,x-envoy-upstream-service-time,x-cache-proxy,x-cache-proxy-key,x-envoy-decorator-operation,x-permitted-cross-domain-policies,content-security-policy,x-content-type-options,referrer-policy,x-amz-cf-pop,x-amz-cf-id], Via-Proxy[1.1 1728256c36c901ee6b9379e91a1c2e68.cloudfront.net [CloudFront]], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[ie=edge], X-KSS-Protection[; mode-block]
```

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]
# curl -I http://www.binance.com
WhatWeb Report: https://www.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: Mon, 09 Oct 2024 18:38:32 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 : 
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
From: https://www.binance.com
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-aspen-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:
Status : 302 Moved Temporarily
Content-Type: text/html; charset=utf-8
Content-Length: 49
Connection: close
Date: Fri, 20 Apr 2024 18:29:21 GMT
Server: Tengine
Location: https://www.binance.com/en
X-Gateway: traefik
X-Traefik-Config-Hash: 714c2f9e5d9d6af07a412b
X-Traefik-Duration: 0.00
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referer-Policy: origin-when-cross-origin
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Cache: Hit From cloudfront
Via: 1.1 74d494d4799f1a252f4bef276.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: M552
X-Amz-Cf-Id: 27ad63x1v6etCPE65APoqThybrcS0Z0zVbtDlRNtIqiRsC9gp8M3A=
Age: 74

Whatweb report for https://www.binance.com/en
Status : 200 OK
Title   : <None>
IP     : 52.19.150.48
Country: United States, US

Summary: Cookies[theme], Email[40d37812f0b4f83941170b560fa1ab029943].ingest.sentry.io,b2a01.1.2.js,common01.3.217.min.js,data01.3.217.min.js,extension01.3.217.min.js,footer01.3.217.min.js,header01.3.217.min.js,http01.15.00.js,styl01.3.217.css,theme00.0.32.js,track00.1.97.js,utils01.3.217.min.js,uuid00.0.0.js,vendor01.3.217.min.js,Frame Google-Analytics[Universal][UA-162512367-1], HTML, HTTPS[server:Tengine], Open-Graph[Protocol], 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-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 05ef390c85f3303ec2fd0ab0e067c170.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 make an attempt to catch email addresses containing @. This plugin catches email addresses like bob@at@gmail.com. This uses the simplified email regular expression from http://www.regular-expressions.info/email.html for valid

String   : theme

[ Email ]
String   : 949d37812f0b4f83941170b560fa1ab029943.ingest.sentry.io,b2a01.1.2.js,common01.3.217.min.js,data01.3.217.min.js,extension01.3.217.min.js,footer01.3.217.min.js,header01.3.217.min.js,http01.15.00.js,styl01.3.217.css,theme00.0.32.js,track00.1.97.js,utils01.3.217.min.js,uuid00.0.0.js,vendor01.3.217.min.js

Frame 1
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 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 browser access from accessing a website without the security of the HTTPS protocol.

String   : max-age=15552000; includeSubDomains, max-age=31536000; includeSubDomains

Tengine-Web-Server ]

nginx/1.20.0
Website   : http://tengine.taobao.org/

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

String   : content-security-policy,expect-ct,x-cache-proxy,x-cache-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 05ef390c85f3303ec2fd0ab0e067c170.cloudfront.net (CloudFront)

[ X-Frame-Options ]
This plugin retrieves the X-Frame-Options value from the HTTP header. - More Info: https://msdn.microsoft.com/en-us/library/cc288472k28v5.85%29.aspx

String   : SAMEORIGIN

[ X-XSS-Protection ]
This plugin retrieves the X-XSS-Protection value from the HTTP header. - More Info: https://msdn.microsoft.com/en-us/library/cc288472k28v5.85%29.aspx

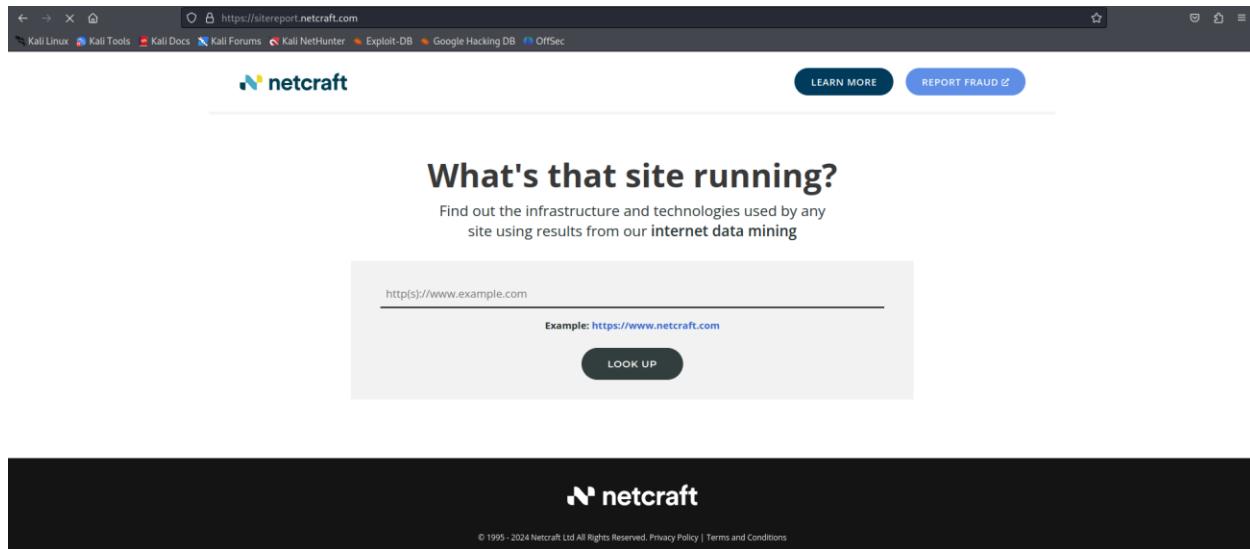
String   : 1; mode=block

