Client – Confidential

Project	Date
Vulnerability Assessment	10/12/25
Document Classification	Version
Client Confidential	1
Prepared By	Suvhankar Dutta

1.Document Control.

1.1. Document Details

Document Refrence	Property
Document Classification	Client Confidential
Client Name	Atha Group
Document Title	Testing Report
Author	Indian Cyber Security Solutions
Date	10/12/25

1.2 Revision History

Version	Date	Issued By	Summary of Changes
1	10/12/2025	Indian Cyber Security Solutions	Final Draft

1.3 Document Distributing List

Name	Organization	Role
Suvhankar Dutta	Indian Cyber Security Solutions	Cybersecurity Analyst

https://athagroup.in/

Scan Time	: 10-12-2025 16:47:07 (UTC+05:30)
Scan Duration	: 00:00:06:33
Total Requests	: 1,291
Average Speed	: 3.3r/s

Risk Level:
MEDIUM

0
HIGH

1
MEDIUM
0
CONFIRMED

0
CRITICAL

Identified Vulnerabilities

Critical	0
High	0
Medium	1
Low	0
Best Practice	0
Information	1
TOTAL	**2**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	0
Low	0
Best Practice	0
Information	0
TOTAL	**0**

LOW

0
BEST PRACTICE

1
INFORMATION

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://athagroup.in/	No Parameters	No Parameter Types
	Apache Web Server Identified	GET	https://athagroup.in/	No Parameters	No Parameter Types

1. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM | 1

Invicti Standard identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Vulnerabilities

1.1. https://athagroup.in/

Certainty

Request | Response

Response

Response Time (ms) : 220.3049
Total Bytes Received : 535
Body Length : 273
Is Compressed : No

```
HTTP/1.1 301 Moved Permanently
Server: Apache
Expires: Fri, 09 Jan 2026 11:17:08 GMT
Content-Length: 273
Content-Type: text/html; charset=iso-8859-1
Location: https://www.athagroup.in/
Date: Wed, 10 Dec 2025 11:17:08 GMT
Cache-Control: max-age=2592000

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.athagroup.in/">here</a>.</p>
</body></html>
```

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
        ServerAlias *
        RewriteEngine On
        RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
        # Use HTTP Strict Transport Security to force client to use secure connections only Header always set Strict-Transport-
        Security "max-age=31536000; includeSubDomains"

        # Further Configuration goes here [...]
</VirtualHost>
```

External References

- Wikipedia - HTTP Strict Transport Security
- Configure HSTS (HTTP Strict Transport Security) for Apache/Nginx • HTTP Strict Transport Security (HSTS) HTTP Header
- Mozilla SSL Configuration Generator

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	523
CAPEC	217
WASC	4
ASVS 4.0	14.4.5
NIST SP 800-53	SC-8
DISA STIG	V-6136
ISO27001	A.14.1.2
ISO27001 2022	A.8.24
OWASP Top Ten 2021	A02

CVSS 3.0 SCORE

Base	7.7 (High)
Temporal	7.7 (High)
Environmental	7.7 (High)

CVSS Vector String

CVSS Vector String
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L

CVSS 3.1 SCORE	
Base	7.7 (High)
Temporal	7.7 (High)
Environmental	7.7 (High)

CVSS Vector String
CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L

CVSS 4.0 Score	
0 / None	
Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low
Exploitation	High
Security requirements	Medium

CVSS Vector String
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N

2. Apache Web Server Identified

INFORMATION | 1

Invicti Standard identified a web server (Apache) in the target web server's HTTP response.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

2.1. https://athagroup.in/

Certainty

Request | Response

Response

Response Time (ms) : 1453.8715
Total Bytes Received : 584
Body Length : 273
Is Compressed : No

```
HTTP/1.1 301 Moved Permanently
Server: Apache

Expires: Fri, 09 Jan 2026 11:17:04 GMT
Connection: Keep-Alive
Keep-Alive: timeout=100
Content-Length: 273
Content-Type: text/html; charset=iso-8859-1
Location: https://www.athagroup.in/
Date: Wed, 10 Dec 2025 11:17:04 GMT
Cache-Control: max-age=2592000

