

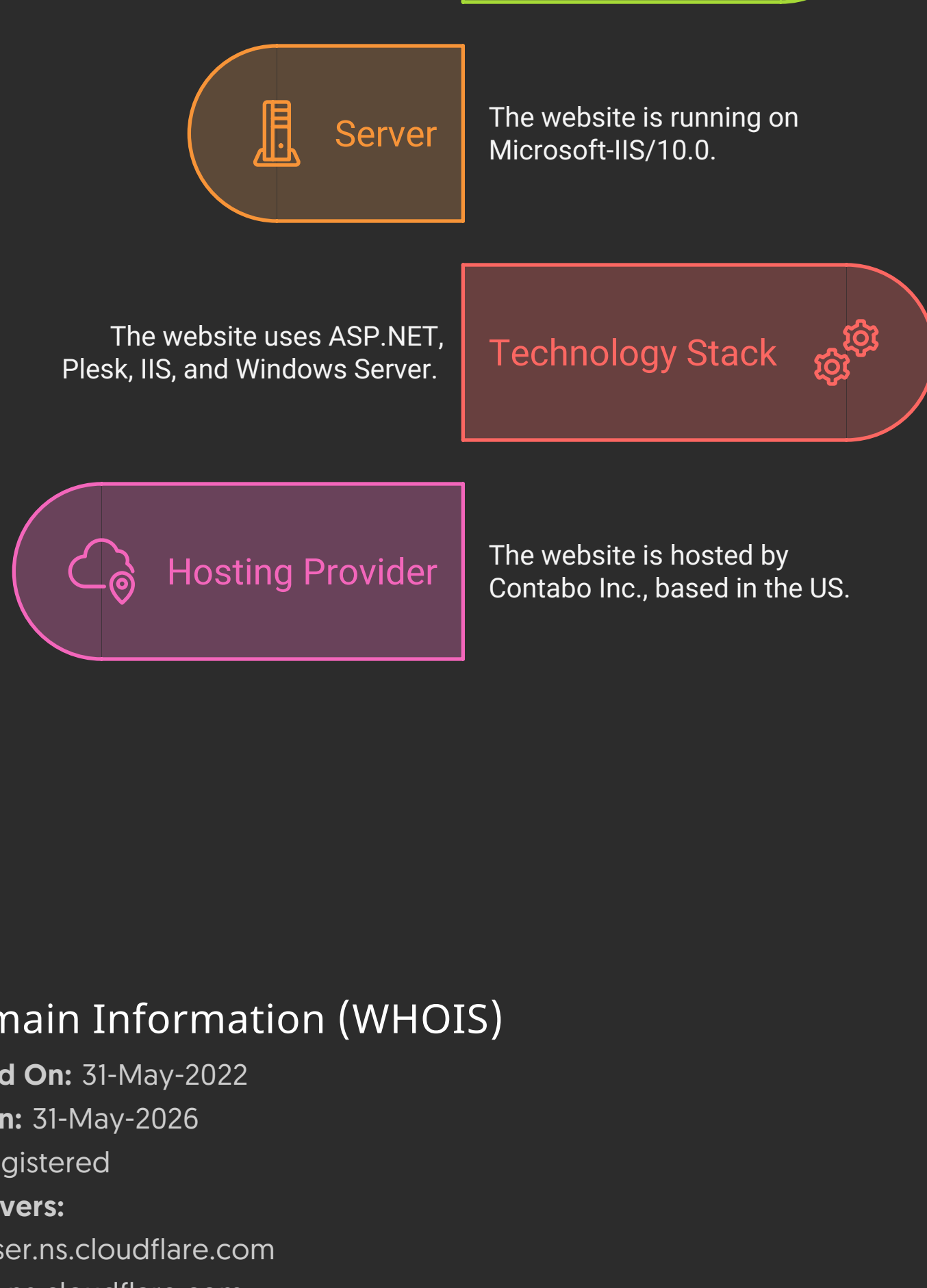
# 🔍!! OSINT Report – Bano Qabil (banoqabil.pk)