```

```
ETag: 35264b-mz20a20314n0gRILjkHt7qkVU
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: df5fbcc053c34096ba966686ae5dc315
X-Traefik-Duration: 2.00
X-Frame-Options: SAMEORIGIN
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Referer-Policy: origin-when-cross-origin
Strict-Transport-Security: max-age=31536000; includeSubdomains
X-Cache: Miss from cloudfront
Via: 1.1 05ef390c85ff3303ec2fddab8e67c170.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: MRS52-C2
X-Amz-Cf-Id: TzR8UAoApAWCRRYClwHp3jhBHQrMTgVPemha_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.



The screenshot shows the Netcraft website at <https://site.report.netcraft.com>. The header includes the Netcraft logo, a search bar with placeholder text "http(s)://www.example.com", and buttons for "LEARN MORE" and "REPORT FRAUD". Below the header, a section titled "What's that site running?" with the subtitle "Find out the infrastructure and technologies used by any site using results from our internet data mining" is visible. A "LOOK UP" button is located below the search bar.

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	whols.markmonitor.com
IPv4 address	52.192.247.165	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 [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=DMARCV1; 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.



○ 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.esig-oei.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.mercadolivre.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.

The screenshot shows the DomainTools website with a search bar at the top containing 'https://www.binance.com'. Below the search bar is a large banner with a desert landscape background and the text 'Whois Lookup' in white. A search input field with placeholder 'Enter a domain or IP address...' and a blue 'SEARCH' button are visible. Below the banner, there's a promotional message about upgrading membership and a 'LEARN MORE' button. The main content area displays the 'Whois Record' for Binance.com, listing various domain metadata such as Registrar, Dates, Name Servers, IP Address, and more.

Whois Record for BiNance.com

Domain Profile	
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) +1.2086851750
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	2,566 days old Created on 2017-04-01 Expires on 2025-04-01 Updated on 2020-12-09
Name Servers	NS-1319.AWSDNS-36.ORG (has 55,613 domains) NS-1701.AWSDNS-20.CO.UK (has 455 domains) NS-234.AWSDNS-29.COM (has 1,569 domains) NS-735.AWSDNS-27.NET (has 28 domains)
IP Address	52.84.150.36 - 6 other sites hosted on this server
IP Location	United States - California - Los Angeles - Amazon.com Inc.
ASN	AS16509 AMAZON-02, US (registered May 04, 2000)
Domain Status	Registered And No Website
IP History	86 changes on 86 unique IP addresses over 14 years
Registrar History	5 registrars with 3 drops
Hosting History	22 changes on 13 unique name servers over 19 years
Whois Record (last updated on 2024-04-10)	

The screenshot shows the DomainTools Iris interface, which is a platform for internet intelligence. It features a sidebar with 'DomainTools Iris' and 'Learn More' buttons, followed by sections for 'Preview the Full Domain Report', 'Tools' (Hosting History, Monitor Domain Properties, Reverse IP Address Lookup, Network Tools), 'Visit Website' (with a preview of Binance's homepage), and 'Available TLDs' (General TLDs, Country TLDs).

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
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
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:

JELIN TIA LAL:
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)

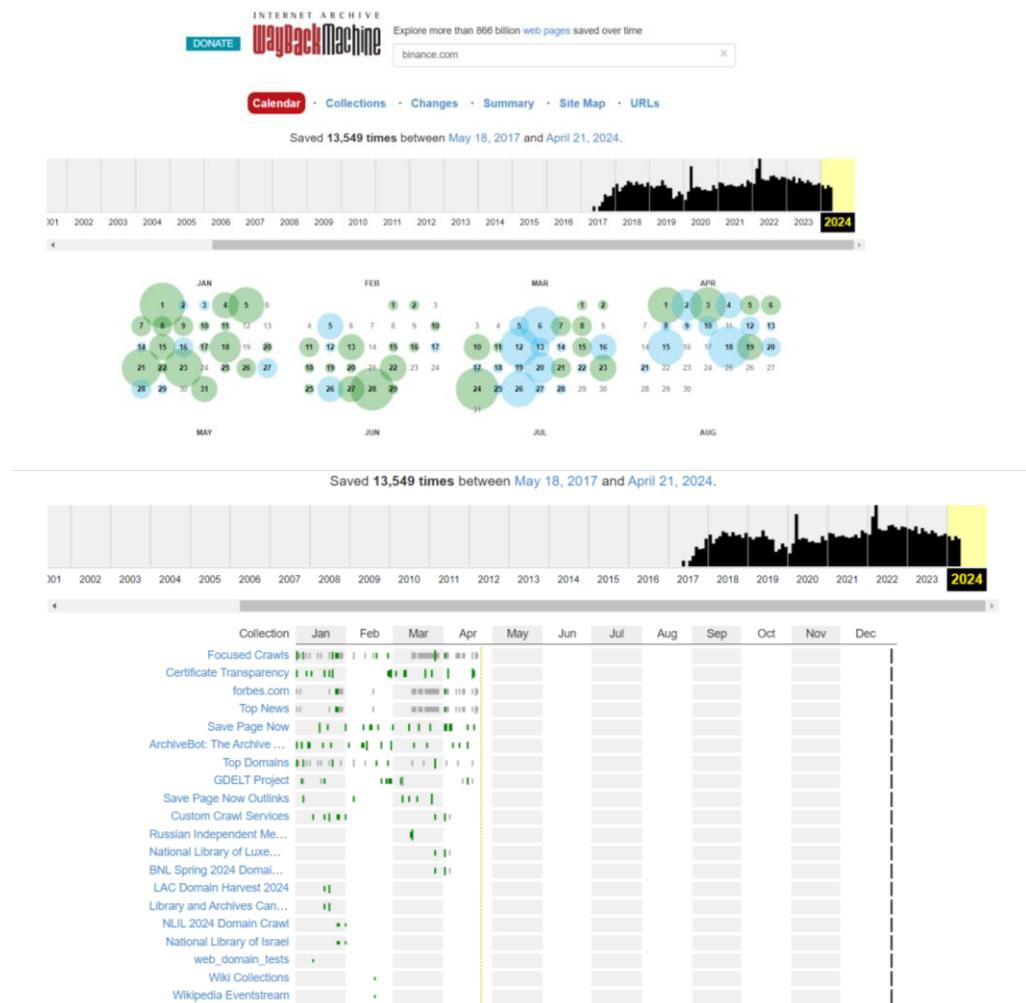
- Taken domain.
- Available domain.
- Deleted previously owned domain.

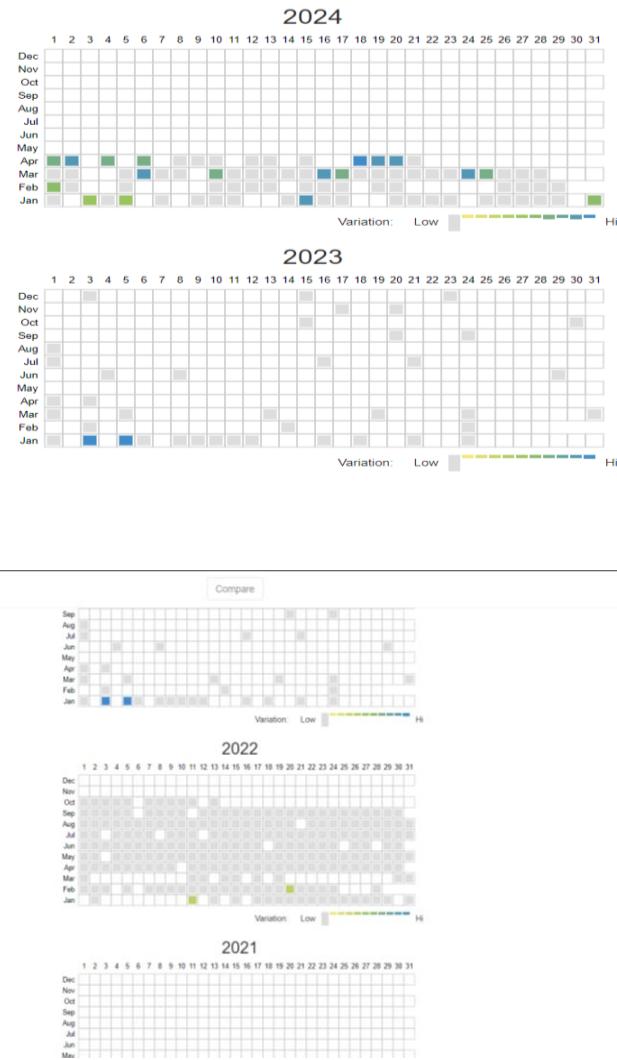
BiNance.com	View Whois
BiNance.org	View Whois
BiNance.info	View Whois
BiNance.biz	View Whois
BiNance.us	View Whois

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.

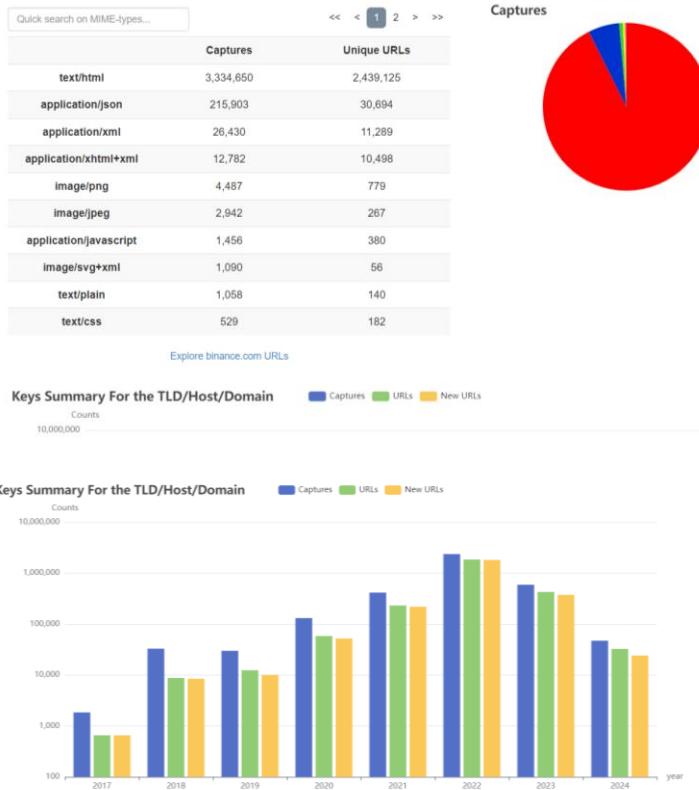




This approach yields some fascinating data, which makes it quite beneficial for information collecting. Examples include:

- Sensitive data;
- Old, forgotten endpoints;
- Interesting JS files

Summary on MIME-types Count



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&newstid=20220510005291&lan=en-US&anchor=Binance.com&index=14&md5=6b47ae79bb8a3b4ea1b64e90b370bd	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/*9993mFinanceLabs	text/html	Jan 18, 2023	Jan 18, 2023	2	1	1
http://binance.com/Лардрбее	text/html	Jan 21, 2023	Jan 21, 2023	2	0	2
http://binance.com/_56087000092e4807bd40c03afbbe8258	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/?i=16788521	text/html	Oct 31, 2020	May 7, 2023	6	2	4
http://binance.com/?11359603	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/?ref=567657	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/?bcld=1wAR1NcHEKchdt_bHqYEiTqJKV-9lgPieTwV3NKa6BYIAaiLcj-LjS_214s	text/html	Nov 14, 2022	Nov 14, 2022	1	0	1
http://binance.com/?bcld=1wAR1TE0A1sqQOWlh4N0RtaejChJg-QP2yOD503R86TTWc9lmxG_P_2RMmD0	text/html	Nov 12, 2020	Nov 12, 2020	2	0	2
http://binance.com/?d=yJMX-NQQ	text/html	Sep 2, 2021	Sep 2, 2021	2	0	2
http://binance.com/?iquid?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.

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sS www.binance.com -oN nmapbinance.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-24 09:24 EDT
Nmap scan report for www.binance.com (52.84.150.36)
Host is up (0.037s latency).
Other addresses for www.binance.com (not scanned): 52.84.150.48 52.84.150.52 52.84.150.65
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
1723/tcp  open  pptp

Nmap done: 1 IP address (1 host up) scanned in 12.67 seconds
```

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.

```
[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] > options
[!] Invalid command: options.
[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
```

```
[*] be.binance .com => No record found.  
[*] backend.binance .com => No record found.  
[*] bea.binance .com => No record found.  
[*] bg.binance .com => No record found.  
[*] bh.binance .com => No record found.  
[*] bi.binance .com => No record found.  
[*] bf.binance .com => No record found.  
[*] billing.binance .com => No record found.  
[*] biztalk.binance .com => No record found.  
[*] biz.binance .com => No record found.  
[*] bbdd.binance .com => No record found.  
[*] bd.binance .com => No record found.  
[*] blog.binance .com => No record found.  
[*] blackberry.binance .com => No record found.  
[*] bj.binance .com => No record found.  
[*] bm.binance .com => No record found.  
[*] beta.binance .com => No record found.  
[*] bnc.binance .com => No record found.  
[*] bo.binance .com => No record found.  
[*] blue.binance .com => No record found.  
[*] bn.binance .com => No record found.  
[*] blogs.binance .com => No record found.  
[*] bolsa.binance .com => No record found.  
[*] black.binance .com => No record found.  
[*] boulder.binance .com => No record found.  
[*] boy.binance .com => No record found.  
[*] border.binance .com => No record found.  
[*] bof.binance .com => No record found.  
[*] bravo.binance .com => No record found.  
[*] brazil.binance .com => No record found.  
[*] boise.binance .com => No record found.  
[*] broker.binance .com => No record found.  
[*] broadcast.binance .com => No record found.  
[*] britian.binance .com => No record found.  
[*] boston.binance .com => No record found.  
[*] bob.binance .com => No record found.  
[*] br.binance .com => No record found.  
[*] bsd0.binance .com => No record found.  
[*] bsd01.binance .com => No record found.  
[*] bronze.binance .com => No record found.  
[*] bsd.binance .com => No record found.  
[*] bs.binance .com => No record found.  
[*] bsd1.binance .com => No record found.  
[*] bsd2.binance .com => No record found.  
[*] bt.binance .com => No record found.  
[*] brown.binance .com => No record found.  
[*] bug.binance .com => No record found.  
[*] buggalo.binance .com => No record found.  
[*] build.binance .com => No record found.  
[*] bugs.binance .com => No record found.  
[*] burn.binance .com => No record found.  
[*] burner.binance .com => No record found.
```

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:          _____
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
address-space
remarks:          _____
remarks:          AFRINIC (Africa)
remarks:          http://www.afrinic.net/ whois.afrinic.net
remarks:          _____
remarks:          APNIC (Asia Pacific)
remarks:          http://www.apnic.net/ whois.apnic.net
remarks:          _____
remarks:          ARIN (Northern America)
remarks:          http://www.arin.net/ whois.arin.net
remarks:          _____
remarks:          LACNIC (Latin America and the Caribbean)
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
DeleteProhibited 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
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
Home Cmadhush... test2
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.

