

megacorpone information gathering report

Submission by: Goutham Vyasroimath Keshava Murthy

Assignment: AEP CS - Ethical Hacking and VAPT

Cohort: PGP AEP CS May 2022 Cohort



August 20, 2022

WHITE HATS organization

White Hat Street, White Hat State, White Hat Nation - 007007

Contents

[1. Disclaimer 2](#_Toc111903918)

[2. Abstract 2](#_Toc111903919)

[3. In-Scope 2](#_Toc111903920)

[4. Out-Of-Scope 2](#_Toc111903921)

[5. Executive Summary 2](#_Toc111903922)

[6. Information Gathering Summary 3](#_Toc111903923)

[7. Tool Wise Information Details 4](#_Toc111903924)

[7.1. OSINT Domain Dossier 4](#_Toc111903925)

[7.2. Dmitry Email & Subdomain Scans 7](#_Toc111903926)

[7.3. Red Hawk Scan 8](#_Toc111903927)

[7.4. OSINT Domain Dossier 9](#_Toc111903928)

[7.5. Nmap Scans 15](#_Toc111903929)

[7.6. Nikto Scan 19](#_Toc111903930)

[7.7. OWASP ZAP Scans 19](#_Toc111903931)

[7.8. theHarvester LinkedIn Users Scan 20](#_Toc111903932)

[7.9. Nessus Scan 21](#_Toc111903933)

# Disclaimer

Information gathering has been conducted within purview of laws governing the jurisdiction

# Abstract

The objective of this report is to find web application vulnerabilities of WebGoat hosted on a VM Linux machine by using manual SQL Injection techniques. A thorough investigation of SQL Injection vulnerabilities was conducted. The impacts and probability of the exploitation of each vulnerability found was graded based on the standard vulnerability scoring scheme. Additionally, the vulnerabilities were graded according to the consequences of the exploitation identified through the findings. This report helps web application developers, providers and all relevant stakeholders on business & product side to better understand the inherent and possible security issues of WebGoat. This report assumes follow up corrective actions by the WebGoat team in implementing protection against reported SQL Injection security vulnerabilities

# In-Scope

Investigate and report SQL Injection vulnerabilities

# Out-Of-Scope

Recommendation to fix the SQL Injection vulnerabilities

# Executive Summary

[www.megacorpone.com](http://www.megacorpone.com) is a publicly accessible web application with static pages as well as login functionality for dynamic content. Login is an intranet functionality and hence has not been accessed as part of information gathering.

Megacorpone.com domain is registered in the name of Alan Grofield who also happens to be the tech contact. Domain registration has been active since around 3500 days.

Below list of tools were leveraged to gather data about [www.megacorpone.com](http://www.megacorpone.com)

* Google
* Kali Linux
* Nmap
* RedHawk
* Nikto
* OSINT
* Dmitry
* OWASP ZAP
* theHarvester
* Nessus
* Linux WhatWeb

# Information Gathering Summary

|  |  |
| --- | --- |
| **Aspect** | **Details** |
| **Organization address** | Registrant Organization: MegaCorpOne  Registrant Street: 2 Old Mill St  Registrant City: Rachel  Registrant State/Province: Nevada  Registrant Postal Code: 89001  Registrant Country: US  Registrant Phone: +1.9038836342  Registrar Abuse Contact Email: abuse@support.gandi.net  Registrar Abuse Contact Phone: +33.170377661 (**more information in OSINT Domain Dossier section**) |
| **Countries hosting the application** | US |
| **Registration details** | Domain Name: MEGACORPONE.COM  Registry Domain ID: 1775445745\_DOMAIN\_COM-VRSN  Registrar WHOIS Server: whois.gandi.net  Registrar URL: http://www.gandi.net  Updated Date: 2022-06-14T18:01:06Z  Creation Date: 2013-01-22T23:01:00Z  Registry Expiry Date: 2024-01-22T23:01:00Z |
| **Registrant in name of + Technical contact** | Alan Grofield |
| **IP address** | 149.56.244.87 |
| **Possible subdomains** | intranel.megacorpone.com, admin.megacorpone.com, beta.megacorpone.com, siem.megacorpone.com, ns1.megacorpone.com, ns2.megacorpone.com, ns3.megacorpone.com, mail.megacorpone.com, Siem.megacorpone.com, mail2.megacorpone.com |
| **Accessible through internet** | Yes |
| **Software** | Apache/2.4.38 |
| **OS** | Linux 2.6.x or 3.1x |
| **Open ports & service** | 22 – ssh  80 – http  135 – msrpc  139 – netbios-ssn  443 – https  445 – Microsoft-ds  1022 – exp2  1023 – netvenuechat  1026 – LSA-or-nterm  9898 - moneycom |
| **IP address** | 149.56.244.87 |

# Tool Wise Information Details

# OSINT Domain Dossier

Whois Record for MegaCorpOne.com

How does this work?

Domain Profile

Registrant Alan Grofield

Registrant Org MegaCorpOne

Registrant Country us

Registrar GANDI SAS Gandi SAS

IANA ID: 81

URL: http://www.gandi.net

Whois Server: whois.gandi.net

(p)

Registrar Status clientTransferProhibited

Dates 3,496 days old

Created on 2013-01-22

Expires on 2024-01-22

Updated on 2022-06-14

Name Servers NS1.MEGACORPONE.COM (has 8 domains)

NS2.MEGACORPONE.COM (has 8 domains)

NS3.MEGACORPONE.COM (has 8 domains)

Tech Contact Alan Grofield

MegaCorpOne

2 Old Mill St,

Rachel, Nevada, 89001, us

(p)

IP Address 149.56.244.87 - 1 other site is hosted on this server

IP Location Canada - Quebec - Montreal - Ovh Hosting Inc.

