

SOC RECONNAISSANCE REPORT

SCOPE: MEGACORP ONE

PREPARED BY: OLUKAYODE AYODELE

OVERVIEW

The Security Operations center is tasked with enumerating the attack surface of megacorp one using open-source intelligence gathering and passive reconnaissance tools to avoid detection by internal detection systems. The point of reconnaissance will be company website www.megacorpone.com to understand the company security posture, find vulnerabilities and recommend mitigation strategies. This will allow megacorp one to proactively identify security weaknesses before they are exploited by threat actors.

OBJECTIVES:

- Enumerate subdomains and IP addresses
- Identify any network security
- Find technology stack, servers and versions
- Find employee data
- Check website security
- OSINT Automation for a comprehensive aggregated data

STRATEGY

Passive reconnaissance tools will be employed to gather any publicly available information on the company, employees and technology, analyze data collected to map the attack surface, find vulnerabilities and overall company security stance.

TOOLS

- Kali linux 2025
- DNSDumpster
- Github
- Google doc
- Amass
- Curl
- Dig
- Wafw00f
- Whatweb
- LinkedIn
- Nslookup
- Twitter
- Spiderfoot
- MS PowerPoint

PASSIVE RECONNAISSANCE METHODOLOGY

I began the planning of the passive reconnaissance by enumerating the strategy and tools to employ. I deployed the kali linux terminal, the command line interface on kali linux operating system where some reconnaissance tools are hosted. The first tool I used was “WHOIS” on the command line and it returned information on three name servers, unsigned DNS security and Admin identity including phone number and some other information on megacorp one.

```
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
```

Next, I used the “dig” tool on Linux terminal, and this returned the website IP address. I also used the dig tool to find information on the name servers and this confirmed that the servers hold A records (IPV4 addresses), the server IP addresses and that name server 1 (ns1.megacorpone.com) is the Start of Authority (SOA), containing critical admin information and files which can be a key target for zone transfer attacks on DNS.

```
dig txt ns1.megacorpone.com
```

```
<<>> DiG 9.20.9-1-Debian <<>> txt ns1.megacorpone.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35619
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
ns1.megacorpone.com.      IN      TXT

;; AUTHORITY SECTION:
megacorpone.com.      300     IN      SOA     ns1.megacorpone.com.
admin.megacorpone.com. 202508051 28800 7200 2419200 300
```

```
└─(kali@kali)~
```

```
└─$ dig ns2.megacorpone.com
```

```
<<>> DiG 9.20.9-1-Debian <<>> ns2.megacorpone.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7797
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
ns2.megacorpone.com.      IN      A

;; ANSWER SECTION:
ns2.megacorpone.com.      300     IN      A       51.222.39.63
```

```
(kali㉿kali)-[~]
└─$ dig ns3.megacorpone.com

; <<>> DiG 9.20.9-1-Debian <<>> ns3.megacorpone.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45240
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 512
;; QUESTION SECTION:
;ns3.megacorpone.com.      IN      A

;; ANSWER SECTION:
ns3.megacorpone.com.  300    IN      A      66.70.207.180
```

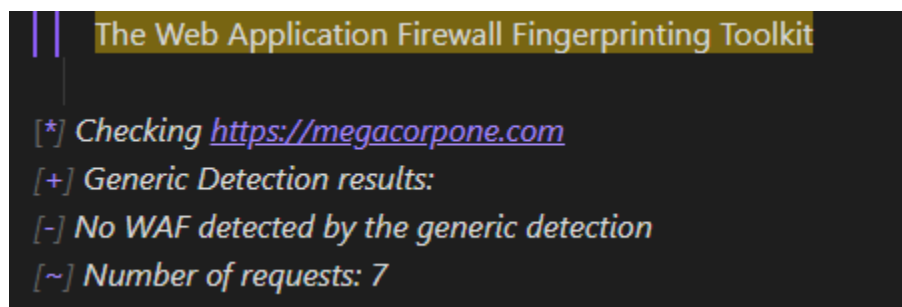
I then used the Nslookup tool to find any other infrastructure like mail servers and this returned four mail exchange servers in addition to the already identified three name servers.

```
└─$ nslookup

Non-authoritative answer:
megacorpone.com nameserver = ns2.megacorpone.com.
megacorpone.com nameserver = ns1.megacorpone.com.
megacorpone.com nameserver = ns3.megacorpone.com.

Non-authoritative answer:
megacorpone.com mail exchanger = 60 mail2.megacorpone.com.
megacorpone.com mail exchanger = 10 fb.mail.gandi.net.
megacorpone.com mail exchanger = 20 spool.mail.gandi.net.
megacorpone.com mail exchanger = 50 mail.megacorpone.com.
```

