

SECURITY REPORT



SCAN TARGET

newgrounds.com

Open ports detected: 0 · Public IP: **15.235.14.84**

A risk score of 4/10 (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 newgrounds.com found 8 issues including 1 high-risk and 5 medium-risk findings. The most critical issue is 'Domain Expiring in 16 Days — Urgent' 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 Domain Expiring in 16 Days — Urgent: Renew the domain now at your registrar — 16 days left.
- 2 Missing HSTS Header: Add the HSTS header to your web server.
- 3 Admin Panel Exposed (Unconfirmed): Restrict access to /admin.

DETAILED FINDINGS

Domain Expiring in 16 Days — Urgent

Port WHOIS · Domain
Registration

HIGH

WHAT IT IS	Domain registration expires in 16 days (registrar: TUCOWS.COM, CO.) — losing it would take down the website and all email
BUSINESS RISK	If this renewal is missed, the website goes offline and every email address on this domain stops working — including invoices, password resets, and customer replies — until it's renewed or, worst case, recovered from whoever registers it after it lapses.
REAL-WORLD EXAMPLE	Example: The card on file for auto-renew has expired without anyone noticing; unless someone renews manually in the next few days, the site and every email address on the domain go dark with no advance warning to customers.
HOW TO FIX	Renew the domain now at your registrar — 16 days left. Turn on auto-renew and confirm the card on file and contact email are current so this never happens silently again.
URGENCY	Fix immediately

Missing HSTS Header

Port HTTPS · HSTS Header

MEDIUM

WHAT IT IS	Missing Strict-Transport-Security (HSTS) — browsers aren't forced to always use HTTPS, leaving visitors open to downgrade attacks
BUSINESS RISK	An attacker on the same network as a visitor (public wifi, a compromised router, etc.) can trick their browser into using the insecure version of your site and intercept what they type — raising the odds of stolen logins or payment details.
REAL-WORLD EXAMPLE	Example: An attacker on a shared network intercepts a visitor's first request (which defaults to HTTP) before the redirect happens, and silently serves them a fake version of the page instead of the real site.
HOW TO FIX	Add the HSTS header to your web server. Nginx: add 'add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;' in your server block. Apache: add 'Header always set Strict-Transport-Security "max-age=31536000"' in your config. Cloudflare: SSL/TLS > Edge Certificates > enable HTTP Strict Transport Security.
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.

Admin Panel Exposed (Unconfirmed)

Port HTTPS · Admin Panel
Exposed

MEDIUM

WHAT IT IS	The path /admin.php returns a restricted-access response (401/403) that is genuinely distinct from how this site handles random nonexistent paths — this confirms *something* is being specially handled at this path, but the response contains no content confirming what it actually is — this exposes administration functionality to anyone on the internet
BUSINESS RISK	Publicly reachable admin panels are a primary target for automated attacks. An attacker who can reach /admin.php can attempt brute-force login, exploit known vulnerabilities in the admin software, or leverage it as a stepping stone to full server compromise — without needing any insider knowledge of the site.
REAL-WORLD EXAMPLE	Example: Automated bots constantly scan the internet for paths like /admin.php. A business that left a default admin URL accessible was compromised when a bot found it, brute-forced a weak password in minutes, and installed backdoor malware — all without any human attacker being involved.
HOW TO FIX	Restrict access to /admin.php by IP allowlist, move it to a non-standard path, or disable it if not needed. Nginx: 'location ^~ /admin.php { allow YOUR_IP; deny all; }'. Also ensure strong, unique credentials are set for any admin accounts, and enable multi-factor authentication where supported.
URGENCY	Fix within 1 week
REFERENCE	CWE-284

ELMAH Error Log Exposed (Unconfirmed)

Port HTTPS · ELMAH Error Log
Exposed

MEDIUM

WHAT IT IS

The path `/elmah.axd` returns a restricted-access response (401/403) that is genuinely distinct from how this site handles random nonexistent paths — this confirms **something** is being specially handled at this path, but the response contains no content confirming what it actually is — this exposes internal server diagnostic information, not a login panel

BUSINESS RISK

This page reveals internal details about the server's configuration, active connections, or recent errors — not something the general public should be able to see, and useful reconnaissance an attacker can use to plan a more targeted attack elsewhere on the site.

REAL-WORLD EXAMPLE

Example: An attacker reviews this page to learn internal server details, request patterns, or recent error messages, then uses that information to plan a more targeted attack elsewhere on the site instead of guessing blind.

