

Sri Lanka Institute of Information Technology



**Sri Lanka Institute of
Information Technology**

IE2072 – WEB SECURITY

Year 2, Semester 2

(Assignment – Individual)-2023

Bug Bounty vulnerabilities scanning Report 1

Student Register Number	Student Name
IT21167096	DE ZOYSA A.S.

Binance (Cryptocurrency Exchange)

The screenshot shows the Bugcrowd interface for the Binance security program. At the top, the Bugcrowd logo and navigation links are visible. The main content area features the Binance logo and program details: "Cryptocurrency Exchange", a reward of "\$200 - \$10,000 per vulnerability", a maximum reward of "Up to \$100,000", and "Partial safe harbor". A "Submit report" button is present. Below this, there are tabs for "Program details", "Announcements", "CrowdStream", and "Hall of Fame". A section titled "For security issues related to cryptocurrencies and their components ONLY:" provides instructions on how to report a security issue. Another section titled "Non-security related issues:" provides instructions on how to report a non-security issue. A sidebar on the right displays statistics: "Vulnerabilities rewarded: 320", "Validation within: 2 days", and "75% of submissions are accepted or rejected within 2 days". At the bottom of the sidebar, there is a "Latest hall of famers" section with circular profile pictures of participants.

Binance
Cryptocurrency Exchange

🏆 \$200 - \$10,000 per vulnerability 🏆 Up to \$100,000 maximum reward 🛡️ Partial safe harbor

[Submit report](#)

[Program details](#) [Announcements](#) [CrowdStream](#) [Hall of Fame](#)

[Tweet](#) [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 number one cryptocurrency exchange, operating in many places throughout the world. Specializing in crypto-to-crypto transactions, we provide access to hundreds of digital currency pairs. As a leading exchange platform, we prioritize security, liquidity, and speed, while maintaining some of the lowest

Vulnerabilities rewarded
320

Validation within
2 days
75% of submissions are accepted or rejected within 2 days

Latest hall of famers

• Overview

Binance is the top cryptocurrency exchange and is present all over the world. With a focus on crypto-to-crypto exchanges, we give users access to thousands of digital currency pairs. We prioritize security, liquidity, and speed as a top exchange platform while also keeping some of the lowest costs in the business. With new cryptocurrencies being listed often, we work to provide our consumers with the greatest experience possible. We also provide them access to some of the most cutting-edge blockchain and DLT technology.

"Binary Finance" is the abbreviation for Binance, which combines digital technology with finance. We are digital currency aficionados, as the name implies, and have more than 20 years of combined expertise in finance, security, and development at leading exchange platforms and businesses, such as the Tokyo Stock Exchange, Morgan Stanley, Accenture, and other Top 100 companies from all over the world.

Scope of the security audit according to <https://bugcrowd.com/binance> is as follows,

Target Information:

Primary Targets - Eligible for bounty from P4 and above

- ✓ *.binance.com (with exceptions, refer to Secondary Targets)
- ✓ api.binance.com
- ✓ binance.us
- ✓ *.bnbchain.org
- ✓ dex.binance.org
- ✓ BNB Beacon Chain
- ✓ BNB Beacon Chain Documentation
- ✓ BNB Beacon Chain Github repositories in scope
- ✓ Binance Wallet - Chrome and Firefox extensions
- ✓ BNB Smart Chain
- ✓ BNB Smart Chain Github repositories in scope
- ✓ Binance Mobile Application for Android
- ✓ Binance Mobile Application for iOS
- ✓ Binance Desktop Application
- ✓ Binance macOS Application
- ✓ Binance Connect

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

- Scope and rewards

In Scope

- ✓ *.binance.com
- ✓ api.binance.com
- ✓ *.bnbchain.org
- ✓ dex.binance.org
- ✓ BNB Beacon Chain
- ✓ binance.us
- ✓ Binance Mobile Application for Android
- ✓ Binance Mobile Application for iOS
- ✓ Binance Desktop Application
- ✓ Binance macOS Application
- ✓ <https://github.com/bnb-chain/tss-lib>
- ✓ <https://github.com/bnb-chain/bep3-smartcontracts>
- ✓ <https://github.com/bnb-chain/bep3-deputy>
- ✓ <https://github.com/bnb-chain/ledger-app-binance>
- ✓ Trustwallet Android App
- ✓ Trustwallet iOS App
- ✓ <https://github.com/trustwallet/wallet-core/>
- ✓ BNB Smart Chain
- ✓ <https://github.com/bnb-chain/bsc-genesis-contract>
- ✓ <https://github.com/bnb-chain/bsc-relayer>
- ✓ <https://github.com/bnb-chain/oracle-relayer>

