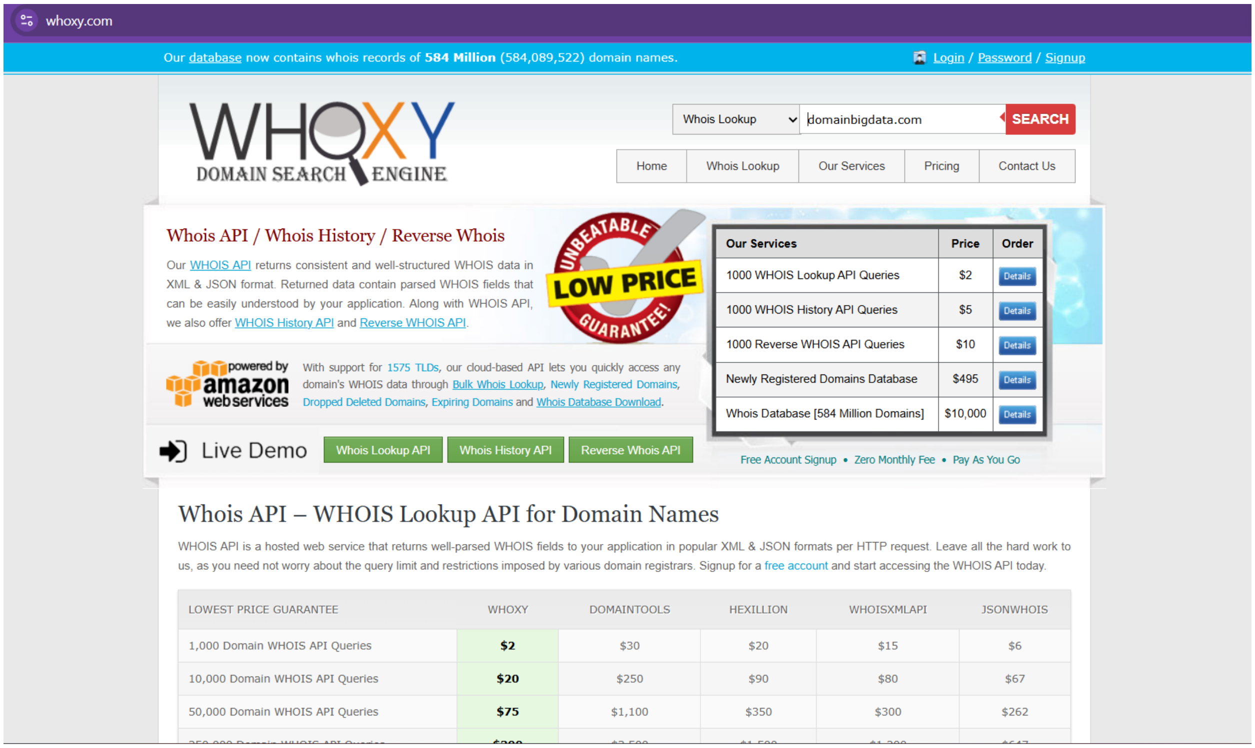
Exercise 1 : Gathering whois and DNS information



whoxy.com

Our database now contains whois records of **584 Million** (584,089,522) domain names.

Login / Password / Signup

Whois API / Whois History / Reverse Whois

Our WHOIS API returns consistent and well-structured WHOIS data in XML & JSON format. Returned data contain parsed WHOIS fields that can be easily understood by your application. Along with WHOIS API, we also offer WHOIS History API and Reverse WHOIS API.

Our Services	Price	Order
1000 WHOIS Lookup API Queries	$2	Details
1000 WHOIS History API Queries	$5	Details
1000 Reverse WHOIS API Queries	$10	Details
Newly Registered Domains Database	$495	Details
Whois Database [584 Million Domains]	$10,000	Details

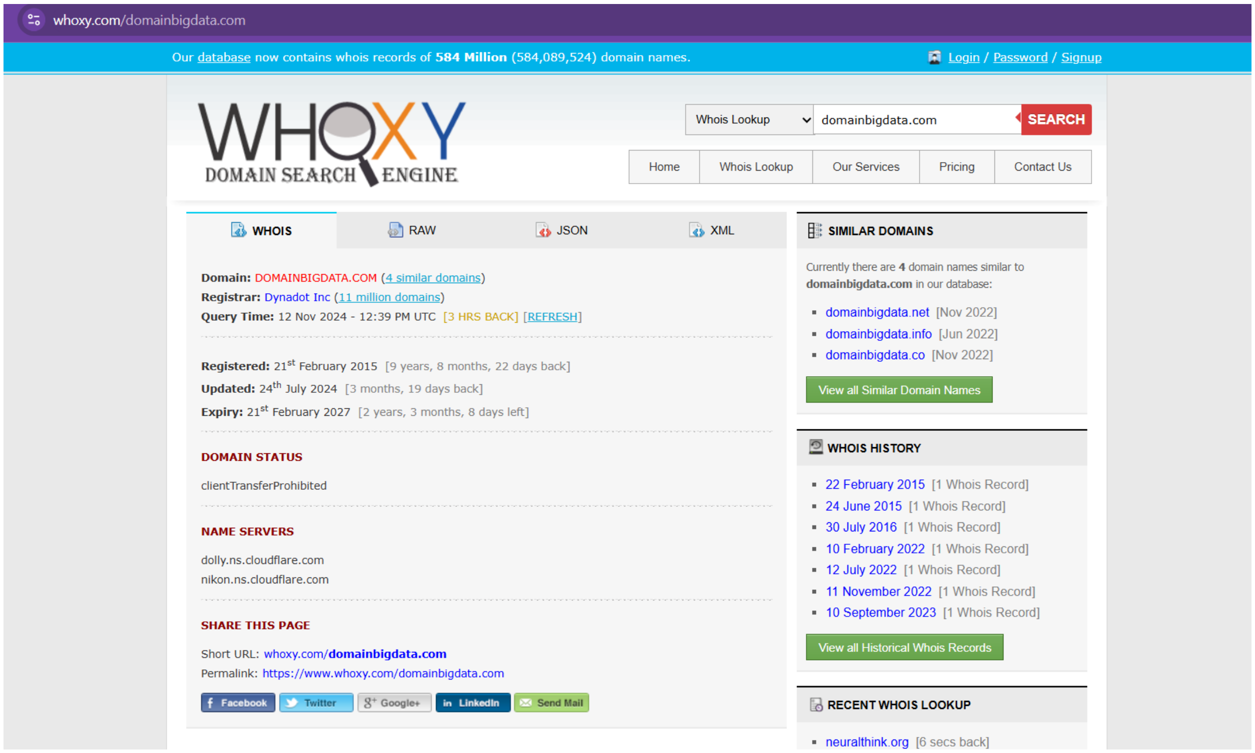
With support for 1575 TLDs, our cloud-based API lets you quickly access any domain's WHOIS data through Bulk Whois Lookup, Newly Registered Domains, Dropped Deleted Domains, Expiring Domains and Whois Database Download.

Free Account Signup • Zero Monthly Fee • Pay As You Go

Whois API – WHOIS Lookup API for Domain Names

WHOIS API is a hosted web service that returns well-parsed WHOIS fields to your application in popular XML & JSON formats per HTTP request. Leave all the hard work to us, as you need not worry about the query limit and restrictions imposed by various domain registrars. Signup for a free account and start accessing the WHOIS API today.

LOWEST PRICE GUARANTEE	WHOXY	DOMAINTOOLS	HEXILLION	WHOISXMLAPI	JSONWHOIS
1,000 Domain WHOIS API Queries	**$2**	$30	$20	$15	$6
10,000 Domain WHOIS API Queries	**$20**	$250	$90	$80	$67
50,000 Domain WHOIS API Queries	**$75**	$1,100	$350	$300	$262



whoxy.com/domainbigdata.com

Our database now contains whois records of **584 Million** (584,089,524) domain names.

Login / Password / Signup

Domain: DOMAINBIGDATA.COM (4 similar domains)
Registrar: Dynadot Inc (11 million domains)
Query Time: 12 Nov 2024 - 12:39 PM UTC [3 HRS BACK] [REFRESH]

Registered: 21st February 2015 [9 years, 8 months, 22 days back]
Updated: 24th July 2024 [3 months, 19 days back]
Expiry: 21st February 2027 [2 years, 3 months, 8 days left]

DOMAIN STATUS

clientTransferProhibited

NAME SERVERS

dolly.ns.cloudflare.com
nikon.ns.cloudflare.com

SHARE THIS PAGE

Short URL: whoxy.com/**domainbigdata.com**
Permalink: https://www.whoxy.com/domainbigdata.com

SIMILAR DOMAINS

Currently there are **4** domain names similar to **domainbigdata.com** in our database:

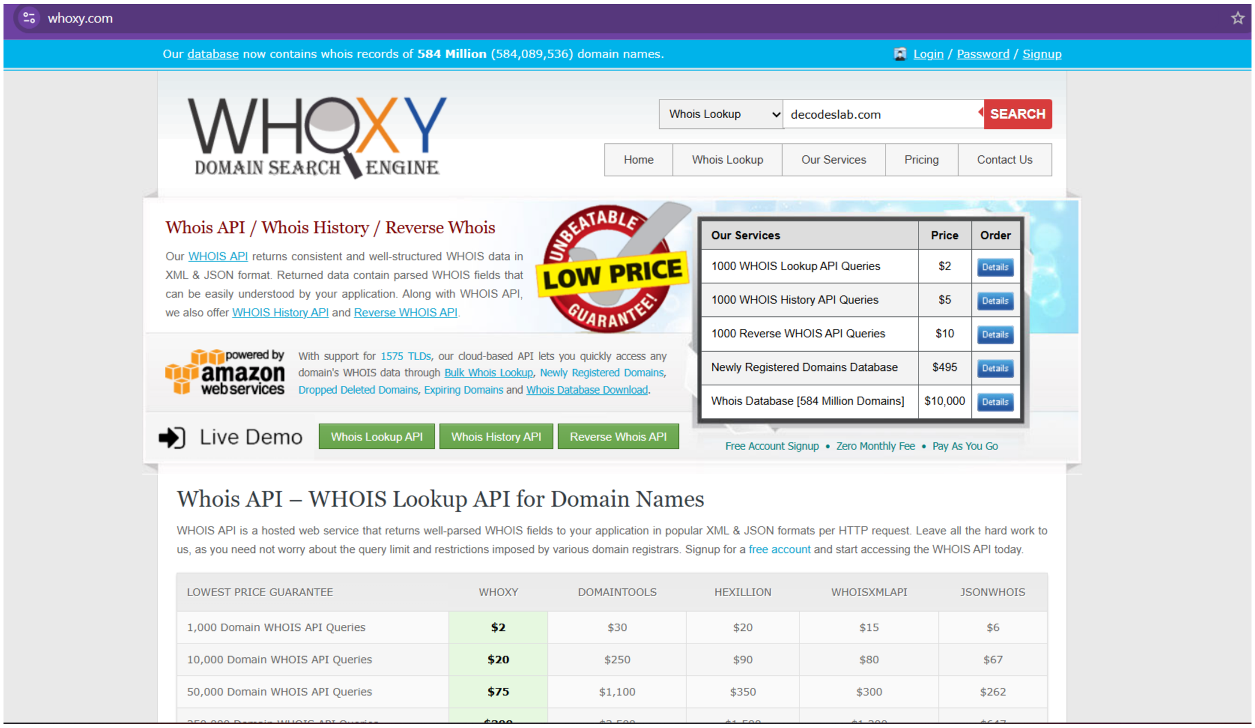
- domainbigdata.net [Nov 2022]
- domainbigdata.info [Jun 2022]
- domainbigdata.co [Nov 2022]

WHOIS HISTORY

- 22 February 2015 [1 Whois Record]
- 24 June 2015 [1 Whois Record]
- 30 July 2016 [1 Whois Record]
- 10 February 2022 [1 Whois Record]
- 12 July 2022 [1 Whois Record]
- 11 November 2022 [1 Whois Record]
- 10 September 2023 [1 Whois Record]

RECENT WHOIS LOOKUP

- neuralthink.org [6 secs back]



Our database now contains whois records of **584 Million** (584,089,536) domain names.

Whois API / Whois History / Reverse Whois

Our WHOIS API returns consistent and well-structured WHOIS data in XML & JSON format. Returned data contain parsed WHOIS fields that can be easily understood by your application. Along with WHOIS API, we also offer WHOIS History API and Reverse WHOIS API.

Our Services	Price	Order
1000 WHOIS Lookup API Queries	$2	Details
1000 WHOIS History API Queries	$5	Details
1000 Reverse WHOIS API Queries	$10	Details
Newly Registered Domains Database	$495	Details
Whois Database [584 Million Domains]	$10,000	Details

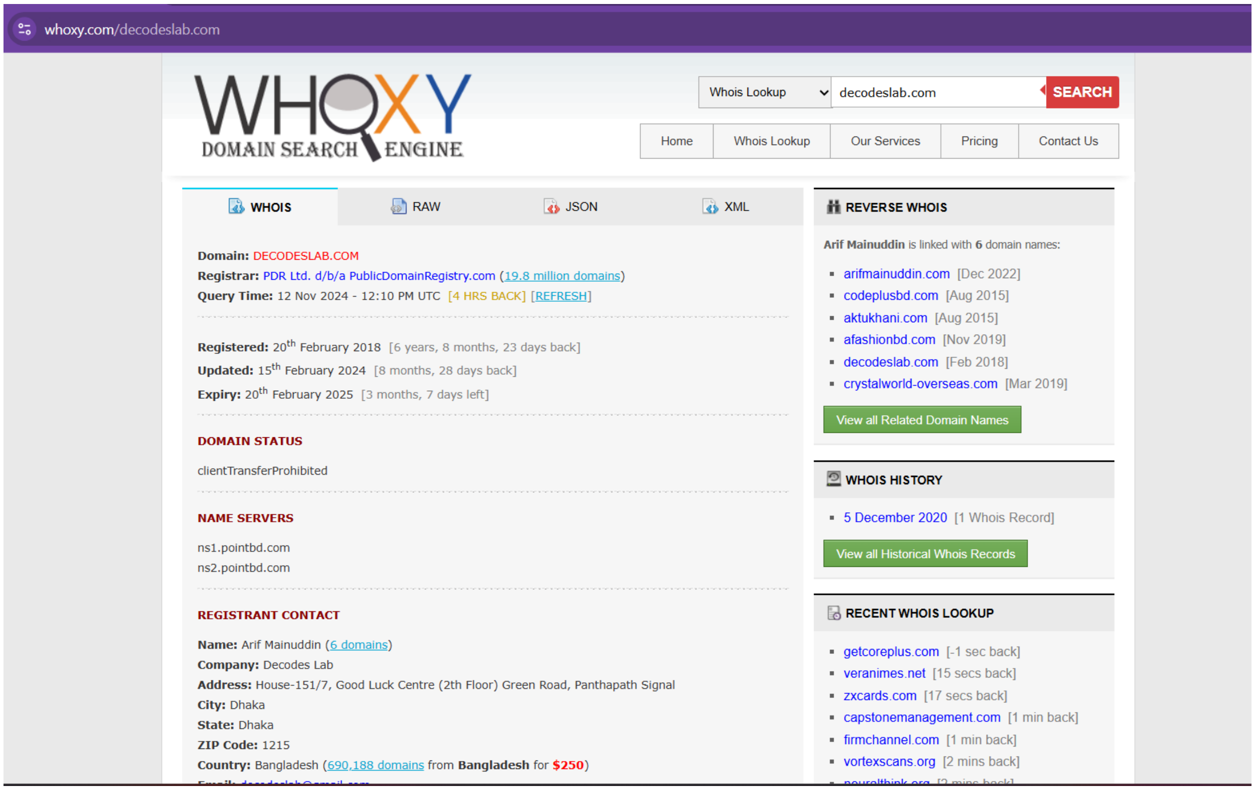
With support for 1575 TLDs, our cloud-based API lets you quickly access any domain's WHOIS data through Bulk Whois Lookup, Newly Registered Domains, Dropped Deleted Domains, Expiring Domains and Whois Database Download.