HOW TO FIX

Restrict access to `/elmah.axd` by IP allowlist, or disable it entirely if not needed. Nginx: `location ^~ /elmah.axd { allow YOUR_IP; deny all; }`. Apache (`'server-status'/'server-info'`): add `'Require ip YOUR_IP'` inside the relevant `<Location>` block, or remove the module if unused.

URGENCY

Fix within 1 week

REFERENCE

CWE-200 — Exposure of Sensitive Information
The system reveals information to someone who shouldn't have access to it.

DMARC Monitor-Only (p=none) — Not Enforced

Port DNS · DMARC Policy

MEDIUM

WHAT IT IS	DMARC is set to monitor-only (p=none) — phishing emails pretending to be you aren't blocked, just reported
BUSINESS RISK	Phishing emails pretending to be your business can still reach customers' inboxes today — you'll get aggregate reports about it after the fact (if 'rua=' reporting is configured), but nothing actually stops the fraudulent emails from being delivered right now. p=none is a legitimate and recommended first step — it lets you review reports and confirm all your real mail sources pass DMARC alignment (the From-header domain matching either an aligned SPF pass or an aligned DKIM signature) before you start blocking anything — the risk is only in staying at p=none indefinitely instead of using it as a monitoring phase.
REAL-WORLD EXAMPLE	Example: Forged emails impersonating the business keep reaching customers' inboxes; DMARC reports quietly pile up showing exactly that it's happening, but because the policy is monitor-only, nothing actually blocks a single one of them.
HOW TO FIX	Review DMARC aggregate reports (they require 'rua=mailto:...' in the record) for a few weeks to confirm every legitimate mail source for this domain is passing DMARC alignment. Once confirmed, move to 'p=quarantine' (suspicious mail goes to spam) and monitor again before finally moving to 'p=reject' (spoofed mail is rejected outright). Don't jump straight to p=reject — if a legitimate sender was missed, that skips straight to real mail being dropped. Example: 'v=DMARC1; p=quarantine; rua=mailto:dmarc@yourdomain.com'
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.

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.

Missing Permissions-Policy Header

Port HTTPS · Permissions Policy

LOW

WHAT IT IS	Missing Permissions-Policy — browser features like camera, microphone, and location aren't restricted for embedded third-party scripts
BUSINESS RISK	If you ever embed third-party ads, widgets, or analytics scripts, they could request a visitor's camera, microphone, or location without you intending to allow it — an avoidable privacy risk for your customers.
REAL-WORLD EXAMPLE	Example: An embedded ad network's script requests the visitor's location or microphone access through a permission prompt the site owner never intended to allow, simply because nothing in the page's headers restricted it.
HOW TO FIX	Add: 'add_header Permissions-Policy "camera=(), microphone=(), geolocation=()" always;' Adjust based on what your site actually uses. This limits what ad/analytics scripts can access.
URGENCY	Monitor
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

No Abuse Reports Found for Public IP

Port HTTPS · IP Reputation

INFO

WHAT IT IS	Public IP 15.235.14.84 (hosted by OVH Hosting, 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

PORT REFERENCE TABLE

PORT	SERVICE	RISK	DESCRIPTION
WHOIS	Domain Registration	HIGH	Domain registration expires in 16 days (registrar: TUCOWS.COM, CO.) — losing it would take down the
HTTPS	HSTS Header	MEDIUM	Missing Strict-Transport-Security (HSTS) — browsers aren't forced to always use HTTPS, leaving visit
HTTPS	Admin Panel Exposed	MEDIUM	The path /admin.php returns a restricted-access response (401/403) that is genuinely distinct from h

HTTPS	ELMAH Error Log Exposed	MEDIUM	The path /elmah.axd returns a restricted-access response (401/403) that is genuinely distinct from h
DNS	DMARC Policy	MEDIUM	DMARC is set to monitor-only (p=none) — phishing emails pretending to be you aren't blocked, just re
DNS	DKIM Record	MEDIUM	No DKIM record found under common selector names — this does not confirm DKIM is unconfigured, only
HTTPS	Permissions Policy	LOW	Missing Permissions-Policy — browser features like camera, microphone, and location aren't restricte
HTTPS	IP Reputation	INFO	Public IP 15.235.14.84 (hosted by OVH Hosting, Inc.) has no abuse reports on AbuseIPDB in the last 9

NEXT STEPS

→ Start with the 1 HIGH risk finding(s) today — these are your most urgent risks. First, address 'Domain Expiring in 16 Days — Urgent': Renew the domain now at your registrar — 16 days left. 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.