Having identified the NS and MX servers, i decided to check if the website is protected by a web application firewall (WAF). This is critical to filter inbound/outbound traffic and inputs into the website based on preset rules by the admin. I used the wafw00f tool to check for the firewall and no web firewall protection was detected. This is a vulnerability as threat actors can send malicious traffic into the network without any hindrance.

A terminal window with a dark background and yellow text. The title bar reads "The Web Application Firewall Fingerprinting Toolkit". The output shows a check for https://megacorpone.com, generic detection results, and a confirmation that no WAF was detected after 7 requests.

```
|| The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://megacorpone.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

The next step was to find the web server and its version. This can be used by threat actors as an attack vector if the web server has known vulnerabilities in the CVE/CWE database (see www.cve.mitre.org). Using the Curl tool on kali linux command line, the web server was detected to be an Apache web server, version 2.4.62 (debian). It also showed that the website uses http protocol version 1.1 which has recently been discovered to be vulnerable to http request smuggling which allows actors to inject malicious requests (<https://portswigger.net/research/http1-must-die#the-fatal-flaw-in-http11>), (<https://gbhackers.com/new-http-smuggling-technique/>). This web server and version was further corroborated by the Whatweb tool . Interestingly, the whatweb tool also revealed some developer tools used in the website viz a viz bootstrap and JQuery 1.11.0.

```
curl -I megacorpone.com
HTTP/1.1 200 OK
Date: Sat, 16 Aug 2025 21:06:51 GMT
Server: Apache/2.4.62 (Debian)
Last-Modified: Wed, 06 Nov 2019 15:04:14 GMT
ETag: "390b-596aedca79780"
Content-Type: text/html