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Pricing | Search... |

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

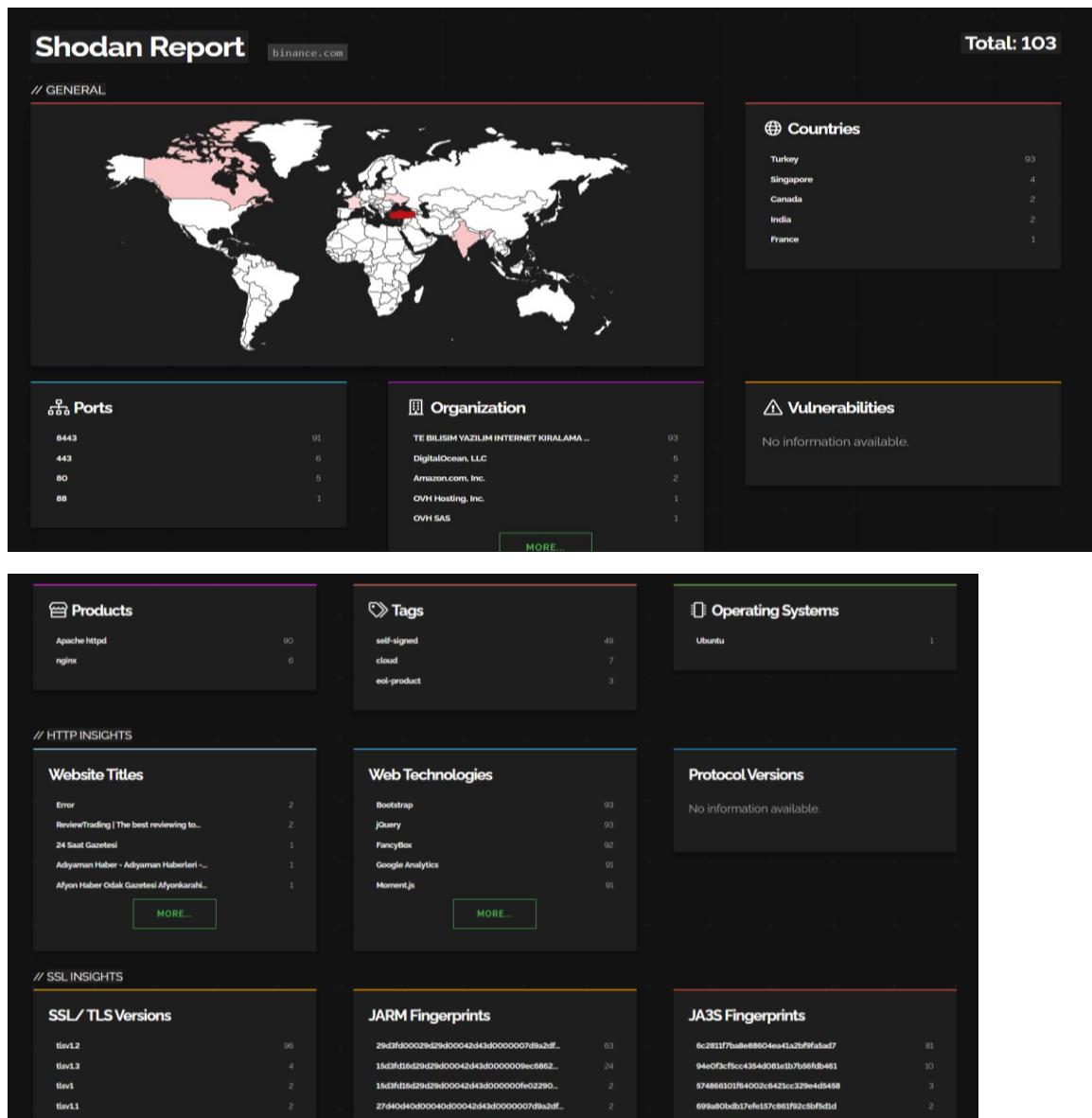
SIGN UP NOW

// EXPLORE THE PLATFORM

Beyond the Web
Websites are just one part of the Internet. Use Shodan to discover everything from power

Monitor Network Exposure
Keep track of all your devices that are directly accessible from the Internet. Shodan provides

Internet Intelligence
Learn more about who is using various products and how they're changing over time.



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.

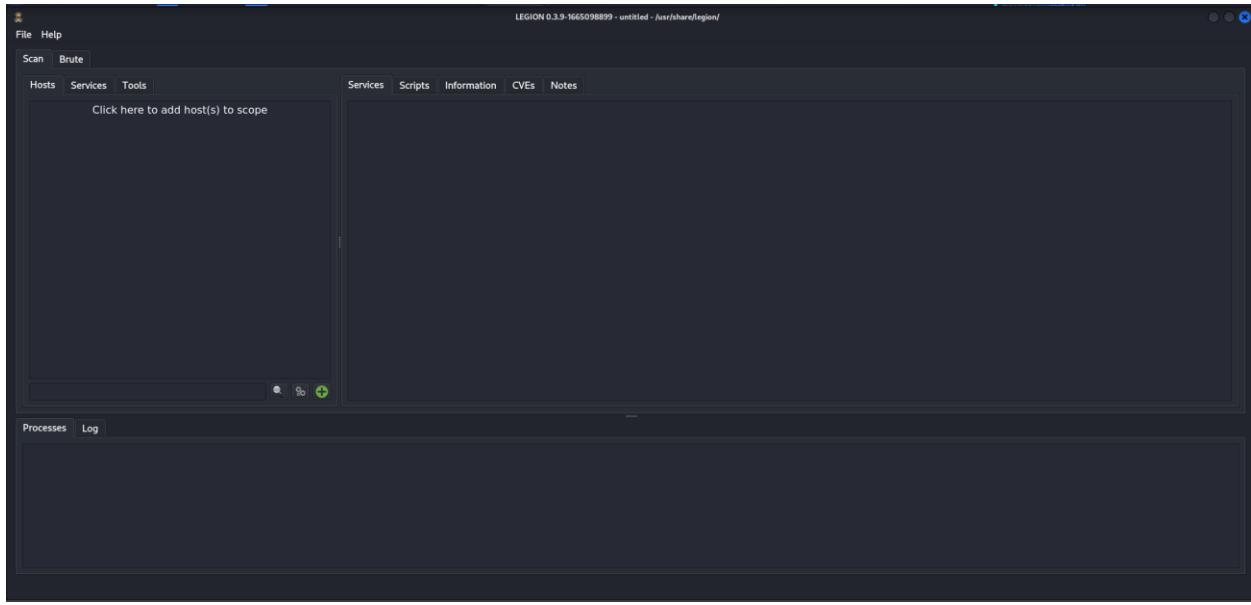
So, detecting those vulnerabilities can be done using the Vulnerability Detection tools.

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

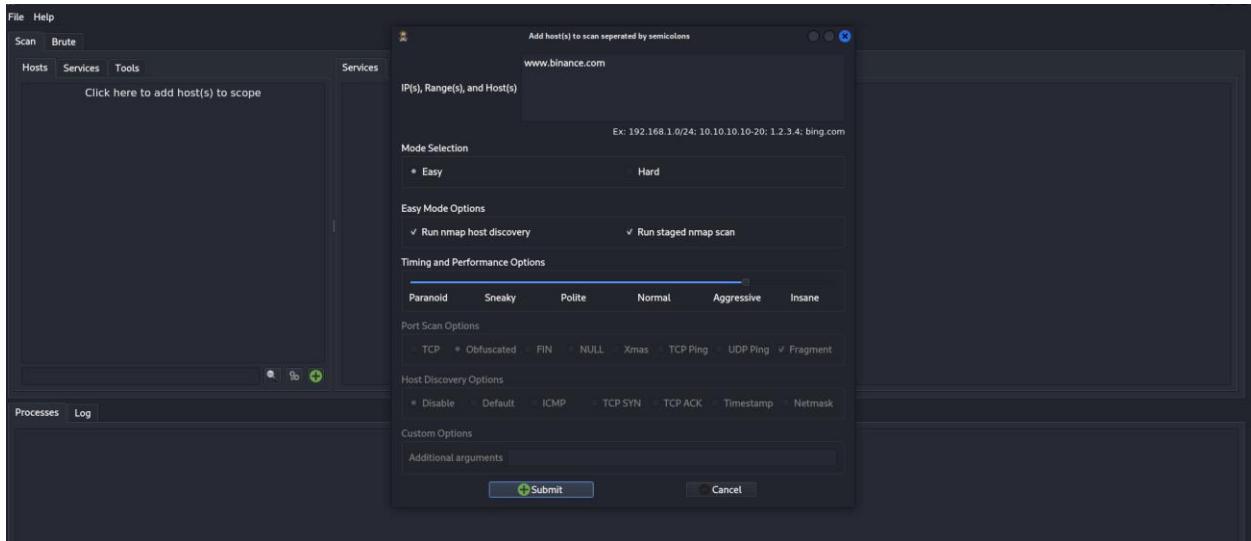
I choose that the most suitable vulnerability detection tool according to the gathered information and the usability of those tools. Because some of those tools are not freeware

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	Protocol	State	Name
21	tcp	open	tcpwrapped
80	tcp	open	tcpwrapped
443	tcp	open	tcpwrapped
554	tcp	open	tcpwrapped
1723	tcp	open	tcpwrapped

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
██████████	18.55s	0.00s	97748	nmap (stage 1)	www.binan...	Finished
██████████	1.67s	0.00s	97922	nmap (stage 2)	www.binan...	Finished
██████████	30.37s	0.00s	97983	nmap (stage 3)	www.binan...	Finished
██████████	0.00s	0.00s	0	screenshot (80/tcp)	52.84.150.65	Finished

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

```

root@kali:~/home/kali/Desktop]
# nikto -h binance.com -p 80
- Nikto v2.5.0

+ Multiple IPs found: 13.113.223.241, 54.249.159.43, 13.230.49.86
+ Target IP: 13.113.223.241
+ Target Port: 80
+ Target URI: binance.com
+ Target Port: 80
+ Start Time: 2024-04-24 15:03:43 (GMT+4)
+ Server: Apache/2.0
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header
+ Host header points to: https://www.binance.com:443
+ No CGI Directories found (use "-C all" to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: getaddrinfo problems (Temporary failure in name resolution): Resource temporarily unavailable
+ Scan terminated: 20 error(s) and 2 item(s) reported on remote host
+ End Time: 2024-04-25 00:17:02 (GMT+4) (33199 seconds)

+ 1 host(s) tested

```

- 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.

