Your Business
August 05, 2026 · 06:17 AM

SECURITY REPORT

5
/10
HIGH

SCAN TARGET

myspace.com

Open ports detected: **0** · Public IP: **34.111.176.156**

A risk score of 5/10 (HIGH) 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 myspace.com found 32 issues including 1 high-risk and 5 medium-risk findings. The most critical issue is 'SSL Certificate Error' 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. SSL Certificate Error: Contact your hosting provider or IT team to inspect and replace the SSL certificate.
2. Weak DKIM Key — 1024-bit RSA (selector: default): Upgrade the DKIM key for selector 'default' to 2048 bits.
3. CSP Missing script-src Restriction: Add a script-src directive listing only the exact domains you actually load scripts from, e.

DETAILED FINDINGS

SSL Certificate Error

Port SSL · SSL Certificate

HIGH

WHAT IT IS	SSL certificate error ([SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get local issuer certificate () — visitors may see browser security warnings
BUSINESS RISK	Unresolved certificate problems quietly erode customer trust and can drive away traffic before you even notice a dip in sales or inquiries.
REAL-WORLD EXAMPLE	Example: Depending on the exact error, visitors may see anything from a vague browser warning to a hard block — either way, an unresolved certificate problem is one of the few security issues a customer can see with their own eyes, and it reads as 'this site isn't safe.'
HOW TO FIX	Contact your hosting provider or IT team to inspect and replace the SSL certificate. Test at https://www.ssllabs.com/ssltest/
URGENCY	**Fix immediately**
REFERENCE	CWE-295 — Improper Certificate Validation The system doesn't properly verify a security certificate, so it could be tricked into trusting an impostor server.

Weak DKIM Key — 1024-bit RSA (selector: default)

Port DNS · DKIM Key Strength

MEDIUM

WHAT IT IS	DKIM key for selector 'default' appears to be approximately 1024 bits — 1024-bit RSA keys are considered weak by modern standards and NIST has deprecated them. A well-resourced attacker could factor this key, breaking your email authentication.
BUSINESS RISK	A forged DKIM signature lets an attacker send phishing or fraud emails that cryptographically appear to come from your domain — bypassing email filters that rely on DKIM as a trust signal, and making impersonation emails indistinguishable from your real ones.
REAL-WORLD EXAMPLE	Example: A security researcher demonstrated in a published study that 512-bit DKIM keys could be factored in under 72 hours using cloud computing resources costing less than $100 — allowing anyone with that capability to forge valid email signatures for the affected domain.
HOW TO FIX	Upgrade the DKIM key for selector 'default' to 2048 bits. Generate a new key through your email provider, update the DNS TXT record to the new public key, and retire the old 1024-bit key.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-326

CSP Missing script-src Restriction

Port HTTPS · Content Security Policy

MEDIUM

WHAT IT IS	CSP is set but has no script-src or default-src directive — script execution isn't restricted at all
BUSINESS RISK	If an attacker compromises any third-party script you load — a classic 'watering hole' tactic, where they hijack a widget or library your site trusts instead of attacking you directly — nothing stops that code from running on every visitor's browser and stealing logins or payment data.
REAL-WORLD EXAMPLE	Example: A third-party widget the site trusts and loads on every page gets compromised by attackers upstream; because nothing restricts which scripts can run, the malicious update executes on every visitor's browser the next time they load the page.
HOW TO FIX	Add a script-src directive listing only the exact domains you actually load scripts from, e.g. "script-src 'self' https://cdn.yourtrustedvendor.com;". Avoid 'unsafe-inline' and wildcards.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

Third-Party Scripts Missing Subresource Integrity (SRI)

Port HTTPS · Third-Party Script Loading

MEDIUM

WHAT IT IS	5 third-party script source(s) loaded without Subresource Integrity (SRI): aim.loc.kr, ajax.googleapis.com, api.fouanalytics.com, cdn.cookielaw.org, x.myspacecdn.com
BUSINESS RISK	If any of these third-party providers is ever compromised — a real, recurring attack pattern called a 'watering hole' or supply-chain attack, where attackers hit a widely-trusted vendor instead of you directly — the malicious code they inject would run on your site with no verification and no warning to you or your visitors.
REAL-WORLD EXAMPLE	Example: A widely-used analytics or widget provider gets compromised (a real, recurring attack pattern), and because the script loads without integrity verification, the malicious version executes on every visitor's browser with no warning to you or them.
HOW TO FIX	Add integrity and crossorigin attributes to each third-party <script> tag, e.g. <script src="..." integrity="sha384-..." crossorigin="anonymous"></script>. Most CDNs (cdnjs, jsdelivr, unpkg) publish the correct hash on their site — copy it directly.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-353 — Missing Support for Integrity Check There's no way to verify that data wasn't altered in transit, so tampering would go unnoticed.