whatweb megacorpone.com
http://megacorpone.com [200 OK] Apache[2.4.62], Bootstrap, CountryUNITED STATES, HTML5, HTTPServerDebian Linux, IP[149.56.244.87], JQuery[1.11.0], Script, Title[MegaCorp One - Nanotechnology Is the Future], X-UA-Compatible[IE=edge]
```

I then furthered the reconnaissance by enumerating subdomains within the company. This information can allow threat actors to map the network infrastructure and identify any subdomains that can be used for typosquatting and subsequently phishing attacks which can have catastrophic consequences even on large enterprises. I used the Amass tool on the command line and this successfully enumerated all subdomains, file server, name servers, mail exchange servers, IP addresses of subdomains, subnets also including router IP address. Below is a list of critical subdomains identified and their IP addresses;

- *siem.megacorpone.com 167.114.21.71*
- *vpn.megacorpone.com 167.114.21.76*
- *syslog.megacorpone.com 167.114.21.73*
- *test.megacorpone.com 167.114.21.75*
- *fs1.megacorpone.com 167.114.21.66*
- *support.megacorpone.com 167.114.21.74*
- *vpn2.megacorpone.com 167.114.21.77*
- *vpndev.megacorpone.com 167.114.21.78*
- *vpnprod.megacorpone.com 167.114.21.79*
- *snmp.megacorpone.com 167.114.21.72*

- admin.megacorpone.com 167.114.21.64

- beta.megacorpone.com 167.114.21.65

- intranet.megacorpone.com 167.114.21.67

- router.megacorpone.com 167.114.21.70

To corroborate the above subdomains, IP addresses and servers detected, I used an online tool DnsDumpster which will give a graphical output of the above data. A summary of the output from Dnsdumpster has been attached to this report in a .pdf file

Host	IP	Type	Reverse DNS	Netblock Owner	HTTP Services	Remote Services
admin.megacorpone.com	167.114.21.64	A	admin.megacorpone.com	OVH, FR 16276 / Canada		
ai.megacorpone.com	149.56.244.87	A	www.megacorpone.com	OVH, FR 16276 / Canada	HTTP: Apache/2.4.62 (Debian) - MegaCorp One	SSH: SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
beta.megacorpone.com	167.114.21.65	A	beta.megacorpone.com	OVH, FR 16276 / Canada	Nanotechnology Is the	
fs1.megacorpone.com	167.114.21.66	A	fs1.megacorpone.com	OVH, FR 16276 / Canada		
intranet.megacorpone.com	167.114.21.67	A	intranet.megacorpone.com	OVH, FR 16276 / Canada		
mail.megacorpone.com	167.114.21.68	A	mail.megacorpone.com	OVH, FR 16276 / Canada		
mail2.megacorpone.com	167.114.21.69	A	mail2.megacorpone.com	OVH, FR 16276 / Canada		
ns1.megacorpone.com	51.79.37.18	A	ns1.megacorpone.com	OVH, FR 16276 / Canada		SSH: SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
ns2.megacorpone.com	51.222.39.63	A	ns2.megacorpone.com	OVH, FR 16276 / Canada		SSH: SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
ns3.megacorpone.com	66.70.207.180	A	ns3.megacorpone.com	OVH, FR 16276 / Canada		SSH: SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
router.megacorpone.com	167.114.21.70	A	router.megacorpone.com	OVH, FR 16276 / Canada		
siem.megacorpone.com	167.114.21.71	A	siem.megacorpone.com	OVH, FR 16276 / Canada		
snmp.megacorpone.com	167.114.21.72	A	snmp.megacorpone.com	OVH, FR 16276 / Canada		
support.megacorpone.com	167.114.21.74	A	support.megacorpone.com	OVH, FR 16276 / Canada		
syslog.megacorpone.com	167.114.21.73	A	syslog.megacorpone.com	OVH, FR 16276 / Canada		
test.megacorpone.com	167.114.21.75	A	test.megacorpone.com	OVH, FR 16276 / Canada		
vpn.megacorpone.com	167.114.21.76	A	vpn.megacorpone.com	OVH, FR 16276 / Canada		
vpndev.megacorpone.com	167.114.21.78	A	vpndev.megacorpone.com	OVH, FR 16276 / Canada		
vpnprod.megacorpone.com	167.114.21.79	A	vpnprod.megacorpone.com	OVH, FR 16276 / Canada		
www.megacorpone.com	149.56.244.87	A	www.megacorpone.com	OVH, FR 16276 / Canada	HTTP: Apache/2.4.62 (Debian) - MegaCorp One	SSH: SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
www2.megacorpone.com	149.56.244.87	A	www.megacorpone.com	OVH, FR 16276 / Canada	HTTP: Apache/2.4.62 (Debian) - MegaCorp One	SSH: SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
60 mail2.megacorpone.com	167.114.21.69	MX	mail2.megacorpone.com	OVH, FR 16276 / Canada		
10 fb.mail.gandi.net	217.70.178.215	MX	spool6.mail.gandi.net	GANDI-AS Domain name registrar - www.gandi.net, FR		
20 spool.mail.gandi.net	217.70.178.1	MX	spool.mail.gandi.net	GANDI-AS Domain name registrar - www.gandi.net, FR		
ns1.megacorpone.com	51.79.37.18	NS	ns1.megacorpone.com	OVH, FR 16276 / Canada		SSH: SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
ns2.megacorpone.com	51.222.39.63	NS	ns2.megacorpone.com	OVH, FR 16276 / Canada		SSH: SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3
ns3.megacorpone.com	66.70.207.180	NS	ns3.megacorpone.com	OVH, FR 16276 / Canada		SSH: SSH-2.0-OpenSSH_9.2p1 Debian-2+deb12u3

Interesting to note from the output of Dnsdumpster is that remote access to the name servers and webserver uses SSH2.0 which is secure but also uses OpenSSH 9.2p1 which is a vulnerable version of openssh notably CVE-2023-38408 and CVE-2023-28531 both of which have a CVSS score of 9.8 (critical).

With these information, I tried to find other technology stack and versions in the website. I searched on GitHub and found a repository used to dump some of the web development tools and developer codes. I was able to find some technologies used in the web development namely bootstrap v3.1.1, JQuery v1.1.0, retina v1.1.0 and isotope v1.5.25 some of which have known vulnerabilities documented in the CVE database. Using URL manipulation, I was able to check that these technologies were indeed used for the website development and also, I found the identity of the web developer (Carlos Alvarez). The GitHub repository also revealed some key team members' names and email contacts including social media handles. This can easily allow actors to perpetrate different types of phishing attacks. See link to the github repository below;

<https://github.com/megacorpone/megacorpone.com/blame/master/megacorpone/index.html>

← → ↻ 🌐 megacorpone.com/assets/

Index of /assets

Name	Last modified	Size	Description
🔙 Parent Directory		-	
📁 css/	2016-08-21 11:21	-	
📁 fonts/	2016-08-21 11:21	-	
📁 img/	2017-10-03 09:08	-	
📁 js/	2016-08-21 11:21	-	

Apache/2.4.62 (Debian) Server at www.megacorpone.com Port 443

← → ↻ 🌐 megacorpone.com/assets/css/bootstrap.css

