EXECUTIVE SUMMARY

Security & Compliance Report

vitasorahealth.com

Scan Timestamp: May 25, 2026 8:08 PM UTC

SECURITY ISSUES DETECTED

Checks Passed

8 / 16 (50% security score)

Check Breakdown

Passed Checks (8):

- SSL/TLS Certificate
- Enhanced TLS
- SPF
- DKIM
- RPKI
- IP Abuse Checks
- Domain Reputation
- WordPress

Failed Checks (8):

- DNSSEC
- IPv6 Support
- Enhanced HTTPS
- Certificate Validation
- Security Headers
- DMARC
- MTA-STS
- TLS-RPT

Risk Posture Statement

This domain has critical security deficiencies that pose significant risk and require immediate remediation.

PrismWeb Security Report

Domain Security Assessment

This security assessment analyzes your domain's security configuration to help protect your business from cyber threats. The results show how well your domain is protected against common security risks that could impact your business operations, customer trust, and data security.

Action Required

Failing even 1 check is a major security concern and should be addressed immediately. Each failing control represents a potential attack vector that could be exploited by malicious actors.

Report Generated By:

PrismWeb - B2B Managed Service Provider

Helping small businesses secure their domains, meet modern cybersecurity standards, and reduce legal and operational risk.

Domain & DNS Security

Layer: Internet resolution and authenticity. Checks included: DNSSEC validation, nameserver configuration. Why this matters: DNS is foundational. If DNS is compromised, everything else is irrelevant. Attackers can redirect traffic, intercept communications, or impersonate your domain if DNS security is weak. Responsibility: Domain administrator manages DNS records, DNSSEC keys, and nameserver configuration.

DNSSEC

FAILED

What is DNSSEC (Domain Name System Security Extensions)?

DNSSEC adds cryptographic signatures to DNS records to protect against DNS spoofing and cache poisoning attacks. It creates a chain of trust from the root DNS zone down to your domain.

Why is this important?

Without DNSSEC, attackers can redirect your domain to malicious servers by poisoning DNS caches. This can lead to phishing attacks, data theft, and loss of trust. DNSSEC ensures that DNS responses are authentic and haven't been tampered with.

What can go wrong?

If DNSSEC is not properly configured: attackers can hijack your DNS, redirect traffic to malicious sites, intercept emails, and compromise your entire domain infrastructure. Improper DNSSEC setup can also cause DNS resolution failures.

Technical Details:

DNSSEC uses public-key cryptography. The root zone has DNSKEY records, which are signed by RRSIG records. Each level (root ? TLD ? domain) has DS (Delegation Signer) records that link the chain together. The domain must have DNSKEY records and RRSIG records for all DNS record types.

Check Details:

Status: DNSSEC is not enabled

Web Transport Security (HTTPS & TLS)

Layer: Client-to-server encryption. Checks included: HTTPS availability, HTTPS redirect enforcement, TLS version support, cipher configuration, TLS renegotiation security, 0-RTT status, compression settings, HSTS configuration. Why this matters: TLS is one logical system that protects data in transit between browsers and servers. Weak TLS configuration allows attackers to intercept, decrypt, or modify communications. Modern standards require TLS 1.2 or higher with secure cipher suites. Responsibility: Web and infrastructure team configures web server TLS settings, certificate deployment, and HTTPS redirect rules.

SSL/TLS Certificate

PASSED

What is SSL/TLS Certificate?

SSL/TLS certificates encrypt data transmitted between web browsers and servers, ensuring that sensitive information cannot be intercepted by attackers.

Why is this important?

SSL/TLS is essential for protecting customer data and preventing man-in-the-middle attacks. Without it, all data transmitted is visible to attackers and browsers will show security warnings.

What can go wrong?

If SSL/TLS is not properly configured: all data is transmitted in plain text, attackers can intercept and modify communications, browsers will show security warnings, and customer trust is compromised.

Technical Details:

SSL/TLS certificates contain: issuer information, subject (domain name), validity dates, public key, and digital signature. Certificates must be valid, not expired, and match the domain name. HTTPS should be forced (HTTP redirects to HTTPS).

Check Details:

SSL Enabled:	Yes
HTTPS Forced:	Yes
Certificate Valid:	Yes
Valid Until:	2027-02-19T23:59:59.000Z
Issuer:	Amazon RSA 2048 M01

Enhanced HTTPS

FAILED

What is Enhanced HTTPS Configuration?

Enhanced HTTPS checks verify that HTTPS is properly configured with redirects, compression, and HSTS (HTTP Strict Transport Security) headers.