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.athagroup.in/">here</a>.</p>
</body></html>
```

External References

- Apache ServerTokens Directive

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

CVSS 3.0 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String

CVSS Vector String
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

CVSS 3.1 SCORE

Base	5.3 (Medium)
Temporal	5.1 (Medium)
Environmental	5.1 (Medium)

CVSS Vector String
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:H/RL:O/RC:C

Show Scan Detail

Enabled Security Checks	:	**ActiveMQ OpenWire RCE, Apache Struts S2-045 RCE, Apache Struts S2-046 RCE, BREACH Attack, Code Evaluation, Code Evaluation (Out of Band), Command Injection, Command Injection (Blind), Content Security Policy, Content-Type Sniffing, Cookie, Cross-Origin Resource Sharing (CORS), Cross-Site Request Forgery, Cross-site Scripting, Cross-site Scripting (Blind), Custom DOM XSS, Drupal Remote Code Execution, Expression Language Injection, File Upload, GraphQL Library Detection,**

		HSTS, **HTML Content,** **HTTP Header Injection,** **HTTP Methods,** **HTTP Status,** **HTTP.sys (CVE-2015-1635),** **IFrame Security,** **Insecure JSONP Endpoint,** **Insecure Reflected Content,** **JavaScript Libraries,** **Local File Inclusion,** **Log4j Code Evaluation (Out of Band),** **Mixed Content,** **MongoDB Injection (Blind), MongoDB Injection (Boolean), MongoDB Injection (Error Based), MongoDB Injection (Operator),** **Open Redirection,** **Oracle EBS RCE,** **Oracle WebLogic Remote Code Execution, Referrer Policy,** **Reflected File Download,** **RegreSSHion Attack,** **Remote File Inclusion,** **Remote File Inclusion (Out of Band),** **RoR Code Execution,** **Security Assertion Markup Language (SAML),** **Sensitive Data,** **Server-Side Request Forgery (DNS),** **Server-Side Request Forgery (Pattern Based),** **Server-Side Template Injection,** **Signatures,** **Spring4Shell Remote Code Execution, SQL Injection (Blind),** **SQL Injection (Boolean),** **SQL Injection (Error Based),** **SQL Injection (Out of Band),** **SSL,** **Static Resources (All Paths),** **Static Resources (Only Root Path),** **TorchServe Management,** **VmWare Aria RCE,** **Web App Fingerprint,** **Web Cache Deception,** **WebDAV,** **Windows Short Filename,** **Wordpress Plugin Detection,** **XML External Entity,** **XML External Entity (Out of Band)**
URL Rewrite Mode	**:**	**Heuristic**

Detected URL Rewrite Rule(s)	:	**None**
Excluded URL Patterns	:	**gtm\.js** **WebResource\.axd** **ScriptResource\.axd**
Authentication	:	**None**
Authentication Profile	:	**None**
Scheduled	:	**No**
Additional Website(s)	:	**https://www.athagroup.in/**

```
┌──(mamba㉿Bheem)-[~]
└─$ gobuster dir \
-u http://athagroup.in \
-w /usr/share/wordlists/dirb/common.txt \
-t 20 \
--no-error

===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://athagroup.in
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8.2
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 0 / 1 (0.00%)
2025/12/15 17:36:59 the server returns a status code that matches the provided options for non existing urls. http://athagroup.in/b22c3975-9f74-4b81-80fc-5ced71c2199a ⇒ 301 (redirect to htt
ps://www.athagroup.in/b22c3975-9f74-4b81-80fc-5ced71c2199a) (Length: 309). Please exclude the response length or the status code or set the wildcard option.. To continue please exclude the s
tatus code or the length