ASN Canada AS16276 OVH, FR (registered Feb 15, 2001)

IP History 8 changes on 8 unique IP addresses over 9 years

Registrar History 1 registrar

Hosting History 2 changes on 3 unique name servers over 9 years

Website

Website Title MegaCorp One - Nanotechnology Is the Future

Server Type Apache/2.4.38 (Debian)

Response Code 200

Terms 276 (Unique: 178, Linked: 117)

Images 0 (Alt tags missing: 0)

Links 32 (Internal: 27, Outbound: 5)

Whois Record ( last updated on 2022-08-19 )

Domain Name: megacorpone.com

Registry Domain ID: 1775445745\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.gandi.net

Registrar URL: http://www.gandi.net

Updated Date: 2022-06-14T18:01:06Z

Creation Date: 2013-01-22T22:01:00Z

Registrar Registration Expiration Date: 2024-01-22T23:01:00Z

Registrar: GANDI SAS

Registrar IANA ID: 81

Registrar Abuse Contact Email:

Registrar Abuse Contact Phone: +33.170377661

Reseller:

Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Domain Status:

Domain Status:

Domain Status:

Domain Status:

Registry Registrant ID:

Registrant Name: Alan Grofield

Registrant Organization: MegaCorpOne

Registrant Street: 2 Old Mill St

Registrant City: Rachel

Registrant State/Province: Nevada

Registrant Postal Code: 89001

Registrant Country: US

Registrant Phone: +1.9038836342

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email:

Registry Admin ID:

Admin Name: Alan Grofield

Admin Organization: MegaCorpOne

Admin Street: 2 Old Mill St

Admin City: Rachel

Admin State/Province: Nevada

Admin Postal Code: 89001

Admin Country: US

Admin Phone: +1.9038836342

Admin Phone Ext:

Admin Fax:

Admin Fax Ext:

Admin Email:

Registry Tech ID:

Tech Name: Alan Grofield

Tech Organization: MegaCorpOne

Tech Street: 2 Old Mill St

Tech City: Rachel

Tech State/Province: Nevada

Tech Postal Code: 89001

Tech Country: US

Tech Phone: +1.9038836342

Tech Phone Ext:

Tech Fax:

Tech Fax Ext:

Tech Email:

Name Server: NS1.MEGACORPONE.COM

Name Server: NS2.MEGACORPONE.COM

Name Server: NS3.MEGACORPONE.COM

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

DNSSEC: Unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

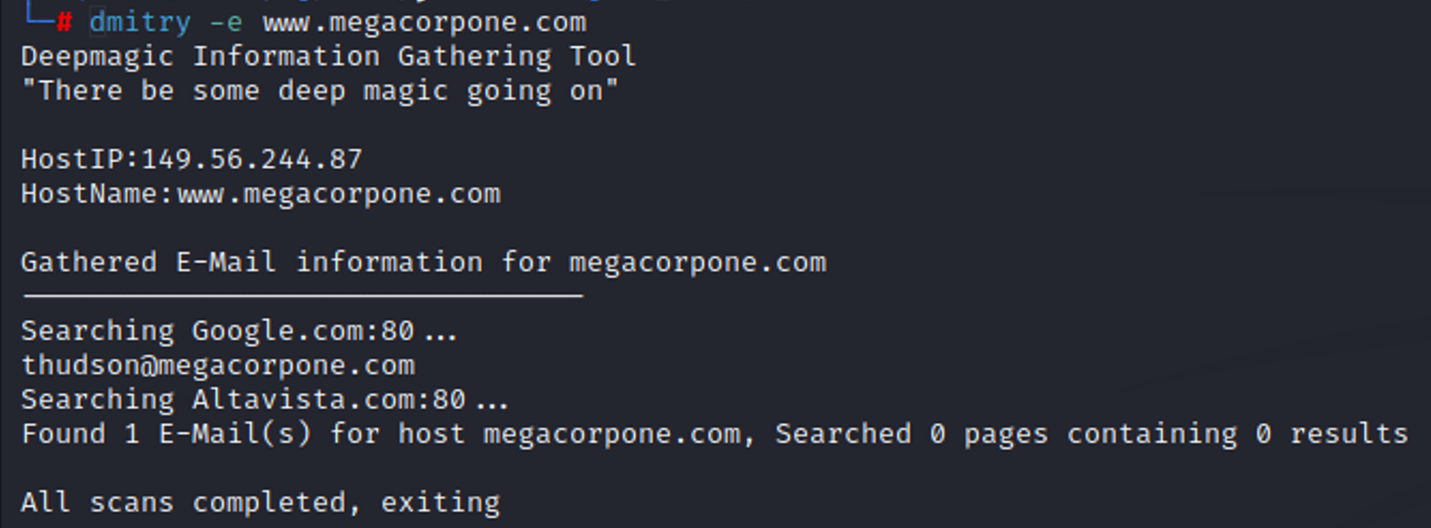
For more information on Whois status codes, please visit

