

SECURITY REPORT



SCAN TARGET

<https://riffarer.com/>

Open ports detected: 0 · Public IP: 172.67.154.129

A risk score of 3/10 (MEDIUM) indicates your business has security issues that need attention. The higher the score, the greater the chance of a breach, ransomware, or data theft.

EXECUTIVE SUMMARY

The security scan of riffarer.com found 39 issues including 2 high-risk and 2 medium-risk findings. The most critical issue is 'Missing SPF Record — Email Spoofing Possible' which requires immediate attention. Full remediation steps are provided for each finding below.

✓ Your server is reachable, which means the web checks and SSL analysis were able to run successfully.

TOP RECOMMENDATIONS

- 1 Missing SPF Record — Email Spoofing Possible: Add an SPF TXT record to your DNS listing every service that actually sends mail for this domain — leaving one out will cause its mail to fail SPF and possibly get rejected.
- 2 Missing DMARC Record — Email Impersonation Risk: Add a DMARC TXT record to your DNS.
- 3 HTTP Not Redirecting to HTTPS: Add a permanent redirect from HTTP to HTTPS.

DETAILED FINDINGS

Missing SPF Record — Email Spoofing Possible

Port DNS · SPF Record

HIGH

WHAT IT IS	No SPF record — there's no DNS-level list of which mail servers are authorized to send using this domain's envelope sender, so any server can pass an SPF check for your domain
BUSINESS RISK	Without SPF, nothing tells receiving mail servers which senders are legitimate for this domain's SMTP envelope, making it easier for forged mail to get through — and easier for your own legitimate mail to be misjudged as spam. Note that SPF on its own, even correctly configured, doesn't stop the visible 'From:' address a recipient sees from being spoofed — that requires DMARC (see below) to enforce alignment between SPF/DKIM and the From header.
REAL-WORLD EXAMPLE	Example: A customer receives an email that looks exactly like it's from the business — same display name, same domain — asking them to 'confirm' a payment or click a link, with nothing in DNS to stop the forgery or warn the recipient.
HOW TO FIX	Add an SPF TXT record to your DNS listing every service that actually sends mail for this domain — leaving one out will cause its mail to fail SPF and possibly get rejected. Log into your domain registrar, go to DNS, add a TXT record for '@' with a value matching your provider: Google Workspace: 'v=spf1 include:_spf.google.com -all' Microsoft 365: 'v=spf1 include:spf.protection.outlook.com -all'. If you use additional senders (helpdesk, marketing platform, invoicing tool, etc.), add each as its own 'include:' entry in the same record — a domain can only have one SPF TXT record, so don't create a second one. Use https://mxtoolbox.com/spf.aspx to verify, then add a DMARC record too so the visible From address is covered as well.
URGENCY	Fix immediately
REFERENCE	CWE-290 — Authentication Bypass by Spoofing The login or identity check can be tricked by faking trusted information, letting an attacker in without real credentials.

Missing DMARC Record — Email Impersonation Risk

Port DNS · DMARC Record

HIGH

WHAT IT IS	No DMARC record — your domain has zero email authentication enforcement, making it trivial to impersonate your business
BUSINESS RISK	This makes it significantly easier for scammers to send convincing fake emails 'from' your business — a common tactic in invoice fraud and phishing — which can directly cost your customers money and damage trust in your brand.
REAL-WORLD EXAMPLE	Example: A scammer sends an invoice-fraud email that appears to come straight from the business's own domain; with no DMARC record in place, nothing tells the recipient's mail provider the message is forged, so it lands in the inbox looking completely legitimate.
HOW TO FIX	Add a DMARC TXT record to your DNS. Go to your domain registrar's DNS settings, add a TXT record for '_dmarc' (not '@') with value: 'v=DMARC1; p=none; rua=mailto:youremail@yourdomain.com' Start at p=none — this only turns on reporting, nothing is blocked yet. Review the aggregate reports for a few weeks to confirm every legitimate mail source for this domain (email provider, helpdesk, marketing tools, etc.) is passing DMARC alignment, then move to p=quarantine, and finally p=reject once you're confident nothing legitimate will be caught. Verify at https://mxtoolbox.com/dmarc.aspx
URGENCY	Fix immediately
REFERENCE	CWE-290 — Authentication Bypass by Spoofing The login or identity check can be tricked by faking trusted information, letting an attacker in without real credentials.