Why is this important?

Proper HTTPS configuration is fundamental to web security. HSTS prevents downgrade attacks and ensures all connections are encrypted. HTTPS redirects ensure users always use secure connections. These protect against man-in-the-middle attacks and are essential for protecting customer data.

What can go wrong?

Without proper HTTPS configuration: users may access your site over unencrypted HTTP, attackers can intercept and modify communications, browsers will show security warnings, and you fail compliance requirements. Missing HSTS allows attackers to force unencrypted connections.

Technical Details:

HTTPS checks verify: 1) HTTPS is available and working, 2) HTTP redirects to HTTPS automatically, 3) HSTS header is present with appropriate max-age, 4) HSTS includes subdomains when appropriate. HTTP compression is informational but improves performance.

Check Details:

HTTPS Available:	Yes
HTTPS Redirect:	Yes
HTTP Compression:	Enabled
HSTS Enabled:	No
HSTS Include Subdomains:	No

Enhanced TLS

PASSED

What is Enhanced TLS Configuration?

TLS (Transport Layer Security) configuration checks verify that your server uses secure TLS versions, proper cipher suites, and secure settings.

Why is this important?

Proper TLS configuration prevents attacks like BEAST, POODLE, and other TLS vulnerabilities. Weak ciphers, TLS compression, or insecure renegotiation can allow attackers to decrypt or intercept communications. This is critical for protecting sensitive business and customer data.

What can go wrong?

Weak TLS configuration: allows attackers to decrypt communications, enables man-in-the-middle attacks, exposes sensitive data, and fails security compliance. TLS compression (CRIME attack) and client-initiated renegotiation are serious vulnerabilities.

Technical Details:

TLS checks verify: 1) TLS version 1.2 or higher (TLS 1.3 preferred), 2) Strong cipher suites with proper ordering, 3) Secure key exchange parameters, 4) No TLS compression (vulnerable to CRIME), 5) Secure renegotiation enabled, 6) Client-initiated renegotiation disabled, 7) 0-RTT (early data) status.

Check Details:

TLS Version:	TLSv1.3
Cipher Order:	Good
Key Exchange Parameters:	Secure
Key Exchange Hash:	Secure
TLS Compression:	Disabled (Secure)
Secure Renegotiation:	Supported
Client-Initiated Renegotiation:	Disabled (Secure)
0-RTT:	Disabled

Certificate & Trust Policy

Layer: Cryptographic trust and issuance control. Checks included: Certificate validity, trust chain verification, public key validation, signature verification, domain name matching, CAA (Certificate Authority Authorization) records. Why this matters: Certificates and CAA are about who is allowed to issue trust, not transport mechanics. Invalid certificates or missing CAA records allow attackers to obtain fraudulent certificates for your domain, enabling man-in-the-middle attacks. Trust chain validation ensures certificates are issued by legitimate Certificate Authorities. Responsibility: Security and PKI administrators manage certificate lifecycle, CAA DNS records, and trust chain configuration.

Certificate Validation

FAILED

What is Certificate Validation?

Certificate validation checks verify that your SSL/TLS certificate has a valid trust chain, proper public key, valid signature, matches your domain, and has CAA records.

Why is this important?

A valid certificate chain ensures browsers trust your certificate. Domain name matching prevents certificate errors. CAA records control which Certificate Authorities can issue certificates for your domain, preventing unauthorized certificate issuance. This is fundamental to HTTPS security.

What can go wrong?

Invalid certificates: browsers show security warnings, users cannot access your site, attackers can issue fake certificates for your domain (without CAA), and you fail compliance requirements. Missing CAA records allow any CA to issue certificates for your domain.

Technical Details:

Certificate validation checks: 1) Trust chain (certificate is signed by trusted CA), 2) Public key validity, 3) Signature validity, 4) Domain name matches certificate (CN or SAN), 5) CAA (Certificate Authority Authorization) DNS records exist to control certificate issuance.

Check Details:

Trust Chain:	Valid
Public Key:	Valid
Signature:	Valid
Domain Name Match:	Matches
CAA Record:	Not Found

HTTP Application Security Headers

Layer: Browser-side attack prevention. Checks included: X-Frame-Options, X-Content-Type-Options, Referrer-Policy, security.txt file presence. Why this matters: Headers mitigate XSS, clickjacking, data leakage. They are not TLS controls but application-level security directives that instruct browsers how to handle your content. Missing headers allow attackers to embed your site in malicious frames, execute XSS attacks, or leak sensitive referrer information. The security.txt file provides a standardized way for security researchers to report vulnerabilities. Responsibility: Web application owner configures HTTP response headers in web server or application framework settings.