Free Account Signup • Zero Monthly Fee • Pay As You Go

Whois API – WHOIS Lookup API for Domain Names

WHOIS API is a hosted web service that returns well-parsed WHOIS fields to your application in popular XML & JSON formats per HTTP request. Leave all the hard work to us, as you need not worry about the query limit and restrictions imposed by various domain registrars. Signup for a free account and start accessing the WHOIS API today.

LOWEST PRICE GUARANTEE	WHOXY	DOMAINTOOLS	HEXILLION	WHOISXMLAPI	JSONWHOIS
1,000 Domain WHOIS API Queries	**$2**	$30	$20	$15	$6
10,000 Domain WHOIS API Queries	**$20**	$250	$90	$80	$67
50,000 Domain WHOIS API Queries	**$75**	$1,100	$350	$300	$262



Domain: DECODESLAB.COM
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com (19.8 million domains)
Query Time: 12 Nov 2024 - 12:10 PM UTC [4 HRS BACK] [REFRESH]

Registered: 20th February 2018 [6 years, 8 months, 23 days back]
Updated: 15th February 2024 [8 months, 28 days back]
Expiry: 20th February 2025 [3 months, 7 days left]

DOMAIN STATUS

clientTransferProhibited

NAME SERVERS

ns1.pointbd.com
ns2.pointbd.com

REGISTRANT CONTACT

Name: Arif Mainuddin (6 domains)
Company: Decodes Lab
Address: House-151/7, Good Luck Centre (2th Floor) Green Road, Panthapath Signal
City: Dhaka
State: Dhaka
ZIP Code: 1215
Country: Bangladesh (690,188 domains from **Bangladesh** for **$250**)

REVERSE WHOIS

Arif Mainuddin is linked with **6** domain names:

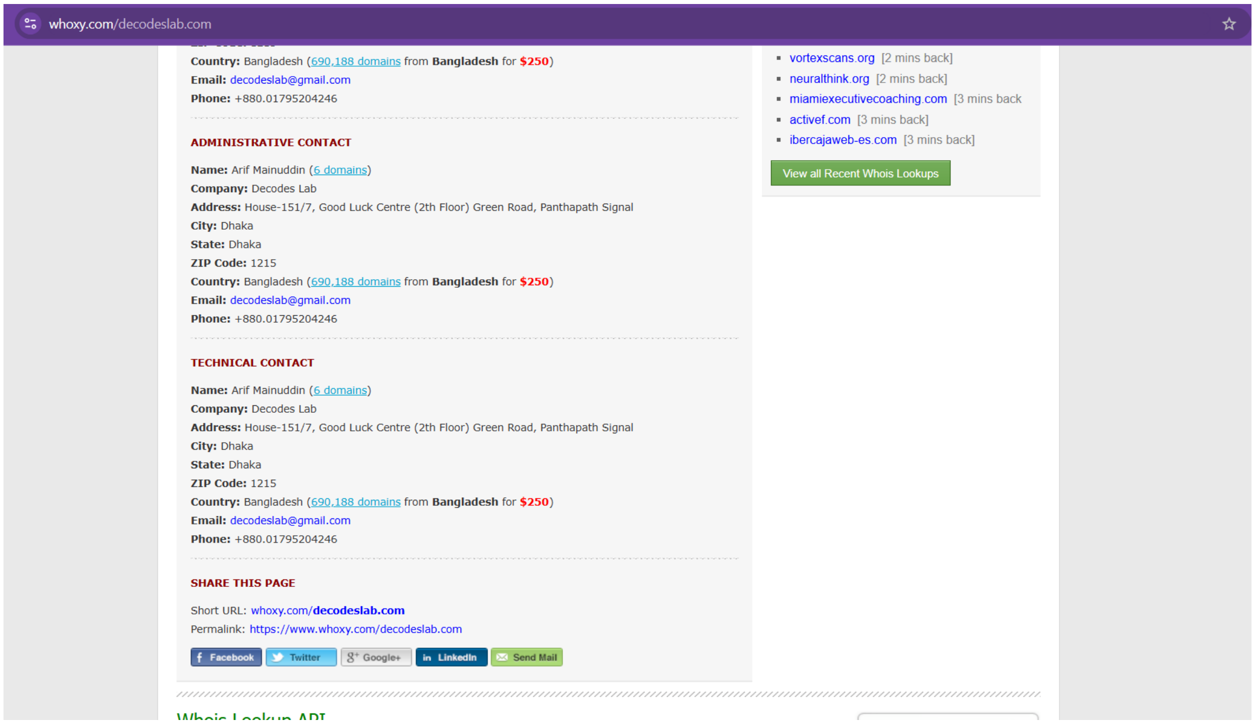
- arifmainuddin.com [Dec 2022]
- codeplusbd.com [Aug 2015]
- aktukhani.com [Aug 2015]
- afashionbd.com [Nov 2019]
- decodeslab.com [Feb 2018]
- crystalworld-overseas.com [Mar 2019]

WHOIS HISTORY

- 5 December 2020 [1 Whois Record]

RECENT WHOIS LOOKUP

- getcoreplus.com [-1 sec back]
- veranimes.net [15 secs back]
- zxcards.com [17 secs back]
- capstonemanagement.com [1 min back]
- firmchannel.com [1 min back]
- vortexscans.org [2 mins back]



whoxy.com/decodeslab.com

Country: Bangladesh (690,188 domains from **Bangladesh** for **$250**)
Email: decodeslab@gmail.com
Phone: +880.01795204246

ADMINISTRATIVE CONTACT

Name: Arif Mainuddin (6 domains)
Company: Decodes Lab
Address: House-151/7, Good Luck Centre (2th Floor) Green Road, Panthapath Signal
City: Dhaka
State: Dhaka
ZIP Code: 1215
Country: Bangladesh (690,188 domains from **Bangladesh** for **$250**)
Email: decodeslab@gmail.com
Phone: +880.01795204246

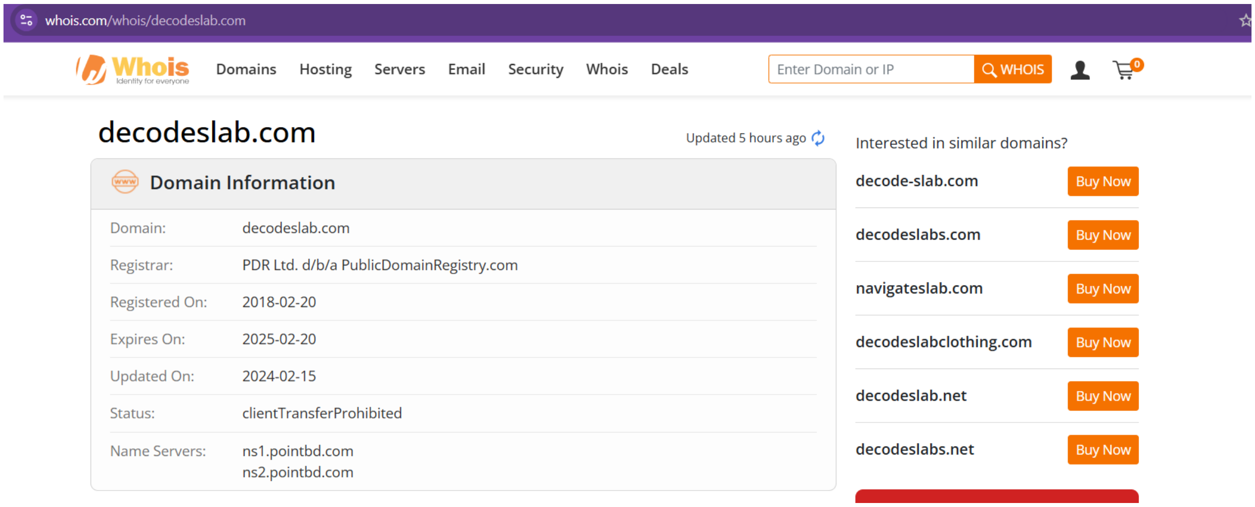
TECHNICAL CONTACT

Name: Arif Mainuddin (6 domains)
Company: Decodes Lab
Address: House-151/7, Good Luck Centre (2th Floor) Green Road, Panthapath Signal
City: Dhaka
State: Dhaka
ZIP Code: 1215
Country: Bangladesh (690,188 domains from **Bangladesh** for **$250**)
Email: decodeslab@gmail.com
Phone: +880.01795204246

SHARE THIS PAGE

Short URL: whoxy.com/**decodeslab.com**
Permalink: https://www.whoxy.com/decodeslab.com

- vortexscans.org [2 mins back]
- neuralthink.org [2 mins back]
- miamiexecutivecoaching.com [3 mins back
- activef.com [3 mins back]
- ibercajaweb-es.com [3 mins back]



whois.com/whois/decodeslab.com

decodeslab.com

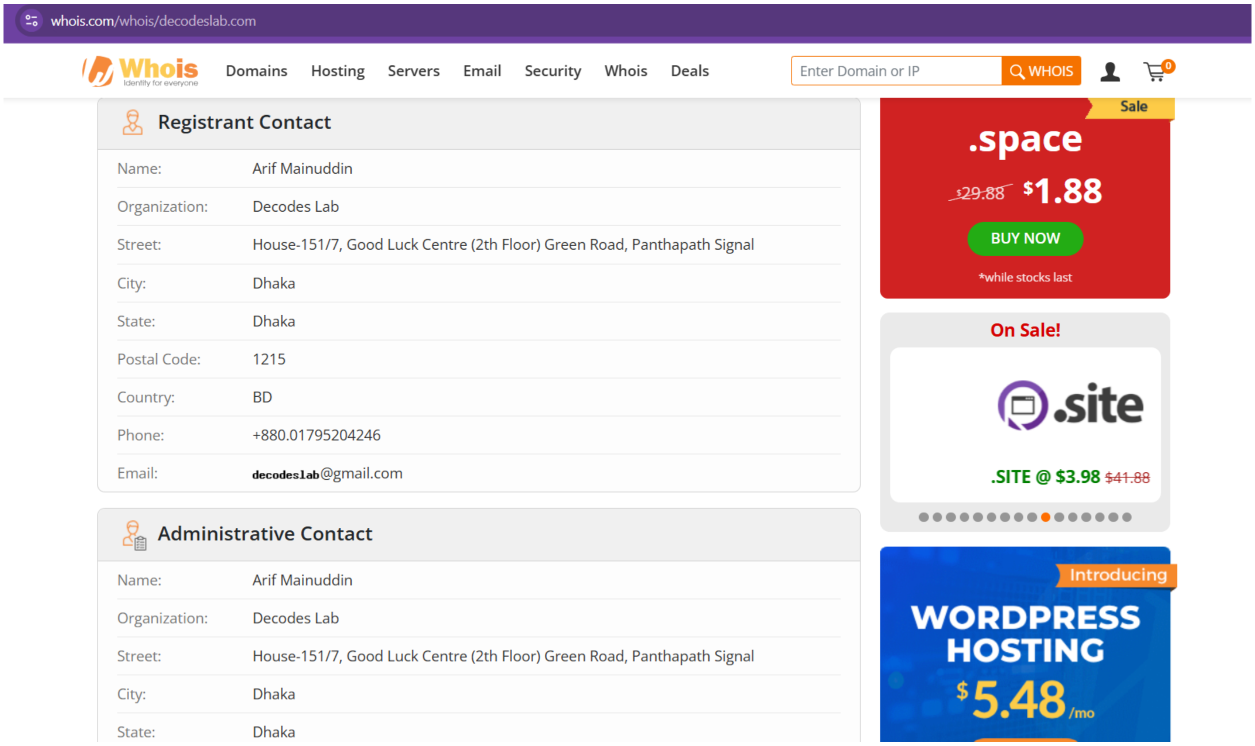
Updated 5 hours ago

Domain Information

Domain:	decodeslab.com
Registrar:	PDR Ltd. d/b/a PublicDomainRegistry.com
Registered On:	2018-02-20
Expires On:	2025-02-20
Updated On:	2024-02-15
Status:	clientTransferProhibited
Name Servers:	ns1.pointbd.com ns2.pointbd.com

Interested in similar domains?

decode-slab.com	Buy Now
decodeslabs.com	Buy Now
navigateslab.com	Buy Now
decodeslabclothing.com	Buy Now
decodeslab.net	Buy Now
decodeslabs.net	Buy Now

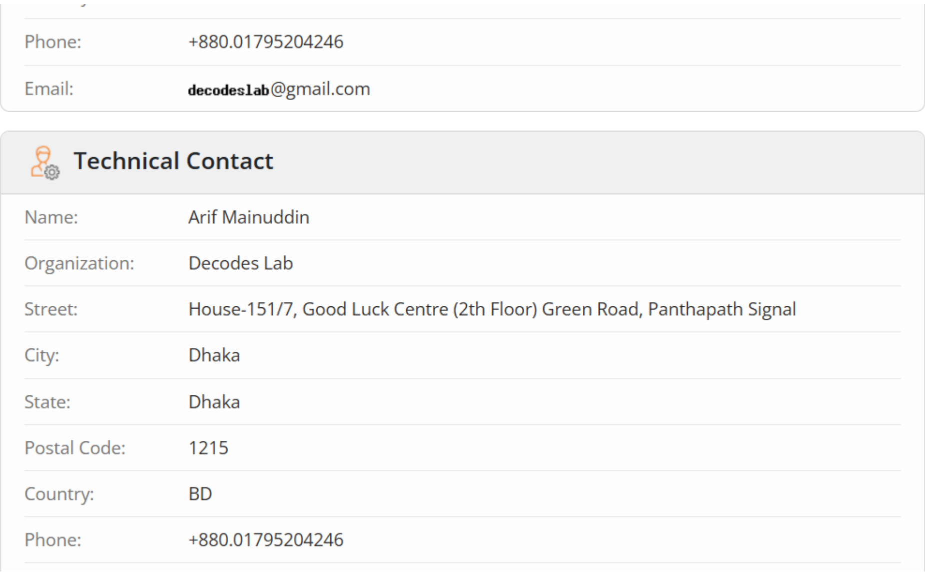


Registrant Contact

Name:	Arif Mainuddin
Organization:	Decodes Lab
Street:	House-151/7, Good Luck Centre (2th Floor) Green Road, Panthapath Signal
City:	Dhaka
State:	Dhaka
Postal Code:	1215
Country:	BD
Phone:	+880.01795204246
Email:	**decodeslab**@gmail.com

Administrative Contact

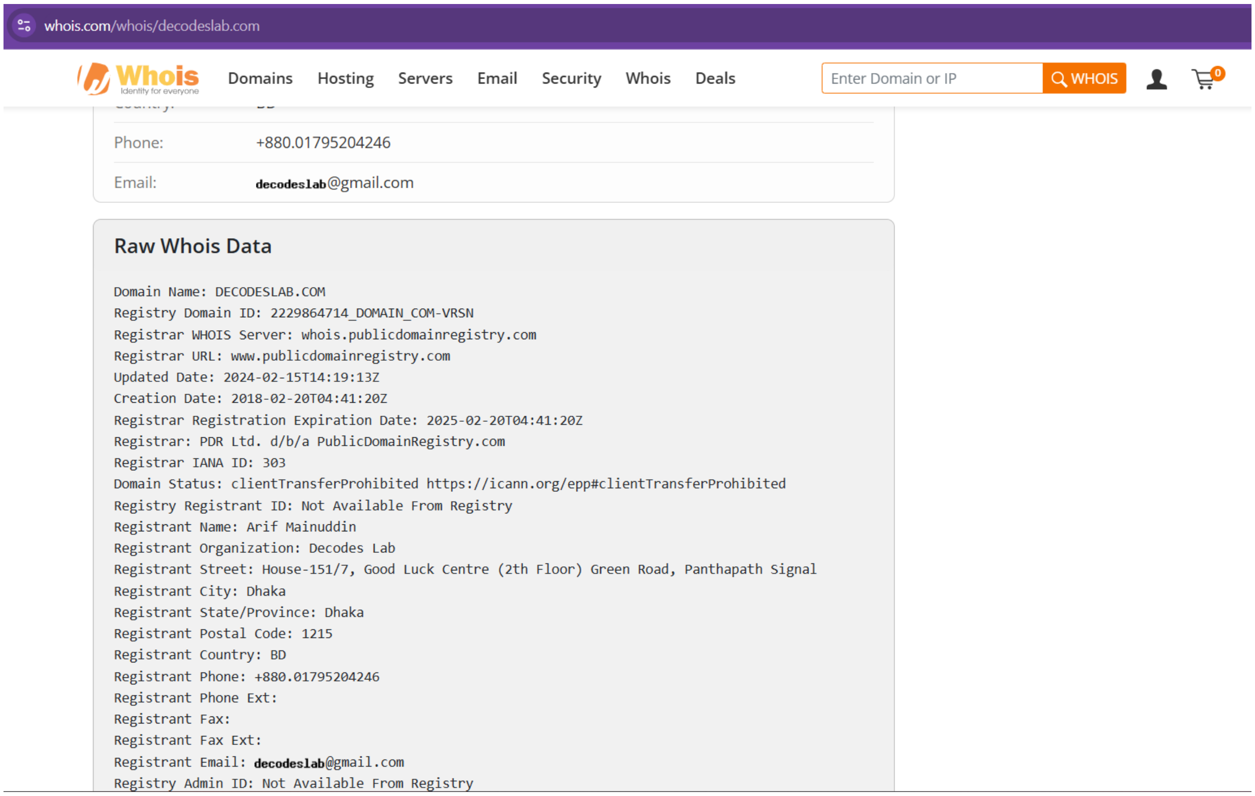
Name:	Arif Mainuddin
Organization:	Decodes Lab
Street:	House-151/7, Good Luck Centre (2th Floor) Green Road, Panthapath Signal
City:	Dhaka
State:	Dhaka