HTTP Not Redirecting to HTTPS

Port HTTP · HTTPS Redirect

MEDIUM

WHAT IT IS	Visiting <code>http://</code> doesn't redirect to <code>https://</code> — some visitors may use an unencrypted connection without knowing
BUSINESS RISK	Anyone who types or clicks an <code>http://</code> link is sending their activity on your site — potentially including form data or passwords — unencrypted, where it can be read by anyone on the same public wifi or compromised network.
REAL-WORLD EXAMPLE	Example: A customer types the domain into their browser without <code>'https://'</code> , lands on the unencrypted version of the site, and submits a form before ever reaching the secure page — sending that data in plain text the whole time.
HOW TO FIX	Add a permanent redirect from HTTP to HTTPS. Nginx: add <code>'return 301 https://\$host\$request_uri;'</code> in your port 80 server block. Apache: add <code>'RewriteRule ^https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]'</code> in your <code>.htaccess</code> . Cloudflare users: go to <code>SSL/TLS > Edge Certificates > enable 'Always Use HTTPS'</code> .
URGENCY	Fix within 1 week
REFERENCE	CWE-319 — Cleartext Transmission of Sensitive Information Sensitive data is sent over the network unencrypted, so anyone monitoring the connection can read it.

DKIM Not Detected Under Common Selectors

Port DNS · DKIM Record

MEDIUM

WHAT IT IS	No DKIM record found under common selector names — this does not confirm DKIM is unconfigured, only that it wasn't found under any of the selector names checked; many providers use a custom or provider-specific selector this check can't guess
BUSINESS RISK	If DKIM genuinely isn't configured, email providers increasingly use it as a trust signal, and its absence can make legitimate emails more likely to be flagged as suspicious or land in spam. But this check only queries a fixed list of common selector names (default, google, mail, etc.) — many providers assign a random or account-specific selector, so this finding should be treated as 'couldn't confirm DKIM,' not 'DKIM is definitely missing.'
REAL-WORLD EXAMPLE	Example: A legitimate invoice email from the business gets flagged as suspicious or dropped into spam by the recipient's mail provider, simply because there's no DKIM signature to prove the message wasn't altered or forged in transit — this only actually happens if DKIM is truly unconfigured, which this check alone can't confirm.
HOW TO FIX	First confirm whether DKIM is actually configured: check your email provider's admin console (Google Workspace: Admin console > Apps > Gmail > Authenticate email; Microsoft 365: Defender > Email authentication > DKIM) for the exact selector name in use, since it's often not one of the common defaults this scan checks. If it turns out DKIM genuinely isn't enabled, turn it on there and add the resulting TXT record to DNS. If you're not sure how to check, share the selector name your provider gives you and this can be verified directly.
URGENCY	Fix within 1 week
REFERENCE	CWE-290 — Authentication Bypass by Spoofing The login or identity check can be tricked by faking trusted information, letting an attacker in without real credentials.

Protected Path — /wp-config.php.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/wp-config.php.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/wp-config.php.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
HOW TO FIX	No action needed if this is intentionally restricted. Confirm the credentials protecting it are strong and not left at a default.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Login/Admin Path Discovered — /dashboard/

Port PATH · Content Discovery

LOW

WHAT IT IS	/dashboard/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry point exists at this path.
BUSINESS RISK	/dashboard/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry point exists at this path.
HOW TO FIX	Confirm this login is protected by a strong password and, ideally, multi-factor authentication. Consider IP-restricting it if it's only used by internal staff.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

Login/Admin Path Discovered — /admin/

Port PATH · Content Discovery

LOW

WHAT IT IS	/admin/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry point exists at this path.
BUSINESS RISK	/admin/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry point exists at this path.
HOW TO FIX	Confirm this login is protected by a strong password and, ideally, multi-factor authentication. Consider IP-restricting it if it's only used by internal staff.
URGENCY	Fix within 1 month
REFERENCE	CWE-284

No Abuse Reports Found for Public IP

Port HTTPS · IP Reputation

INFO

WHAT IT IS	Public IP 172.67.154.129 (hosted by Cloudflare, Inc.) has no abuse reports on AbuseIPDB in the last 90 days.
BUSINESS RISK	A clean IP reputation is a good sign — no other indication needed here.
HOW TO FIX	No action required.
URGENCY	Informational