Sensitive Path Publicly Accessible — /server-status

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/server-status returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup/debug/admin-tooling) shouldn't normally be reachable by the public.
BUSINESS RISK	/server-status returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup/debug/admin-tooling) shouldn't normally be reachable by the public.
HOW TO FIX	Remove /server-status from the public web root, or restrict access to it by IP allowlist.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-552 — Files or Directories Accessible to External Parties Files that should be private can be reached by people who shouldn't have access to them.

Sensitive Path Publicly Accessible — /old.old

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/old.old returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup/debug/admin-tooling) shouldn't normally be reachable by the public.
BUSINESS RISK	/old.old returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup/debug/admin-tooling) shouldn't normally be reachable by the public.
HOW TO FIX	Remove /old.old from the public web root, or restrict access to it by IP allowlist.
URGENCY	**Fix within 1 week**
REFERENCE	CWE-552 — Files or Directories Accessible to External Parties Files that should be private can be reached by people who shouldn't have access to them.

Missing MIME Sniffing Protection

Port HTTPS · MIME Sniffing — LOW

WHAT IT IS	Missing X-Content-Type-Options — browsers may guess file types incorrectly, which can enable content injection
BUSINESS RISK	This is a minor gap on its own, but it slightly raises the odds that a malicious file could be misread as something else by a visitor's browser, helping a separate attack succeed.
REAL-WORLD EXAMPLE	Example: A user-uploaded file intended to be harmless (like an image) is reinterpreted by the browser as executable script because the server never told it what the file actually was, letting an unrelated vulnerability turn into a working attack.
HOW TO FIX	Add: 'add_header X-Content-Type-Options "nosniff" always;' (Nginx) or 'Header always set X-Content-Type-Options nosniff' (Apache). This is a one-line fix that takes 2 minutes.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-693 — Protection Mechanism Failure A security safeguard that should be protecting the system is missing, disabled, or not strong enough.

Missing Referrer-Policy Header

Port HTTPS · Referrer Policy — LOW

WHAT IT IS	Missing Referrer-Policy — page URLs (which may include sensitive data) are shared with third-party sites your pages link to
BUSINESS RISK	If any of your page addresses contain sensitive details (like a password-reset token or account ID), that information could leak to outside sites your pages link to — a small but easily avoidable privacy gap.
REAL-WORLD EXAMPLE	Example: A customer clicks an outbound link from a page whose URL happens to include an account ID or a password-reset token, and that full address — token included — is handed to the destination site in the Referer header.
HOW TO FIX	Add: 'add_header Referrer-Policy "strict-origin-when-cross-origin" always;' (Nginx) or 'Header always set Referrer-Policy strict-origin-when-cross-origin' (Apache).
URGENCY	**Fix within 1 month**
REFERENCE	CWE-16 — Configuration The weakness comes from how the software was configured, not from a flaw in its code.

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.

Insecure Cookie Flags (persistent_id)