- ✓ <https://github.com/bnb-chain/bsc>
- ✓ Binance Wallet - Chrome Extension
- ✓ Binance Wallet - Firefox Extension
- ✓ Binance Connect
- ✓ 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

In Scope					✓ In scope
EA \$200 – \$600	EX \$600 – \$1500	EA \$1500 – \$5000	EX \$5000 – \$10000	EX \$100000	
*.binance.com			ReactJS AWS Amazon Cloudfr... +2		
api.binance.com			API Testing HTTP Cryptocurrency		
*.brbchain.org			ReactJS AWS Amazon Cloudfr... +2		
dex.binance.org			API Testing HTTP Cryptocurrency		
BNB Beacon Chain			Cryptocurrency		
binance.us			ReactJS AWS Amazon Cloudfr... +4		
Binance Mobile Application for Android			Java Android Mobile Applicati... +2		
Binance Mobile Application for iOS			Objective-C SwiftUI Swift +2		
Binance Desktop Application			Cryptocurrency Desktop Applicat...		
Binance macOS Application			macOS Cryptocurrency		
https://github.com/brb-chain/tss-lib			Cryptography Cryptocurrency		
https://github.com/brb-chain/bep3-smartcontracts			Cryptocurrency		
https://github.com/brb-chain/bep3-deputy			Cryptocurrency		
https://github.com/brb-chain/ledger-app-binance			Cryptocurrency		
Trustwallet Android App					
Trustwallet iOS App					
https://github.com/trustwallet/wallet-core/					
BNB Smart Chain					
https://github.com/brb-chain/bsc-genesis-contract					
https://github.com/brb-chain/bsc-relayer					
https://github.com/brb-chain/oracle-relayer					
https://github.com/brb-chain/bsc					
Binance Wallet - Chrome Extension					
Binance Wallet - Firefox Extension					
Binance Connect			Java AWS HTTP +1		
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					

Out Scope

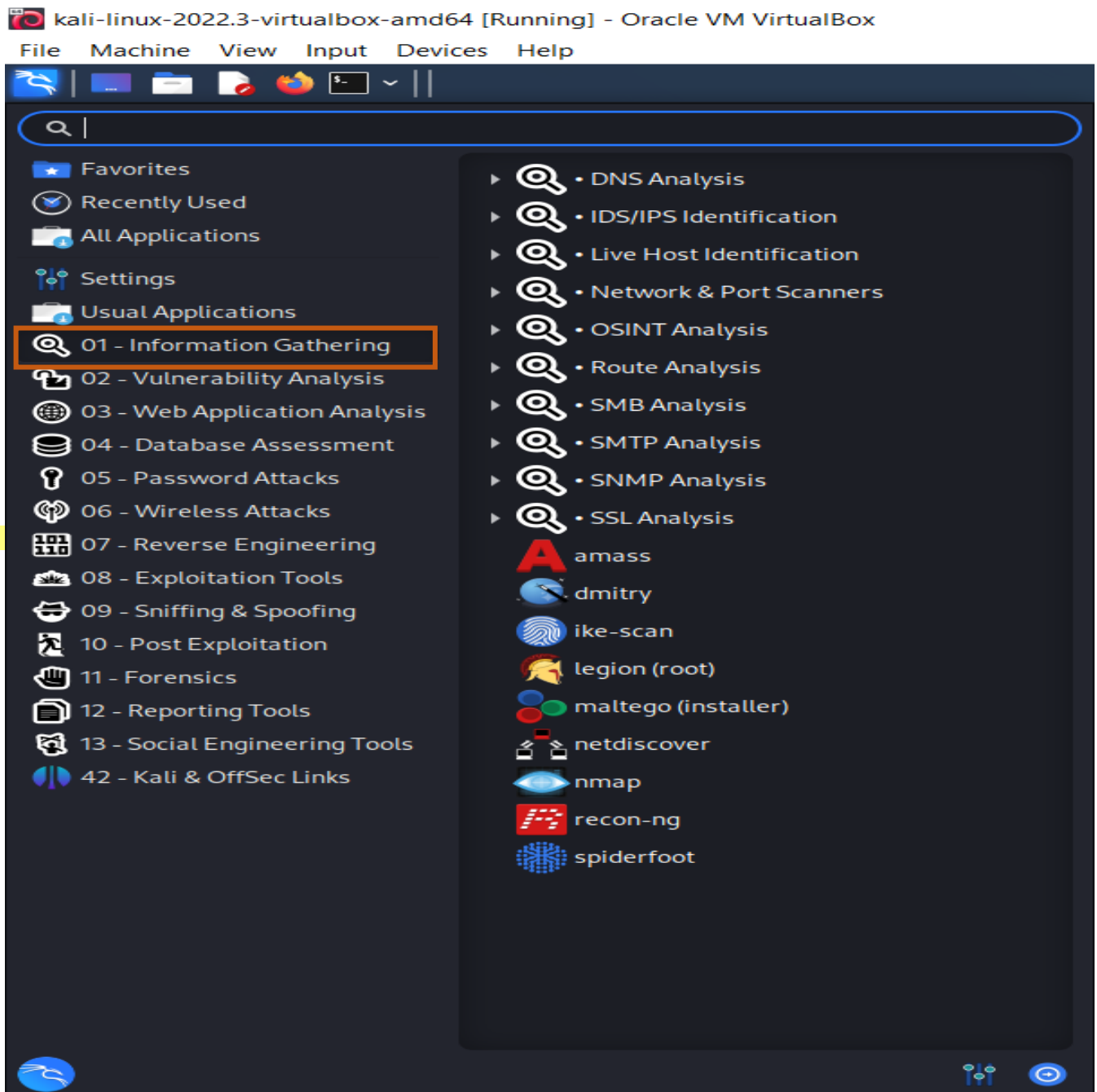
- ✓ support.binance.*
- ✓ community.binance.org
- ✓ *.trustwallet.com
- ✓ *.trustwalletapp.com
- ✓ *.binance.org
- ✓ *.buildnbuild.dev
- ✓ binance.sg
- ✓ blog.coinmarketcap.com
- ✓ support.coinmarketcap.com
- ✓ jobs.coinmarketcap.com
- ✓ blockchain.coinmarketcap.com
- ✓ *.coinmarketcap.com