┌──(mamba㉿Bheem)-[~]
└─$ curl -I http://athagroup.in/thispathdoesnotexist123

HTTP/1.1 301 Moved Permanently
Date: Mon, 15 Dec 2025 12:07:21 GMT
Server: Apache
Location: https://www.athagroup.in/thispathdoesnotexist123
Cache-Control: max-age=2592000
Expires: Wed, 14 Jan 2026 12:07:21 GMT
Content-Type: text/html; charset=iso-8859-1
```

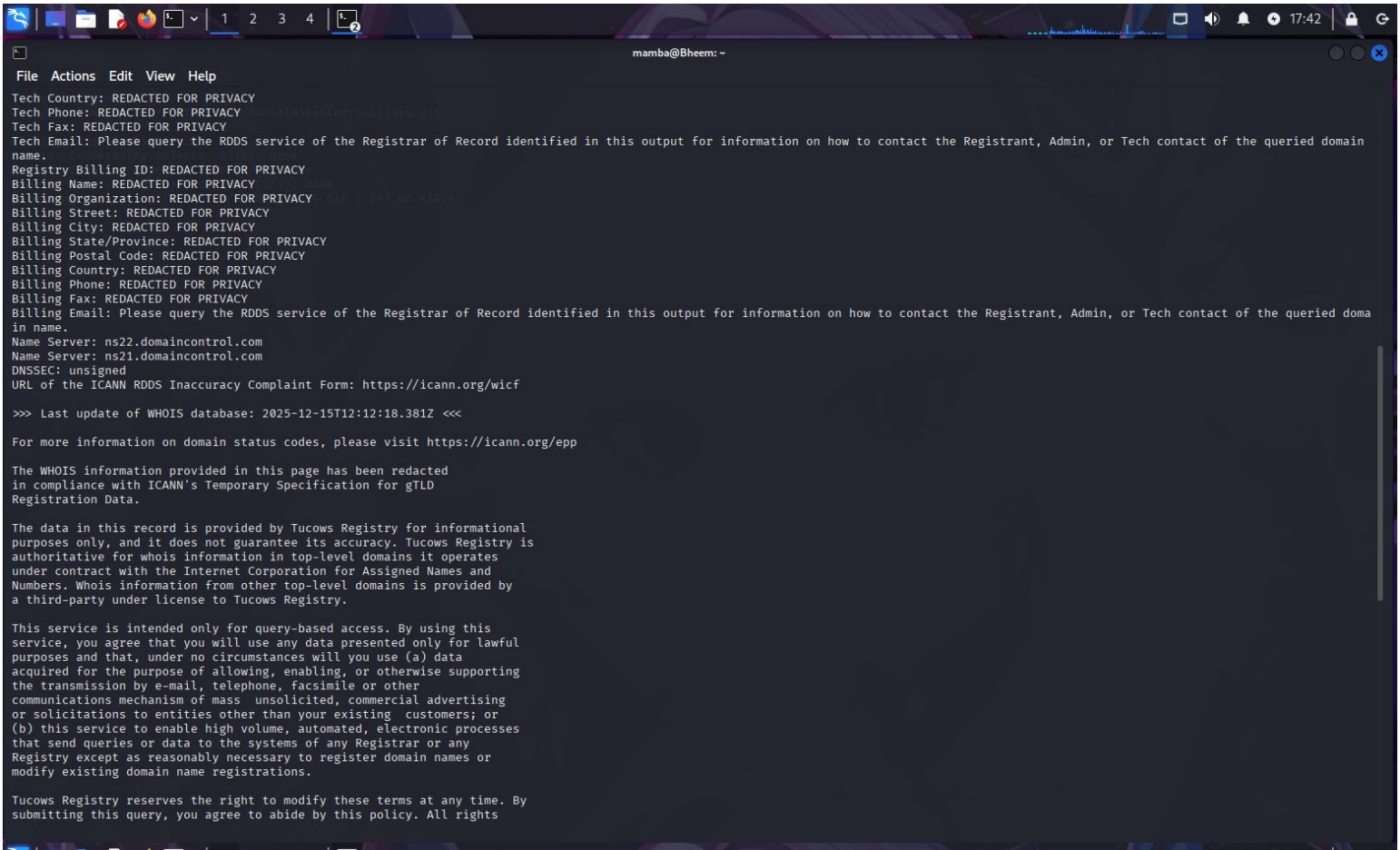
```
┌──(mamba㉿Bheem)-[~]
└─$ curl -I http://athagroup.in/thispathdoesnotexist123

HTTP/1.1 301 Moved Permanently
Date: Mon, 15 Dec 2025 12:07:21 GMT
Server: Apache
Location: https://www.athagroup.in/thispathdoesnotexist123
Cache-Control: max-age=2592000
Expires: Wed, 14 Jan 2026 12:07:21 GMT
Content-Type: text/html; charset=iso-8859-1


┌──(mamba㉿Bheem)-[~]
└─$ gobuster dir \
-u http://athagroup.in \
-w /usr/share/wordlists/dirb/common.txt \
-t 20 \
--no-error \
--exclude-length 12345