Prepared By: Daniyal Rashid  
Phone: 0313-7840038  
Roll Number: 582297  
Submission Date: 31 July 2025

## 1. 🎯 Target Overview

**Target Domain:** https://banoqabil.pk **Current Status:** Active **Server:** Microsoft-IIS/10.0  
**Technology Stack:** ASP.NET, Plesk, IIS, Windows Server **Hosting Provider:** Contabo Inc. [US-Based]

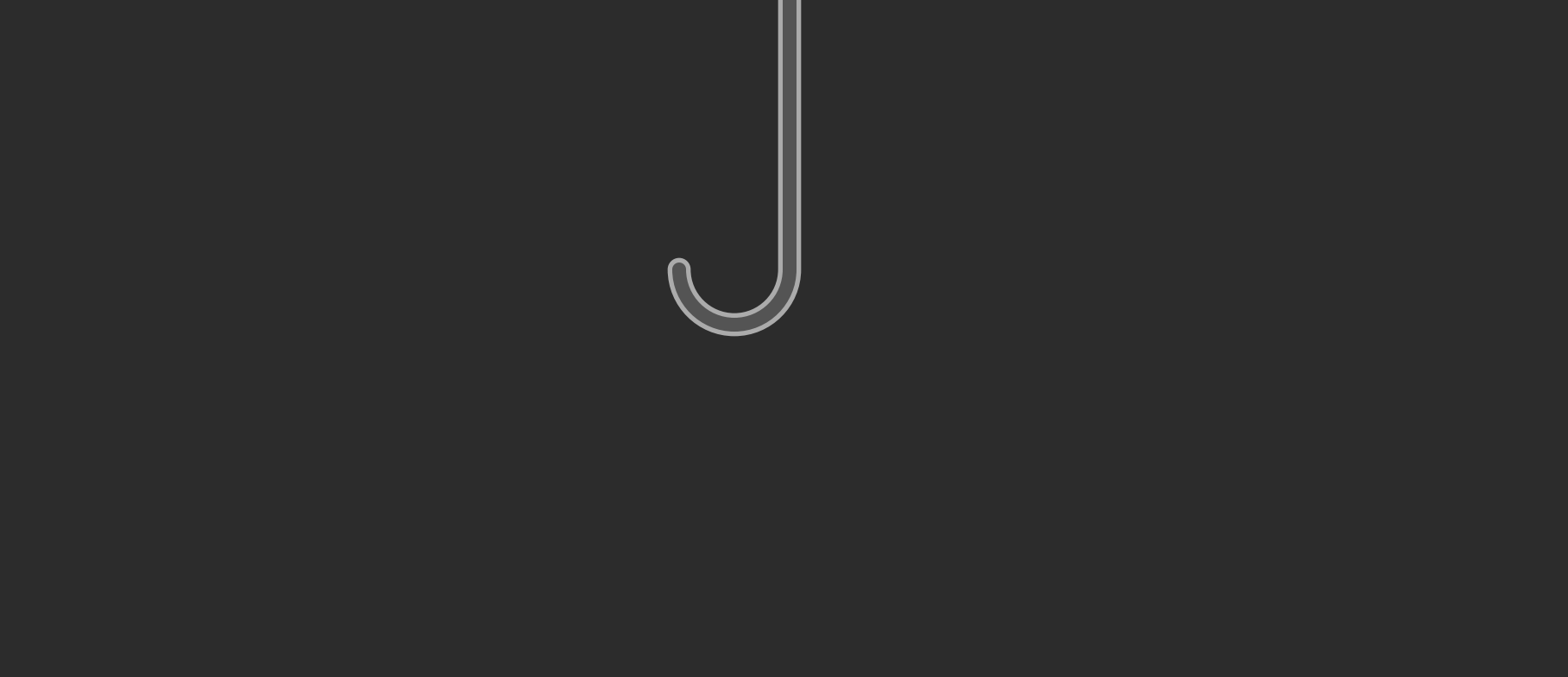
## Website Information



## 2. 📄 Domain Information (WHOIS)

- Registered On:** 31-May-2022
- Expires On:** 31-May-2026
- Status:** Registered
- Name Servers:**
  - kaiser.ns.cloudflare.com
  - ulla.ns.cloudflare.com