Out of Scope✕ Out of scope

🌐 support.binance.*	Website Testing
🌐 community.binance.org	Website Testing
🌐 *.trustwallet.com	
🌐 *.trustwalletapp.com	
🌐 *.binance.org	
🌐 *.buildnbuild.dev	
🌐 binance.sg	ReactJS Website Testing Cryptocurrency +1
🌐 blog.coinmarketcap.com	
🌐 support.coinmarketcap.com	
🌐 jobs.coinmarketcap.com	
🌐 blockchain.coinmarketcap.com	
🌐 *.coinmarketcap.com	

Information gathering

It is the process of collecting data from many sources for a range of purposes. Learning to create efficient information-gathering techniques will benefit studying in a variety of ways. Effective information collecting involves making better use of time, fostering critical thinking through the use of shifting/sorting strategies, and enlarging one's perspective and topic knowledge through the investigation of new sources. Additionally, obtaining knowledge may be useful for a number of purposes, but the major advantage in terms of academic studies is that one will become aware of more varied sources, viewpoints, and techniques that can improve one's academic work.



• Subdomains for Hunting

Sub-domain enumeration is the process of listing sub-domains for one or more domains. In the process of reconnaissance, it's a crucial phase. Sub-domain enumeration can reveal several domains and sub-domains that are included in a security assessment, which increases the chance of finding vulnerabilities.

Finding applications using cryptic, abandoned sub-domains may reveal serious bugs.

Within a single company, the same vulnerabilities are routinely discovered across many domains and applications.

What is Knockpy?

With only a few lines of code, knockpy's python version of the knockoffs framework makes it simple to use knockoff-based inference. The modular design of Knockpy makes it simple for researchers and analysts to add features on top of it.

- searching subdomain by knockpy,

Knockpy is a portable and flexible Python3 utility that uses passive reconnaissance and dictionary scanning to swiftly enumerate subdomains on a specified domain.

How to Find Subdomain in Knockpy: `knockpy <Domain Name>`

```
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
$ knockpy binance.com

v6.1.0

local: 10757 | remote: 592
Wordlist: 11349 | Target: binance.com | Ip: 54.150.4.131
05:02:05
```