Security Headers

FAILED

What is Security Headers?

Security headers are HTTP response headers that instruct browsers on how to handle content and protect against various attacks.

Why is this important?

Security headers protect against XSS attacks, clickjacking, MIME-type sniffing, and other web vulnerabilities. They are essential for protecting your business website and customer data.

What can go wrong?

Without proper security headers: websites are vulnerable to XSS attacks, clickjacking, data injection, and other security threats. Browsers cannot enforce security policies.

Technical Details:

Important headers include: Strict-Transport-Security (HSTS), Content-Security-Policy (CSP), X-Frame-Options, X-Content-Type-Options, X-XSS-Protection, Referrer-Policy, and Permissions-Policy.

Check Details:

X-Frame-Options:	Missing
X-Content-Type-Options:	Missing
Referrer-Policy:	Not Set
security.txt:	Not Found (FAIL)

Email Authentication & Transport Security

Layer: Identity and message integrity. Checks included: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DMARC (Domain-based Message Authentication, Reporting & Conformance), MTA-STS (Mail Transfer Agent Strict Transport Security), TLS-RPT (TLS Reporting). Why this matters: Email is a completely separate attack surface from web security. Without proper authentication, attackers can spoof emails from your domain, leading to phishing attacks, reputation damage, and email delivery failures. SPF defines authorized sending servers, DKIM cryptographically signs messages, DMARC provides policy enforcement, MTA-STS enforces secure email transport, and TLS-RPT provides visibility into email transport security issues. Responsibility: Email and messaging administrators configure DNS records for SPF, DKIM, and DMARC, deploy MTA-STS policies, and monitor TLS-RPT reports.

SPF Record

PASSED

What is SPF (Sender Policy Framework)?

SPF is a DNS record that specifies which mail servers are authorized to send email on behalf of your domain.

Why is this important?

SPF prevents email spoofing. Without it, anyone can send emails claiming to be from your domain. The "-all" mechanism is critical - it means "reject all emails from servers not listed", providing strict protection.

What can go wrong?

If SPF is missing or improperly configured: attackers can spoof emails from your domain, leading to phishing attacks, reputation damage, and email delivery failures. Using "~all" or "?all" instead of "-all" provides weak protection.

Technical Details:

SPF records use mechanisms like: "include:" (authorize other domains), "a" (authorize A records), "mx" (authorize MX records), "ip4:" (authorize specific IPs), "-all" (reject all others - STRICT), "~all" (soft fail - WEAK), "?all" (neutral - NO PROTECTION).

Check Details:

SPF Record: v=spf1 include:spf.protection.outlook.com -all

DKIM Record

PASSED

What is DKIM (DomainKeys Identified Mail)?

DKIM cryptographically signs outgoing emails using a private key. The public key is published in DNS, allowing recipients to verify the email's authenticity.

Why is this important?

DKIM proves that emails actually came from your domain and haven't been modified in transit. It works with SPF and DMARC to provide complete email authentication.

What can go wrong?

If DKIM is missing: recipients cannot verify email authenticity, emails may be marked as spam, and you cannot prove emails came from your domain in legal disputes.

Technical Details:

DKIM uses a selector (like "google", "default", "mail") combined with "_domainkey" subdomain. The selector._domainkey.domain.com DNS record contains the public key. We check 250+ common selectors to find DKIM records.

Check Details:

Record 1:
Selector: selector2
Domain: selector2._domainkey.vitasorahealth.com
Record: v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA39u5qkRKigtfmA0o/W5ifHu5uryNYBIg+fx/FW7kws5PtwRp8EXsUp7V+Gz/dAXivc32oJrc4icwnYpUweJyTL97h2ynrPZGeuoaW6I5X3uhTqc14jlOvanz7kLGv9luHGcE+VFm7BYXHUYhsxdesEfqFvGEyVprxhUmgkJg+ltlrg7cgn7naDfOubScKNLDa unTh2XYQBxexA/k0qdudSdxIhYsvwaAOyFwQ25Y1UgihvWLlQtY0KA6fzEJfzjrJGXJDub7qaoxef/m0wSeZyARqFQ6/mqlMq4kaS1XrkPkLpWGryTFxlrMmTWBlN16GCWJozYZpDNFhGQJAxGJGQIDAQAB;

DMARC Record

FAILED

What is DMARC (Domain-based Message Authentication, Reporting & Conformance)?

DMARC tells receiving mail servers what to do with emails that fail SPF or DKIM checks. It also provides reporting on email authentication.

Why is this important?