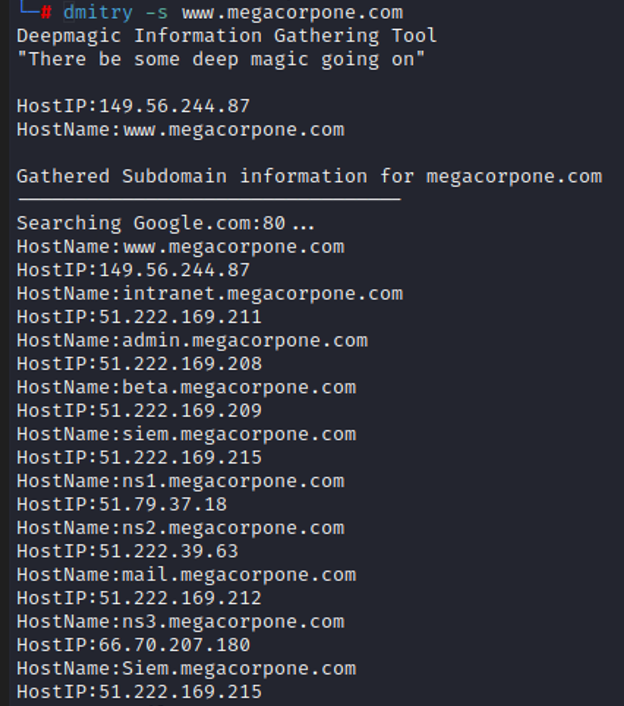
https://www.icann.org/epp

Reseller Email:

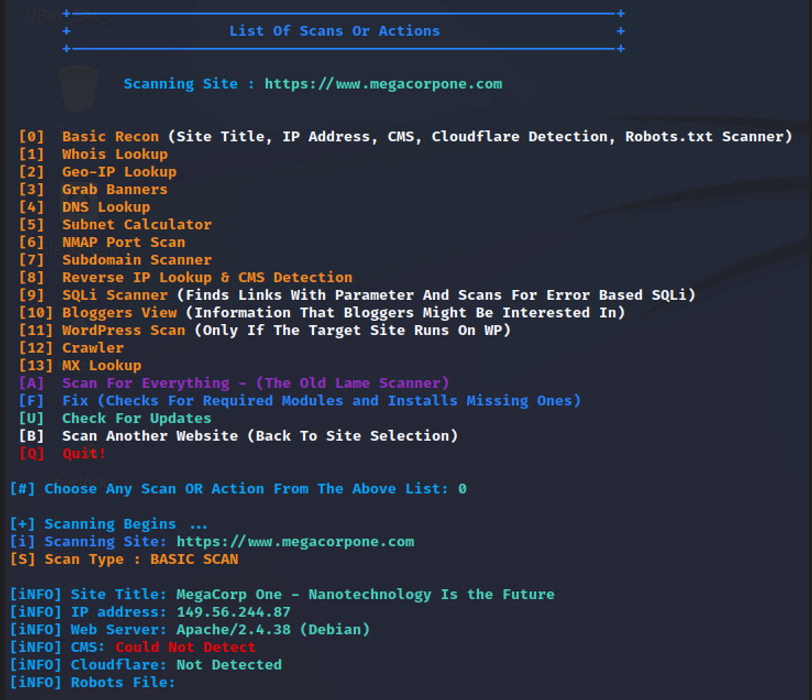
Reseller URL:

# Dmitry Email & Subdomain Scans





# Red Hawk Scan



# OSINT Domain Dossier

Queried whois.internic.net with "dom megacorpone.com"...

Domain Name: MEGACORPONE.COM

Registry Domain ID: 1775445745\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.gandi.net

Registrar URL: http://www.gandi.net

Updated Date: 2022-06-14T18:01:06Z

Creation Date: 2013-01-22T23:01:00Z

Registry Expiry Date: 2024-01-22T23:01:00Z

Registrar: Gandi SAS

Registrar IANA ID: 81

Registrar Abuse Contact Email: abuse@support.gandi.net

Registrar Abuse Contact Phone: +33.170377661

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Name Server: NS1.MEGACORPONE.COM

Name Server: NS2.MEGACORPONE.COM

Name Server: NS3.MEGACORPONE.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2022-08-19T07:28:08Z <<<

Queried whois.gandi.net with "megacorpone.com"...

Domain Name: megacorpone.com

Registry Domain ID: 1775445745\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.gandi.net

Registrar URL: http://www.gandi.net

Updated Date: 2022-06-14T18:01:06Z

Creation Date: 2013-01-22T22:01:00Z

Registrar Registration Expiration Date: 2024-01-22T23:01:00Z

Registrar: GANDI SAS

Registrar IANA ID: 81

Registrar Abuse Contact Email: abuse@support.gandi.net

Registrar Abuse Contact Phone: +33.170377661

Reseller:

Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Domain Status:

Domain Status:

Domain Status:

Domain Status:

Registry Registrant ID:

Registrant Name: Alan Grofield

Registrant Organization: MegaCorpOne

Registrant Street: 2 Old Mill St

Registrant City: Rachel

Registrant State/Province: Nevada

Registrant Postal Code: 89001

Registrant Country: US

Registrant Phone: +1.9038836342

Registrant Phone Ext:

Registrant Fax:

Registrant Fax Ext:

Registrant Email: 3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net

Registry Admin ID:

Admin Name: Alan Grofield

Admin Organization: MegaCorpOne

Admin Street: 2 Old Mill St

Admin City: Rachel

Admin State/Province: Nevada

Admin Postal Code: 89001

Admin Country: US

Admin Phone: +1.9038836342

Admin Phone Ext:

Admin Fax:

Admin Fax Ext:

Admin Email: 3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net

Registry Tech ID:

Tech Name: Alan Grofield

Tech Organization: MegaCorpOne

Tech Street: 2 Old Mill St

Tech City: Rachel

Tech State/Province: Nevada

Tech Postal Code: 89001

Tech Country: US

Tech Phone: +1.9038836342

Tech Phone Ext:

Tech Fax:

Tech Fax Ext:

Tech Email: 3310f82fb4a8f79ee9a6bfe8d672d87e-1696395@contact.gandi.net

Name Server: NS1.MEGACORPONE.COM

Name Server: NS2.MEGACORPONE.COM

Name Server: NS3.MEGACORPONE.COM

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

Name Server:

DNSSEC: Unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

>>> Last update of WHOIS database: 2022-08-19T07:28:22Z <<<

Network Whois record

Queried whois.arin.net with "n ! NET-149-56-244-0-1"...

NetRange: 149.56.244.0 - 149.56.244.255

CIDR: 149.56.244.0/24

NetName: OVH-DEDICATED-FO

NetHandle: NET-149-56-244-0-1

Parent: HO-2 (NET-149-56-0-0-1)

NetType: Reassigned

OriginAS: AS16276

Organization: OVH Hosting, Inc. (HO-2)

RegDate: 2017-07-05

Updated: 2017-07-05

Comment: Failover IPs

Ref: https://rdap.arin.net/registry/ip/149.56.244.0

OrgName: OVH Hosting, Inc.

OrgId: HO-2

Address: 800-1801 McGill College

City: Montreal

StateProv: QC

PostalCode: H3A 2N4

Country: CA

RegDate: 2011-06-22

Updated: 2017-01-28

Ref: https://rdap.arin.net/registry/entity/HO-2

OrgTechHandle: NOC11876-ARIN

OrgTechName: NOC

OrgTechPhone: +1-855-684-5463

OrgTechEmail: noc@ovh.net

OrgTechRef: https://rdap.arin.net/registry/entity/NOC11876-ARIN

OrgAbuseHandle: ABUSE3956-ARIN

OrgAbuseName: Abuse

OrgAbusePhone: +1-855-684-5463

OrgAbuseEmail: abuse@ovh.ca

OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE3956-ARIN

DNS records

name class type data time to live

www.megacorpone.com IN A 149.56.244.87 300s (00:05:00)

megacorpone.com IN SOA

server: ns1.megacorpone.com

email: admin@megacorpone.com

serial: 202102161

refresh: 28800

retry: 7200

expire: 2419200

minimum ttl: 300

300s (00:05:00)

megacorpone.com IN TXT google-site-verification=U7B\_b0HNeBtY4qYGQZNsEYXfCJ32hMNV3GtC0wWq5pA 300s (00:05:00)

megacorpone.com IN TXT Try Harder 300s (00:05:00)

megacorpone.com IN MX

preference: 20

exchange: spool.mail.gandi.net

300s (00:05:00)

megacorpone.com IN MX

preference: 10

exchange: fb.mail.gandi.net

300s (00:05:00)

megacorpone.com IN MX

preference: 60

exchange: mail2.megacorpone.com

300s (00:05:00)

megacorpone.com IN MX

preference: 50

exchange: mail.megacorpone.com

300s (00:05:00)

megacorpone.com IN NS ns3.megacorpone.com 300s (00:05:00)

megacorpone.com IN NS ns1.megacorpone.com 300s (00:05:00)

megacorpone.com IN NS ns2.megacorpone.com 300s (00:05:00)

87.244.56.149.in-addr.arpa IN PTR www.megacorpone.com 86400s (1.00:00:00)

244.56.149.in-addr.arpa IN SOA

server: dns10.ovh.ca

email: tech@ovh.net

serial: 2022081800

refresh: 43200

retry: 4320

expire: 2419200

minimum ttl: 86400

86400s (1.00:00:00)

244.56.149.in-addr.arpa IN NS ns10.ovh.ca 86400s (1.00:00:00)

244.56.149.in-addr.arpa IN NS dns10.ovh.ca 86400s (1.00:00:00)

Traceroute

Tracing route to www.megacorpone.com [149.56.244.87]...

hop rtt rtt rtt ip address fully qualified domain name

1 3 1 0 169.254.158.58

2 1 1 0 169.48.118.158 ae103.ppr02.dal13.networklayer.com

3 0 3 0 169.48.118.130 82.76.30a9.ip4.static.sl-reverse.com

4 2 2 2 169.45.18.86 ae16.cbs01.eq01.dal03.networklayer.com

5 1 1 1 50.97.17.53 ae33.bbr01.eq01.dal03.networklayer.com

6 \* \* \*

7 \* \* \*

8 23 23 23 178.32.135.152 be100-1241.chi-5-a9.il.us

9 41 41 41 192.99.146.140 be103.bhs-g2-nc5.qc.ca

10 \* \* \*

11 \* \* \*

12 \* \* \*

13 \* \* \*

Trace aborted

Service scan

FTP - 21 Error: ConnectionRefused

SMTP - 25 Error: ConnectionRefused

HTTP - 80 HTTP/1.1 200 OK

Date: Fri, 19 Aug 2022 07:28:43 GMT

Server: Apache/2.4.38 (Debian)

Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT

ETag: "390b-596aedca79780"