## Domain Information Breakdown

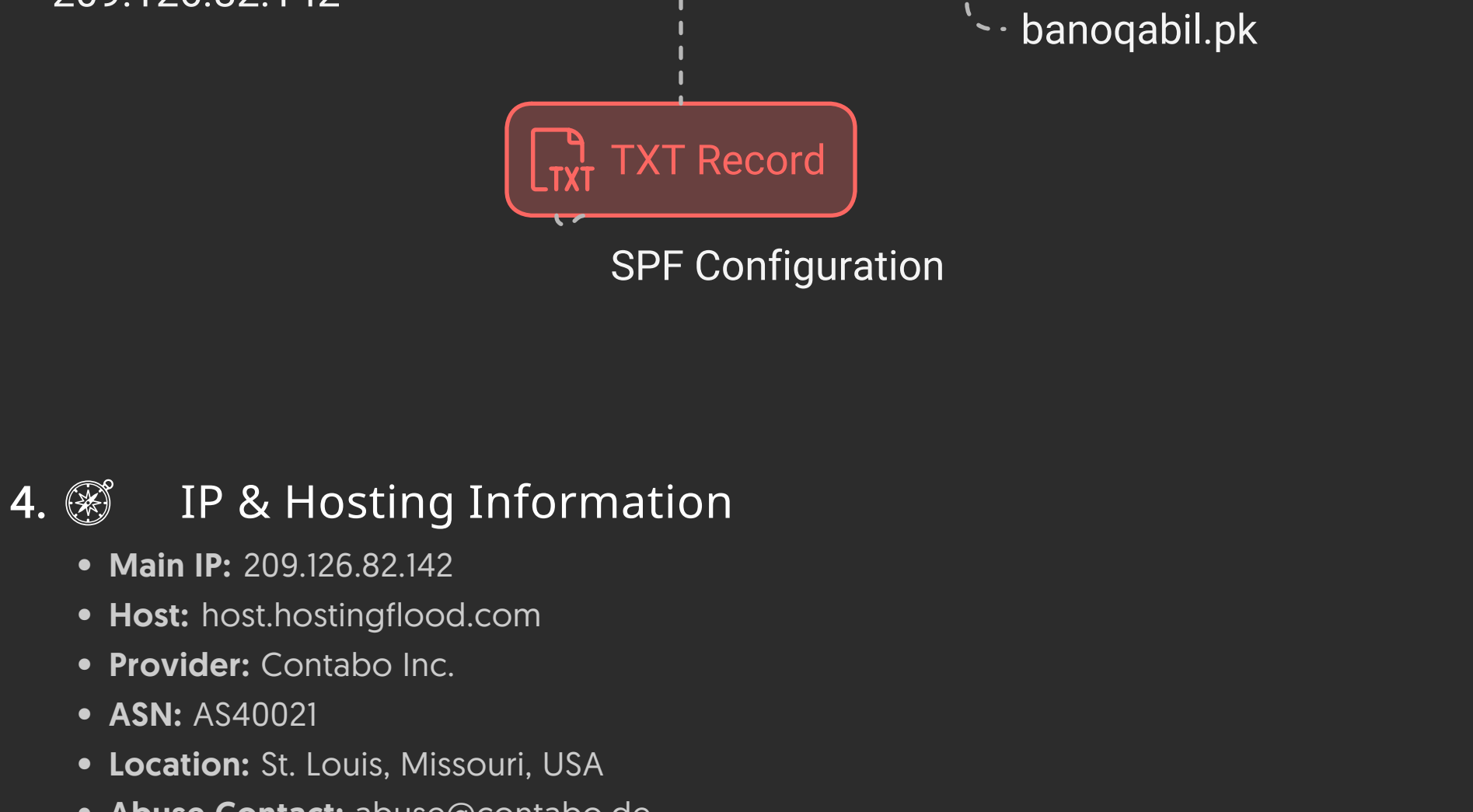


## 3. 🌐 DNS Records

- A Record:** 209.126.82.142
- MX Record:** mail.banoqabil.pk → 209.126.82.142
- NS Records:**
  - kaiser.ns.cloudflare.com [108.162.195.9]
  - ulla.ns.cloudflare.com [108.162.192.233]
- CNAME:** www.banoqabil.pk → banoqabil.pk
- TXT Record:**

```
"v=spf1 +a +mx +a:blissful-mcnulty.209-126-82-142.plesk.page ~all"
```

## DNS Records of Bano Qabil



## 4. 🌐 IP & Hosting Information

- Main IP:** 209.126.82.142