Phone:	+880.01795204246
Email:	**decodeslab**@gmail.com

Technical Contact

Name:	Arif Mainuddin
Organization:	Decodes Lab
Street:	House-151/7, Good Luck Centre (2th Floor) Green Road, Panthapath Signal
City:	Dhaka
State:	Dhaka
Postal Code:	1215
Country:	BD
Phone:	+880.01795204246

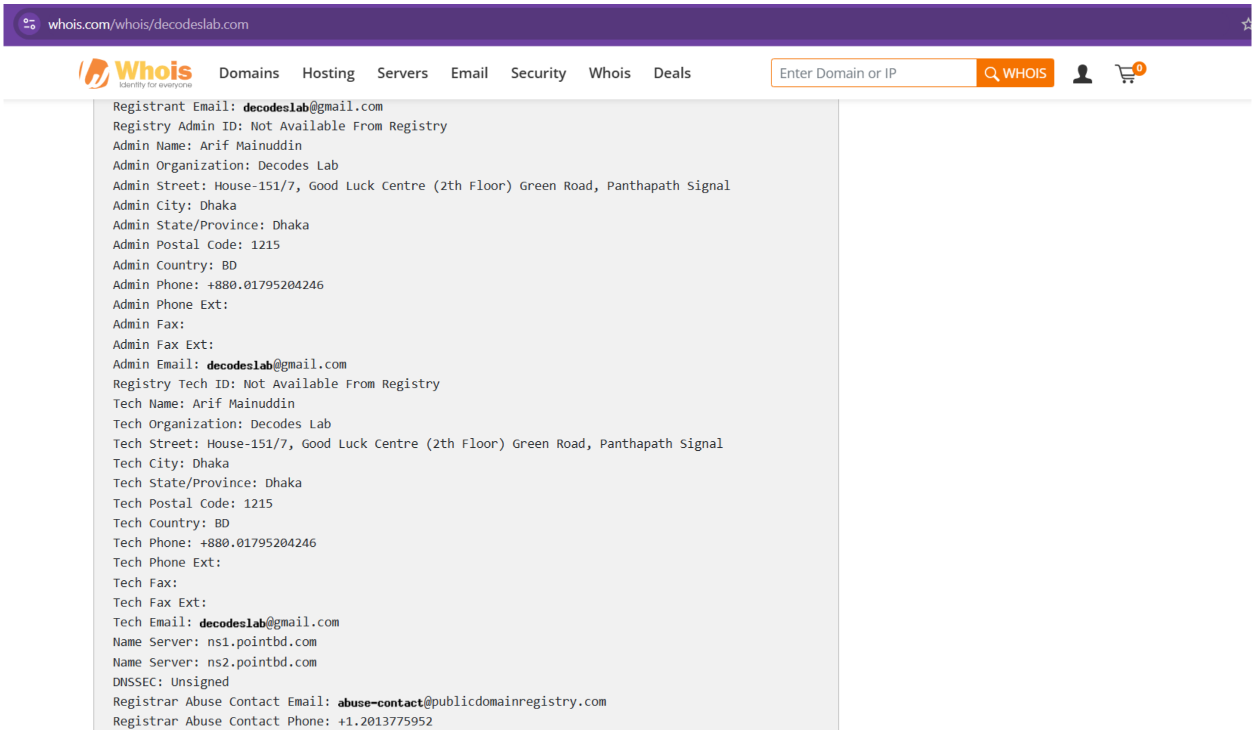


Phone: +880.01795204246

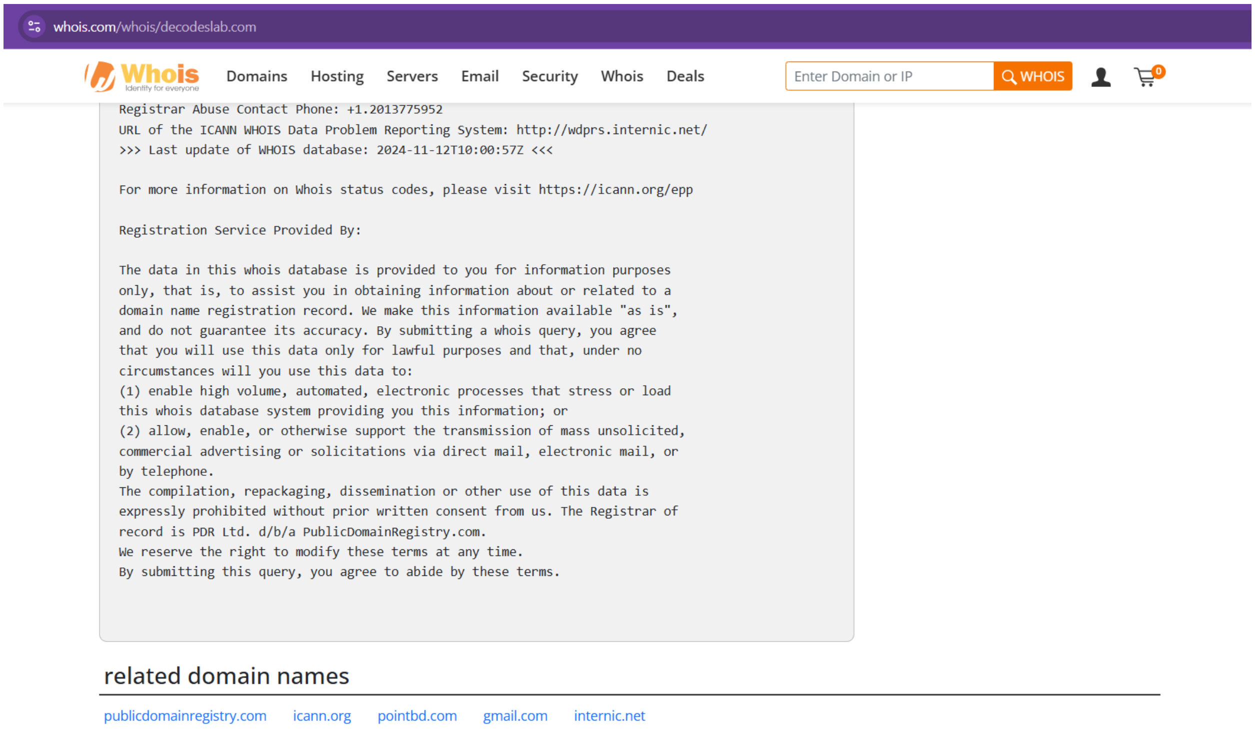
Email: decodeslab@gmail.com

Raw Whois Data

```
Domain Name: DECODESLAB.COM
Registry Domain ID: 2229864714_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2024-02-15T14:19:13Z
Creation Date: 2018-02-20T04:41:20Z
Registrar Registration Expiration Date: 2025-02-20T04:41:20Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Arif Mainuddin
Registrant Organization: Decodes Lab
Registrant Street: House-151/7, Good Luck Centre (2th Floor) Green Road, Panthapath Signal
Registrant City: Dhaka
Registrant State/Province: Dhaka
Registrant Postal Code: 1215
Registrant Country: BD
Registrant Phone: +880.01795204246
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: decodeslab@gmail.com
Registry Admin ID: Not Available From Registry
```



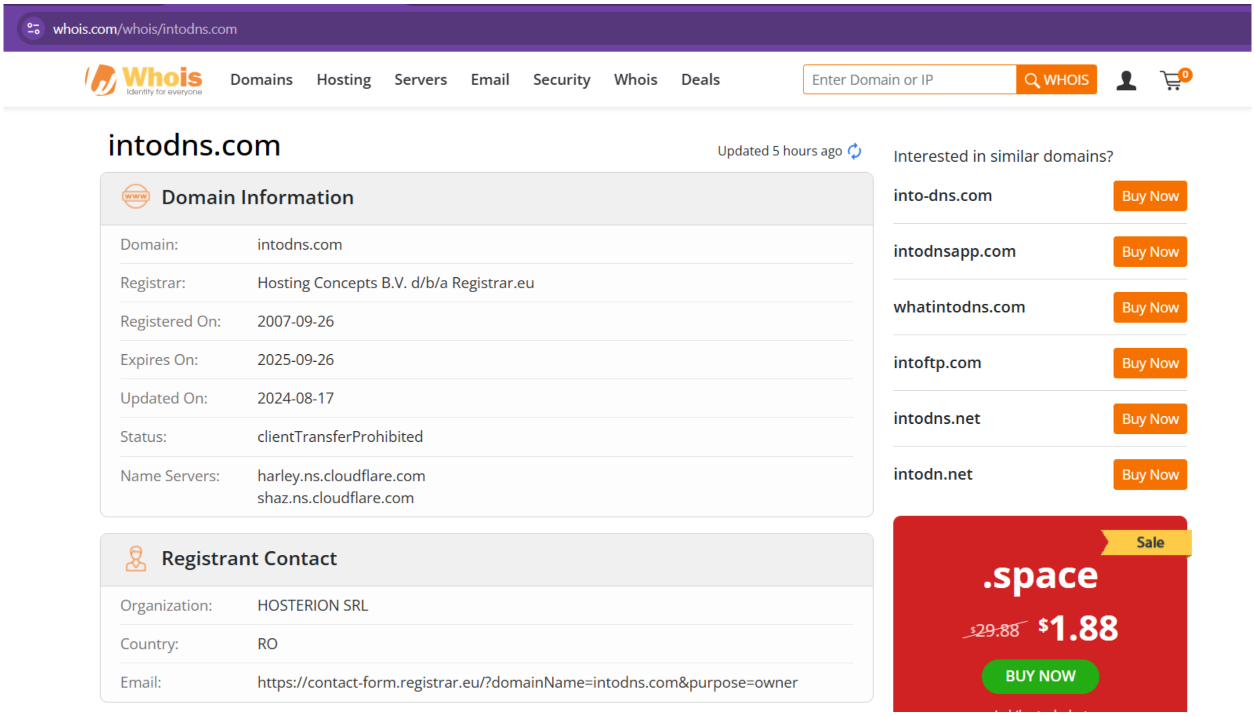
```
Registrant Email: decodeslab@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: Arif Mainuddin
Admin Organization: Decodes Lab
Admin Street: House-151/7, Good Luck Centre (2th Floor) Green Road, Panthapath Signal
Admin City: Dhaka
Admin State/Province: Dhaka
Admin Postal Code: 1215
Admin Country: BD
Admin Phone: +880.01795204246
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: decodeslab@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: Arif Mainuddin
Tech Organization: Decodes Lab
Tech Street: House-151/7, Good Luck Centre (2th Floor) Green Road, Panthapath Signal
Tech City: Dhaka
Tech State/Province: Dhaka
Tech Postal Code: 1215
Tech Country: BD
Tech Phone: +880.01795204246
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: decodeslab@gmail.com
Name Server: ns1.pointbd.com
Name Server: ns2.pointbd.com
DNSSEC: Unsigned
Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
```



```
Registrar Abuse Contact Phone: +1.2013775952
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-11-12T10:00:57Z <<<

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

Registration Service Provided By:

The data in this whois database is provided to you for information purposes
only, that is, to assist you in obtaining information about or related to a
domain name registration record. We make this information available "as is",
and do not guarantee its accuracy. By submitting a whois query, you agree
that you will use this data only for lawful purposes and that, under no
circumstances will you use this data to:
(1) enable high volume, automated, electronic processes that stress or load
this whois database system providing you this information; or
(2) allow, enable, or otherwise support the transmission of mass unsolicited,
commercial advertising or solicitations via direct mail, electronic mail, or
by telephone.
The compilation, repackaging, dissemination or other use of this data is
expressly prohibited without prior written consent from us. The Registrar of
record is PDR Ltd. d/b/a PublicDomainRegistry.com.
We reserve the right to modify these terms at any time.
By submitting this query, you agree to abide by these terms.
```

related domain names

publicdomainregistry.com icann.org pointbd.com gmail.com internic.net



intodns.com

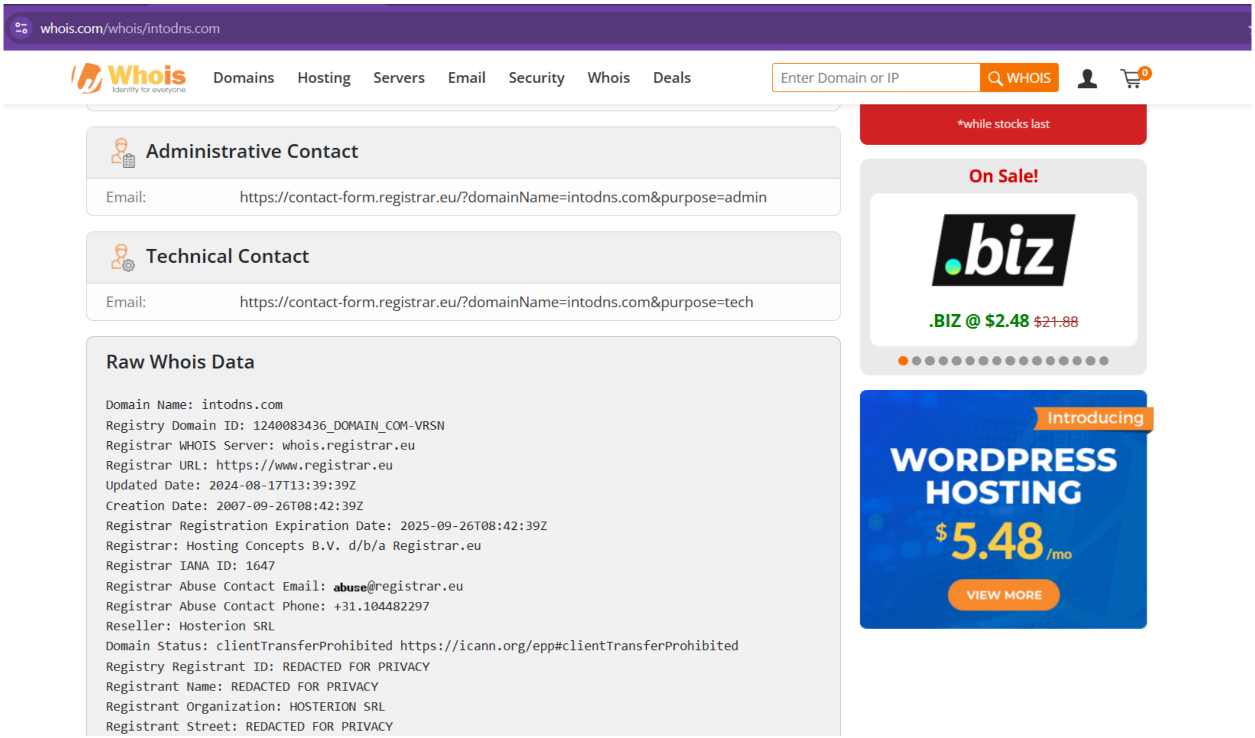
Updated 5 hours ago

Domain Information

Domain:	intodns.com
Registrar:	Hosting Concepts B.V. d/b/a Registrar.eu
Registered On:	2007-09-26
Expires On:	2025-09-26
Updated On:	2024-08-17
Status:	clientTransferProhibited
Name Servers:	harley.ns.cloudflare.com shaz.ns.cloudflare.com