===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://athagroup.in
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] Exclude Length:          12345
[+] User Agent:              gobuster/3.8.2
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 0 / 1 (0.00%)
2025/12/15 17:37:48 the server returns a status code that matches the provided options for non existing urls. http://athagroup.in/27bef87c-32c2-4da7-9c33-7afb5b8fcf0d ⇒ 301 (redirect to https://www.athagroup.in/27bef87c-32c2-4da7-9c33-7afb5b8fcf0d) (Length: 309). Please exclude the response length or the status code or set the wildcard option.. To continue please exclude the status code or the length
```

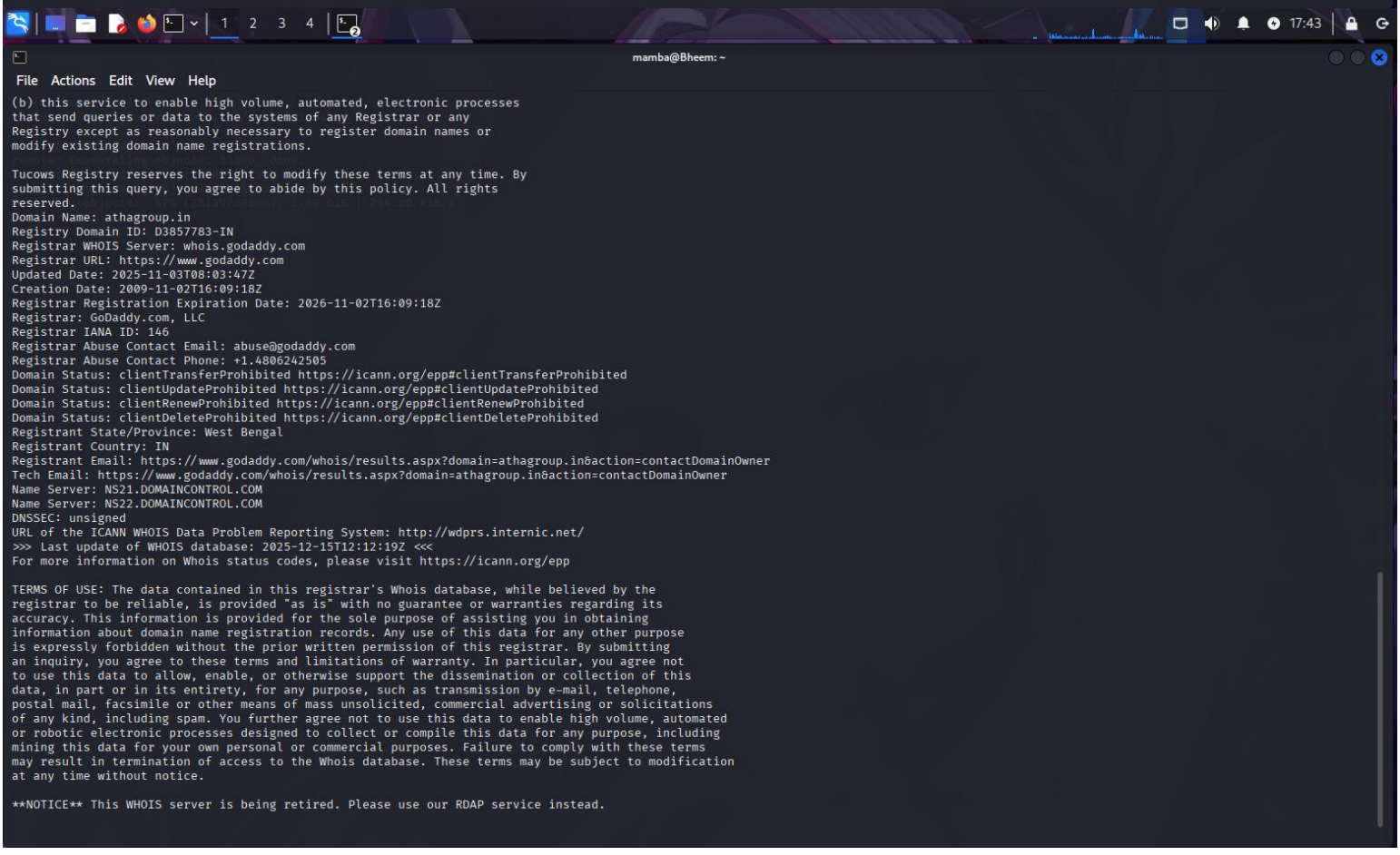
PASSIVE RECON

FOUND:

- **Domain owner info**
- **Registrar**
- **Name servers**

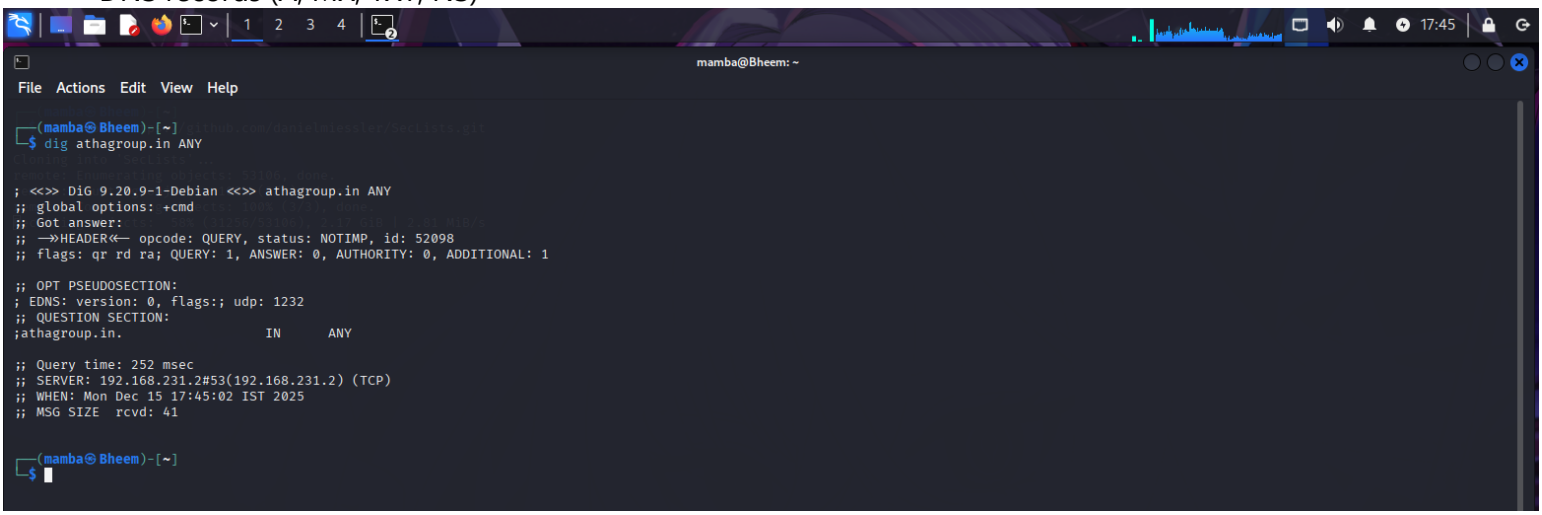
```
1 2 3 4                                                    17:42
mamba@Bheem: ~
File Actions Edit View Help