- Host:** host.hostingflood.com
- Provider:** Contabo Inc.
- ASN:** AS40021
- Location:** St. Louis, Missouri, USA
- Abuse Contact:** abuse@contabo.de

## Unveiling Bano Qabil's Digital Footprint

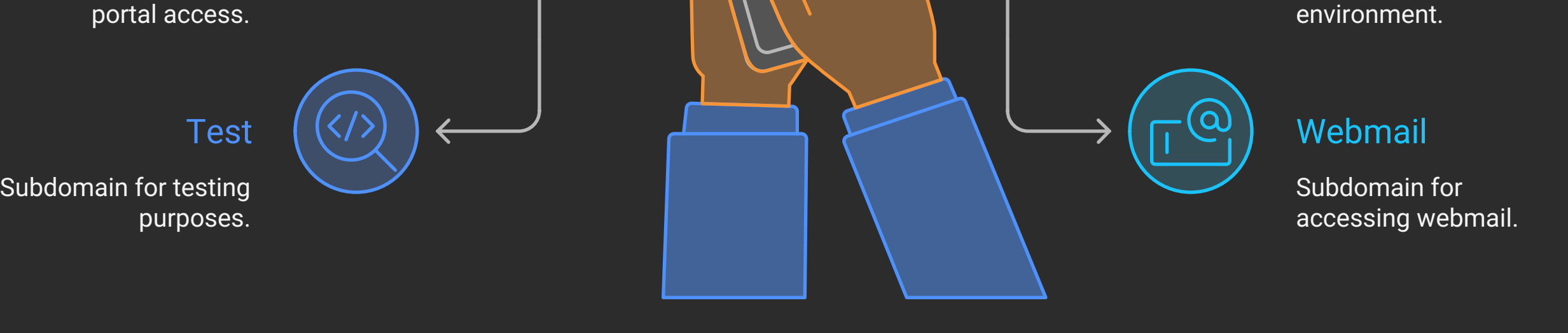


## 5. 🔍 Subdomain Discovery

**Total Found:** 38 Examples include:

- admin.banoqabil.pk
- app.banoqabil.pk
- courses.banoqabil.pk
- ecommerce.banoqabil.pk
- portal.banoqabil.pk
- staging.banoqabil.pk
- test.banoqabil.pk
- webmail.banoqabil.pk