Registrant Contact

Organization:	HOSTERION SRL
Country:	RO
Email:	https://contact-form.registrar.eu/?domainName=intodns.com&purpose=owner



Administrative Contact

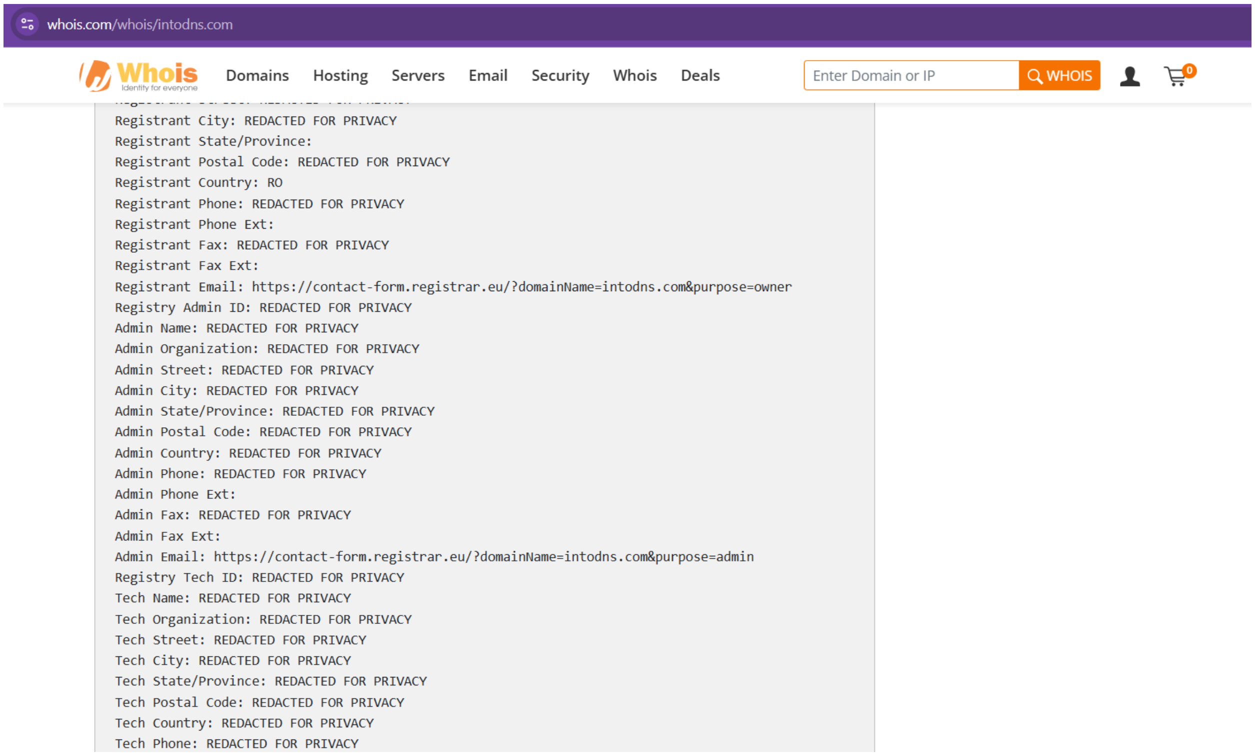
Email: https://contact-form.registrar.eu/?domainName=intodns.com&purpose=admin

Technical Contact

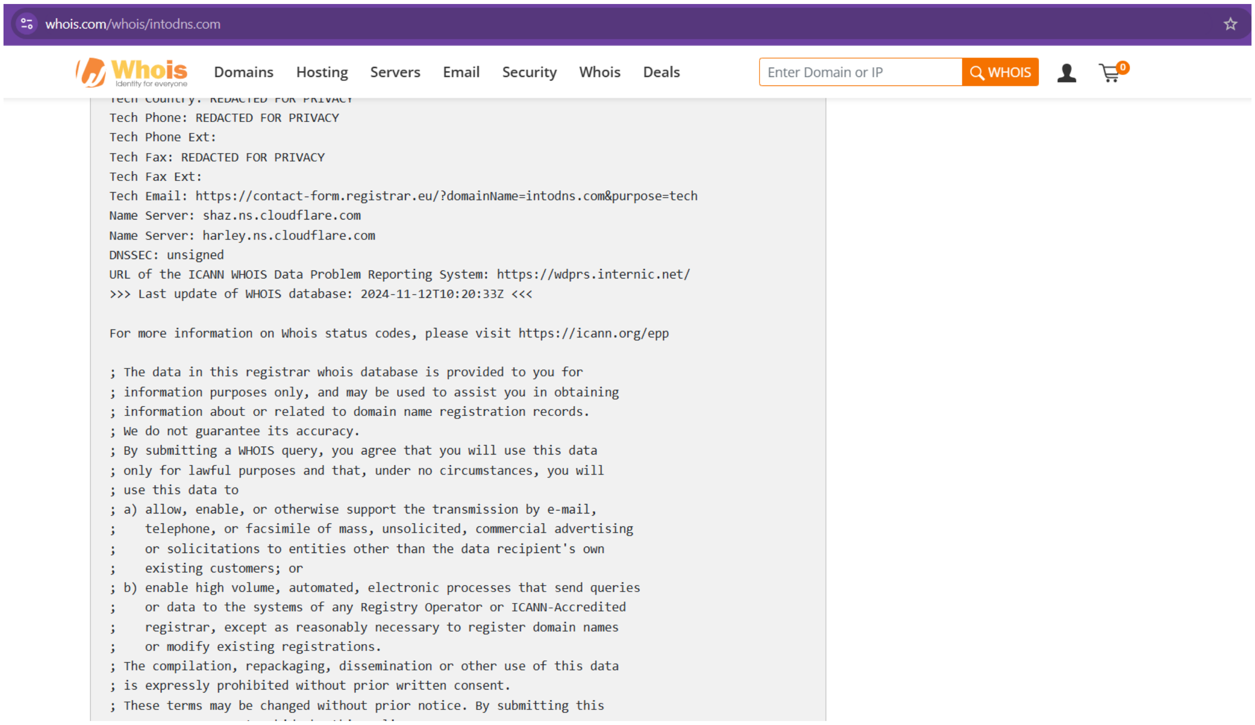
Email: https://contact-form.registrar.eu/?domainName=intodns.com&purpose=tech

Raw Whois Data

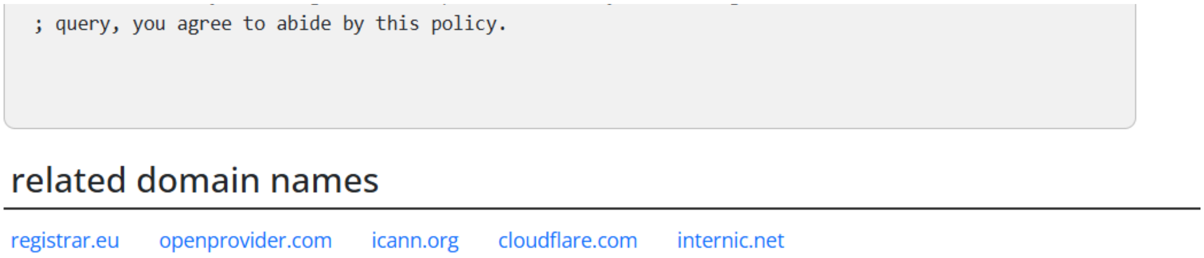
```
Domain Name: intodns.com
Registry Domain ID: 1240083436_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.eu
Registrar URL: https://www.registrar.eu
Updated Date: 2024-08-17T13:39:39Z
Creation Date: 2007-09-26T08:42:39Z
Registrar Registration Expiration Date: 2025-09-26T08:42:39Z
Registrar: Hosting Concepts B.V. d/b/a Registrar.eu
Registrar IANA ID: 1647
Registrar Abuse Contact Email: abuse@registrar.eu
Registrar Abuse Contact Phone: +31.104482297
Reseller: Hosterion SRL
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: HOSTERION SRL
Registrant Street: REDACTED FOR PRIVACY
```



```
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: RO
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext:
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext:
Registrant Email: https://contact-form.registrar.eu/?domainName=intodns.com&purpose=owner
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext:
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext:
Admin Email: https://contact-form.registrar.eu/?domainName=intodns.com&purpose=admin
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
```



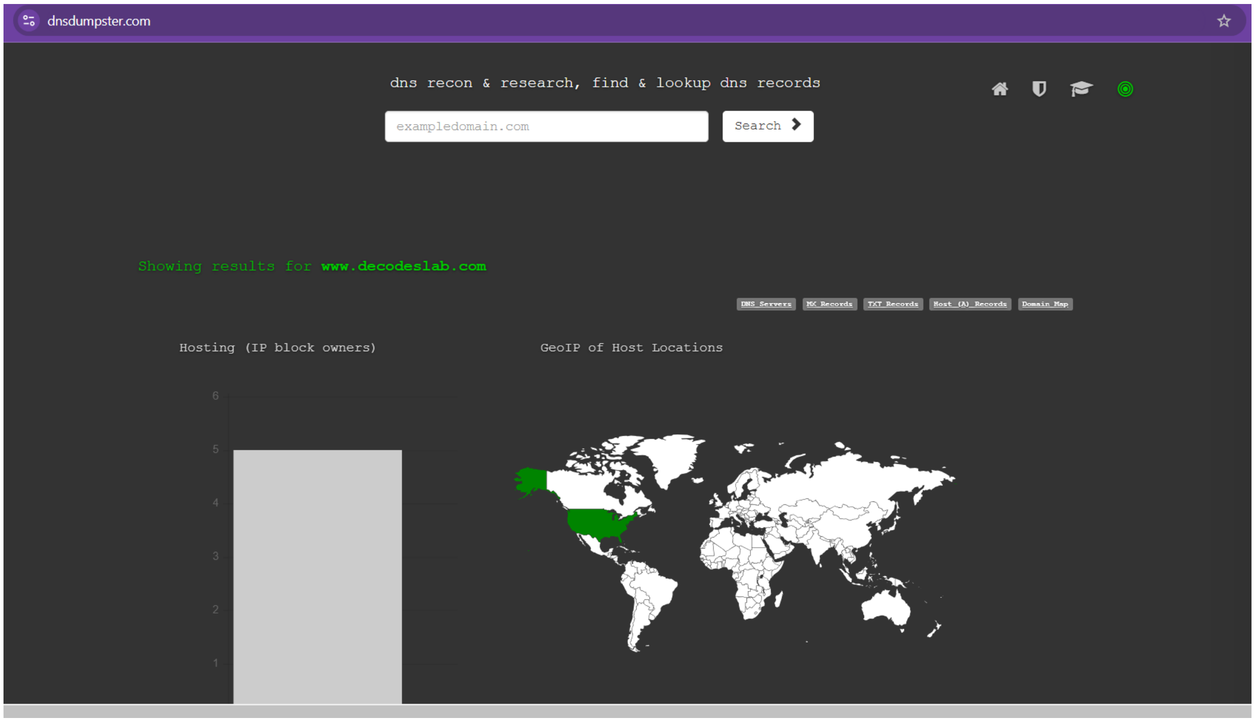
```
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext:
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext:
Tech Email: https://contact-form.registrar.eu/?domainName=intodns.com&purpose=tech
Name Server: shaz.ns.cloudflare.com
Name Server: harley.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: https://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-11-12T10:20:33Z <<<

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

; The data in this registrar whois database is provided to you for
; information purposes only, and may be used to assist you in obtaining
; information about or related to domain name registration records.
; We do not guarantee its accuracy.
; By submitting a WHOIS query, you agree that you will use this data
; only for lawful purposes and that, under no circumstances, you will
; use this data to
; a) allow, enable, or otherwise support the transmission by e-mail,
;    telephone, or facsimile of mass, unsolicited, commercial advertising
;    or solicitations to entities other than the data recipient's own
;    existing customers; or
; b) enable high volume, automated, electronic processes that send queries
;    or data to the systems of any Registry Operator or ICANN-Accredited
;    registrar, except as reasonably necessary to register domain names
;    or modify existing registrations.
; The compilation, repackaging, dissemination or other use of this data
; is expressly prohibited without prior written consent.
; These terms may be changed without prior notice. By submitting this
```



```
; query, you agree to abide by this policy.
```

related domain names

registrar.eu openprovider.com icann.org cloudflare.com internic.net



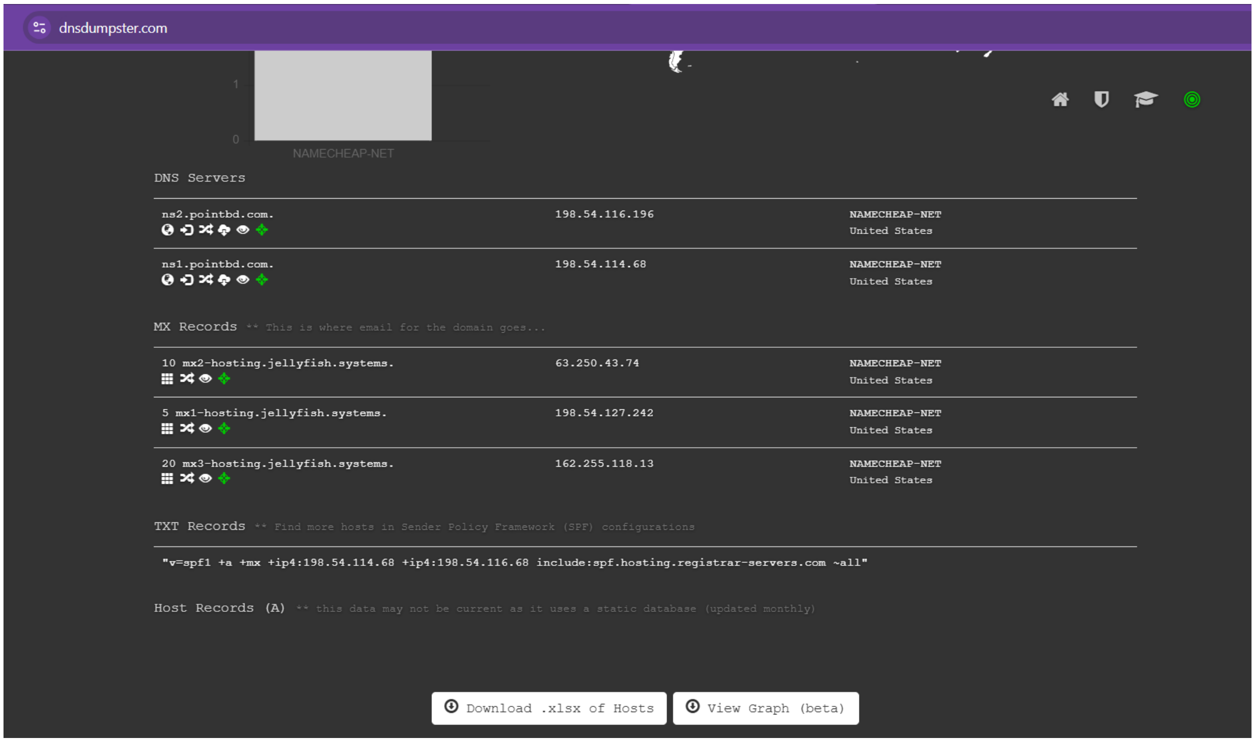
dns recon & research, find & lookup dns records

exampledomain.com

Showing results for **www.decodeslab.com**

Hosting (IP block owners)

GeoIP of Host Locations



DNS Servers

ns2.pointbd.com.	198.54.116.196	NAMECHEAP-NET United States
ns1.pointbd.com.	198.54.114.68	NAMECHEAP-NET United States