Accept-Ranges: bytes

Content-Length: 14603

Vary: Accept-Encoding

Connection: close

Content-Type: text/html

POP3 - 110 Error: ConnectionRefused

IMAP - 143 Error: ConnectionRefused

HTTPS - 443 Certificate validation errors: None

Signature algorithm: sha256RSA

Public key size: 2048 bits

Issuer: CN=R3, O=Let's Encrypt, C=US

Subject: CN=www.megacorpone.com

Subject Alternative Name: DNS Name=www.megacorpone.com

Serial number: 0309015DEE48539F8B3930973FD4B68C2D7A

Not valid before: 2022-06-30 06:35:08Z

Not valid after: 2022-09-28 06:35:07Z

SHA1 fingerprint: F3DBA07FD47CCFFC32AE94F8EE23968077CB9F39

HTTP/1.1 200 OK

Date: Fri, 19 Aug 2022 07:28:45 GMT

Server: Apache/2.4.38 (Debian)

Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT

ETag: "390b-596aedca79780"

Accept-Ranges: bytes

Content-Length: 14603

Vary: Accept-Encoding

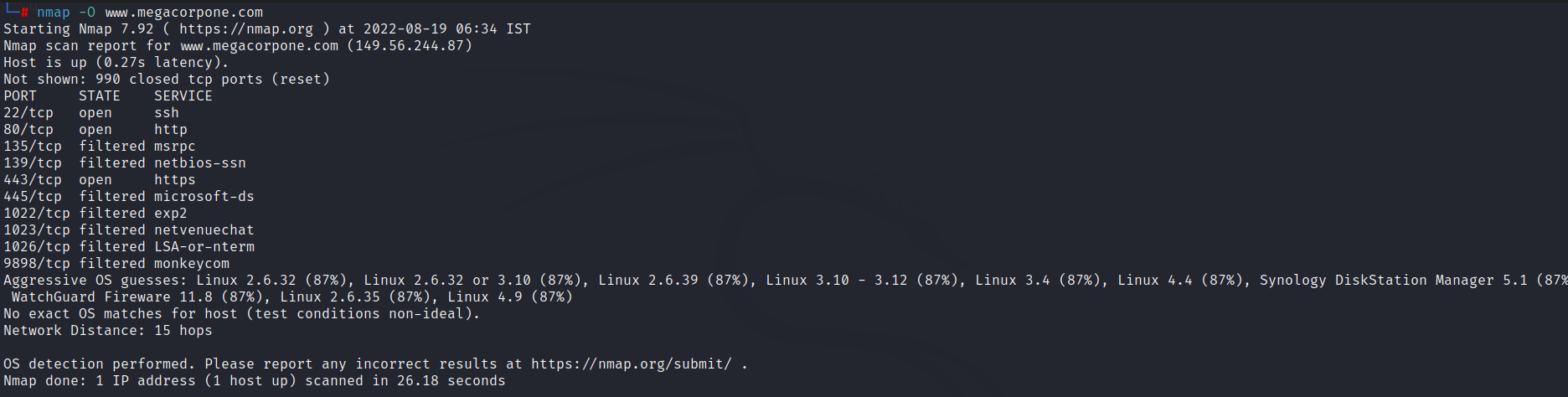
Connection: close

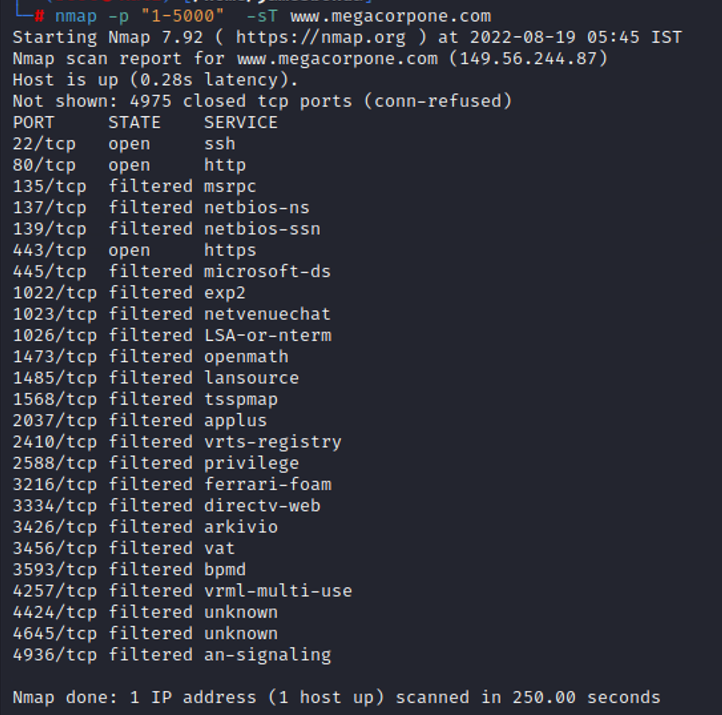
Content-Type: text/html

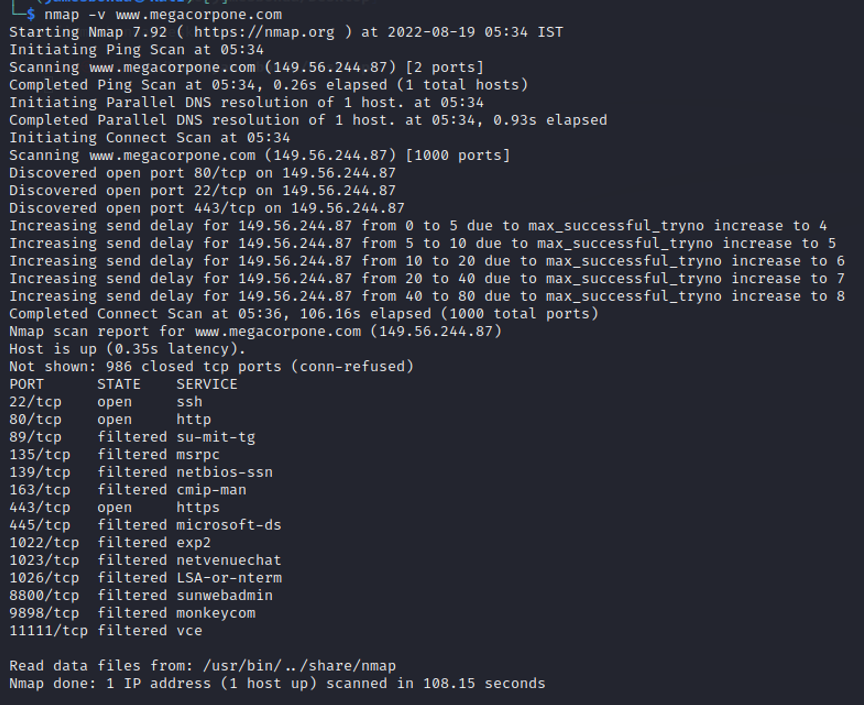
-- end --

URL for this output | return to CentralOps.net, a service of Hexillion

# Nmap Scans







└─# nmap -A www.megacorpone.com

Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-19 06:28 IST

Nmap scan report for www.megacorpone.com (149.56.244.87)

Host is up (0.27s latency).

Not shown: 990 closed tcp ports (reset)

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

| ssh-hostkey:

| 2048 cd:bd:1d:f0:c2:fb:c3:d8:48:ef:7f:5f:ba:34:1f:06 (RSA)

| 256 05:4e:c7:97:80:2e:68:73:64:9a:6f:4d:a3:6b:dd:1f (ECDSA)