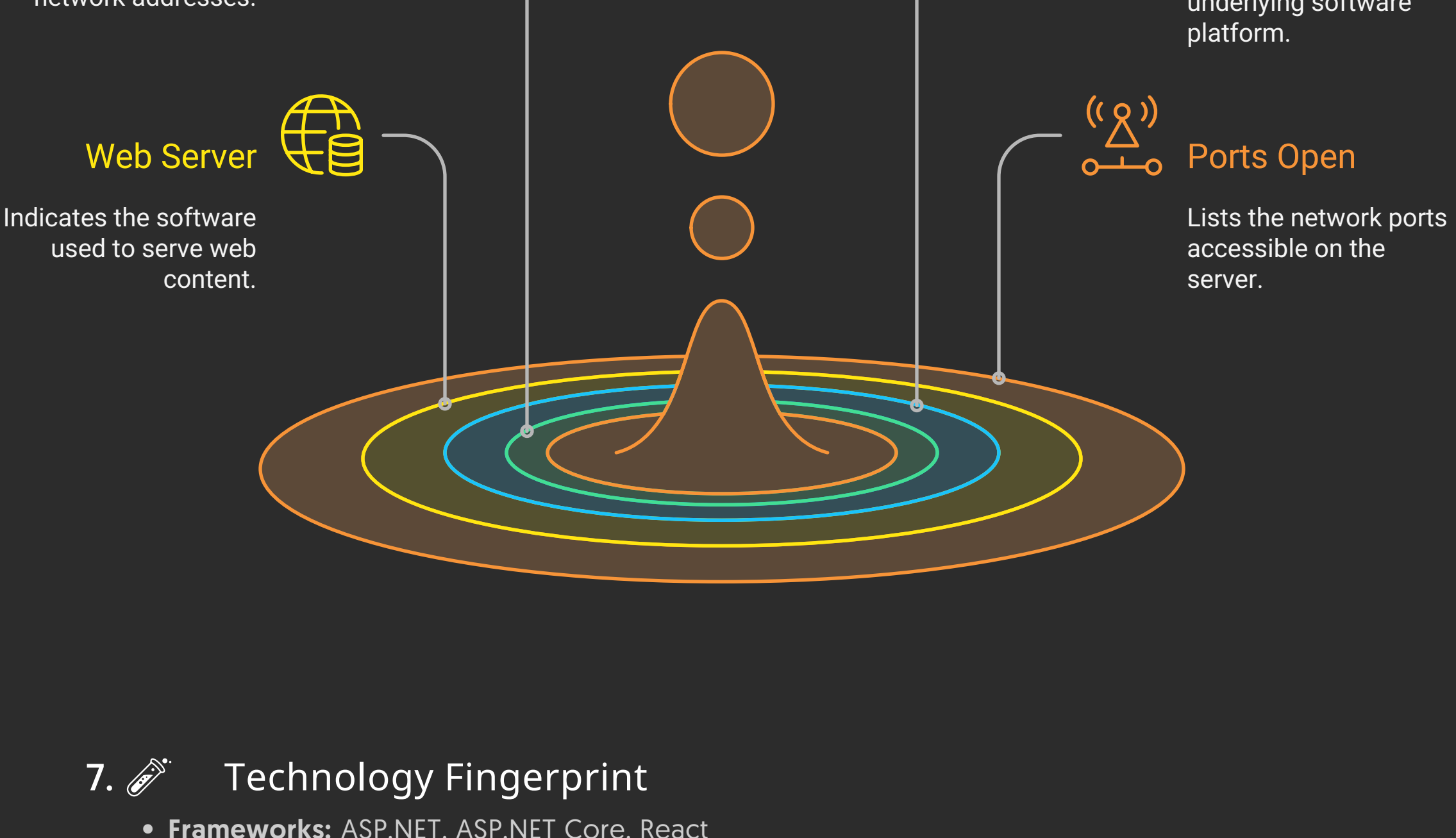
## Bano Qabil Subdomains



## 6. 🔍 Shodan Results

- Hostnames:**
  - host.hostingflood.com
  - blissful-mcnulty.209-126-82-142.plesk.page
- Operating System:** Windows Server
- Web Server:** Microsoft IIS 10.0
- Ports Open:** 21, 25, 53, 80, 110, 135, 443, 465, 993, 995, 1433, 3306, 3389, 8443, 8880