```
/*!
 * Bootstrap v3.1.1 (http://getbootstrap.com)
 * Copyright 2011-2014 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 */

/*! normalize.css v3.0.0 | MIT License | git.io/normalize */
html {
  font-family: sans-serif;
  -webkit-text-size-adjust: 100%;
  -ms-text-size-adjust: 100%;
}
body {
  margin: 0;
```

```
megacorpone.com/assets/css/style.css

/* #####
Author: Carlos Alvarez
URL: http://alvarez.is

Project Name: SOLID - Bootstrap 3 Theme
Version: 1.0
URL: http://alvarez.is

##### */
@import url(http://fonts.googleapis.com/css?family=Raleway:400,700,900);
@import url(http://fonts.googleapis.com/css?family=Lato:400,900);
@import url("prettyPhoto.css") screen;
@import url("hoverex-all.css") screen;

/* #####
1. GENERAL STRUCTURES
##### */
* {
    margin: 0;
    padding: 0px;
}

body {
    background: #ffffff;
    margin: 0;
    width: 100%;
```

```
Click to go back, hold to see history

/**
 * Isotope v1.5.25
 * An exquisite jQuery plugin for magical layouts
 * http://isotope.metafizzy.co
 *
 * Commercial use requires one-time purchase of a commercial license
 * http://isotope.metafizzy.co/docs/license.html
 *
 * Non-commercial use is licensed under the MIT License
 *
 * Copyright 2013 Metafizzy
 */
(function(a,b,c){"use strict";var d=a.document,e=a.Modernizr,f=function(a){return
```

```
<h4>Tanya Rivera</h4>
<h5 class="ctitle">LEAD DEVELOPER</h5>
<p>Email: trivera@megacorpone.com</p>
<p>Twitter: <a href="https://twitter.com/TanyaRiveraMCO" target="_blank">@TanyaRiveraMCO</a></p>
```

```
<h4>Tom Hudson</h4>
<h5 class="ctitle">LEAD DESIGNER</h5>
<p>Email:thudson@megacorpone.com</p>
<p>Twitter: <a href="https://twitter.com/TomHudsonMCO" target="_blank">@TomHudsonMCO</a></p>
```