- 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, blindsqli, 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/ #
#####
/. 6.3

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

—(root@kali)-[~/home/kali/Desktop] nikto_binan...
# 
| Domain: https://www.binance.com/
| IP: 52.84.150.65
| 

PING
--- dobbmei4jnjlh.cloudfront.net - NetScanner
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

```
| NSLOOKUP  
|  
| Server: 192.168.43.1  
| Address: 192.168.43.1#53  
  
| Non-authoritative answer:  
| www.binance.com canonical name = dobbmei4jnjlh.cloudfront.net.  
| Authoritative answers can be found from:  
| dobbmei4jnjlh.cloudfront.net  
|     origin = ns-324.awsdns-40.com  
|     mail addr = awsdns-hostmaster.amazon.com  
|     serial = 1  
|     refresh = 7200  
|     retry = 900  
|     expire = 1209600  
|     minimum = 86400  
| dobbmei4jnjlh.cloudfront.net nameserver = ns-1364.awsdns-42.org.  
| dobbmei4jnjlh.cloudfront.net nameserver = ns-1620.awsdns-10.co.uk.  
| dobbmei4jnjlh.cloudfront.net nameserver = ns-324.awsdns-40.com.  
| dobbmei4jnjlh.cloudfront.net nameserver = ns-995.awsdns-60.net.  
| ns-324.awsdns-40.com internet address = 205.251.193.68  
| ns-995.awsdns-60.net internet address = 205.251.195.227  
| ns-1364.awsdns-42.org internet address = 205.251.197.84  
| ns-1620.awsdns-10.co.uk internet address = 205.251.198.84  
| ns-324.awsdns-40.com has AAAA address 2600:9000:5301:4400::1  
| ns-995.awsdns-60.net has AAAA address 2600:9000:5303:e300::1  
| ns-1364.awsdns-42.org has AAAA address 2600:9000:5305:5400::1  
| ns-1620.awsdns-10.co.uk has AAAA address 2600:9000:5306:5400::1  
| Name: dobbmei4jnjlh.cloudfront.net  
| Address: 52.84.150.36  
| Address: 52.84.150.48  
| Address: 52.84.150.65  
| Address: 52.84.150.52
```

Uniscan nmap report

```
NMAP
| Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-01 11:47 EDT
| NSE: Loaded 156 scripts for scanning.
| NSE: Script Pre-scanning.
| Initiating NSE at 11:47
| Completed NSE at 11:47, 0.00s elapsed
| Initiating NSE at 11:47
| Completed NSE at 11:47, 0.00s elapsed
| Initiating NSE at 11:47
| Completed NSE at 11:47, 0.00s elapsed
| Initiating Ping Scan at 11:47 testz nikto_binan...
| Scanning www.binance.com (52.84.150.48) [4 ports]
| Completed Ping Scan at 11:47, 0.03s elapsed (1 total hosts)
| Initiating Parallel DNS resolution of 1 host. at 11:47
| Completed Parallel DNS resolution of 1 host. at 11:47, 0.20s elapsed
| Initiating SYN Stealth Scan at 11:47
| Scanning www.binance.com (52.84.150.48) [1000 ports]
| Discovered open port 21/tcp on 52.84.150.48
| Discovered open port 554/tcp on 52.84.150.48
| Discovered open port 443/tcp on 52.84.150.48
| Discovered open port 1723/tcp on 52.84.150.48
| Discovered open port 80/tcp on 52.84.150.48
| Completed SYN Stealth Scan at 11:48, 11.77s elapsed (1000 total ports)
| Initiating Service scan at 11:48
| Scanning 5 services on www.binance.com (52.84.150.48)
| Completed Service scan at 11:48, 5.00s elapsed (5 services on 1 host)
| Initiating OS detection (try #1) against www.binance.com (52.84.150.48)
| Retrying OS detection (try #2) against www.binance.com (52.84.150.48)
| Initiating Traceroute at 11:48
| Completed Traceroute at 11:48, 0.02s elapsed
| Initiating Parallel DNS resolution of 2 hosts. at 11:48
| Completed Parallel DNS resolution of 2 hosts. at 11:48, 13.01s elapsed
| NSE: Script scanning 52.84.150.48.
| Initiating NSE at 11:48
| Completed NSE at 11:49, 32.25s elapsed
| Initiating NSE at 11:49
| Completed NSE at 11:49, 41.78s elapsed
| Initiating NSE at 11:49
| Completed NSE at 11:49, 0.00s elapsed
| Nmap scan report for www.binance.com (52.84.150.48)
| Host is up (0.0056s latency).
| Other addresses for www.binance.com (not scanned): 52.84.150.65 52.84.150.52 52.84.150.36
| Not shown: 995 filtered tcp ports (no-response)
| PORT      STATE SERVICE      VERSION
| 21/tcp    open  tcpwrapped
| 80/tcp    open  tcpwrapped
| |_http-title: Did not follow redirect to https://www.binance.com/
| 
60/tcp    open  tcpwrapped
| |_http-title: Did not follow redirect to https://www.binance.com/
| http-methods:
| |_ Supported Methods: OPTIONS
| |_ _Supported Methods: OPTIONS
443/tcp   open  tcpwrapped
ssl-cert Subject: commonName=*.binance.com/organizationName=Binance Holdings Limited/countryName=KY
Subject Alternative Name: DNS=*.binance.com, DNS=binance.com
Issuer: commonName=GeoTrust TLS RSA CA GI/organizationName=DigiCert Inc/countryName=US
Public Key type: RSA
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2024-01-11T00:00:00
Not valid after: 2025-02-10T23:59:59
MD5: 65b17d34bb37:cd6b79a1:f29fae60:c3d0
SHA-1: 9bda:1fbc:5db7:2c25:7e2d:84ea:f7f03:7a89:d7d5:c944
http-methods:
|_ _Supported Methods: OPTIONS
554/tcp   open  tcpwrapped
1723/tcp  open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: switch/bridge/general purpose/VoIP adapter
Running (JUST GUESSING): Cisco embedded (88%), Oracle Virtualbox (86%), QEMU (86%)
Aggressive OS guesses: Cisco Catalyst 1900 switch (88%), Oracle Virtualbox (86%), QEMU user mode network gateway (86%), Cisco ATA 188 VoIP adapter (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  2.58 ms 10.0.2.2
2  3.47 ms 52.84.150.48

NSE: Script Post-scanning.
| Initiating NSE at 11:49
| Completed NSE at 11:49, 0.00s elapsed
| Initiating NSE at 11:49
| Completed NSE at 11:49, 0.00s elapsed
| Initiating NSE at 11:49
| Completed NSE at 11:49, 0.00s elapsed
| Read data files from: /usr/bin/../share/nmap
| OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
| Nmap done: 1 IP address (1 host up) scanned in 111.82 seconds
| Raw packets sent: 2134 (99.340KB) | Rcvd: 36 (1.726KB)
```

File check report 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: sh... test2 nikto... 

PHP CGI Argument Injection:

Remote Command Execution:
  -drwxr-xr-x  2 root root 4096 Dec 15 10:20 binance.txt
  -rwxr--r--  1 root root  128 Dec 15 10:20 Netsparker... 

Remote File Include:

SQL Injection:
  -rwxr--r--  1 root root  128 Dec 15 10:20 nmap.txt
  -rwxr--r--  1 root root  128 Dec 15 10:20 binance2.txt
  -rwxr--r--  1 root root  128 Dec 15 10:20 Netsparker... 

Cross-Site Scripting (XSS):

Web Shell Finder:
  -rwxr--r--  1 root root  128 Dec 15 10:20 robots.txt

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:
  -rwxr--r--  1 root root  128 Dec 15 10:20 robots.txt
  -rwxr--r--  1 root root  128 Dec 15 10:20 nmap.txt

Remote Command Execution:

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

```

```

Check robots.txt:
[*] User-agent: Bairduspider
[*] User-agent: BaiduBot
[*] 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: */referringHistory
[*] Disallow: */tradingRules
[*] 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: */api/v1/test/
[*] 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: */user-support/feedback/
[*] Disallow: */fiat/deposit/result/order/
[*] Disallow: */bapi/