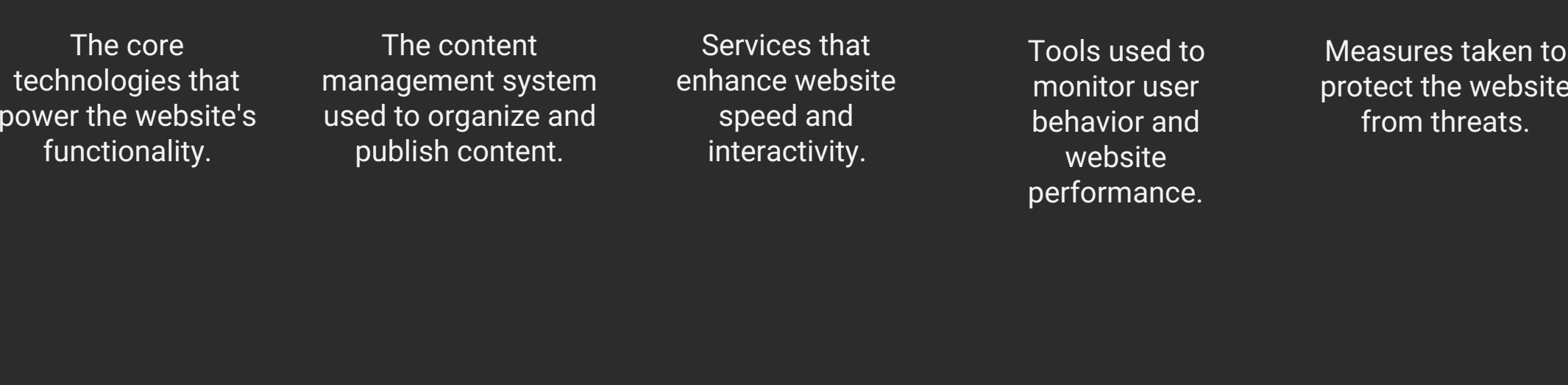
## Server Configuration Analysis



## 7. 🖋️ Technology Fingerprint

- Frameworks:** ASP.NET, ASP.NET Core, React
- CMS:** Plesk
- CDN & JS:** Cloudflare, jsDelivr, Google Font API, JQuery
- Tracking Tools:**
  - Google Analytics, Facebook Pixel
  - Google Tag Manager
  - Conversion Linkers (Facebook + Google)
- Security:** SSL (Let's Encrypt), SPF, DMARC