```
← → ↻ 🔍 megacorpone.com/assets/js/retina-1.1.0.js

*!
* Retina.js v1.1.0
*
* Copyright 2013 Imulus, LLC
* Released under the MIT license
*
* Retina.js is an open source script that makes it easy to serve
* high-resolution images to devices with retina displays.
*/
function() {

  var root = (typeof exports == 'undefined' ? window : exports);

  var config = {
    // Ensure Content-Type is an image before trying to load @2x image
    // https://github.com/imulus/retinajs/pull/45)
    check_mime_type: true
  };

  /**
   * jquery.hoverdir.js v1.1.0
   * http://www.codrops.com
   *
   * Licensed under the MIT license.
   * http://www.opensource.org/licenses/mit-license.php
   *
   * Copyright 2012, Codrops
   * http://www.codrops.com
   */
  ;( function( $, window, undefined ) {

<h4>Tom Hudson</h4>
<h5 class="ctitle">LEAD DESIGNER</h5>
<p>Email: thudson@megacorpone.com</p>
<p>Twitter: <a href="https://twitter.com/TomHudsonMCO" target="_blank">@TomHudsonMCO</a></p>

</div><!-- the wrap -->
<h4>Joe Sheer</h4>
<h5 class="ctitle">CEO</h5>
<p>Email: joe@megacorpone.com</p>
<p>Twitter: <a href="https://twitter.com/joe_sheer/" target="_blank">@Joe_Sheer</a></p>
```

To confirm the employees data found on GitHub, I searched them out on the company website, social media sites LinkedIn and Twitter. A lot more employee data was revealed as they all linked up on social media. Most employees also stated on their profiles they work at megacorp

one and their positions in the company. This is an easy win for potential attackers looking to conduct phishing attacks on the company.

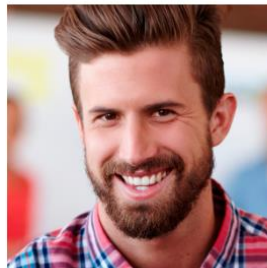
The job advert on the company website for a firewall administrator also revealed that they use Firepass firewall. Further research into this type of firewall showed that the firewall has known vulnerabilities documented in the CVE database as CVE-2012-1777 and a CVSS score of 7.5 (high) <https://www.cve.org/CVERecord/SearchResults?query=CVE-2012-1777>.



Joe Sheer
CHIEF EXECUTIVE OFFICER

Email: joe@megacorpone.com

Twitter: [@Joe_Sheer](https://twitter.com/Joe_Sheer)



Tom Hudson
WEB DESIGNER

Email: thudson@megacorpone.com

Twitter: [@TomHudsonMCO](https://twitter.com/TomHudsonMCO)



Tanya Rivera
SENIOR DEVELOPER

Email: trivera@megacorpone.com

Twitter: [@TanyaRiveraMCO](https://twitter.com/TanyaRiveraMCO)




Matt Smith
MARKETING DIRECTOR

Email: msmith@megacorpone.com

Twitter: [@MattSmithMCO](https://twitter.com/MattSmithMCO)






...

Follow

Ed Mackey
@EdMackey_Mega

Shipping for MegaCorpOne. Respect shipping. If it don't ship, you don't get it. It matters the most.

 Joined March 2013

3 Following 9 Followers



...

Follow

Handy McKay
@McKayHandy

Recruiter for MegaCorpOne.

 Joined March 2013

2 Following 8 Followers



...

Follow

Alan Grofield
@Grofield

I am IT and Security Director for MegaCorpOne. If its electronic, its mine.

 Joined March 2013

3 Following 10 Followers

Not followed by anyone you're following



...

Follow

Gabriel Cook
@GabrielCookMCO

MegaCorp One | Leaders in Nano-Technology research and practical application

📍 Nevada

🌐 megacorpone.com

📅 Joined April 2021

9 Following 3 Followers





...

Follow

Tom Hudson
@TomHudsonMCO

Lead Designer, Nano-Tech company

📍 Nevada, USA

🌐 megacorpone.com

📅 Born 1977

📅 Joined August 2016





...

Follow

Matt Smith
@MattSmithMCO

Marketing and Sales

🌐 megacorpone.com

📅 Joined August 2016



Index of contact profiles from MegaCorp One