┌──(mamba㉿Bheem)-[~]
└─$ whois athagroup.in

Domain Name: athagroup.in
Registry Domain ID: D3857783-IN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: www.godaddy.com
Updated Date: 2025-11-03T08:03:49.382Z
Creation Date: 2009-11-02T16:09:18.275Z
Registry Expiry Date: 2026-11-02T16:09:18.275Z
Registrar: GoDaddy
Registrar IANA ID: 146
Registrar Abuse Contact Email: reg_admin@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: autoRenewPeriod https://icann.org/epp#autoRenewPeriod
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Atha Group
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: West Bengal
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin 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 Fax: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry 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
```


1 2 3 4
17:42
mamba@Bheem: ~
File Actions Edit View Help
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Billing ID: REDACTED FOR PRIVACY
Billing Name: REDACTED FOR PRIVACY
Billing Organization: REDACTED FOR PRIVACY
Billing Street: REDACTED FOR PRIVACY
Billing City: REDACTED FOR PRIVACY
Billing State/Province: REDACTED FOR PRIVACY
Billing Postal Code: REDACTED FOR PRIVACY
Billing Country: REDACTED FOR PRIVACY
Billing Phone: REDACTED FOR PRIVACY
Billing Fax: REDACTED FOR PRIVACY
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: ns22.domaincontrol.com
Name Server: ns21.domaincontrol.com
DNSSEC: unsigned
URL of the ICANN RDDS Inaccuracy Complaint Form: https://icann.org/wicf
>>> Last update of WHOIS database: 2025-12-15T12:12:18.381Z <<<
For more information on domain status codes, please visit https://icann.org/epp
The WHOIS information provided in this page has been redacted
in compliance with ICANN's Temporary Specification for gTLD
Registration Data.
The data in this record is provided by Tucows Registry for informational
purposes only, and it does not guarantee its accuracy. Tucows Registry is
authoritative for whois information in top-level domains it operates