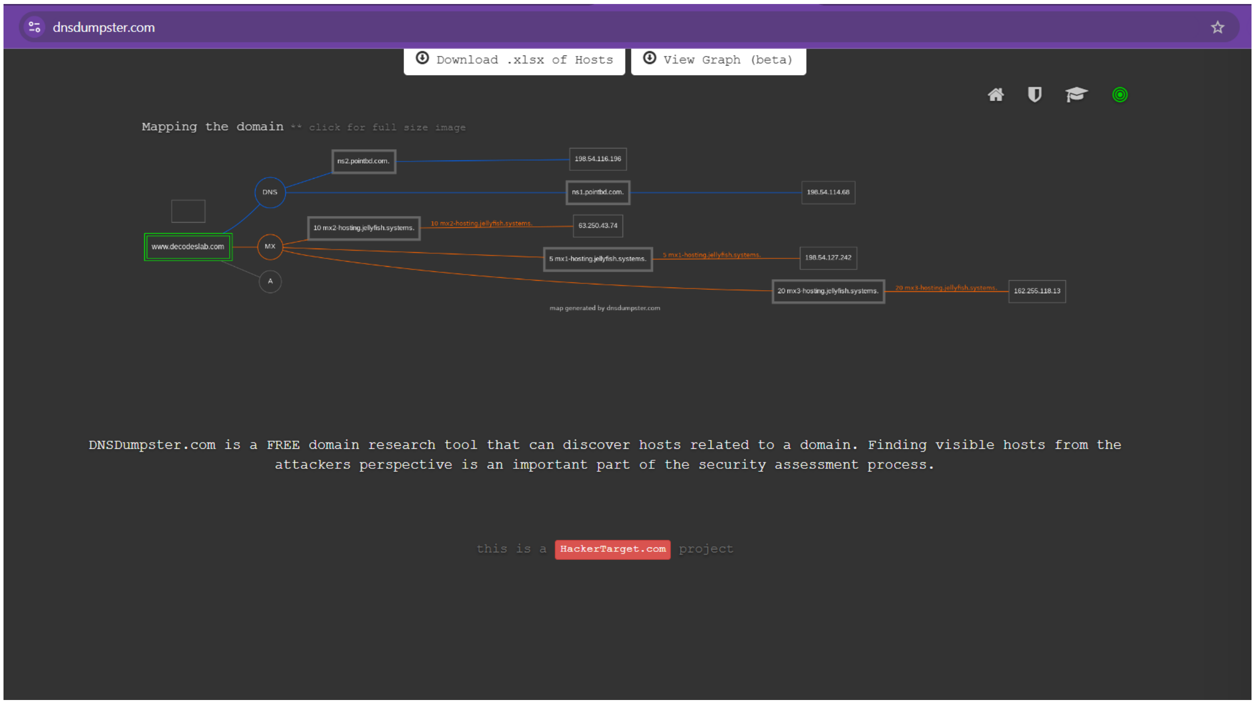
MX Records ** This is where email for the domain goes...

10 mx2-hosting.jellyfish.systems.	63.250.43.74	NAMECHEAP-NET United States
5 mx1-hosting.jellyfish.systems.	198.54.127.242	NAMECHEAP-NET United States
20 mx3-hosting.jellyfish.systems.	162.255.118.13	NAMECHEAP-NET United States

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

```
"v=spf1 +a +mx +ip4:198.54.114.68 +ip4:198.54.116.68 include:spf.hosting.registrar-servers.com ~all"
```

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

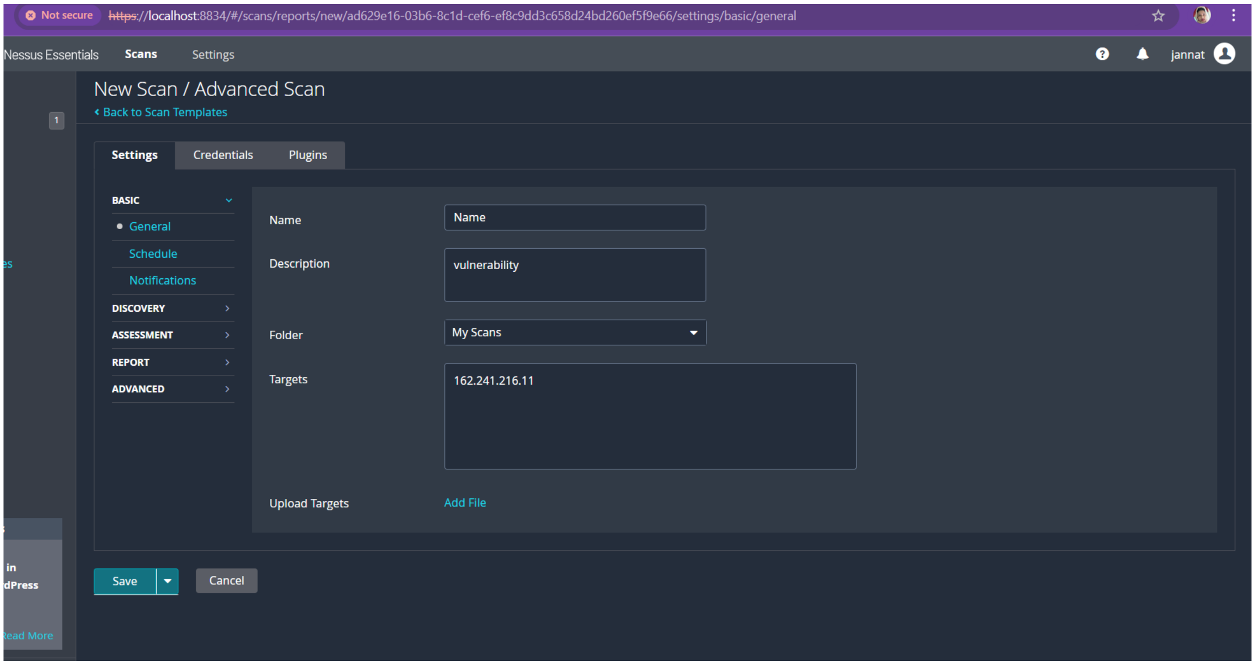

dnsdumpster.com
Download .xlsx of Hosts
View Graph (beta)
ns2.pointbd.com.
198.54.116.196
DNS
ns1.pointbd.com.
198.54.114.68
10 mx2-hosting.jellyfish.systems.
10 mx2-hosting.jellyfish.systems.
63.250.43.74
www.decodeslab.com
MX
5 mx1-hosting.jellyfish.systems.
5 mx1-hosting.jellyfish.systems.
198.54.127.242
A
20 mx3-hosting.jellyfish.systems.
20 mx3-hosting.jellyfish.systems.
162.255.118.13
map generated by dnsdumpster.com

Mapping the domain ** click for full size image

DNSDumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.