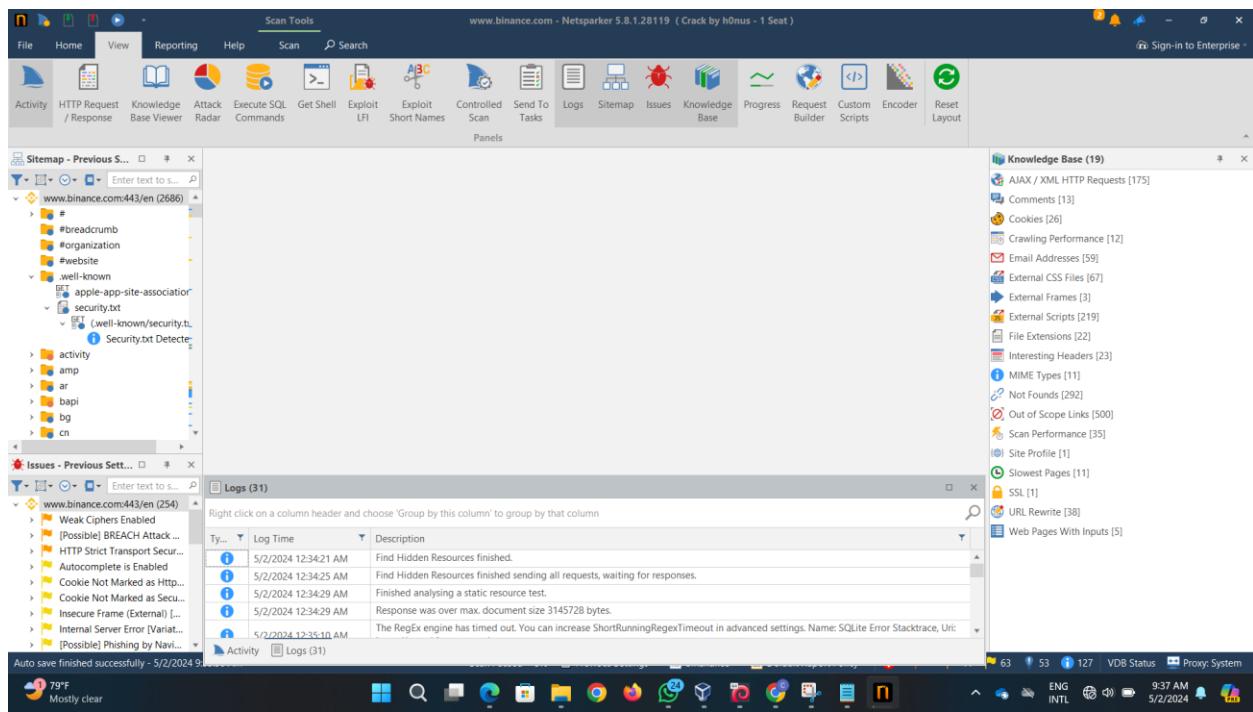
```

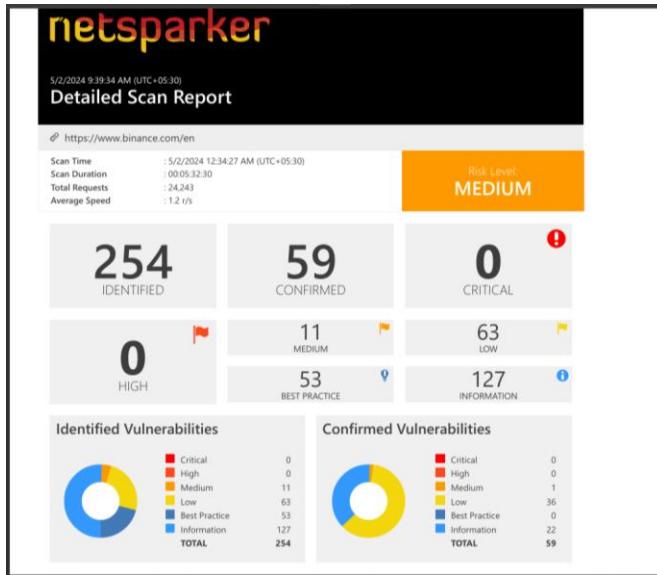
this is the scan result we can get from this tool. So, there are no vulnerabilities captured by this tool. But Nmap and other scan results are important to find vulnerabilities in the targeted system.

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.

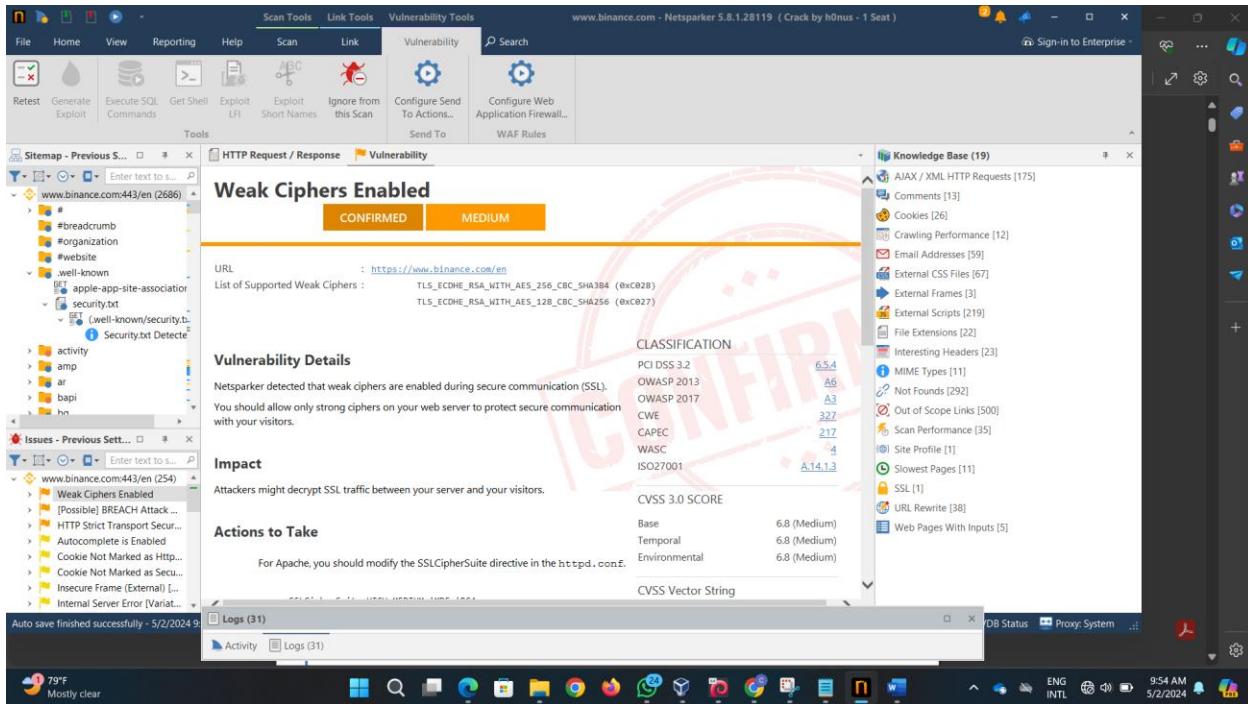
Netsparker typically provides a user-friendly interface for configuring scans, reviewing scan results, and generating detailed reports. It's often used by security professionals, penetration testers, and developers to identify and remediate security flaws in web applications before they can be exploited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





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/srp	
!	[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

- For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
- Lighttpd:
3.ssl.honor-cipher-order = "enable"
- ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
- 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	

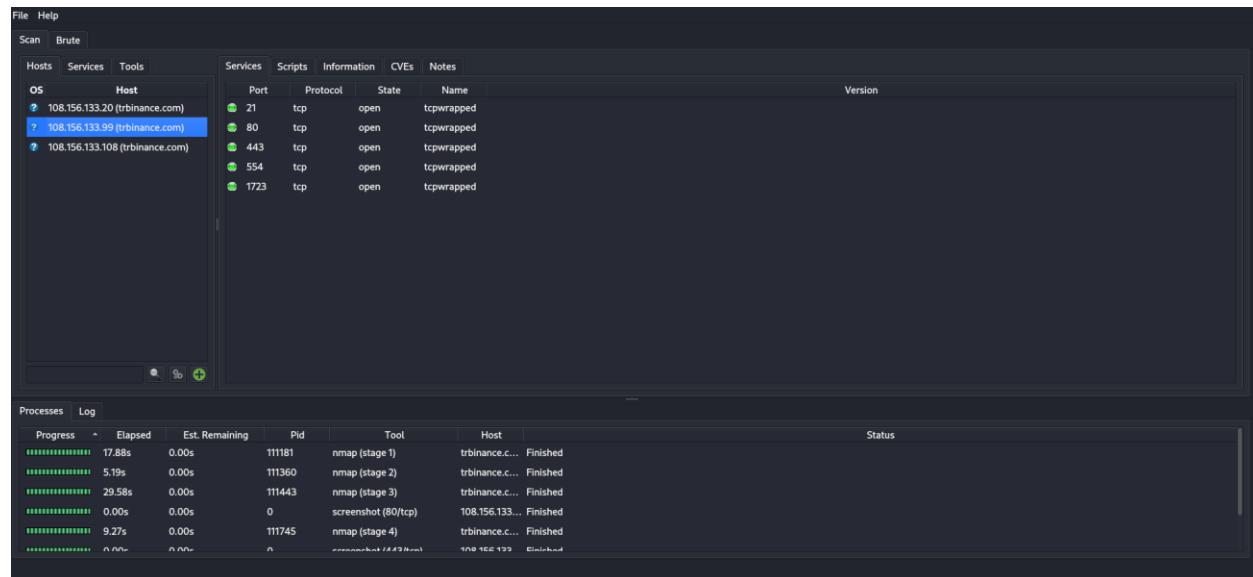
mitigation

- Configure your web server to disallow using weak ciphers.

Sub domain 02

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

Legion



Nikto

```
[root@kali] - /home/kali/Desktop
# nikto -h https://www.trbinance.com/
- Nikto v2.5.0

+ Multiple IPs found: 108.156.133.108, 108.156.133.99, 108.156.133.20, 108.156.133.22
+ Target IP: 108.156.133.108
+ Target Hostname: www.trbinance.com
+ Target Ports: 443

+ SSL Info: Subject: /CN=*.trbinance.com
    Ciphers: ECDHE-RSA-AES256-GCM-SHA384
    Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M03
+ Start Time: 2024-05-01 01:55:41 (GMT+0)

+ Server: Tengine
+ X-Frame-Options header was retrieved via header: 1.1 094f321aee7e1611835f5b53fa21a4,CloudFront.net (CloudFront).
+ The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-from-dispatcher' found, with contents: cloud-web-ui.
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The Content-Security-Policy 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /r/h7OyW.eml: Cookies lBBn_redirected created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /r/h7OyW.eml: Cookies lBBn_redirected created without the httpOnly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /r/h7OyW.eml: Cookies lBBn_redirected created without the path flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ No CGI Directories Found (use '-c.cgi' to force check all possible dirs)
+ Server.banner changed from 'Tengine' to 'CloudFront'
+ robots.txt contains no entries which should be mainly viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /robots.txt contains no entries which mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ Server is using a wildcard certificate: *.trbinance.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
+ /static/_cloud-web-ui/_cloud-tr/static/favicon.ico: Uncommon header 'x-amz-server-side-encryption' found, with contents: AES256.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:04000040:SSL routines::ssl3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 errors(s) and 13 items(s) reported on remote host
+ End Time: 2024-05-01 02:04:00 (GMT+0) (499 seconds)

+ 1 host(s) tested
```

- 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

```
[root@kali:~] /home/kali/Desktop
# wapiti -u https://www.trbinance.com/
[!] Connection error with URL https://www.trbinance.com/
[*] Saving scan state, please wait ...

Note
This scan has been saved in the file /root/.wapiti/scans/www.trbinance.com_folder_e54a7353.db
[*] Wapiti Found 0 URLs and Forms during the scan
[*] Loading modules:
    backup, blindsqli, 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...
Error downloading wapp database.

[*] Launching module csp
1 requests were skipped due to network issues

[*] Launching module http_headers
1 requests were skipped due to network issues

[*] Launching module cookieflags

[*] Launching module exec

[*] Launching module file

[*] Launching module sql
    balance3.db

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=450szv for results, please wait ...
[!] Unable to request endpoint URL 'https://wapiti3.ovh/'

[*] Launching module redirect

[*] Launching module blindsqli

[*] Launching module permanentxss
```

- 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 : 0:00:54.16	Total Requests : 25,169	Average Speed : 7.7 t/s	Risk Level: HIGH
---	----------------------------	-------------------------	-------------------------	-------------------------

216
IDENTIFIED
1 HIGH

56
CONFIRMED
2 MEDIUM
56 BEST PRACTICE

0
CRITICAL
81 LOW
76 INFORMATION

Identified Vulnerabilities

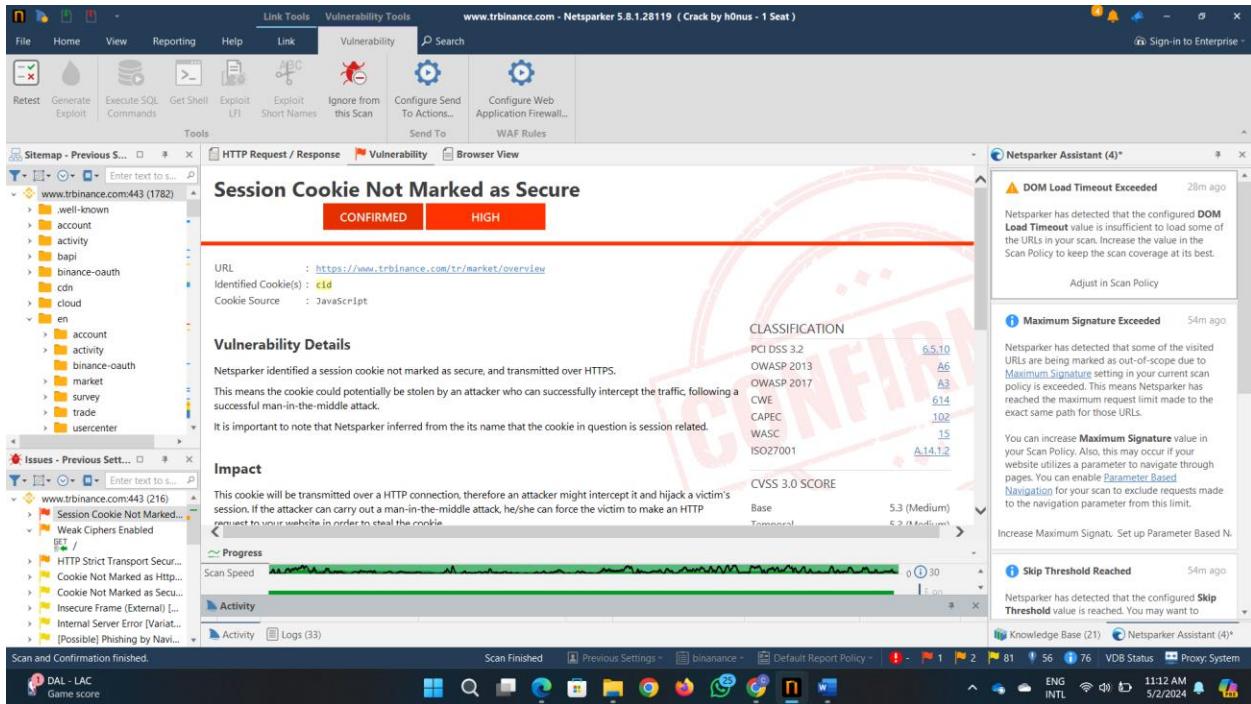

Critical	0
High	1
Medium	2
Low	81

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/?nssextt=%0d%0ans%3anetsp...rker056650%3dvuln	nssextt
!	[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/gel%C5%9fmeier/	
!	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.trbinance.com/tr/blog/gel%C5%9fmeier/?nssextt=%0d%0ans%3anetsparker056650%3dvuln	nssextt
!	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.trbinance.com/tr/blog/gel%C5%9fmeier/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

The screenshot shows the Nikto tool interface. At the top, there's a menu bar with File, Help, Scan, and Bruteforce. Below it is a toolbar with Scan, Services, Tools, Services, Scripts, Information, CVes, Notes, ftp-default (21/tcp), screenshot (80/tcp), and screenshot (443/tcp). A table below lists open ports and their details:

OS	Host	Port	Protocol	State	Name	Version
?	18.155.68.31 (academy.binance.co...)	21	tcp	open	ftp	
?	18.155.68.55 (academy.binance.co...)	80	tcp	open	http	Amazon CloudFront httpd
?	18.155.68.107 (academy.binance.co...)	443	tcp	open	http	Amazon CloudFront httpd
		554	tcp	open	tcpwrapped	
		1723	tcp	open	pptp	
		5060	tcp	open	sip	

Below this is a "Processes" tab showing the progress of the scan:

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
██████████	16.17s	0.00s	5440	nmap (stage 1)	academy.bi...	Finished
██████████	0.03s	0.00s	5598	nmap (stage 2)	academy.bi...	Finished
██████████	35.29s	0.00s	5651	nmap (stage 3)	academy.bi...	Finished
██████████	0.00s	0.00s	0	screenshot (80/tcp)	18.155.68.107	Finished
██████████	0.00s	0.00s	0	screenshot (443/tcp)	18.155.68.107	Finished
██████████	5.11s	0.00s	5600	nmap (stage 4)	academy.bi...	Finished

✓ Nikto