under contract with the Internet Corporation for Assigned Names and
Numbers. Whois information from other top-level domains is provided by
a third-party under license to Tucows Registry.
This service is intended only for query-based access. By using this
service, you agree that you will use any data presented only for lawful
purposes and that, under no circumstances will you use (a) data
acquired for the purpose of allowing, enabling, or otherwise supporting
the transmission by e-mail, telephone, facsimile or other
communications mechanism of mass unsolicited, commercial advertising
or solicitations to entities other than your existing customers; or
(b) this service to enable high volume, automated, electronic processes
that send queries or data to the systems of any Registrar or any
Registry except as reasonably necessary to register domain names or
modify existing domain name registrations.
Tucows Registry reserves the right to modify these terms at any time. By
submitting this query, you agree to abide by this policy. All rights


1 2 3 4
17:43
mamba@Bheem: ~
File Actions Edit View Help
(b) this service to enable high volume, automated, electronic processes
that send queries or data to the systems of any Registrar or any
Registry except as reasonably necessary to register domain names or
modify existing domain name registrations.
Tucows Registry reserves the right to modify these terms at any time. By
submitting this query, you agree to abide by this policy. All rights
reserved.
Domain Name: athagroup.in
Registry Domain ID: D3857783-IN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2025-11-03T08:03:47Z
Creation Date: 2009-11-02T16:09:18Z
Registrar Registration Expiration Date: 2026-11-02T16:09:18Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant State/Province: West Bengal
Registrant Country: IN
Registrant Email: https://www.godaddy.com/whois/results.aspx?domain=athagroup.in&action=contactDomainOwner
Tech Email: https://www.godaddy.com/whois/results.aspx?domain=athagroup.in&action=contactDomainOwner