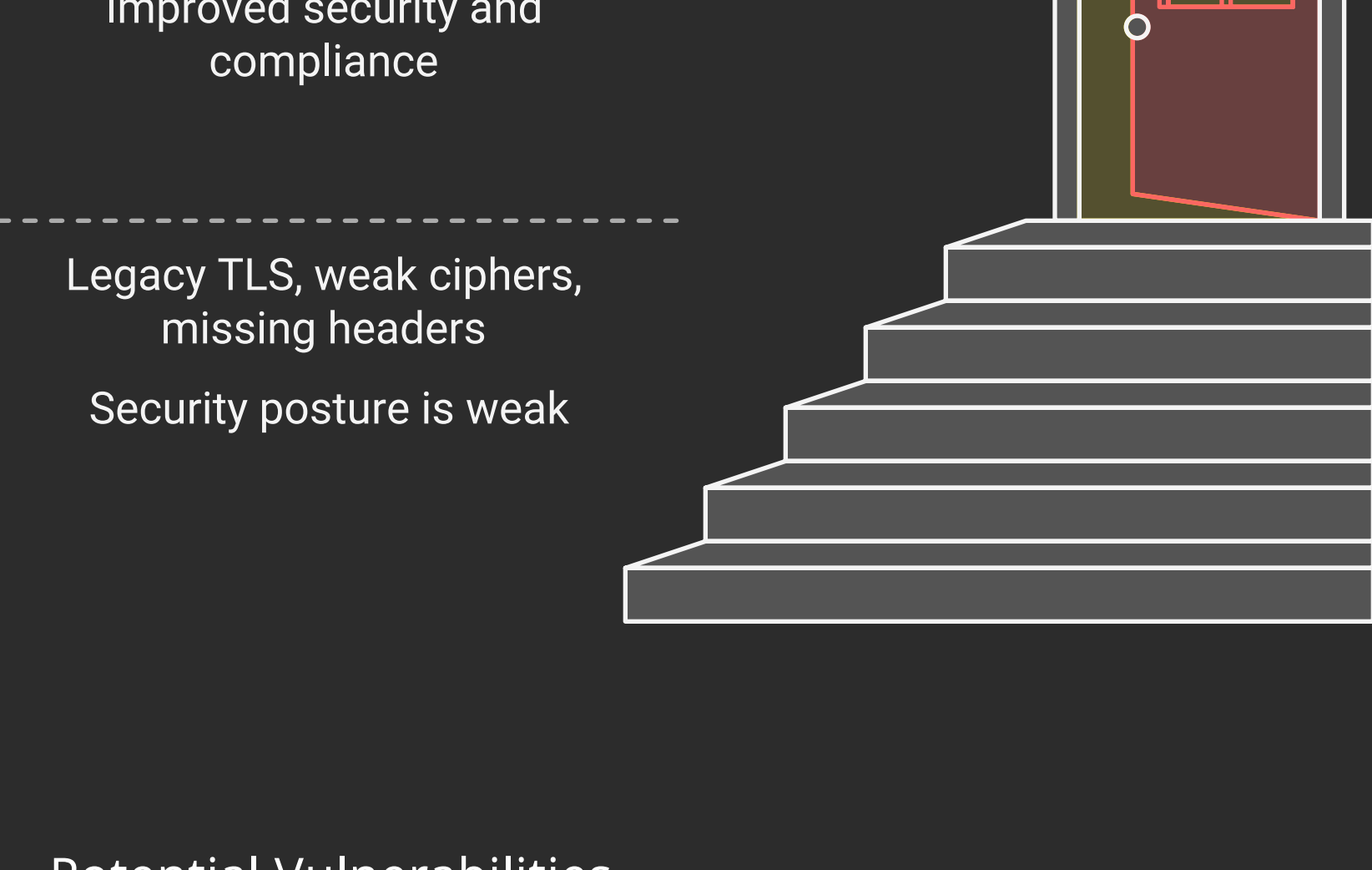
## Bano Qabil's Digital Infrastructure



## 8. 🛡️ Security & SSL Report

- Grade:** B
- TLS Support:** TLS 1.0, 1.1, 1.2 [No TLS 1.3]
- Weak Cipher Suites:** Present
- Certificate Issuer:** Let's Encrypt (RSA 2048-bit)
- Valid Till:** 16-Oct-2025
- Security Headers Missing:**
  - Content-Security-Policy
  - X-Content-Type-Options
  - Referrer-Policy
  - Permissions-Policy