this is a HackerTarget.com project

Exercise 2 : Overview of Vulnerability Scanning



New Scan / Advanced Scan

‹ Back to Scan Templates

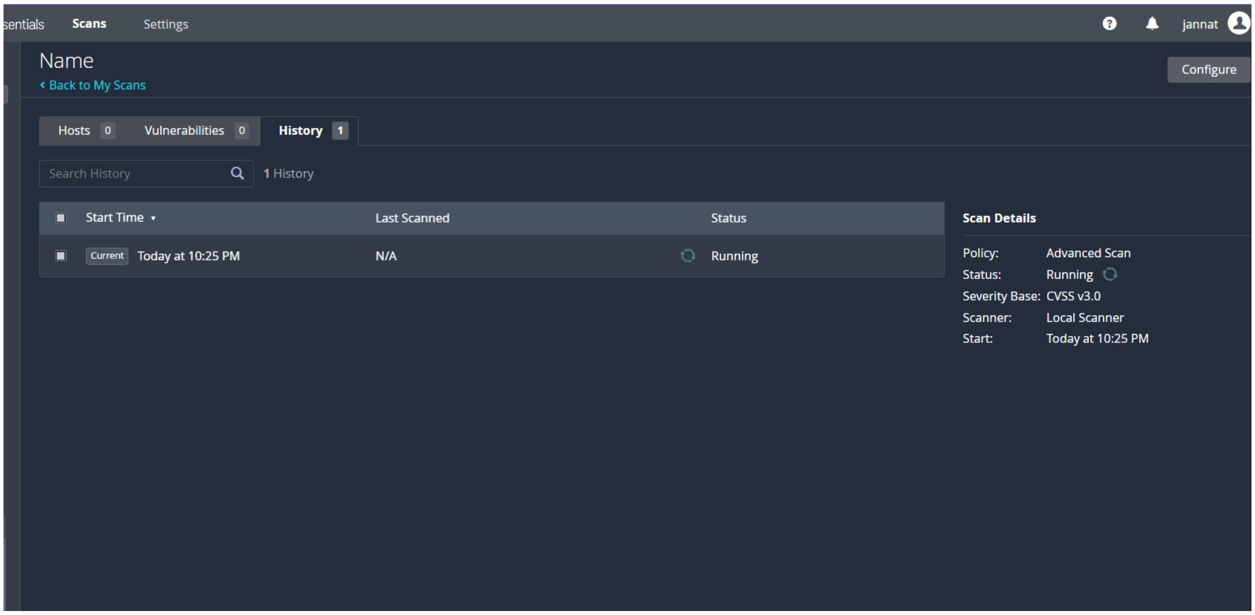
Name: Name

Description: vulnerability

Folder: My Scans

Targets: 162.241.216.11

Upload Targets: Add File



Name

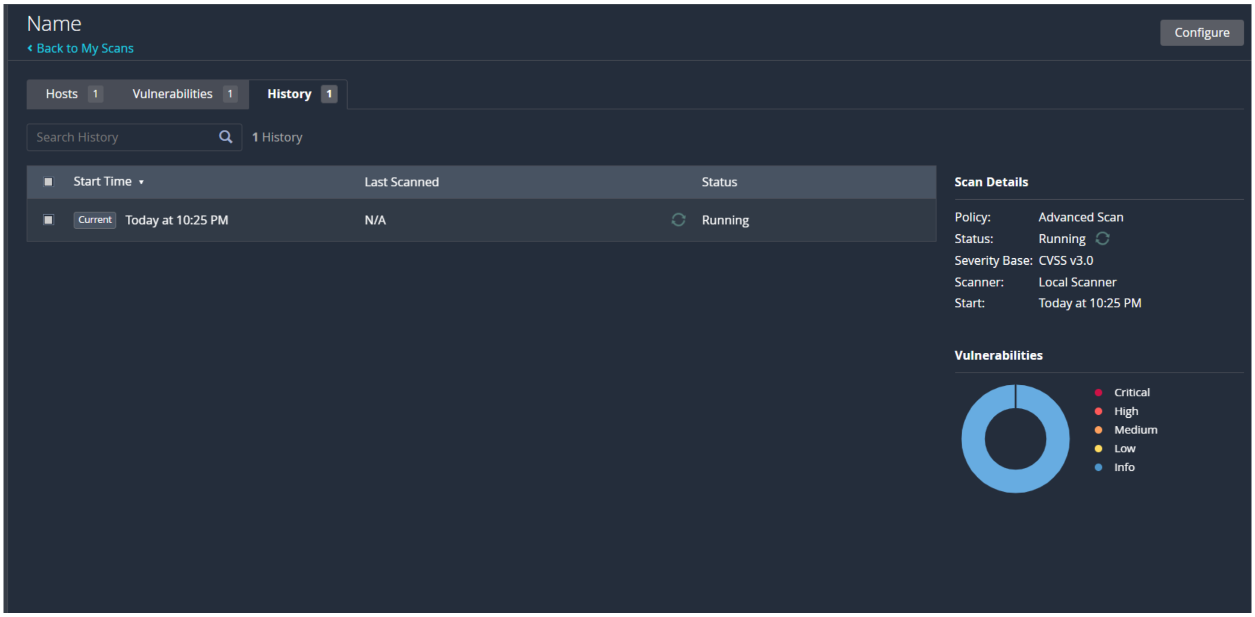
‹ Back to My Scans

1 History

■	Start Time ▾	Last Scanned	Status
■	Current Today at 10:25 PM	N/A	Running

Scan Details

Policy:	Advanced Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:25 PM



Name

‹ Back to My Scans

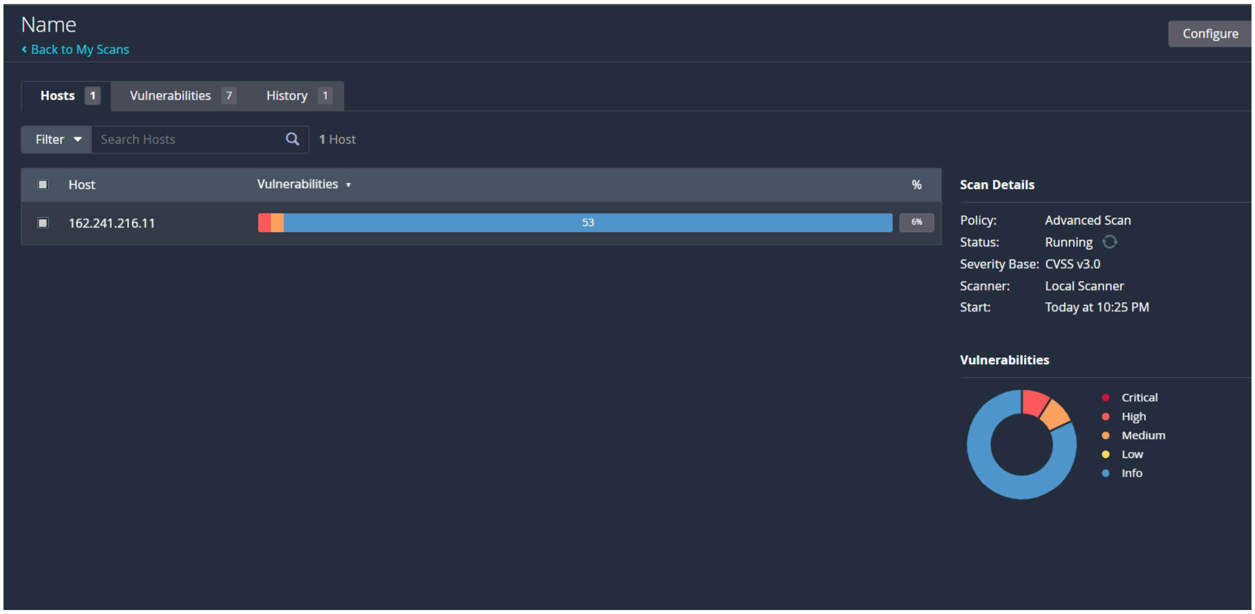
1 History

■	Start Time ▾	Last Scanned	Status
■	Current Today at 10:25 PM	N/A	Running

Scan Details

Policy:	Advanced Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:25 PM

Vulnerabilities



Name

‹ Back to My Scans

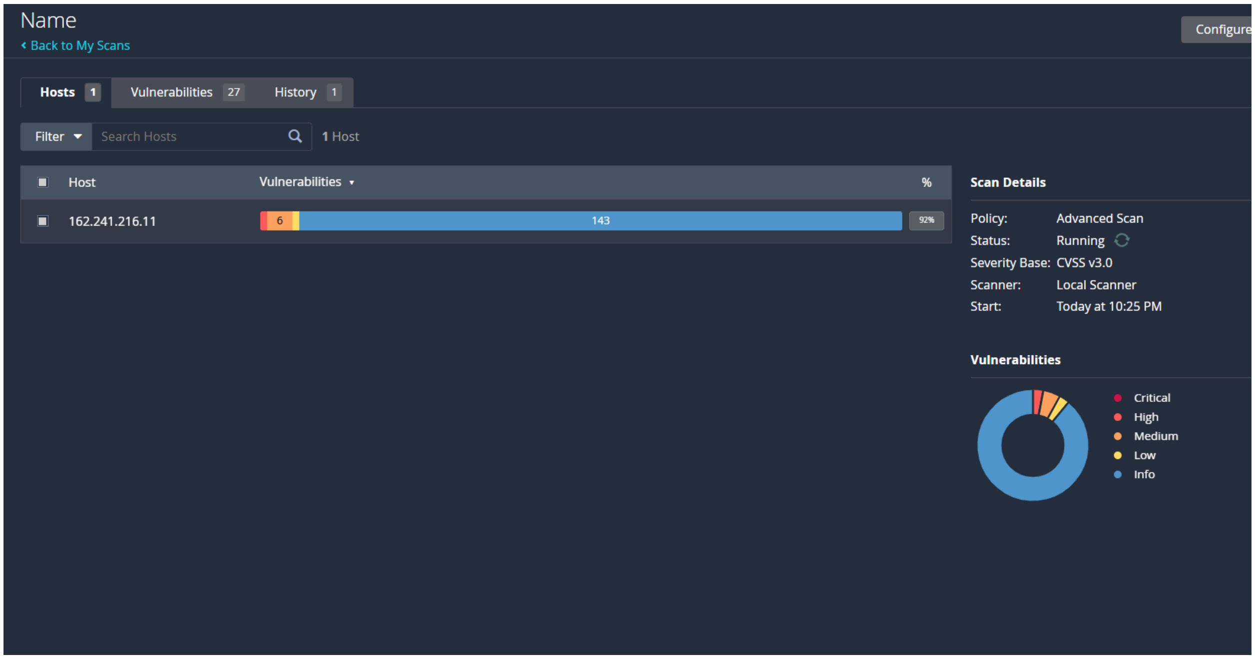
1 Host

■	Host	Vulnerabilities ▾	%
■	162.241.216.11	53	6%

Scan Details

Policy: Advanced Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:25 PM

Vulnerabilities



Name

‹ Back to My Scans

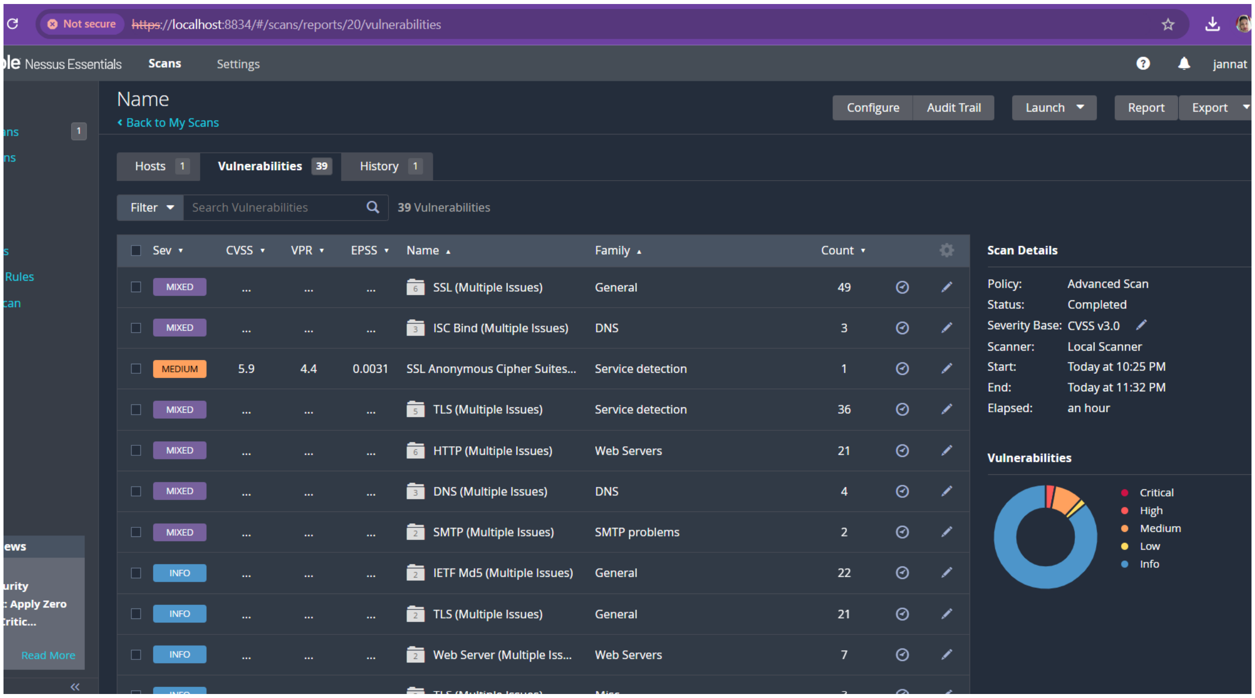
1 Host

■	Host	Vulnerabilities ▾	%
■	162.241.216.11	6 143	92%

Scan Details

Policy: Advanced Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:25 PM

Vulnerabilities



Not secure ~~https~~://localhost:8834/#/scans/reports/20/vulnerabilities

Nessus Essentials | Scans | Settings | jannat

Name

‹ Back to My Scans

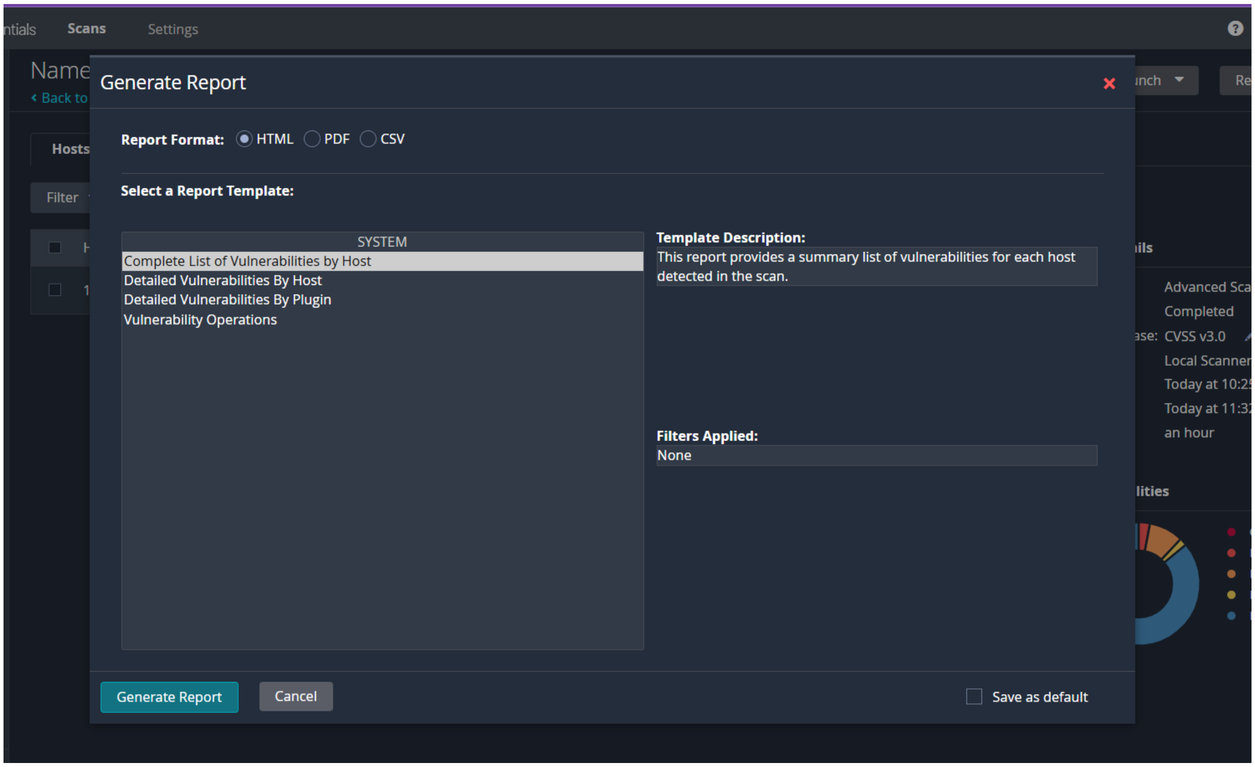
39 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MIXED	...	...	...	6 SSL (Multiple Issues)	General	49
MIXED	...	...	...	3 ISC Bind (Multiple Issues)	DNS	3
MEDIUM	5.9	4.4	0.0031	SSL Anonymous Cipher Suites...	Service detection	1
MIXED	...	...	...	5 TLS (Multiple Issues)	Service detection	36
MIXED	...	...	...	6 HTTP (Multiple Issues)	Web Servers	21
MIXED	...	...	...	3 DNS (Multiple Issues)	DNS	4
MIXED	...	...	...	2 SMTP (Multiple Issues)	SMTP problems	2
INFO	...	...	...	2 IETF Md5 (Multiple Issues)	General	22
INFO	...	...	...	2 TLS (Multiple Issues)	General	21
INFO	...	...	...	2 Web Server (Multiple Iss...	Web Servers	7

Scan Details

Policy:	Advanced Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:25 PM
End:	Today at 11:32 PM
Elapsed:	an hour

Vulnerabilities



Generate Report

Report Format: ● HTML ○ PDF ○ CSV

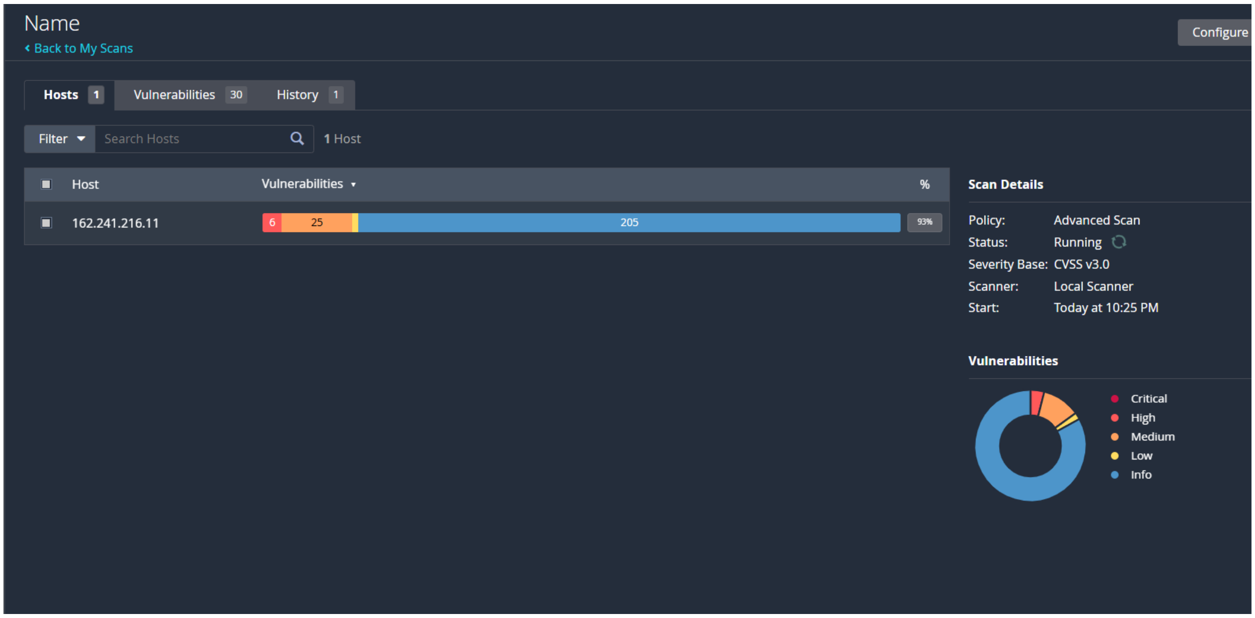
Select a Report Template:

SYSTEM
- Complete List of Vulnerabilities by Host
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

□ Save as default



Name

1 Host

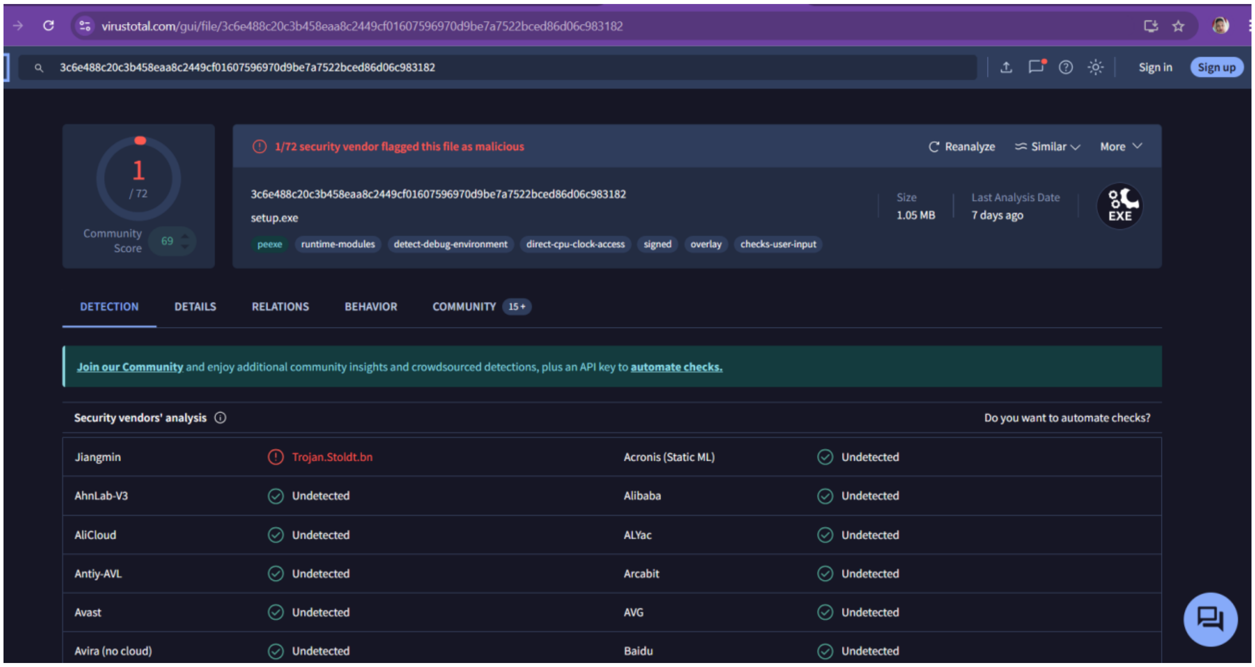
■	Host	Vulnerabilities	%
■	162.241.216.11	6 25 205	93%

Scan Details

Policy: Advanced Scan
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:25 PM

Vulnerabilities

Exercise 3 : Perform static malware analysis



virustotal.com/gui/file/3c6e488c20c3b458eaa8c2449cf01607596970d9be7a7522bced86d06c983182

3c6e488c20c3b458eaa8c2449cf01607596970d9be7a7522bced86d06c983182

1 / 72

Community Score 69

1/72 security vendor flagged this file as malicious

3c6e488c20c3b458eaa8c2449cf01607596970d9be7a7522bced86d06c983182
setup.exe

peexe runtime-modules detect-debug-environment direct-cpu-clock-access signed overlay checks-user-input

Size 1.05 MB

Last Analysis Date 7 days ago

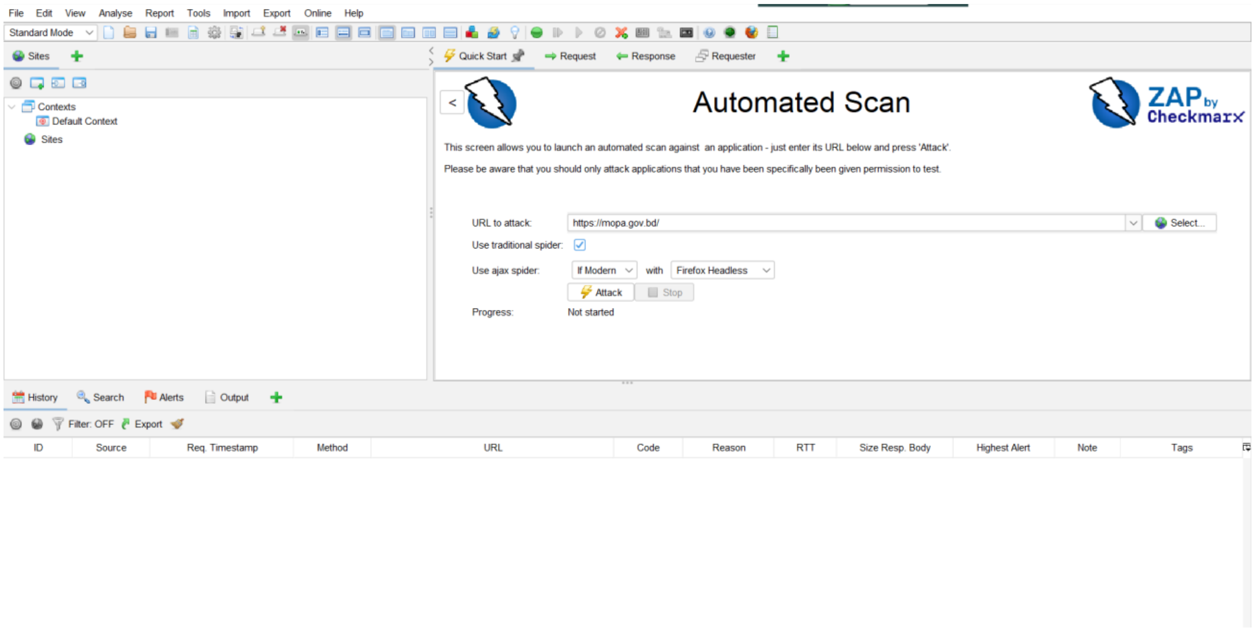
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Security vendors' analysis ⓘ

Do you want to automate checks?