Name Server: NS21.DOMAINCONTROL.COM
Name Server: NS22.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2025-12-15T12:12:19Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
TERMS OF USE: The data contained in this registrar's Whois database, while believed by the
registrar to be reliable, is provided "as is" with no guarantee or warranties regarding its
accuracy. This information is provided for the sole purpose of assisting you in obtaining
information about domain name registration records. Any use of this data for any other purpose
is expressly forbidden without the prior written permission of this registrar. By submitting
an inquiry, you agree to these terms and limitations of warranty. In particular, you agree not
to use this data to allow, enable, or otherwise support the dissemination or collection of this
data, in part or in its entirety, for any purpose, such as transmission by e-mail, telephone,
postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations
of any kind, including spam. You further agree not to use this data to enable high volume, automated
or robotic electronic processes designed to collect or compile this data for any purpose, including
mining this data for your own personal or commercial purposes. Failure to comply with these terms
may result in termination of access to the Whois database. These terms may be subject to modification
at any time without notice.
NOTICE This WHOIS server is being retired. Please use our RDAP service instead.

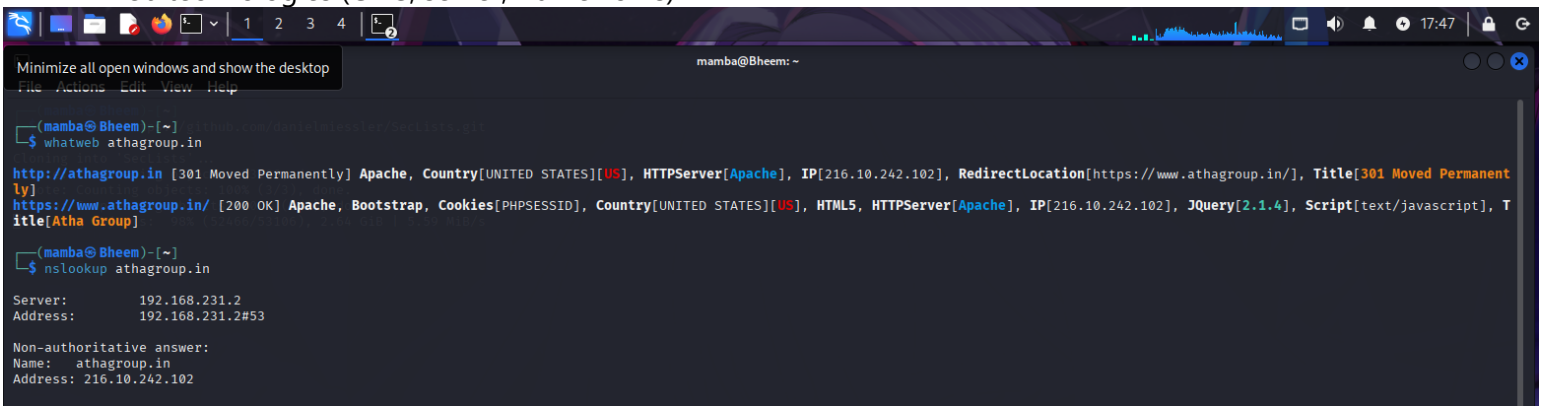
FOUND :

- DNS records (A, MX, TXT, NS)



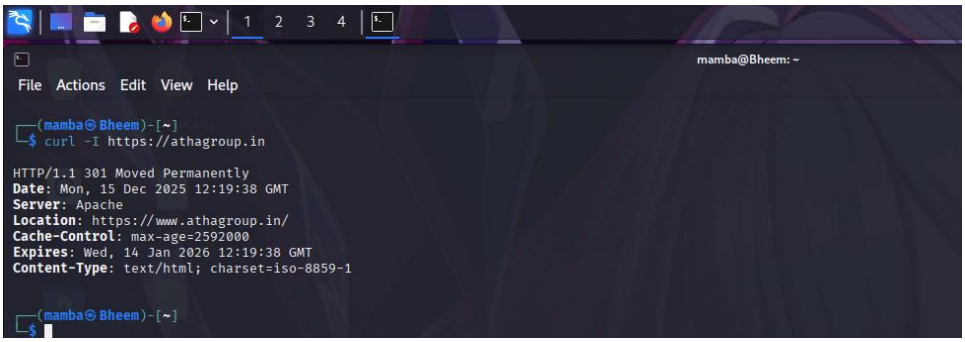
FOUND

- Web technologies (CMS, server, frameworks)



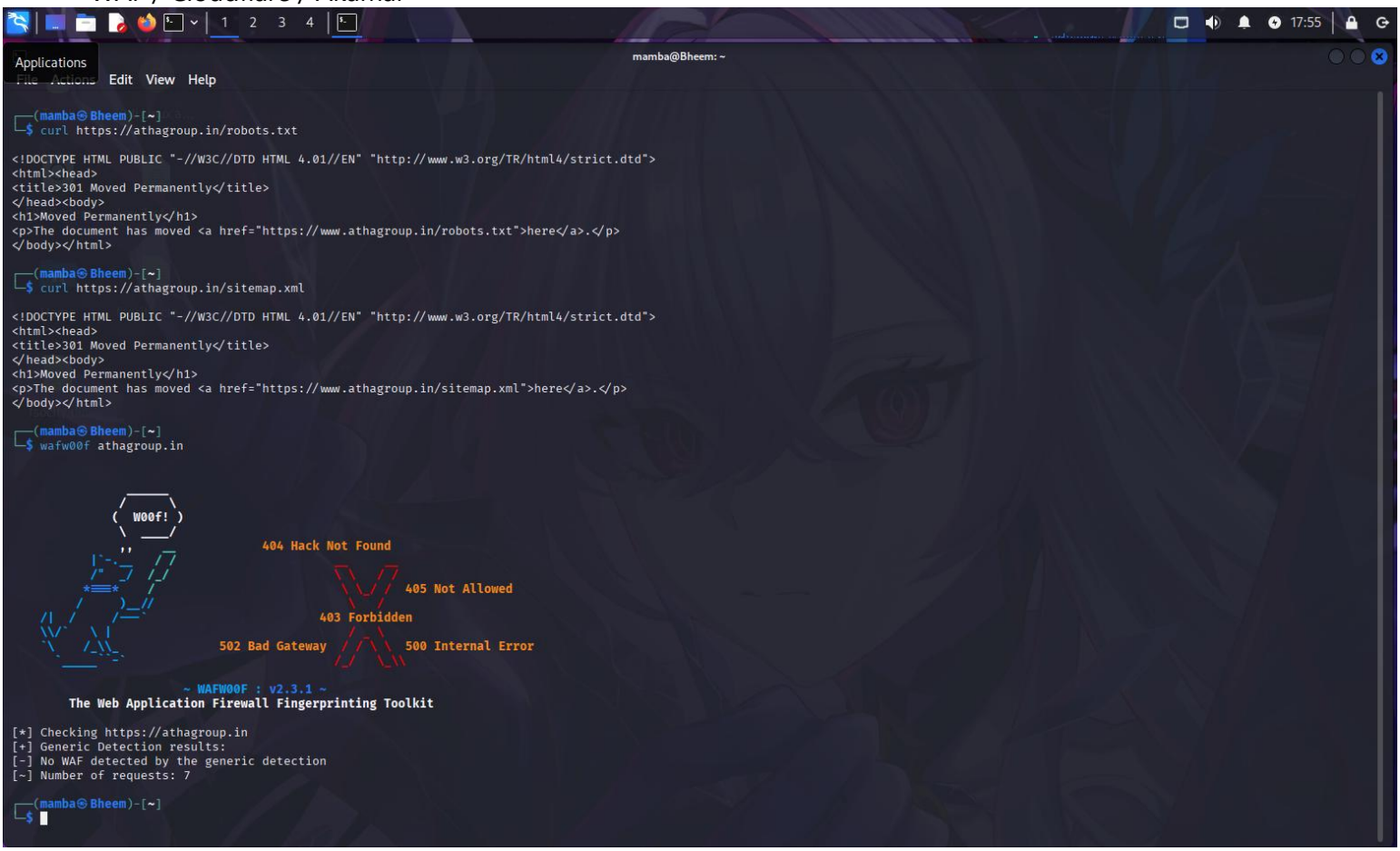
Checked:

- Security headers
- Server info

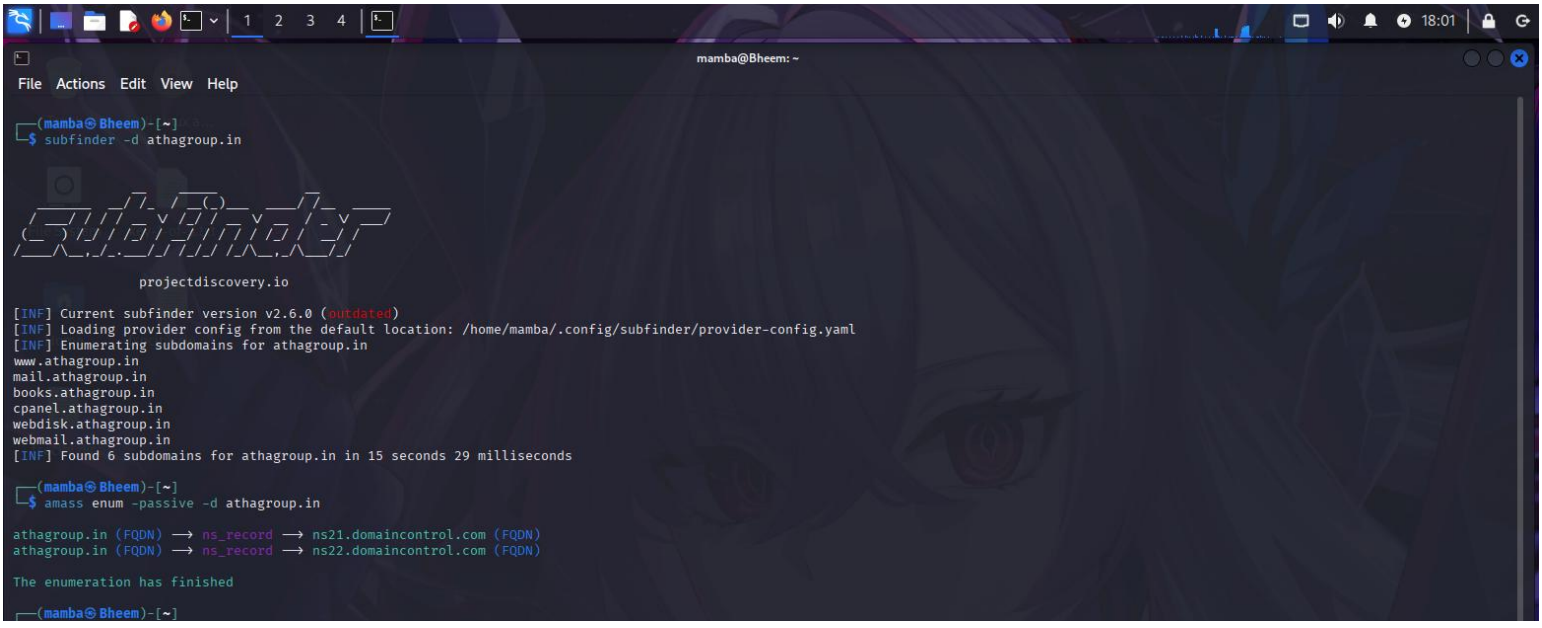


Detects:

- WAF / Cloudflare / Akamai



Subdomain Enumeration




(mamba㉿Bheem)-[~]
$ assetfinder athagroup.in
www.athagroup.webdesignservice.co.in
athagroup.in
mail.athagroup.in