```
[root@kali] ~ /home/kali/Desktop]
# nikto -h https://www.trbinance.com/
- Nikto v2.5.0

+ Multiple IPs found: 108.156.133.22, 108.156.133.20, 108.156.133.108, 108.156.133.99
+ Target IP: 108.156.133.22
+ Target Hostname: www.trbinance.com
+ Target Port: 443

+ SSL Info: Subject: /CN=*.trbinance.com
Ciphers: TLS_AE_128_GCM_SHA256
Issued: /C=US/O=Amazon.com/OU=Amazon RSA 2048 M03
+ Start Time: 2024-05-01 08:07:47 (GMT-4)

+ Server: Tengine
+ X-Frame-Options header: 1.1 $2aa004537a7b0981b097483fcffbc. CloudFront.net (CloudFront).
+ The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-from-dispatcher' found, with contents: cloud-web-ui.
+ /: The site uses TLS, but the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /nXqcGmG.listprint: Cookie l10n_redirected created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /nXqcGmG.listprint: Cookie l10n_redirected created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /nXqcGmG.listprint: Header 'x-frame-options' found, with contents: plain.
+ No CGI Directories Found (was -t=1 to force check all possible dirs)
+ Server banner changed from 'Tengine' to 'CloudFront'.
+ /robots.txt contains 11 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ /robots.txt: The Content-Security-Policy header is set to 'none', leaving the server vulnerable to the BREACH attack. See: http://breachattack.com/
+ Server is using a wildcard certificate: *.trbinance.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
+ /static/cdn-web-ui/cloud-tr/static/favicon.ico: Uncommon header 'x-amz-server-side-encryption' found, with contents: AES256.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:04000410:SSL routines::ssl3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
+ At least one error was found.
+ at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 errors(s) and 13 items(s) reported on remote host
+ End Time: 2024-05-01 08:16:29 (GMT-4) (522 seconds)

+ 1 host(s) tested
```

- 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

```
(root㉿kali):~/home/kali/Desktop
# wapiti -u https://academy.binance.com/en


This scan has been saved in the file /root/.wapiti/scans/academy.binance.com_folder_0e768bc8.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
    backup, blindsqli, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe
[*] 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=0r104i for results, please wait ...
[*] Launching module redirect
[*] Launching module blindsqli
[*] Launching module permanentxss
Report
A report has been generated in the file /root/.wapiti/generated_report
Open /root/.wapiti/generated_report/academy.binance.com_05012024_0526.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 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

The screenshot shows the NetworkMiner interface. The top navigation bar includes 'File', 'Help', 'Scan', and 'Brute' buttons. Below the navigation is a tabs bar with 'Hosts', 'Services', 'Tools', 'Services' (selected), 'Scripts', 'Information', 'CVEs', and 'Notes'. A screenshot tab for port 80/tcp and 443/tcp is also present.

The main pane displays host information and service details:

OS	Host
?	13.33.88.17 (info.binance.com)
?	13.33.88.76 (info.binance.com)
?	13.33.88.112 (info.binance.com)

Port	Protocol	State	Name	Version
80	tcp	open	http	Amazon CloudFront httpd
443	tcp	open	http	Amazon CloudFront httpd

At the bottom, there are search, refresh, and add icons. The bottom navigation bar includes 'Processes' and 'Log' tabs, and a status bar indicating '.....'.

The 'Processes' tab shows the following table:

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
██████████	0.00s	0.00s	0	nmap (stage 2)	13.33.88.17	Finished
██████████	0.00s	0.00s	0	screenshot (443/tcp)	13.33.88.17	Finished
██████████	8.83s	0.00s	10066	nmap (stage 4)	info.binance...	Finished
██████████	9.65s	0.00s	10168	nmap (stage 5)	info.binance...	Finished
██████████	9.60s	0.00s	10262	nmap (stage 6)	info.binance...	Finished

Nikto

```
[root@kali] -/home/kali/Desktop
# nikto -h https://www.binance.com/en/price
- Nikto v2.5.8

Multiple IPs found: 52.84.150.52, 52.84.150.48, 52.84.150.65, 52.84.150.36
+ Target IP: 52.84.150.52
+ Target Hostname: www.binance.com
+ Target Port: 443
+ SSL Info: Subject: /C=KY/L=GEOGE TOWN/O=Binance Holdings Limited/CN=*.binance.com
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=GeoTrust TLS RSA CA G1
+ Start Time: 2024-05-01 00:38:04 (GMT-4)

Server: Tengine
+ /en/price/: Cookie theme created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /en/price/: Cookies them created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /en/price/: Uncommon header 'x-ua-compatible' found, with contents: 'ie=edge'.
+ /en/price/: Uncommon header 'x-cache-proxy-rtt' found, with contents: 'www-default-net'.
+ /en/price/: Uncommon header 'x-cluster-id' found, with contents: '9a092c78ffda4e8ff6477432b9ecb93'.
+ /en/price/: Uncommon header 'x-forwarded-for' found, with contents: '10.0.0.1'.
+ /en/price/: Uncommon header 'x-envoy-decorator-operation' found, with contents: 'cache-proxy.cache-proxy.svc.cluster.local:80+'.
+ /en/price/: Uncommon header 'x-cache-proxy-key' found, with contents: 'cpu2_gzip_79d9c37f663b7190ea5e49e2b1b78728'.
+ /en/price/: Uncommon header 'x-service-name' found, with contents: 'se-u1'.
+ /en/price/: Uncommon header 'x-traffik-id' found, with contents: '10000000000000000000000000000000'.
+ /en/price/: Uncommon header 'x-trace-id' found, with contents: '30'.
+ No CGI Directories found (use '-C.cgi' to force check all possible dirs)
- ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000418:SSL routines::sslv3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
at /var/lib/nikto/plugins/LW2.pm line 5254.
- ERROR: Error limit (20) reached for host, giving up. Last error:
+ : Server banner changed from 'Tengine' to 'Cloudfront'.
- ERROR: Error limit (20) reached for host, giving up. Last error:
+ /en/price/: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
- ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 18 target(s) and 15 item(s) reported on remote host
+ End Time: 2024-05-01 00:54:08 (GMT-4) (964 seconds)

+ 1 host(s) tested
```

- 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



Kali Linux
"the quieter you become, the more you are able to hear"

```
Court@kali:~/home/kali/Desktop
└─# wapiti -u https://www.binance.com/en/price
[!] Saving scan state, please wait...
Note: This scan has been saved in the file /root/.wapiti/scans/www.binance.com_folder_352de991.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
    backup, blindsqli, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe
[*] 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 Content-Security-Policy-Options :
Content-Security-Policy-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=pnw10s for results, please wait ...
[*] Launching module redirect
[*] Launching module blindsqli
[*] Launching module permanentxss
Report
A report has been generated in the file /root/.wapiti/generated_report
Open /root/.wapiti/generated_report/www.binance.com_05012024_0535.html with a browser to see this report.
```

- 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.

[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:

- Inject partial plaintext they have uncovered into a victim's requests

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

CVSS3.0:AV:N/AC:L/PR:N/UI:R/S:U/CH:L/N:A/N

CVSS 3.1 SCORE

Base	6.5 (Medium)
Temporal	6.5 (Medium)
Environmental	6.5 (Medium)

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 Found [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-cryptotrading-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

The screenshot shows the Nikto application interface. The main window has tabs for Scan, Brute, Hosts, Services, Scripts, Information, CVEs, and Notes. The Services tab is active, displaying a table of open ports and their corresponding protocols and names. The Processes tab shows the status of multiple concurrent scans.

Port	Protocol	State	Name
21	tcp	open	tcpwrapped
80	tcp	open	tcpwrapped
443	tcp	open	tcpwrapped
554	tcp	open	tcpwrapped
1723	tcp	open	tcpwrapped

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
34.61s	0.00s	11435	nmap (stage 3)	coinmarket...	Finished	
0.00s	0.00s	0	screenshot (80/tcp)	13.35.18.71	Finished	
0.00s	0.00s	0	screenshot (443/tcp)	13.35.18.71	Finished	
9.75s	0.00s	11772	nmap (stage 4)	coinmarket...	Finished	
8.84s	0.00s	11883	nmap (stage 5)	coinmarket...	Finished	

Nikto

```
[root@kali] - /home/kali/Desktop/
└─# nikto -h https://coinmarketcap.com/
- Nikto v2.5.0

+ Multiple IPs found: 13.35.18.61, 13.35.18.48, 13.35.18.71, 13.35.18.59
+ Target IP: 13.35.18.61
+ Target Hostname: coinmarketcap.com
+ Target Port: 443
+ SSL Info: Subject: /CN=coinmarketcap.com
    Ciphers: ECDHE-RSA-AES128-GCM-SHA256
    Issuer: /C=US/O=Amazon/CN=Amazon RSA 2048 M01
+ Start Time: 2024-05-01 01:21:27 (GMT+0)

+ Server: Tengine
+ /: Retrieved via header: 1.1 ae495479ab1766473f411ebddd0ba98.cloudflare.net (CloudFront).
+ /: Uncommon header 'x-envoy-upstream-service-time' found, with contents: 2.
+ /: Uncommon header 'x-cache-proxy-key' found, with contents: cpv2_gzip_idc69732b0af8ee839620e644d6262bc.
+ /: Uncommon header 'x-turbine-id' found, with contents: 1.
+ /: Uncommon header 'x-traefik-route' found, with contents: coinmarketcap-next.
+ /: Uncommon header 'x-envoy-decorator-operation' found, with contents: cache-proxy.cache-proxy-v2.svc.cluster.local:80/.
+ /cgi-bin/: Uncommon header 'refresh' found, with contents: @url/cgi-bin.cgi.
+ No CGI directories found. You will need to force check all possible dirs.
+ robots.txt: Found 9 entries which should be checked.
+ : Server banner changed from 'Tengine' to 'CloudFront'.
+ 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misconfigurations/x-content-type-options-header/
+ The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::sslv3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
at /var/lib/nikto/plugins/LW2.pm line 5254.
+ Total time: 20 seconds (11.111111111111111 seconds), reported on remote host
+ End Time: 2024-05-01 01:27:23 (GMT+0) (359 seconds)
+ 1 host(s) tested
```

- 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

Screenshot of the Netsparker Enterprise interface showing a security scan of coinmarketcap.com.