Hosting Network Identified

Port HTTPS · IP WHOIS /
Network Ownership

INFO

WHAT IT IS	Public IP 172.67.154.129 is registered to Cloudflare, Inc. — network: CLOUDFLARENET — block: 172.64.0.0 – 172.71.255.255.
BUSINESS RISK	This is informational — it tells you (and anyone else who looks it up) which hosting provider or network actually operates this IP. Useful for confirming you're hosted where you expect, or for context if the IP reputation check above flags anything.
HOW TO FIX	No action required — this is identifying information, not a vulnerability.
URGENCY	Informational

Path Discovered — /dev/

Port PATH · Content Discovery

INFO

WHAT IT IS	/dev/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/dev/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /test/

Port PATH · Content Discovery

INFO

WHAT IT IS	/test/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/test/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

robots.txt Present

Port PATH · Content Discovery

INFO

WHAT IT IS /robots.txt is present and was used to seed additional path checks.

BUSINESS RISK /robots.txt is present and was used to seed additional path checks.

HOW TO FIX No action needed — robots.txt is meant to be public.

URGENCY Fix within 1 month

sitemap.xml Present

Port PATH · Content Discovery

INFO

WHAT IT IS /sitemap.xml is present and was used to seed additional path checks.

BUSINESS RISK /sitemap.xml is present and was used to seed additional path checks.

HOW TO FIX No action needed — sitemap.xml is meant to be public.

URGENCY Fix within 1 month

Path Discovered — /admin

Port PATH · Content Discovery

INFO

WHAT IT IS /admin returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.

BUSINESS RISK /admin returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.

HOW TO FIX Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.

URGENCY Fix within 1 month

Path Discovered — /o

Port PATH · Content Discovery

INFO

WHAT IT IS	/o returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/o returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /support

Port PATH · Content Discovery

INFO

WHAT IT IS	/support returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/support returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /inbox

Port PATH · Content Discovery

INFO

WHAT IT IS	/inbox returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/inbox returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /viewer

Port PATH · Content Discovery

INFO

WHAT IT IS	/viewer returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/viewer returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /account

Port PATH · Content Discovery

INFO

WHAT IT IS	/account returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/account returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /adventure

Port PATH · Content Discovery

INFO

WHAT IT IS	/adventure returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/adventure returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /team

Port PATH · Content Discovery

INFO

WHAT IT IS	/team returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/team returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /dashboard

Port PATH · Content Discovery

INFO

WHAT IT IS	/dashboard returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/dashboard returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /operations

Port PATH · Content Discovery

INFO

WHAT IT IS	/operations returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/operations returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /beta-access

Port PATH · Content Discovery

INFO

WHAT IT IS	/beta-access returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/beta-access returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /presentation

Port PATH · Content Discovery

INFO

WHAT IT IS	/presentation returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/presentation returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /settings

Port PATH · Content Discovery

INFO

WHAT IT IS	/settings returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/settings returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /character

Port PATH · Content Discovery

INFO

WHAT IT IS	/character returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/character returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /showcase

Port PATH · Content Discovery

INFO

WHAT IT IS	/showcase returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/showcase returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /signin

Port PATH · Content Discovery

INFO

WHAT IT IS	/signin returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/signin returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /signed-out

Port PATH · Content Discovery

INFO

WHAT IT IS	/signed-out returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/signed-out returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /beta

Port PATH · Content Discovery

INFO

WHAT IT IS	/beta returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/beta returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /setup

Port PATH · Content Discovery

INFO

WHAT IT IS	/setup returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/setup returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /realities

Port PATH · Content Discovery

INFO

WHAT IT IS	/realities returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/realities returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /auth

Port PATH · Content Discovery

INFO

WHAT IT IS	/auth returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/auth returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /test

Port PATH · Content Discovery

INFO

WHAT IT IS	/test returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/test returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /giveaway

Port PATH · Content Discovery

INFO

WHAT IT IS	/giveaway returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/giveaway returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /callback

Port PATH · Content Discovery

INFO

WHAT IT IS	/callback returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/callback returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