Thousands of professionals searching for MegaCorp One have connected with key decision-makers. [Join them?](#)

Contact Name	Contact Info	Job Title	Location
 Mike Carlow	 Email  Direct	Vice President, Legal Affairs	United States , Nevada , Rachel
 Joe Sheer	 Email  Direct	Chief Executive Officer	United States , Nevada , Rachel
 Stan Denvers	 Email  Direct	Collections	United States , Nevada , Rachel
 Tom Hudson	 Email  Direct	Web Designer	United States , Nevada , Rachel
 Soum Test	 Email  Direct	System Analyst	United States , Nevada , Rachel
 Mutunga Muli	 Email  Direct	Electrical Specialist	United States , Nevada , Rachel
 Ga Rod	 Email  Direct	Boss	United States , Nevada , Rachel
 Fred Ducasse	 Email  Direct	Investments	United States , Nevada , Rachel

MegaCorp One

HOME

ABOUT

CONTACT

SUPPORT

CAREERS

LOG IN

Careers.



IT Positions

Citrix Administrator

Maintain, secure, and expand the MegaCorp One Citrix installation. Applicant must be well versed with remote work conditions and understand endpoint security solutions.

Firewall Administrator

Position is responsible for the administration of the Firepass firewall. Applicant must have at least 3 years experience with firewall administration and 5 years networking experience.

RECONNAISSANCE AUTOMATION:

With all the above results, I automated the reconnaissance process using Spiderfoot tool which uses both the command line interface on kali linux and a web interface to display results in bar chart. All the information obtained using various reconnaissance tools above were presented wholistically and easily interpretable bar chart by clicking on any individual bar. Each bar represents a set of data.

[illegible]

RISK ASSESSMENT MATRIX FOR ALL FINDINGS

Finding	Description	Likelihood	Impact	Risk Level	Recommended mitigation
Unsigned DNSSEC	Users are exposed to DNS spoofing, hijacking and cache poisoning	High	High	Critical	Enable DNSSEC
No Web Application Firewall	Inbound/outbound web traffic and web inputs are not filtered	High	High	Critical	Implement Web application Firewall
Vulnerable web server	Apache 2.4.62 has known vulnerabilities. One CVE has CVSS score of 9.1	High	High	Critical	Upgrade to latest version or use proxy server Nginx
JQuery v1.1.0	Vulnerable to XSS attacks	High	Medium	High	Use latest version
Bootstrap v3.1.1	Vulnerable to XSS attacks	High	High	High	Use latest version
HTTP/1.1	Could allow http request smuggling, malicious requests	Medium	Medium	Medium	Upgrade to HTTP/3
OpenSSH 9.2p1	Known vulnerabilities could allow RCE	Medium	Medium	Medium	Upgrade to version 10
Firepass Firewall	Vulnerable to SQLi	High	High	Critical	Strict rules and access controls
Exposed employee	Publicly available employee data could be used to orchestrate phishing attacks	High	Medium	High	User training, use generic contact forms

Finding	Description	Likelihood	Impact	Risk Level	Recommended mitigation
URL manipulation	Adding parameters to URL to find background resources	High	High	High	Use input validation, implement Web application firewall
Unprotected subdomains	Subdomains could be used for typosquatting, phishing attacks	High	Medium	High	Restrict public access, require authentication, implement network segmentation

CONCLUSION

Given all the above findings, it is critical to close loopholes and subsequently reduce or eliminate any attack vectors that could be of advantage to threat actors. Robust security controls must be always implemented to ensure regulatory compliance, avoid Cyber attacks, reputational damage, financial loss and penalties.