Scan Details: coinmarketcap.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)

Tools Bar: File, Home, View, Reporting, Help, Scan Tools, Link Tools, Vulnerability Tools, Vulnerability, Scan, Link, Configure Send To Actions..., Configure Web Application Firewall..., WAF Rules.

Left Panel: Sitemap - Previous Sett... (412 issues), coinmarketcap.com:443 (104 issues), Weak Ciphers Enabled (CONFIRMED, MEDIUM).

Middle Panel:

- Weak Ciphers Enabled** (CONFIRMED, MEDIUM):
 - URL: <https://coinmarketcap.com/>
 - List of Supported Weak Ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028) and 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.
 - CVSS 3.0 SCORE:** Base: 6.8 (Medium), Temporal: 6.8 (Medium), Environmental: 6.8 (Medium).
 - CVSS Vector String:** CVSS:3.0/AV:N/AC:L/PR:H/C:L/I:L/A:L

Right Panel: Knowledge Base (21) (AJAX / XML, HTTP Requests [43], Comments [501], Cookies [8], Crawling Performance [3], Email Addresses [3], External CSS Files [23], External Frames [1], External Scripts [180], File Extensions [5], Form Validation Errors [1], Interesting Headers [11], JavaScript Files [4], MIME Types [13], Not Found [76], Out of Scope Links [500], Scan Performance [35], Site Profile [1], Slowest Pages [10], SSL [1], URL Rewrite [42], Web Pages With Inputs [3]).

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.in	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	

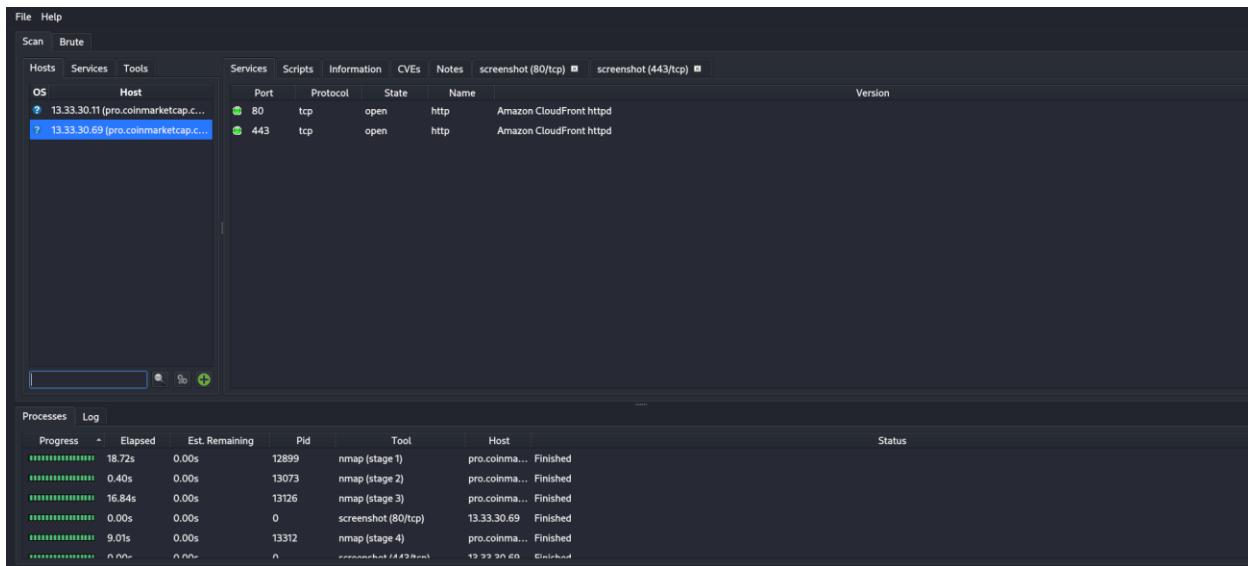
mitigation

- Configure your web server to disallow using weak ciphers

Sub domain 06

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

Legion



Nikto

```
(root@kali):~/home/kali/Desktop
└─# nikto -h https://pro.coinmarketcap.com/
  Nikto v2.5.0

+ Multiple IPs found: 18.155.68.31, 18.155.68.43, 18.155.68.59, 18.155.68.22
+ Target IP:   18.155.68.31
+ Target Hostname: pro.coinmarketcap.com
+ Target Port:  443

+ SSL Info:   Subject: /CN=coinmarketcap.com
              Ciphers: ECDHE-RSA-AES128-GCM-SHA256
              Issuer: /C=US/O=DigiCert/CN=DigiCert RSA 2048 M01
+ Start Time: 2024-05-01 01:24:44 (GMT-4)

+ Server: Tengine
+ /: Retrieved via header 'x-traejk-route' found, with contents: coinmarketcap-portal.
+ /: Uncommon header 'x-envoy-decorator-service-time' found, with contents: 8.
+ /: Uncommon header 'x-envoy-upstream-service-time' found, with contents: 8.
+ No CGI Directories found (use --list-cgi to check all possible dirs)
+ Server banner changed from 'Tengine' to 'CloudFront'.
+: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misconfig-content-type-header/
+: The Content-Type-Header header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ Hostname 'pro.coinmarketcap.com' does not match certificate's names: coinmarketcap.com. See: https://cwe.mitre.org/data/definitions/297.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A00041B:SSL routines::sslv3 alert handshake failure at /var/lib/nikto/plugins/lW2.pm line 5254.
at /var/lib/nikto/plugins/lW2.pm line 5254.
+ Scan terminated: 19 errors(s) and 8 item(s) reported on remote host
+ End Time: 2024-05-01 01:30:50 (GMT-4) (366 seconds)

+ 1 host(s) tested
```

- 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

```
(root㉿kali)-[~/home/kali/Desktop]
└─# wapiti -u https://pro.coinmarketcap.com



[*] Wapiti found 27 URLs and forms during the scan
[*] Loading modules:
    backup, blindsqli, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe
[*] Launching module csp
CSP is not set
[*] Launching module http_headers
Checking X-Frame-Options :
OK
Checking Content-Security-Policy :
OK
Checking X-XSS-Protection :
OK
Checking X-Content-Type-Options :
OK
Checking Strict-Transport-Security :
OK
[*] Launching module cookieflags
[*] Launching module exec
[*] 17 pages were previously attacked and will be skipped
[*] Launching module file
[*] Launching module sql
[*] Launching module xss
[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=4q8p7d for results, please wait ...
[*] Launching module redirect
[*] Launching module blindsqli
[*] Launching module permanentxss

Report
A report has been generated in the file /root/.wapiti/generated_report
Open /root/.wapiti/generated_report/pro.coinmarketcap.com_05012024_0603.html with a browser to see this report.

```

- 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

The screenshot shows the Legion interface. At the top, a navigation bar includes File, Help, Scan, and Brute. Below it is a table for hosts and services. The table has columns for OS, Host, Port, Protocol, State, Name, and Version. Two hosts are listed: 108.157.254.65 (binance.us) and 108.157.254.82 (binance.us). Both are marked as open on port 80 (http) and port 443 (http). In the bottom half of the interface, there's a Processes tab showing a list of tasks with progress bars. One task, 'nmap', is shown with a progress of 18.62s, while others like 'nmap (stage 1)' have 0.00s.

Nikto

```
(root@kali): /home/kali/Desktop
└─# nikto -h https://www.binance.us/
- Nikto v2.5.0

+ Multiple IPs found: 108.157.254.58, 108.157.254.65, 108.157.254.82, 108.157.254.76
+ Target IP: 108.157.254.58
+ Target Hostname: www.binance.us
+ Target Port: 443

+ SSL Info:
  Subject: /C=US/ST=California/L=Palo Alto/O=BAM TRADING SERVICES INC./CN=*.binance.us
  Ciphers: ECDHE-RSA-AES_128-GCM-SHA256
  ISSUED BY: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=GeoTrust TLS RSA CA G1
+ Start Time: 2024-05-01 01:25:12 (GMT+4)

+ Server: No Server header retrieved
+ Retrieved via header: 1.1 0909a7a07bd63ce0fab7d5d8ab8f6eaa.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misconfiguring-x-content-type-options/
+ /ImdbR13.blt: Uncommon header 'x-amz-server-side-encryption' found, with contents: AES256.
+ No CGI Directories Found (use -c all to force check all possible dirs)
+ /gateway/api/v1/item/byPasscode/product/getProduct/getProducts: Retrieved access-control-allow-origin header: +
+ /product-api/v1/friendly/api/v1/markets/product/get-products/: It returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 8 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ : Server banner changed from 'AmazonS3' to 'CloudFront'.
+ /: The Content-Security-Policy header "upgrade-insecure-requests" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ Server uses a wildcard certificate: *.binance.us. See: https://en.wikipedia.org/wiki/Wildcard_certificate
+ ERROR: Error limit (20) reached for host, giving up. last error: opening stream can't connect: SSL negotiation failed: error:0A00010B:SSL routines::ssl3 alert handshake failure at /var/lib/nikto/plugins/LW2.pm line 5254.
+ /: /var/lib/nikto/plugins/LW2.pm line 5254.
+ Scan terminated: 20 errors(s) and 0 items(s) reported on remote host
+ End Time: 2024-05-01 01:26:54 (GMT+4)
+ 1 host(s) tested
```

- 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

The screenshot shows the Wapiti tool interface. At the top, a terminal window displays the command: `wapiti -u https://www.binance.us/`. Below the terminal is a large banner for "KALI LINUX" with the tagline "the quieter you become, the more you are able to hear". The main area contains the Wapiti scan report for the Binance website. The report lists various security findings:

- Wapiti-3.0.4 (wapiti.sourceforge.io)
- Wapiti Found 34 URLs and forms during the scan
- Loading modules: backup, blindsqli, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe
- 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 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
(*) 6 pages were previously attacked and will be skipped
- Launching module file
(*) 5 pages were previously attacked and will be skipped
- Launching module sql
- Launching module xss
- Launching module ssrf
(*) Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=19y4hd for results, please wait ...
- Launching module redirect
- Launching module blindsqli
- Launching module permanentxss

At the bottom of the report, it says: "[*] Launching module permanentxss". Below that is a "Report" section with the message: "A report has been generated in the file /root/.wapiti/generated_report Open /root/.wapiti/generated_report/www.binance.us_05012024_0659.html with a browser to see this report."