|\_ 256 d3:ac:5a:e7:e4:55:49:29:4c:58:9f:23:ee:5e:14:bd (ED25519)

80/tcp open http Apache httpd 2.4.38 ((Debian))

|\_http-title: MegaCorp One - Nanotechnology Is the Future

|\_http-server-header: Apache/2.4.38 (Debian)

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

443/tcp open ssl/http Apache httpd 2.4.38

|\_http-title: MegaCorp One - Nanotechnology Is the Future

| tls-alpn:

|\_ http/1.1

| ssl-cert: Subject: commonName=www.megacorpone.com

| Subject Alternative Name: DNS:www.megacorpone.com

| Not valid before: 2022-06-30T06:35:08

|\_Not valid after: 2022-09-28T06:35:07

|\_http-server-header: Apache/2.4.38 (Debian)

|\_ssl-date: TLS randomness does not represent time

445/tcp filtered microsoft-ds

1022/tcp filtered exp2

1023/tcp filtered netvenuechat

1026/tcp filtered LSA-or-nterm

9898/tcp filtered monkeycom

Aggressive OS guesses: Linux 2.6.32 (87%), Linux 2.6.32 or 3.10 (87%), Linux 2.6.39 (87%), Linux 3.10 - 3.12 (87%), Linux 3.4 (87%), Linux 3.5 (87%), Linux 4.2 (87%), Linux 4.4 (87%), Synology DiskStation Manager 5.1 (87%), WatchGuard Fireware 11.8 (87%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 15 hops

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

TRACEROUTE (using port 3389/tcp)

HOP RTT ADDRESS

1 3.48 ms 192.168.1.1

2 6.95 ms 223.178.56.1

3 6.13 ms nsg-corporate-101.95.187.122.airtel.in (122.187.95.101)

4 257.29 ms 116.119.68.58

5 ... 8

9 261.11 ms nyc-ny1-sbb2-8k.nj.us (192.99.146.133)

10 258.32 ms be102.bhs-g2-nc5.qc.ca (192.99.146.138)