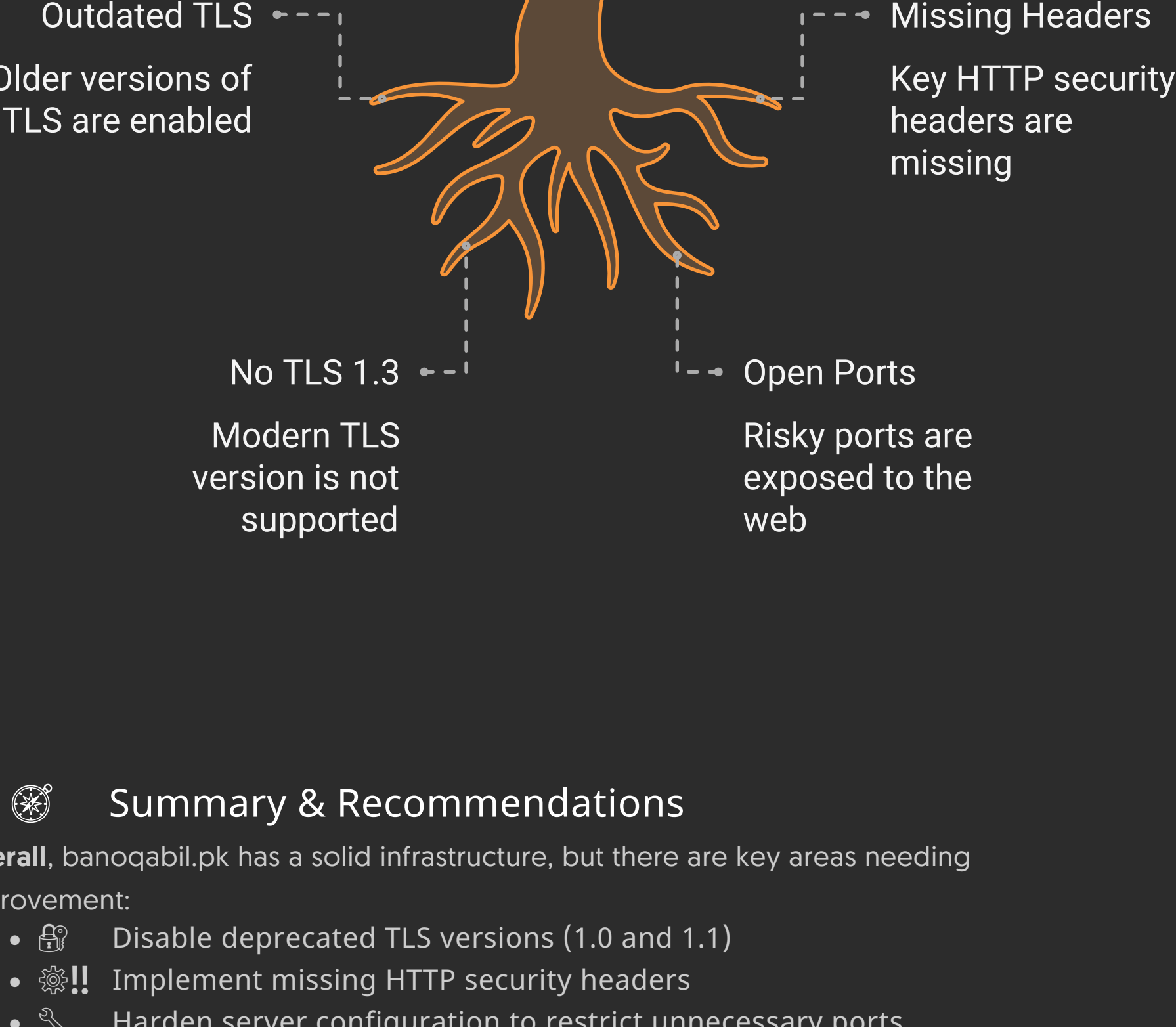
## Enhance website security through modern protocols and headers.



## 9. 📋 Potential Vulnerabilities

- TLS 1.0 and TLS 1.1 are still enabled – outdated and insecure.
- Lacking key HTTP security headers.
- No support for TLS 1.3 – recommended for modern security.
- Possible exposure through open ports like 3389, 3306, and 1433.

## Insecure Bano Qabil website configuration



## 10. 📋 Summary & Recommendations

**Overall,** banoqabil.pk has a solid infrastructure, but there are key areas needing improvement:

- 🛡️ Disable deprecated TLS versions (1.0 and 1.1)
- 🔒 Implement missing HTTP security headers
- 🔒 Harden server configuration to restrict unnecessary ports
- 🔒 Enable TLS 1.3 for modern encryption
- 🔒 Sanitize subdomains to reduce attack surface

## Enhancing Website Security