Ip address	Code	Subdomain	Server	Real hostname
52.192.247.79	200	05251fwww0.binance.com	Tengine	
18.176.5.40	200	0-20.binance.com	Tengine	
18.176.5.40	200	0-529.binance.com	Tengine	
54.150.4.131	200	0-11.binance.com	Tengine	
54.150.4.131	200	0-30.binance.com	Tengine	
18.176.5.40	200	00.binance.com	Tengine	

```

kali@kali: ~
File Actions Edit View Help
18.176.5.40 addresses zen.binance.com resolver (can be used multiple times)
  -f, --force value
54.150.4.131 to 403 zhaopin.binance.com DNS resolvers awsclb/2.0
  -t, --trips int
18.176.5.40 num 403 zim.binance.com per second for each trusted resolver awsclb/2.0
  -s, --output string /path/to/output/creating/crowdshooting/info
18.176.5.40 403 zh.binance.com awsclb/2.0
  -w, --path-to-a-different-wordlist-file-for-brute-forcing
54.150.4.131 403 zebra.binance.com awsclb/2.0
  -m, --mask string /path/to/mask-file-for-DNS-brute-forcing
18.176.5.40 403 zhidao.binance.com awsclb/2.0
54.150.4.131 in 403 zh-cn.binance.com awsclb/2.0
  -u, --url string /path/to/your/own/wordlist/for-DNS-brute-forcing
54.150.4.131 403 zimbra.binance.com awsclb/2.0
  -c, --config string /path/to/your/own/config-file
18.176.5.40 sub 403 zenoss.binance.com awsclb/2.0
  -p, --port int
18.176.5.40 top 403 zpanel.binance.com awsclb/2.0
  -d, --domain string /path/to/your/own/domain
18.176.5.40 403 zpush.binance.com awsclb/2.0
52.192.247.79 403 zt.binance.com awsclb/2.0
  -e, --enum string /path/to/your/own/enum-file
05:35:44
kali@kali: ~$
Ip address: 79 | Subdomain: 6775 | elapsed time: 00:33:39
  
```

- Open Ports Enumeration applying with nmap

A port that is open is one that is actively receiving TCP or UDP packets. A port is in use and cannot be used for anything else if a service uses it. Open ports offer a security risk if the services operating on them are improperly configured, unsecure, or unpatched.

Using Nmap to List Open Ports

The most popular port security network scanner in the world is called Nmap. You may assess the efficacy of your firewall and security settings with the help of the Nmap hosted security tool.

```
https://github.com/nmap/nmap/blob/master/doc/tutorial.md
(kali㉿kali)-[~]
└─$ sudo nmap -sS binance.com
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-27 01:58 EDT
Nmap scan report for binance.com (52.192.247.79)
Host is up (0.026s latency).
Other addresses for binance.com (not scanned): 18.176.5.40 54.150.4.131
rDNS record for 52.192.247.79: ec2-52-192-247-79.ap-northeast-1.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 10.26 seconds
```

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

PORT	STATE	SERVICE
80/tcp	open	http
443/tcp	open	https

Checking for Vulnerabilities using NIKTO

vulnerabilities are scanned by Nikto. But not any found vulnerability.

A security program called the Nikto web server scanner scans a website for thousands of possible security holes. This includes malicious files, services that have been set up improperly, vulnerable scripts, and other issues. It was created using plugins and is open source to allow for feature expansion. New security checks are frequently added to these plugins through regular updates. Many penetration testers and security analysts maintain the famous Nikto Web Vulnerability Scanner in their toolkit. It typically unearths valuable data about a web server or website that may be used for subsequent exploitation or vulnerability analysis.