DMARC is the final layer of email security. It enforces SPF and DKIM policies and provides visibility into email authentication failures. Essential for protecting your business from email-based attacks.

What can go wrong?

If DMARC is missing: you have no control over what happens to spoofed emails, no visibility into authentication failures, and cannot achieve complete email security.

Technical Details:

DMARC policies: "none" (monitor only), "quarantine" (send to spam), "reject" (reject email). Should include "pct=100" (apply to 100% of emails) and "rua=" (reporting email address).

Check Details:

DMARC Record: v=DMARC1; p=none;

MTA-STS

FAILED

What is MTA-STS (Mail Transfer Agent Strict Transport Security)?

MTA-STS enforces secure TLS connections for email transmission, preventing man-in-the-middle attacks on email delivery.

Why is this important?

MTA-STS prevents attackers from intercepting emails in transit by forcing encrypted connections. Critical for protecting business email communications.

What can go wrong?

If MTA-STS is not configured: email transmission can be intercepted, attackers can downgrade to unencrypted connections, and sensitive business communications are at risk.

Technical Details:

MTA-STS requires: 1) _mta-sts.domain.com TXT record with "v=STSv1", 2) Policy file at https://mta-sts.domain.com/.well-known/mta-sts.txt with "mode: enforce", 3) Valid SSL certificate. Mode "enforce" means strict enforcement, "testing" is monitoring only.

Check Details:

Domain Setup:	No
Config Exists:	Yes
Enforced:	No

TLS-RPT

FAILED

What is TLS-RPT (TLS Reporting)?

TLS-RPT provides reports on TLS connection failures for email transmission, helping identify and fix email delivery issues.

Why is this important?

TLS-RPT gives visibility into email delivery problems, helps identify misconfigurations, and ensures email security is working properly.

What can go wrong?

Without TLS-RPT: you have no visibility into email delivery failures, cannot identify security issues, and may not know when email is being intercepted.

Technical Details:

TLS-RPT uses _smtp._tls.domain.com TXT record with "v=TLSRPTv1" and "rua=" email address for reports. Reports are sent in JSON format showing TLS connection failures.

Network & Infrastructure Trust

Layer: Internet routing and reputation. Checks included: RPKI (Resource Public Key Infrastructure) validation for route origin authorization, IP abuse checks against blacklists, domain reputation analysis, PTR record validation. Why this matters: These controls protect against hijacking, spoofing, and reputation-based blocking. RPKI prevents BGP route hijacking by cryptographically validating that IP address blocks are announced by authorized networks. IP abuse checks identify if your IP addresses are on spam or malware blacklists, which can cause email delivery failures and website blocking. Domain reputation affects email deliverability and search engine rankings. Responsibility: ISP and infrastructure providers manage RPKI ROA (Route Origin Authorization) records, IP address allocation, and network routing announcements.

Domain Reputation

PASSED

This check analyzes domain reputation configuration and status for security and compliance purposes.

Check Details:

Status: Pass
Blacklist Detections: 0
Detection Rate: 0%
Risk Score: 0/100

Hosting & Platform Information

Layer: Transparency and context. Information included: Hosting provider identification, web and email IP addresses, MX record configuration, platform detection (WordPress), website scanning results (email addresses found, broken links), IPv6 support. Why this matters: This section provides context for auditors and IT staff but does not represent security controls. Understanding hosting infrastructure helps assess risk exposure, identify shared hosting concerns, and track platform dependencies. WordPress detection helps identify if version monitoring is required. Website scanning identifies potential information disclosure issues. IPv6 support ensures future compatibility and redundancy. Responsibility: IT staff and auditors use this information for risk assessment and compliance documentation.

Hosting Provider

INFORMATIONAL

What is Hosting Provider?

Identifies the Internet Service Provider (ISP) or hosting company that provides the infrastructure where your website and email are hosted.

Why is this important?

Understanding your hosting provider helps assess infrastructure security, identify potential shared hosting risks, and ensure your business website is on reliable infrastructure.

What can go wrong?

If hosting is not properly secured: your website may be on shared infrastructure with compromised sites, provider security issues can affect your domain, and you may face increased security risks.

Technical Details:

Hosting provider is identified through IP geolocation and ASN (Autonomous System Number) lookup. The ASN identifies the organization that owns the IP address range.

Check Details:

Web IP Address: 54.230.79.45
Email MX Record: vitasorahealth-com.mail.protection.outlook.com
Email IP Address: 52.101.194.17

Website Scanning

INFORMATIONAL

What is Website Scanning?