- 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

The screenshot shows the Legion interface. At the top, there's a navigation bar with 'File', 'Help', 'Scan', and 'Brute' tabs. Below it is a 'Hosts' tab with two entries: '108.157.254.21 (c2c.binance.com)' and '108.157.254.119 (c2c.binance.com)'. The main panel displays a table of open ports:

Port	Protocol	State	Name
21	tcp	open	tcpwrapped
80	tcp	open	tcpwrapped
443	tcp	open	tcpwrapped
554	tcp	open	tcpwrapped
1723	tcp	open	tcpwrapped

Below this is a 'Processes' tab showing the status of various tools:

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
18.52s	0.00s	101890	nmap (stage 1)	c2c.binance...	Finished	
0.38s	0.00s	102078	nmap (stage 2)	c2c.binance...	Finished	
34.65s	0.00s	102142	nmap (stage 3)	c2c.binance...	Finished	
0.00s	0.00s	0	screenshot (80/tcp)	108.157.25...	Finished	
0.00s	0.00s	0	screenshot (443/tcp)	108.157.25...	Finished	
44.70s	0.00s	0	Nikto	c2c.binance...	Completed	

Nikto

```
root@kali:~/Desktop
# curl https://c2c.binance.com/en
Nikto v2.5.0

Multiple IPs Found: 13.33.30.25, 13.33.30.17, 13.33.30.123, 13.33.30.75
Target IP: 13.33.30.25
Target Hostname: c2c.binance.com
Target Port: 443

SSL Info:
  Subject: /C=KY/L=GEORGE TOWN/O=Binance Holdings Limited/CN=*.binance.com
  Ciphers: TLS_AES_128_GCM_SHA256
  Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/N=GeoTrust TLS RSA CA G1
  Start Time: 2024-05-01 14:01:50 (GMT-4)

  Server: Tengine
  /en/: Cookie name created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
  /en/: Cookie name created without the http-only flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
  /en/: Setting a cookie with ETag=62489494-0000-0000-0000-5e5623f110000000000000000000000000000000000000000000000000000000
  /en/: Uncommon header 'x-envoy-decorator-operation' found, with contents: cache-proxy.cache-proxy.svc.cluster.local:80/
  /en/: Uncommon header 'x-envoy-forward-path' found, with contents: true
  /en/: Uncommon header 'x-envoy-headers' found, with contents: Bit
  /en/: Uncommon header 'x-envoy-service-name' found, with contents: c2c-user-ui
  /en/: Uncommon header 'x-traefik-duration' found, with contents: 4.00
  /en/: Uncommon header 'x-traefik-proxyprefix' found, with contents: /c2c-default-ui
  /en/: Uncommon header 'x-cluster-info' found, with contents: fe-can-1
  /en/: Uncommon header 'x-envoy-upstream-service-time' found, with contents: 4.00
  /en/: No Content-Type header was set. This could allow the user agent to render the content in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
  /en/: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-options-header/
  /en/: Server is using a wildcard certificate: *.binance.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
  ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error:0A000410:SSL routines::sslv3 alert handshake failure at /var/lib/nikto/plugins/lm2.pm line 5254.
at /var/lib/nikto/plugins/lm2.pm line 5254.
  Scan terminated (19 errors) and 17 item(s) reported on remote host
End Time: 2024-05-01 14:05:34 (GMT-4) (224 seconds)
1 host(s) tested
```

- 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

```

root@kali:~/Desktop
└─# wapiti -u https://c2c.binance.com/en

[!] Launching module csp_header
[!] Launching module http_headers
[!] 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=5c6565 for results, please wait ...
[!] Launching module redirect
[!] Launching module blindsqli
[!] Launching module blindsqli
[!] Launching module permanentxss
Report
A report has been generated in the file /root/.wapiti/generated_report
Open /root/.wapiti/generated_report/c2c.binance.com_05012024_1803.html with a browser to see this report.

```

- 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

The Legion interface displays a scan results table and a process log table.

Scan Results Table:

OS	Host
?	52.84.150.36 (support.binance.com)
?	52.84.150.48 (support.binance.com)

Process Log Table:

Progress	Elapsed	Est. Remaining	Pid	Tool	Host	Status
██████████	17.57s	0.00s	104619	nmap (stage 1)	support.bin...	Finished
██████████	2.30s	0.00s	104790	nmap (stage 2)	support.bin...	Finished
██████████	21.61s	0.00s	104870	nmap (stage 3)	support.bin...	Finished
██████████	0.00s	0.00s	0	screenshot (80/tcp)	52.84.150.36	Finished
██████████	14.02s	0.00s	105091	nmap (stage 4)	support.bin...	Finished
██████████	0.00s	0.00s	0	screenshot (443/tcp)	52.84.150.36	Finished

Nikto

```
# ./nikto -n https://support.binance.com/
 Nikto v2.5.0

Multiple IPs found: 52.84.150.36, 52.84.150.52, 52.84.150.48, 52.84.150.65
 Target IP: 52.84.150.36
 Target Hostname: support.binance.com
 Target Port: 443

SSL Info: Subject: /-KYL-GEORGE TOWN/0-Binance Holdings Limited/CN=*.binance.com
Ciphers: TLS_AES_128_GCM_SHA256
Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/N=GeoTrust TLS RSA CA G1
Start Time: 2024-05-01 14:18:23 (GMT-4)

Server: Tengine
/: Retrieved via header: 1.1 cloud8c2634c5d977a3ab7f53a-cloudfront.net (CloudFront).
No CGI Directives to: https://www.binance.com/en/support/
No CGI Directories Found (use '-C all' to force check all possible dirs)
/robots.txt: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/robots.txt: Set Content-Type header to 'CloudFront'.
/robots.txt: contains 67 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
Server is using a wildcard certificate: *.binance.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
ERROR: Error in init (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: error@0000410:SSL routines::sslv3 alert handshake failure at /var/lib/nikto/plugins/tW2.pm line 5254.
at /var/lib/nikto/plugins/tW2.pm line 5254.
Scan terminated: 20 error(s) and 5 item(s) reported on remote host
End Time: 2024-05-01 14:23:38 (GMT-4) (315 seconds)

1 host(s) tested
```

- 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

```
(root㉿kali)-[~/home/kali/Desktop]
# wapiti -u https://support.binance.com/
[!] Wapiti found 1 URLs and forms during the scan
[*] Saving scan state, please wait...
Note
This scan has been saved in the file /root/.wapiti/scans/support.binance.com_Folder_519a549f.db
Check the content of the file in a different fashion to the WAPi type, see: https://www.rapidapi.com/document/wapiti

[*] Loading modules:
    backup, blindsqli, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, wapp, xss, xxe

[*] Launching module csp
CSP is not set

[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options 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=w12j79 for results, please wait...

[*] Launching module redirect

[*] Launching module blindsqli

[*] Launching module blindsqli
[*] Launching module permanentxss

Report
A report has been generated in the file /root/.wapiti/generated_report
Open /root/.wapiti/generated_report/support.binance.com_05012024_1804.html with a browser to see this report.
```

- 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

The screenshot shows the Legion interface with two main panels. The left panel displays a network scan results table with columns for OS, Host, Port, Protocol, State, and Name. It lists several open ports (21, 80, 443, 554, 1723) on hosts 35.77.182.129 and 54.95.67.67. The right panel shows a process log table with columns for Progress, Elapsed, Est. Remaining, Pid, Tool, Host, and Status. The log shows the execution of nmap (stage 1, 2, 3) and screenshots (80/tcp, 443/tcp) which have all completed successfully.

Nikto

```
(root@kali)-[~/home/kali/Desktop] ↵ nikto -h https://account.binance.com/
- Nikto v2.5.0

+ Multiple IPs found: 54.95.67.67, 35.77.182.129, 54.249.140.131
+ Target IP:      54.95.67.67
+ Target Hostname: account.binance.com
+ Target Port:    443

+ SSL Info:      Subject: /C=KY/L=GEORGE TOWN/O=Binance Holdings Limited/CN=*.binance.com
                  Ciphers: ECDHE-RSA-AES128-GCM-SHA256
                  Issuer: /C=US/O=DigiCert Inc/OU=www.digicert.com/CN=GeoTrust TLS RSA CA G1
+ Start Time:    2024-05-01 13:52:38 (GMT-4)

+ Server: Tengine (Ubuntu 20.04.6 LTS) /nginx/1.18.0
+ Root page / redirects to: https://www.binance.com/en
+ : Server banner changed from 'Tengine' to 'awselb/2.0'.
+ ./KMLZJdh.sh: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server is using a wildcard certificate: *.binance.com. See: https://en.wikipedia.org/wiki/Wildcard_certificate
- STATUS: Completed 2150 requests (~31% complete, 1.9 hours left): currently in plugin 'Nikto Tests'
```

- 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

```
[root@kali] ~ /home/kali/Desktop
# wapiti -u https://account.binance.com/
[!] Wapiti-3.0.4 (wapiti.sourceforge.io) https://sourceforge.net/projects/wapiti/files/Wapiti%203.0.4/wapiti-3.0.4.tar.gz
[*] Saving scan state, please wait...
Note
This scan has been saved in the file /root/.wapiti/scans/account.binance.com_folder_c231e008.db
[*] Wapiti found 1 URLs and forms during the scan
[*] Loading modules:
    backup, blindsqli, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe
[*] Launching module csp
CSP is not set
[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking 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=ui3pt5 for results, please wait ...
[*] Launching module redirect
[*] Launching module blindsqli
[*] Launching module permanentxss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=ui3pt5 for results, please wait ...
[*] Launching module redirect
[*] Launching module blindsqli
[*] Launching module permanentxss

Report
A report has been generated in the file /root/.wapiti/generated_report
Open /root/.wapiti/generated_report/account.binance.com_05012024_1815.html with a browser to see this report.
```

- 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

- [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:
1] <https://www.helpnetsecurity.com/2021/09/24/owasp-top-10-2021/>.
- [O. Foundation, "OWASP Top Ten," [Online]. Available: <https://owasp.org/www-project-top-ten/>.
2
]
3
]
- ["bugcrowd," [Online]. Available: <https://bugcrowd.com/binance>.
3
]
4
- [S. Rahalkar, " Network Vulnerability Assessment," [Online]. Available:
4] <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..>
- ["Sublist3r," [Online]. Available: <https://www.kali.org/tools/sublist3r/>.
5
]
6
- [C. P. S. T. Ltd., "Cyber Hub Secure The Cloud Application Security (AppSec): Threats, Tools, and Techniques OWASP Top 10 Vulnerabilities," [Online]. Available:
6] <https://www.checkpoint.com/cyber-hub/cloud-security/what-is-application-security-appsec/owasp-top-10-vulnerabilities/>.