Jiangmin	Trojan.Stoldt.bn	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
AliCloud	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	AVG	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected

Exercise 4 : Detect web application vulnerabilities using OWASP ZAP



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://mopa.gov.bd/ Select...

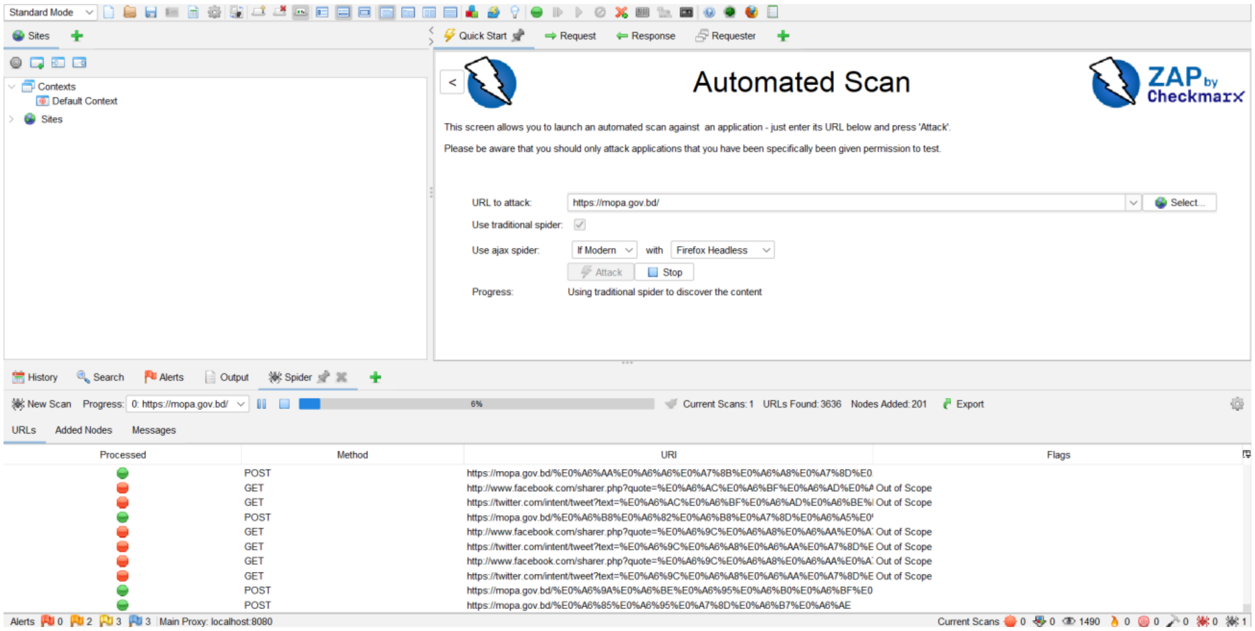
Use traditional spider: ☑

Use ajax spider: ☐ If Modern with Firefox Headless

Attack Stop

Progress: Not started

ID	Source	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://mopa.gov.bd/ Select...

Use traditional spider: ☑

Use ajax spider: ☐ If Modern with Firefox Headless

Attack Stop

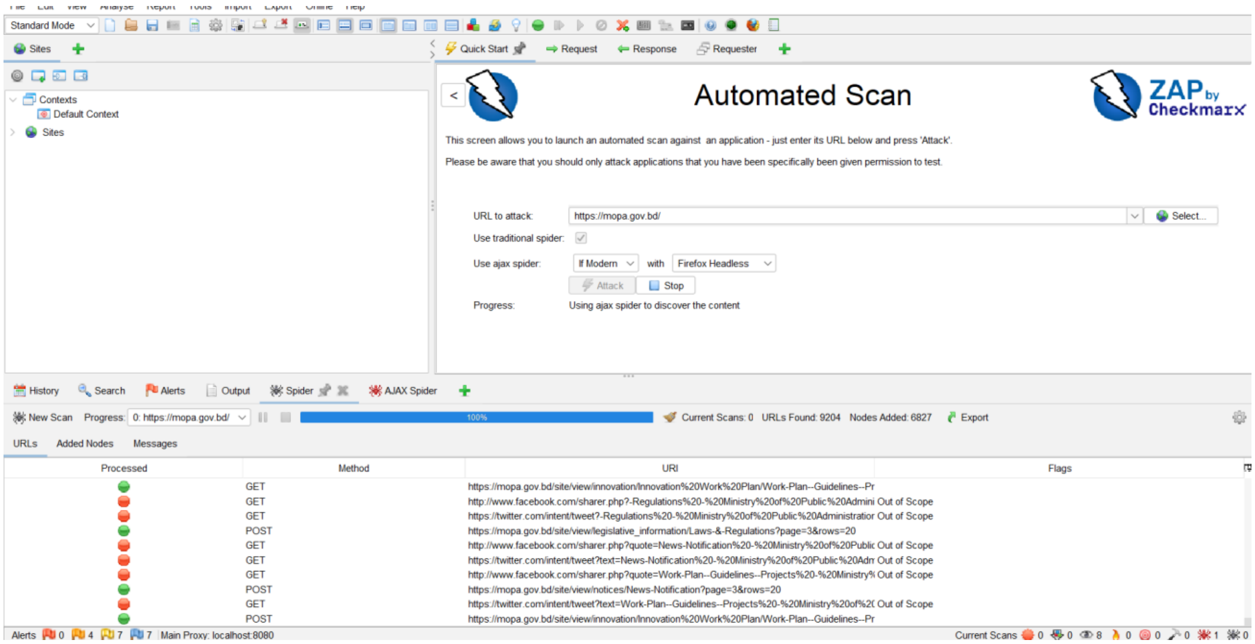
Progress: Using traditional spider to discover the content

New Scan Progress: 0: https://mopa.gov.bd/ 6% Current Scans: 1 URLs Found: 3636 Nodes Added: 201 Export

URLs Added Nodes Messages

Processed	Method	URI	Flags
●	POST	https://mopa.gov.bd/%E0%A6%AA%E0%A6%A6%E0%A7%8B%E0%A6%A8%E0%A7%8D%E0	
●	GET	http://www.facebook.com/sharer.php?quote=%E0%A6%AC%E0%A6%BF%E0%A6%AD%E0%A	Out of Scope
●	GET	https://twitter.com/intent/tweet?text=%E0%A6%AC%E0%A6%BF%E0%A6%AD%E0%A6%BE%	Out of Scope
●	POST	https://mopa.gov.bd/%E0%A6%B8%E0%A6%82%E0%A6%B8%E0%A7%8D%E0%A6%A5%E0	
●	GET	http://www.facebook.com/sharer.php?quote=%E0%A6%9C%E0%A6%A8%E0%A6%AA%E0%A	Out of Scope
●	GET	https://twitter.com/intent/tweet?text=%E0%A6%9C%E0%A6%A8%E0%A6%AA%E0%A7%8D%E	Out of Scope
●	GET	http://www.facebook.com/sharer.php?quote=%E0%A6%9C%E0%A6%A8%E0%A6%AA%E0%A	Out of Scope
●	GET	https://twitter.com/intent/tweet?text=%E0%A6%9C%E0%A6%A8%E0%A6%AA%E0%A7%8D%E	Out of Scope
●	POST	https://mopa.gov.bd/%E0%A6%9A%E0%A6%BE%E0%A6%95%E0%A6%B0%E0%A6%BF%E0	
●	POST	https://mopa.gov.bd/%E0%A6%85%E0%A6%95%E0%A7%8D%E0%A6%B7%E0%A6%AE	

Alerts 0 2 3 3 Main Proxy: localhost:8080 Current Scans 0 0 1490 0 0 0 0 1



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: https://mopa.gov.bd/

Use traditional spider: ☑

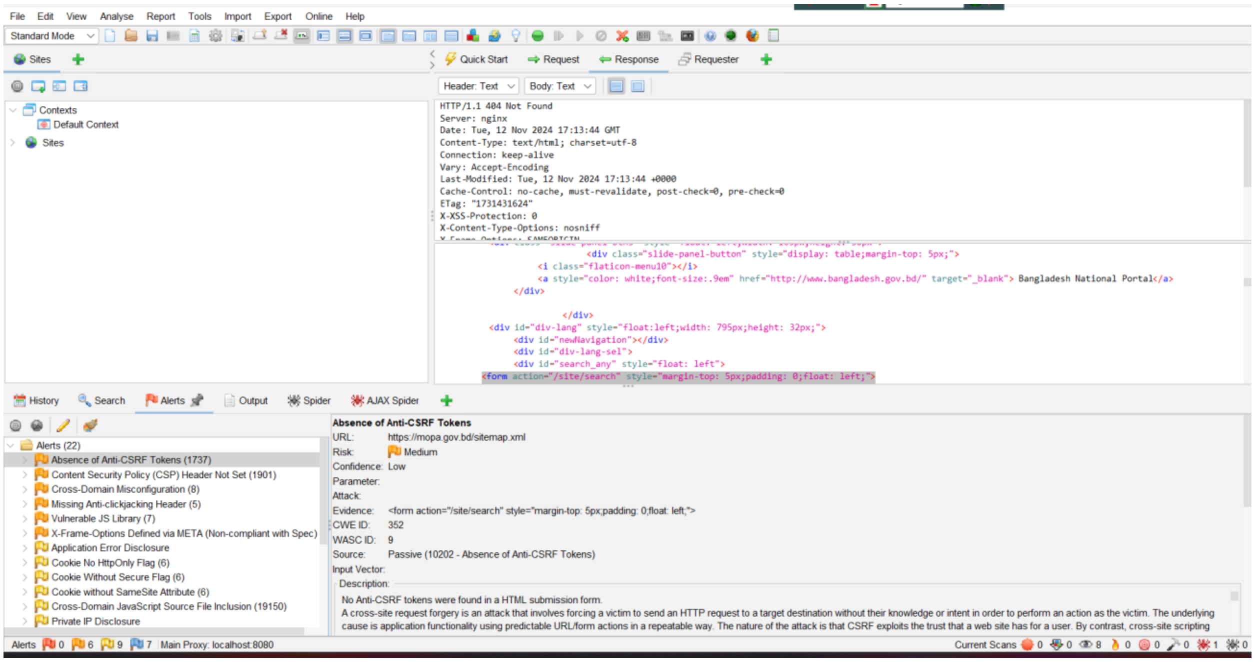
Use ajax spider: If Modern with Firefox Headless

Progress: Using ajax spider to discover the content

Progress: 0: https://mopa.gov.bd/ 100% Current Scans: 0 URLs Found: 9204 Nodes Added: 6827

Processed	Method	URI	Flags
🟢	GET	https://mopa.gov.bd/site/view/innovation/Innovation%20Work%20Plan/Work-Plan--Guidelines--Pr	
🔴	GET	http://www.facebook.com/sharer.php?-Regulations%20-%20Ministry%20of%20Public%20Admini	Out of Scope
🔴	GET	https://twitter.com/intent/tweet?-Regulations%20-%20Ministry%20of%20Public%20Administratior	Out of Scope
🟢	POST	https://mopa.gov.bd/site/view/legislative_information/Laws-&-Regulations?page=3&rows=20	
🔴	GET	http://www.facebook.com/sharer.php?quote=News-Notification%20-%20Ministry%20of%20Public	Out of Scope
🔴	GET	https://twitter.com/intent/tweet?text=News-Notification%20-%20Ministry%20of%20Public%20Adm	Out of Scope
🔴	GET	http://www.facebook.com/sharer.php?quote=Work-Plan--Guidelines--Projects%20-%20Ministry%	Out of Scope
🟢	POST	https://mopa.gov.bd/site/view/notices/News-Notification?page=3&rows=20	
🔴	GET	https://twitter.com/intent/tweet?text=Work-Plan--Guidelines--Projects%20-%20Ministry%20of%2(	Out of Scope
🟢	POST	https://mopa.gov.bd/site/view/innovation/Innovation%20Work%20Plan/Work-Plan--Guidelines--Pr	

Alerts 0 4 7 7 Main Proxy: localhost:8080 Current Scans 0 0 8 0 0 0 1 0



```
HTTP/1.1 404 Not Found
Server: nginx
Date: Tue, 12 Nov 2024 17:13:44 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
Vary: Accept-Encoding
Last-Modified: Tue, 12 Nov 2024 17:13:44 +0000
Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0
ETag: "1731431624"
X-XSS-Protection: 0
X-Content-Type-Options: nosniff
```

```
                <div class="slide-panel-button" style="display: table;margin-top: 5px;">
            <i class="flaticon-menu10"></i>
            <a style="color: white;font-size:.9em" href="http://www.bangladesh.gov.bd/" target="_blank"> Bangladesh National Portal</a>
        </div>

                </div>
    <div id="div-lang" style="float:left;width: 795px;height: 32px;">
        <div id="newNavigation"></div>
        <div id="div-lang-sel">
        <div id="search_any" style="float: left">
   <form action="/site/search" style="margin-top: 5px;padding: 0;float: left;">
```

Alerts (22)
- Absence of Anti-CSRF Tokens (1737)
- Content Security Policy (CSP) Header Not Set (1901)
- Cross-Domain Misconfiguration (8)
- Missing Anti-clickjacking Header (5)
- Vulnerable JS Library (7)
- X-Frame-Options Defined via META (Non-compliant with Spec)
- Application Error Disclosure
- Cookie No HttpOnly Flag (6)
- Cookie Without Secure Flag (6)
- Cookie without SameSite Attribute (6)
- Cross-Domain JavaScript Source File Inclusion (19150)
- Private IP Disclosure

Absence of Anti-CSRF Tokens

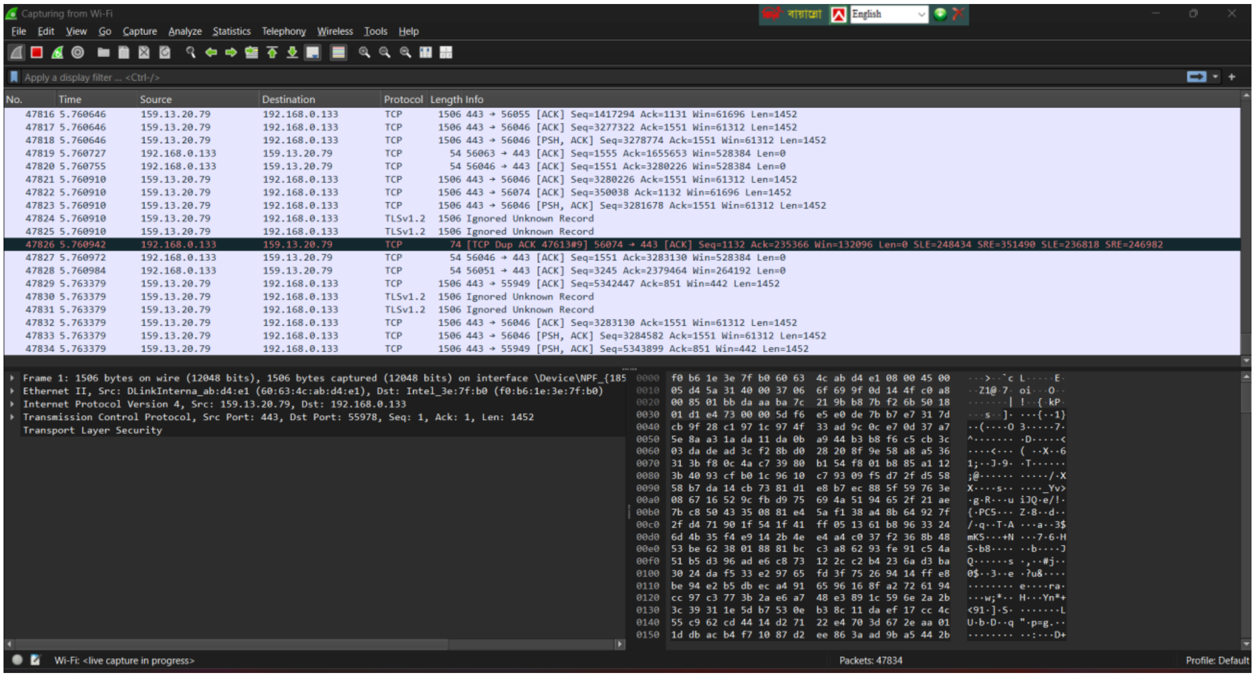
URL:	https://mopa.gov.bd/sitemap.xml
Risk:	Medium
Confidence:	Low
Parameter:	
Attack:	
Evidence:	<form action="/site/search" style="margin-top: 5px;padding: 0;float: left;">
CWE ID:	352
WASC ID:	9
Source:	Passive (10202 - Absence of Anti-CSRF Tokens)
Input Vector:	