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox


File Machine View Input Devices Help

```
kali@kali:~$ sudo nikto -h binance.com
- Nikto v2.5.0

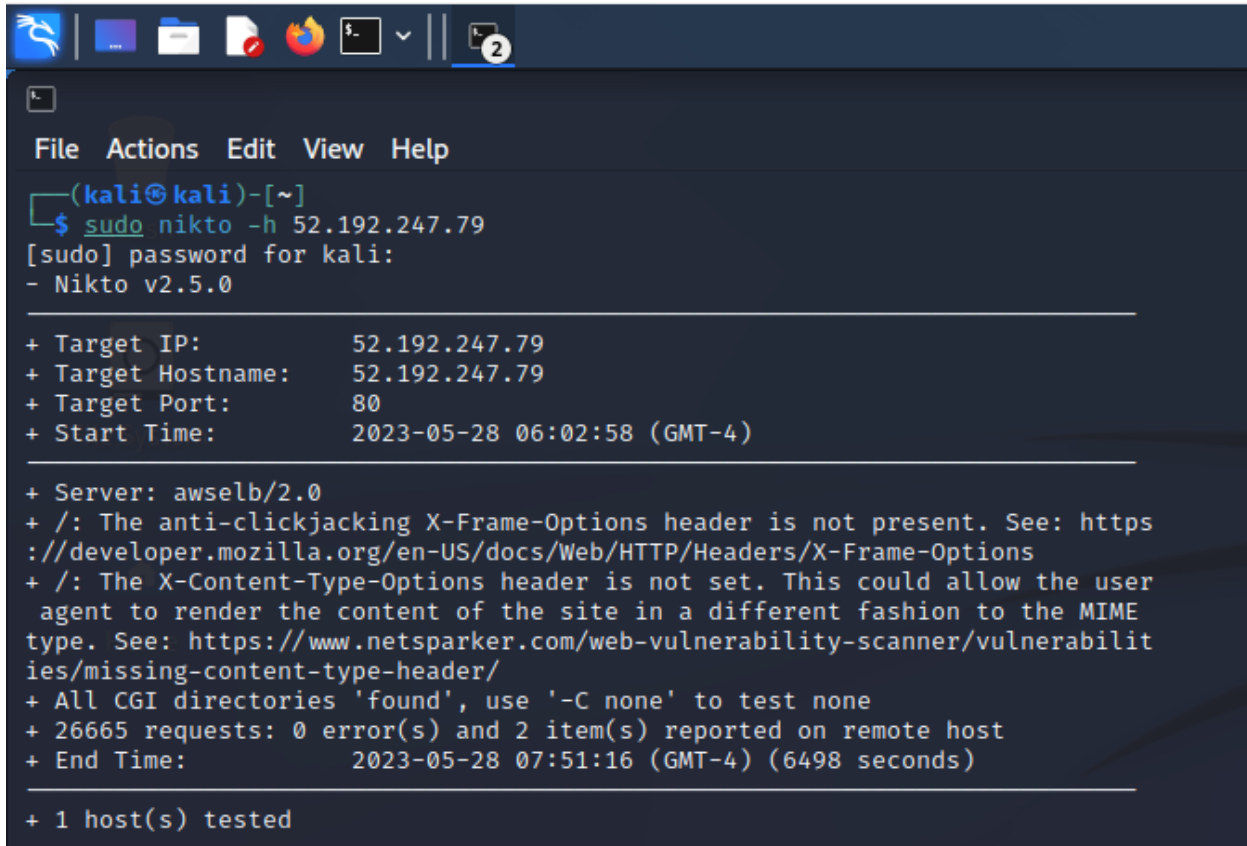
+ Multiple IPs found: 52.192.247.79, 18.176.5.40, 5
4.150.4.131
+ Target IP: 52.192.247.79
+ Target Hostname: binance.com
+ Target Port: 80
+ Start Time: 2023-05-27 02:02:57 (GMT-4)

+ Server: awselb/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/
+ Root page / redirects to: https://www.binance.com:443/
+ All CGI directories 'found', use '-C none' to test none
+ /SiteServer/admin/: Site Server components admin. Default account may be 'LDAP_Anonymous', pass is 'LdapPassword_1'. See: https://github.com/sullo/advisory-archives/blob/master/RFP2201.txt
+ 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: 19 error(s) and 3 item(s) reported on remote host
+ End Time: 2023-05-27 03:02:10 (GMT-4) (3553 seconds)

+ 1 host(s) tested
```

 kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



```
(kali㉿kali)-[~]
$ sudo nikto -h 52.192.247.79
[sudo] password for kali:
- Nikto v2.5.0

+ Target IP:          52.192.247.79
+ Target Hostname:    52.192.247.79
+ Target Port:        80
+ Start Time:         2023-05-28 06:02:58 (GMT-4)

+ Server: awselb/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/
+ All CGI directories 'found', use '-C none' to test none
+ 26665 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2023-05-28 07:51:16 (GMT-4) (6498 seconds)

+ 1 host(s) tested
```

Scanned Vulnerabilities Using Netsparker

1) Weak Ciphers Enabled

The screenshot displays the Netsparker 5.8.1.28119 interface. The main panel shows a vulnerability titled "Weak Ciphers Enabled" with a "CONFIRMED" status and a "MEDIUM" severity. The URL is <https://www.binance.com/>. The report details the list of supported weak ciphers: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) and TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027). It includes a classification table, CVSS 3.0 scores, and actions to take, such as modifying the SSLCipherSuite directive in the httpd.conf file.

CLASSIFICATION	
PCI DSS 3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
CWE	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

CVSS 3.0 SCORE	
Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String	
CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/CH:lh/A:N	

Risk type : Medium

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

URL :<https://www.casper.com/>

List of Supported Weak Ciphers :TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

- **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:

```
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

- **Remedy**

Configure your web server to disallow using weak ciphers.