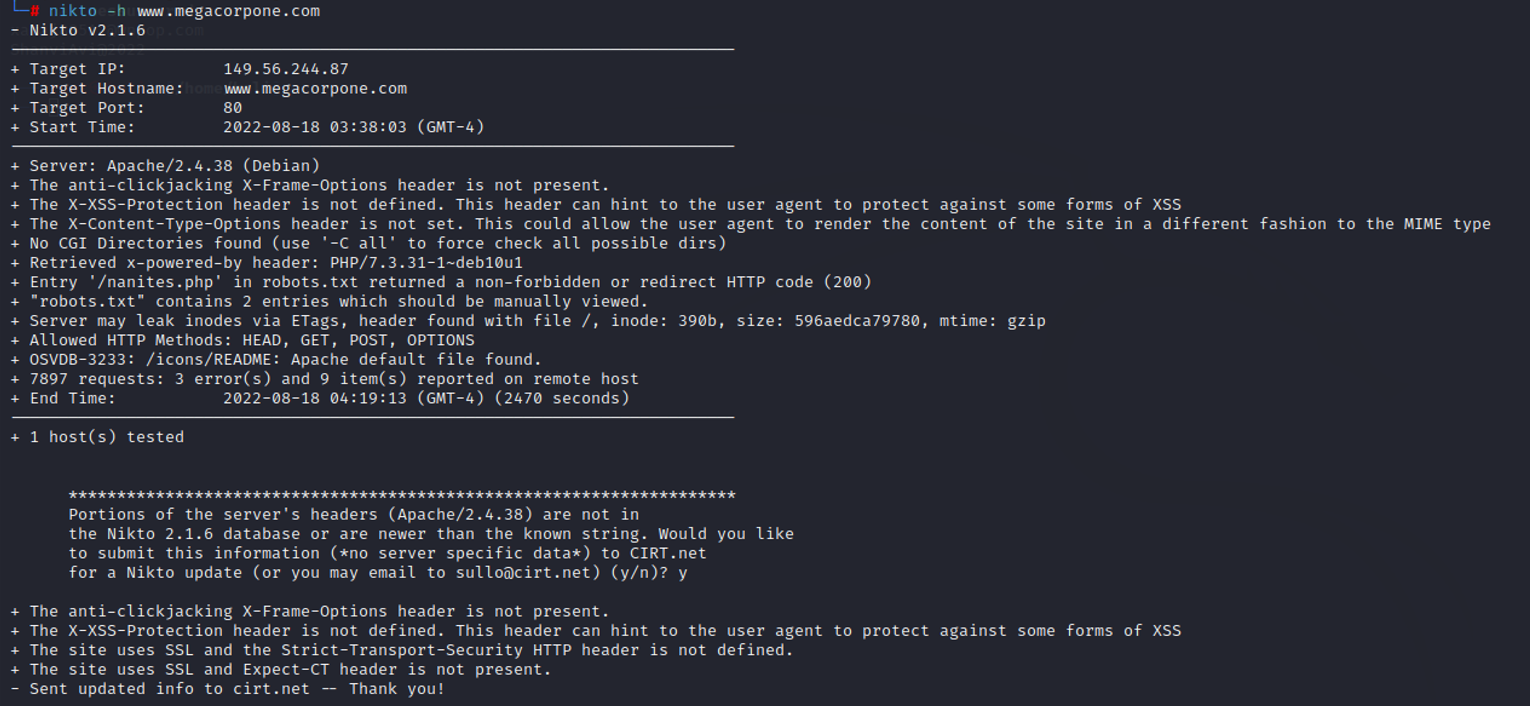
11 ... 14

15 271.86 ms www.megacorpone.com (149.56.244.87)

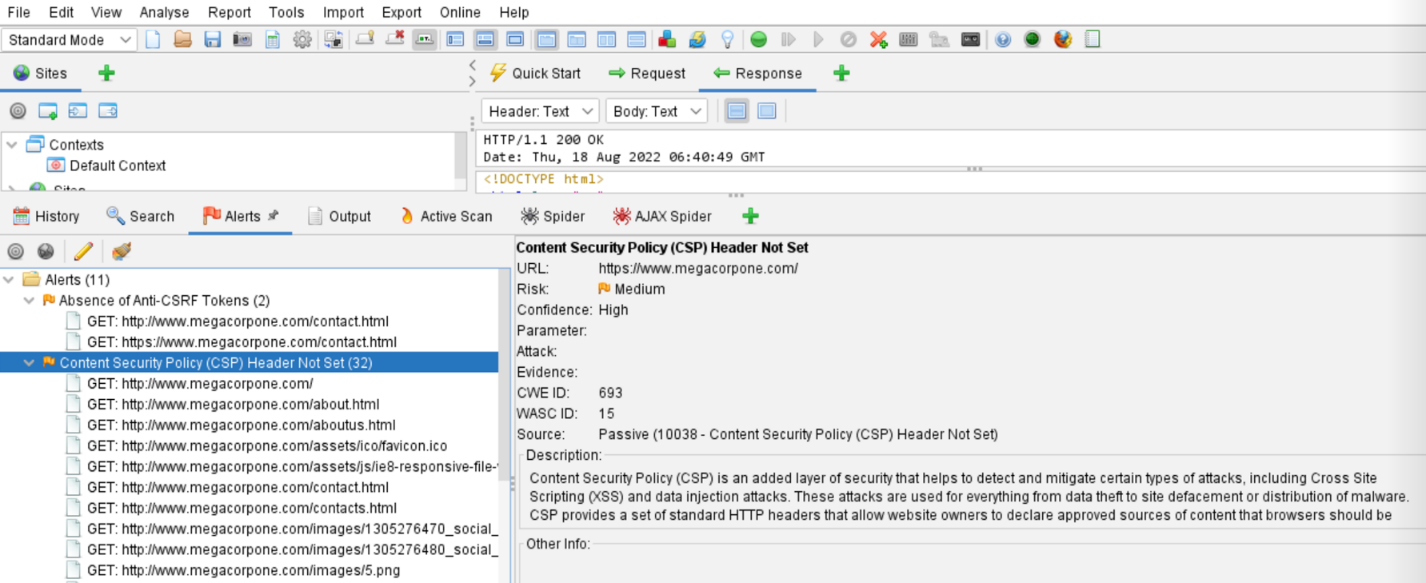
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