Path Discovered — /dev

Port PATH · Content Discovery

INFO

WHAT IT IS	/dev returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/dev returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

WHAT IT IS	/oauth returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
BUSINESS RISK	/oauth returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't one a typical visitor would stumble onto by browsing the site normally, which is why it's worth a quick manual look — but its existence alone isn't a vulnerability.
HOW TO FIX	Open the path yourself and confirm it's meant to be public. If it's leftover debug/test/admin tooling that should have been removed, take it down or restrict it by IP allowlist. If it's intentional, no action needed.
URGENCY	Fix within 1 month

PORT REFERENCE TABLE

PORT	SERVICE	RISK	DESCRIPTION
DNS	SPF Record	HIGH	No SPF record — there's no DNS-level list of which mail servers are authorized to send using this do
DNS	DMARC Record	HIGH	No DMARC record — your domain has zero email authentication enforcement, making it trivial to impers
HTTP	HTTPS Redirect	MEDIUM	Visiting http:// doesn't redirect to https:// — some visitors may use an unencrypted connection with
DNS	DKIM Record	MEDIUM	No DKIM record found under common selector names — this does not confirm DKIM is unconfigured, only
PATH	Content Discovery	LOW	/wp-config.php.bak returned HTTP 403. This confirms the path exists, but access control prevented ac
PATH	Content Discovery	LOW	/dashboard/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry
PATH	Content Discovery	LOW	/admin/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry poi
HTTPS	IP Reputation	INFO	Public IP 172.67.154.129 (hosted by Cloudflare, Inc.) has no abuse reports on AbuseIPDB in the last
HTTPS	IP WHOIS / Network Ownership	INFO	Public IP 172.67.154.129 is registered to Cloudflare, Inc. — network: CLOUDFLARENET — block: 172.64.

PATH	Content Discovery	INFO	/dev/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path is
PATH	Content Discovery	INFO	/test/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path i
PATH	Content Discovery	INFO	/robots.txt is present and was used to seed additional path checks.
PATH	Content Discovery	INFO	/sitemap.xml is present and was used to seed additional path checks.
PATH	Content Discovery	INFO	/admin returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path i
PATH	Content Discovery	INFO	/o returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn't
PATH	Content Discovery	INFO	/support returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	INFO	/inbox returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path i
PATH	Content Discovery	INFO	/viewer returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	INFO	/account returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	INFO	/adventure returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pa
PATH	Content Discovery	INFO	/team returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path is
PATH	Content Discovery	INFO	/dashboard returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pa
PATH	Content Discovery	INFO	/operations returned HTTP 200, a real distinct response rather than the site's soft-404 page. This p
PATH	Content Discovery	INFO	/beta-access returned HTTP 200, a real distinct response rather than the site's soft-404 page. This
PATH	Content Discovery	INFO	/presentation returned HTTP 200, a real distinct response rather than the site's soft-404 page. This
PATH	Content Discovery	INFO	/settings returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pat
PATH	Content Discovery	INFO	/character returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pa

PATH	Content Discovery	INFO	/showcase returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pat
PATH	Content Discovery	INFO	/signin returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	INFO	/signed-out returned HTTP 200, a real distinct response rather than the site's soft-404 page. This p
PATH	Content Discovery	INFO	/beta returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path is
PATH	Content Discovery	INFO	/setup returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path i
PATH	Content Discovery	INFO	/realities returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pa
PATH	Content Discovery	INFO	/auth returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path is
PATH	Content Discovery	INFO	/test returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path is
PATH	Content Discovery	INFO	/giveaway returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pat
PATH	Content Discovery	INFO	/callback returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pat
PATH	Content Discovery	INFO	/dev returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path isn
PATH	Content Discovery	INFO	/oauth returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path i

NEXT STEPS

→ Start with the 2 HIGH risk finding(s) today — these are your most urgent risks. First, address 'Missing SPF Record — Email Spoofing Possible': Add an SPF TXT record to your DNS listing every service that actually sends mail for this domain — leaving one out will cause its mail to fail SPF and possibly get rejected. Then work through the remaining findings in order of severity.

This report is for informational purposes only and represents a point-in-time automated scan. It is not a substitute for a professional penetration test.