Description:

No Anti-CSRF tokens were found in a HTML submission form.
A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting

Alerts 0 6 9 7 Main Proxy: localhost:8080 Current Scans 0 0 8 0 0 0 1 0

Exercise 5: Use wire shark to capture network traffic

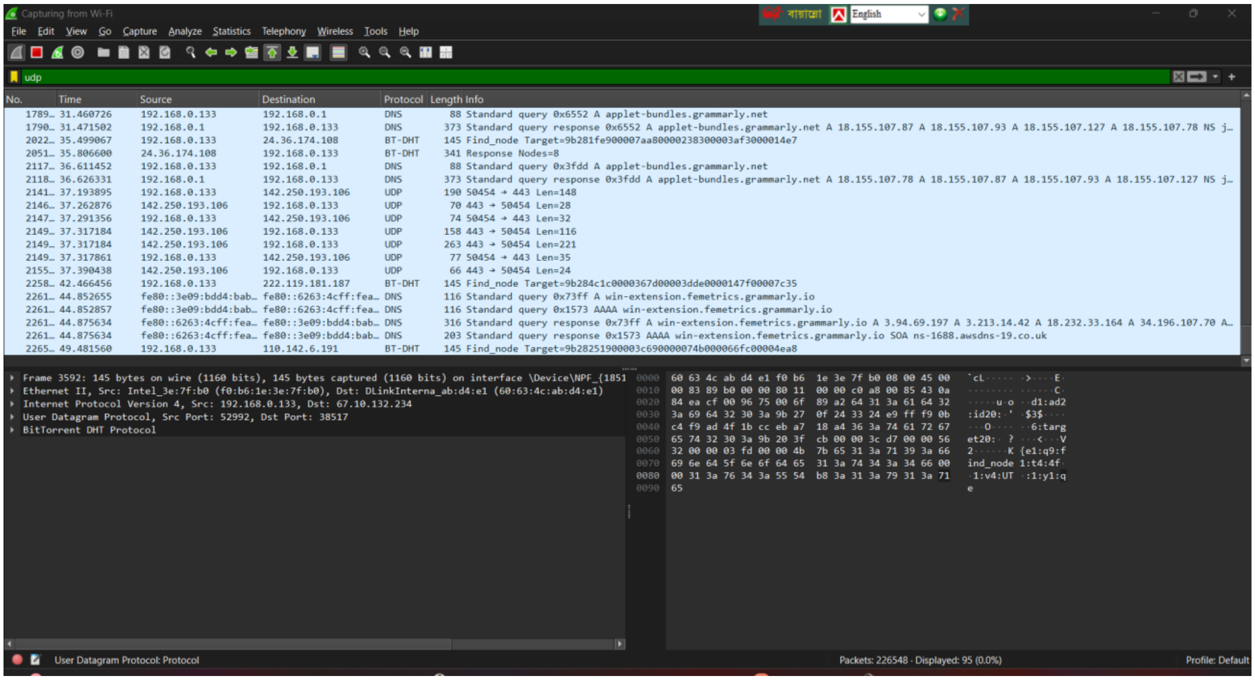

Capturing from Wi-Fi
বায়াজো
English
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.     Time      Source          Destination     Protocol Length Info
  47816 5.760646  159.13.20.79    192.168.0.133   TCP      1506 443 → 56055 [ACK] Seq=1417294 Ack=1131 Win=61696 Len=1452
  47817 5.760646  159.13.20.79    192.168.0.133   TCP      1506 443 → 56046 [ACK] Seq=3277322 Ack=1551 Win=61312 Len=1452
  47818 5.760646  159.13.20.79    192.168.0.133   TCP      1506 443 → 56046 [PSH, ACK] Seq=3278774 Ack=1551 Win=61312 Len=1452
  47819 5.760727  192.168.0.133   159.13.20.79    TCP        54 56063 → 443 [ACK] Seq=1555 Ack=1655653 Win=528384 Len=0
  47820 5.760755  192.168.0.133   159.13.20.79    TCP        54 56046 → 443 [ACK] Seq=1551 Ack=3280226 Win=528384 Len=0
  47821 5.760910  159.13.20.79    192.168.0.133   TCP      1506 443 → 56046 [ACK] Seq=3280226 Ack=1551 Win=61312 Len=1452
  47822 5.760910  159.13.20.79    192.168.0.133   TCP      1506 443 → 56074 [ACK] Seq=350038 Ack=1132 Win=61696 Len=1452
  47823 5.760910  159.13.20.79    192.168.0.133   TCP      1506 443 → 56046 [PSH, ACK] Seq=3281678 Ack=1551 Win=61312 Len=1452
  47824 5.760910  159.13.20.79    192.168.0.133   TLSv1.2  1506 Ignored Unknown Record
  47825 5.760910  159.13.20.79    192.168.0.133   TLSv1.2  1506 Ignored Unknown Record
  47826 5.760942  192.168.0.133   159.13.20.79    TCP        74 [TCP Dup ACK 47613#9] 56074 → 443 [ACK] Seq=1132 Ack=235366 Win=132096 Len=0 SLE=248434 SRE=351490 SLE=236818 SRE=246982
  47827 5.760972  192.168.0.133   159.13.20.79    TCP        54 56046 → 443 [ACK] Seq=1551 Ack=3283130 Win=528384 Len=0
  47828 5.760984  192.168.0.133   159.13.20.79    TCP        54 56051 → 443 [ACK] Seq=3245 Ack=2379464 Win=264192 Len=0
  47829 5.763379  159.13.20.79    192.168.0.133   TCP      1506 443 → 55949 [ACK] Seq=5342447 Ack=851 Win=442 Len=1452
  47830 5.763379  159.13.20.79    192.168.0.133   TLSv1.2  1506 Ignored Unknown Record
  47831 5.763379  159.13.20.79    192.168.0.133   TLSv1.2  1506 Ignored Unknown Record
  47832 5.763379  159.13.20.79    192.168.0.133   TCP      1506 443 → 56046 [ACK] Seq=3283130 Ack=1551 Win=61312 Len=1452
  47833 5.763379  159.13.20.79    192.168.0.133   TCP      1506 443 → 56046 [PSH, ACK] Seq=3284582 Ack=1551 Win=61312 Len=1452
  47834 5.763379  159.13.20.79    192.168.0.133   TCP      1506 443 → 55949 [PSH, ACK] Seq=5343899 Ack=851 Win=442 Len=1452
```

```
▸ Frame 1: 1506 bytes on wire (12048 bits), 1506 bytes captured (12048 bits) on interface \Device\NPF_{185
▸ Ethernet II, Src: DLinkInterna_ab:d4:e1 (60:63:4c:ab:d4:e1), Dst: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0)
▸ Internet Protocol Version 4, Src: 159.13.20.79, Dst: 192.168.0.133
▸ Transmission Control Protocol, Src Port: 443, Dst Port: 55978, Seq: 1, Ack: 1, Len: 1452
  Transport Layer Security
```

```
0000  f0 b6 1e 3e 7f b0 60 63  4c ab d4 e1 08 00 45 00   ···>··`c L·····E·
0010  05 d4 5a 31 40 00 37 06  6f 69 9f 0d 14 4f c0 a8   ··Z1@·7· oi···O··
0020  00 85 01 bb da aa ba 7c  21 9b b8 7b f2 6b 50 18   ·······| !··{·kP·
0030  01 d1 e4 73 00 00 5d f6  e5 e0 de 7b b7 e7 31 7d   ···s··]· ···{··1}
0040  cb 9f 28 c1 97 1c 97 4f  33 ad 9c 0c e7 0d 37 a7   ··(····O 3·····7·
0050  5e 8a a3 1a da 11 da 0b  a9 44 b3 b8 f6 c5 cb 3c   ^······· ·D·····<
0060  03 da de ad 3c f2 8b d0  28 20 8f 9e 58 a8 a5 36   ····<··· ( ··X··6
0070  31 3b f8 0c 4a c7 39 80  b1 54 f8 01 b8 85 a1 12   1;··J·9· ·T······
0080  3b 40 93 cf b0 1c 96 10  c7 93 09 f5 d7 2f d5 58   ;@······ ·····/·X
0090  58 b7 da 14 cb 73 81 d1  e8 b7 ec 88 5f 59 76 3e   X····s·· ····_Yv>
00a0  08 67 16 52 9c fb d9 75  69 4a 51 94 65 2f 21 ae   ·g·R···u iJQ·e/!·
00b0  7b c8 50 43 35 08 81 e4  5a f1 38 a4 8b 64 92 7f   {·PC5··· Z·8··d··
00c0  2f d4 71 90 1f 54 1f 41  ff 05 13 61 b8 96 33 24   /·q··T·A ···a··3$
00d0  6d 4b 35 f4 e9 14 2b 4e  e4 a4 c0 37 f2 36 8b 48   mK5···+N ···7·6·H
00e0  53 be 62 38 01 88 81 bc  c3 a8 62 93 fe 91 c5 4a   S·b8···· ··b····J
00f0  51 b5 d3 96 ad e6 c8 73  12 2c c2 b4 23 6a d3 ba   Q······s ·,··#j··
0100  30 24 da f5 33 e2 97 65  fd 3f 75 26 94 14 ff e8   0$··3··e ·?u&····
0110  be 94 e2 b5 db ec a4 91  65 96 16 8f a2 72 61 94   ········ e····ra·
0120  cc 97 c3 77 3b 2a e6 a7  48 e3 89 1c 59 6e 2a 2b   ···w;*·· H···Yn*+
0130  3c 39 31 1e 5d b7 53 0e  b3 8c 11 da ef 17 cc 4c   <91·]·S· ·······L
0140  55 c9 62 cd 44 14 d2 71  22 e4 70 3d 67 2e aa 01   U·b·D··q "·p=g.··
0150  1d db ac b4 f7 10 87 d2  ee 86 3a ad 9b a5 44 2b   ········ ··:···D+
```

Wi-Fi: <live capture in progress>   Packets: 47834   Profile: Default


Capturing from Wi-Fi
বায়াজো
English
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp

```
No.     Time       Source               Destination          Protocol Length Info
  1789… 31.460726  192.168.0.133        192.168.0.1          DNS       88 Standard query 0x6552 A applet-bundles.grammarly.net
  1790… 31.471502  192.168.0.1          192.168.0.133        DNS      373 Standard query response 0x6552 A applet-bundles.grammarly.net A 18.155.107.87 A 18.155.107.93 A 18.155.107.127 A 18.155.107.78 NS j…
  2022… 35.499067  192.168.0.133        24.36.174.108        BT-DHT   145 Find_node Target=9b281fe900007aa80000238300003af3000014e7
  2051… 35.806600  24.36.174.108        192.168.0.133        BT-DHT   341 Response Nodes=8
  2117… 36.611452  192.168.0.133        192.168.0.1          DNS       88 Standard query 0x3fdd A applet-bundles.grammarly.net
  2118… 36.626331  192.168.0.1          192.168.0.133        DNS      373 Standard query response 0x3fdd A applet-bundles.grammarly.net A 18.155.107.78 A 18.155.107.87 A 18.155.107.93 A 18.155.107.127 NS j…
  2141… 37.193895  192.168.0.133        142.250.193.106      UDP      190 50454 → 443 Len=148
  2146… 37.262876  142.250.193.106      192.168.0.133        UDP       70 443 → 50454 Len=28
  2147… 37.291356  192.168.0.133        142.250.193.106      UDP       74 50454 → 443 Len=32
  2149… 37.317184  142.250.193.106      192.168.0.133        UDP      158 443 → 50454 Len=116
  2149… 37.317184  142.250.193.106      192.168.0.133        UDP      263 443 → 50454 Len=221
  2149… 37.317861  192.168.0.133        142.250.193.106      UDP       77 50454 → 443 Len=35
  2155… 37.390438  142.250.193.106      192.168.0.133        UDP       66 443 → 50454 Len=24
  2258… 42.466456  192.168.0.133        222.119.181.187      BT-DHT   145 Find_node Target=9b284c1c0000367d00003dde0000147f00007c35
  2261… 44.852655  fe80::3e09:bdd4:bab… fe80::6263:4cff:fea… DNS      116 Standard query 0x73ff A win-extension.femetrics.grammarly.io
  2261… 44.852857  fe80::3e09:bdd4:bab… fe80::6263:4cff:fea… DNS      116 Standard query 0x1573 AAAA win-extension.femetrics.grammarly.io
  2261… 44.875634  fe80::6263:4cff:fea… fe80::3e09:bdd4:bab… DNS      316 Standard query response 0x73ff A win-extension.femetrics.grammarly.io A 3.94.69.197 A 3.213.14.42 A 18.232.33.164 A 34.196.107.70 A…
  2261… 44.875634  fe80::6263:4cff:fea… fe80::3e09:bdd4:bab… DNS      203 Standard query response 0x1573 AAAA win-extension.femetrics.grammarly.io SOA ns-1688.awsdns-19.co.uk
  2265… 49.481560  192.168.0.133        110.142.6.191        BT-DHT   145 Find_node Target=9b28251900003c690000074b000066fc00004ea8
```

```
▸ Frame 3592: 145 bytes on wire (1160 bits), 145 bytes captured (1160 bits) on interface \Device\NPF_{1851
▸ Ethernet II, Src: Intel_3e:7f:b0 (f0:b6:1e:3e:7f:b0), Dst: DLinkInterna_ab:d4:e1 (60:63:4c:ab:d4:e1)
▸ Internet Protocol Version 4, Src: 192.168.0.133, Dst: 67.10.132.234
▸ User Datagram Protocol, Src Port: 52992, Dst Port: 38517
▸ BitTorrent DHT Protocol
```

```
0000  60 63 4c ab d4 e1 f0 b6  1e 3e 7f b0 08 00 45 00   `cL····· ·>····E·
0010  00 83 89 b0 00 00 80 11  00 00 c0 a8 00 85 43 0a   ········ ······C·
0020  84 ea cf 00 96 75 00 6f  89 a2 64 31 3a 61 64 32   ·····u·o ··d1:ad2
0030  3a 69 64 32 30 3a 9b 27  0f 24 33 24 e9 ff f9 0b   :id20:·' ·$3$····
0040  c4 f9 ad 4f 1b cc eb a7  18 a4 36 3a 74 61 72 67   ···O···· ··6:targ
0050  65 74 32 30 3a 9b 20 3f  cb 00 00 3c d7 00 00 56   et20:· ? ···<···V
0060  32 00 00 03 fd 00 00 4b  7b 65 31 3a 71 39 3a 66   2······K {e1:q9:f
0070  69 6e 64 5f 6e 6f 64 65  31 3a 74 34 3a 34 66 00   ind_node 1:t4:4f·
0080  00 31 3a 76 34 3a 55 54  b8 3a 31 3a 79 31 3a 71   ·1:v4:UT ·:1:y1:q
0090  65                                                 e
```

User Datagram Protocol: Protocol   Packets: 226548 · Displayed: 95 (0.0%)   Profile: Default