Scans your website for exposed email addresses and broken links that could pose security or compliance risks.

Why is this important?

Exposed email addresses can be harvested by spammers. Broken links indicate poor maintenance and can impact user experience and compliance.

What can go wrong?

Exposed emails lead to spam, broken links damage credibility, and both indicate poor security practices that can impact compliance.

Technical Details:

Email extraction uses regex patterns to find email addresses in HTML. External emails (not from your domain) are flagged. Broken links are detected by checking HTTP status codes (400+).

Check Details:

Emails Found: 0
Broken Links: 0

WordPress Detection

INFORMATIONAL

What is WordPress Detection?

Identifies if WordPress is used and detects the version by analyzing HTML code, meta tags, and file signatures.

Why is this important?

WordPress versions have known vulnerabilities. Outdated versions are frequently exploited. Detection helps identify security risks.

What can go wrong?

If WordPress is outdated: known vulnerabilities can be exploited, websites can be hacked, data can be stolen, and malware can be installed.

Technical Details:

Detection methods: wp-content/wp-includes paths in HTML, generator meta tags, wp-json API endpoints, version numbers in JavaScript/CSS file URLs. Version detection helps identify security vulnerabilities.

Check Details:

WordPress Detected: No
Status: Current version

End of Report

8 of 16 checks failed

Failing even 1 check is a major security concern and should be addressed immediately. Please review the failed checks in this report and take corrective action.

This security and compliance report has been generated by PrismWeb's automated scanning system. For questions about this report or assistance with addressing any issues identified, please contact PrismWeb.

Next Steps:

1. Review all failed and warning checks in this report.
2. Address security issues immediately to protect your domain and business from cyber threats.
3. Contact PrismWeb for professional assistance with domain security, compliance, and managed hosting services.

About PrismWeb

Who We Are

PrismWeb is a B2B managed service provider that helps small businesses secure their domains, meet modern cybersecurity standards, and reduce legal and operational risk. We focus on protecting your business from cyber threats and ensuring your online presence is secure.

What We Do

PrismWeb provides comprehensive security and compliance services for small businesses, including:

- Domain security management and monitoring
- Website creation, migration, or security remediation
- All security requirements: SSL/TLS, DNSSEC, monitoring, logging, testing
- Email security: SPF, DKIM, DMARC, MTA-STS, TLS-RPT
- Infrastructure security on hardware we control
- Backups and disaster recovery
- 24/7 Network Operations Center monitoring and support
- All documentation for compliance and insurance

Why We're Different

- B2B Focus: We specialize in helping small businesses secure their online presence
- Complete Protection: We handle everything from domain security to compliance documentation
- Managed Service Provider: We provide ongoing security monitoring and support
- Cost-Effective: Transparent pricing designed for small business budgets
- Liability Protection: We ensure you have documentation for insurance and legal protection

Pricing

Simple, Transparent Pricing

PrismWeb offers straightforward pricing designed for small businesses. Choose the option that best fits your needs.

PrismWeb Secure Hosting

Monthly	**$49/month**
Annual (save $129)	**$459/year**

Per website

MSP Website Security Management

For sites hosted on non-PrismWeb platforms

Hourly Rate	**$125/hour**
Monthly Average (3 hours)	**$375/month**
Annual Estimate	**~$4,500/year**

What's Included:

Every PrismWeb plan includes comprehensive security and compliance services:

- Domain security management and monitoring
- Website creation, migration, or security remediation
- Secure infrastructure hosting on hardware we control
- Unlimited secure email with SPF, DKIM, DMARC, MTA-STS, TLS-RPT
- Complete security compliance (SSL/TLS, DNSSEC, monitoring, logging, testing)
- 24/7 Network Operations Center monitoring, threat response, and technical support

- All documentation for insurance and compliance

Get Started Today

Contact PrismWeb to discuss your security needs and get a customized quote. We offer flexible payment options and can work with your business to find the best solution.

Contact PrismWeb

Get Protected Today

Ready to secure your business domain and protect your online presence? Contact PrismWeb to get started with your free 30-day trial.

Email

info@PrismWeb.com

Phone

888-777-8984

Address

1639 Medical Center Parkway

Murfreesboro, TN 37129

Sales Hours

Monday - Friday, 9:00 AM - 5:00 PM CST

Support

24/7/365 Network Operations Center

Website

https://PrismWeb.com

Our Commitment

PrismWeb is committed to protecting small businesses from cyber liability. We understand the stakes: data breaches, customer trust, legal liability, and insurance denials. We take this responsibility seriously and are dedicated to ensuring your business achieves and maintains strong security posture.