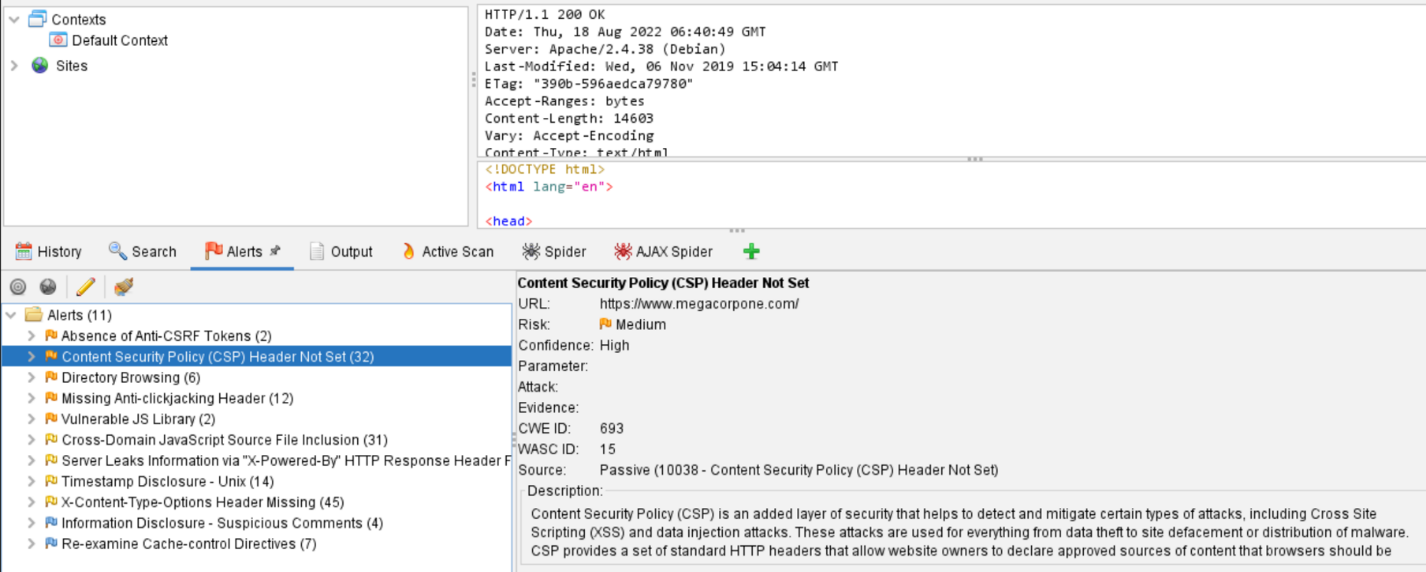
Nmap done: 1 IP address (1 host up) scanned in 56.92 seconds

# Nikto Scan

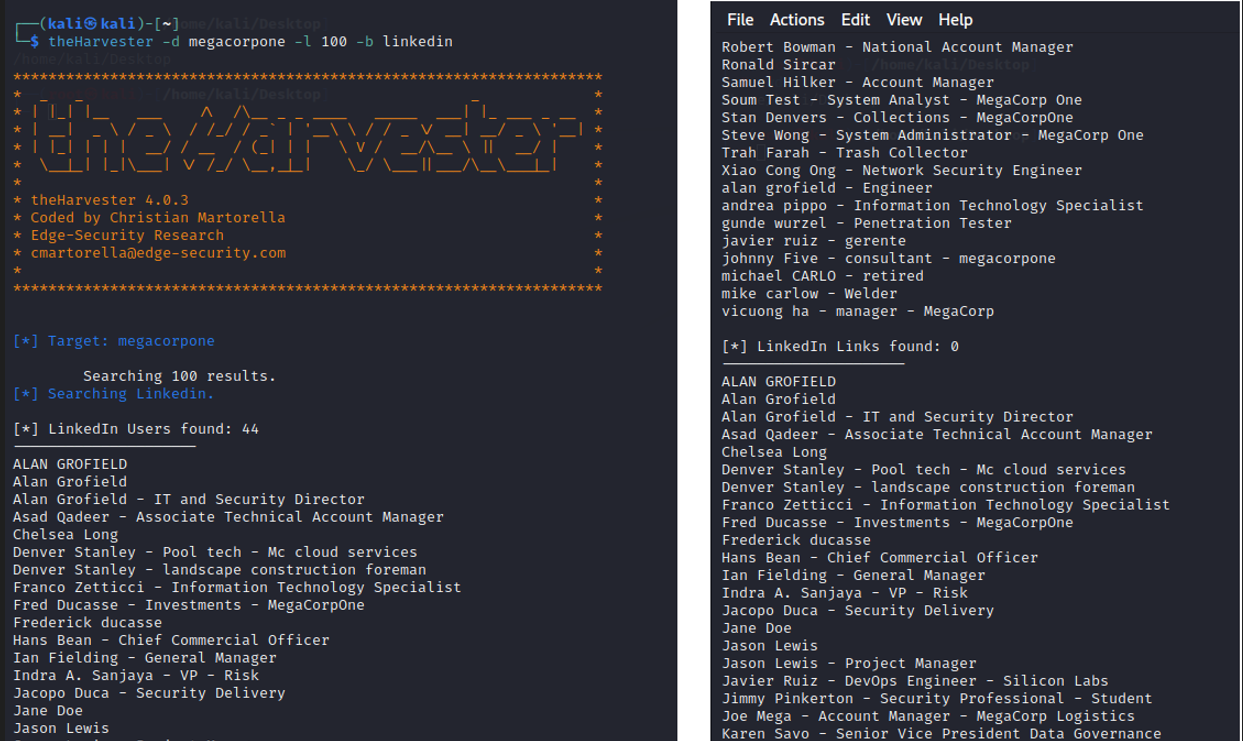


# OWASP ZAP Scans





# theHarvester LinkedIn Users Scan



# Nessus Scan