Port HTTPS · Cookie Security

LOW

WHAT IT IS	Cookie 'persistent_id' is missing the Secure, SameSite flag(s). Observed attributes: domain=.myspace.com, path=/, expires=Tue, 31 Jul 2046 07:04:07 GMT, httpOnly.
BUSINESS RISK	This cookie's name doesn't clearly indicate it holds session or authentication data, so the practical impact depends on what value it actually stores — anywhere from low-stakes (a UI preference) to more sensitive (tracking or personalization data). Missing these flags means whatever the cookie does hold is more exposed than it needs to be to interception or script access.
REAL-WORLD EXAMPLE	Example: whatever value 'persistent_id' holds could be read by an injected script (no HttpOnly) or intercepted on an unencrypted connection (no Secure) — the actual severity depends on how sensitive that value turns out to be.
HOW TO FIX	Add the missing flag(s) when setting this cookie: Secure (only send over HTTPS), HttpOnly (block JavaScript access), SameSite=Lax or Strict (limit cross-site sending). Most frameworks expose this as a one-line config option — e.g. Flask: app.config['SESSION_COOKIE_SECURE']=True, SESSION_COOKIE_HTTPONLY=True, SESSION_COOKIE_SAMESITE='Lax'.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-614, CWE-1275 — Sensitive Cookie in HTTPS Session Without 'Secure' Attribute; Sensitive Cookie with Improper SameSite Attribute The cookie isn't marked Secure, so a browser could send it over an unencrypted connection where it can be intercepted. The cookie's SameSite attribute isn't set to a safe value, making it easier for other sites to trick a visitor's browser into sending it in cross-site requests.

Insecure Cookie Flags (visit_id)

Port HTTPS · Cookie Security

LOW

WHAT IT IS	Cookie 'visit_id' is missing the Secure, SameSite flag(s). Observed attributes: domain=.myspace.com, path=/, expires=Wed, 05 Aug 2026 07:34:07 GMT, httpOnly.
BUSINESS RISK	This cookie's name doesn't clearly indicate it holds session or authentication data, so the practical impact depends on what value it actually stores — anywhere from low-stakes (a UI preference) to more sensitive (tracking or personalization data). Missing these flags means whatever the cookie does hold is more exposed than it needs to be to interception or script access.
REAL-WORLD EXAMPLE	Example: whatever value 'visit_id' holds could be read by an injected script (no HttpOnly) or intercepted on an unencrypted connection (no Secure) — the actual severity depends on how sensitive that value turns out to be.
HOW TO FIX	Add the missing flag(s) when setting this cookie: Secure (only send over HTTPS), HttpOnly (block JavaScript access), SameSite=Lax or Strict (limit cross-site sending). Most frameworks expose this as a one-line config option — e.g. Flask: app.config['SESSION_COOKIE_SECURE']=True, SESSION_COOKIE_HTTPONLY=True, SESSION_COOKIE_SAMESITE='Lax'.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-614, CWE-1275 — Sensitive Cookie in HTTPS Session Without 'Secure' Attribute; Sensitive Cookie with Improper SameSite Attribute The cookie isn't marked Secure, so a browser could send it over an unencrypted connection where it can be intercepted. The cookie's SameSite attribute isn't set to a safe value, making it easier for other sites to trick a visitor's browser into sending it in cross-site requests.

Insecure Cookie Flags (beacons_enabled)

Port HTTPS · Cookie Security

LOW

WHAT IT IS	Cookie 'beacons_enabled' is missing the Secure, HttpOnly, SameSite flag(s). Observed attributes: domain=.myspace.com, path=/, expires=Wed, 05 Aug 2026 07:34:07 GMT.
BUSINESS RISK	This cookie's name doesn't clearly indicate it holds session or authentication data, so the practical impact depends on what value it actually stores — anywhere from low-stakes (a UI preference) to more sensitive (tracking or personalization data). Missing these flags means whatever the cookie does hold is more exposed than it needs to be to interception or script access.
REAL-WORLD EXAMPLE	Example: whatever value 'beacons_enabled' holds could be read by an injected script (no HttpOnly) or intercepted on an unencrypted connection (no Secure) — the actual severity depends on how sensitive that value turns out to be.
HOW TO FIX	Add the missing flag(s) when setting this cookie: Secure (only send over HTTPS), HttpOnly (block JavaScript access), SameSite=Lax or Strict (limit cross-site sending). Most frameworks expose this as a one-line config option — e.g. Flask: app.config['SESSION_COOKIE_SECURE']=True, SESSION_COOKIE_HTTPONLY=True, SESSION_COOKIE_SAMESITE='Lax'.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-614, CWE-1004, CWE-1275 — Sensitive Cookie in HTTPS Session Without 'Secure' Attribute; Sensitive Cookie Without 'HttpOnly' Flag; Sensitive Cookie with Improper SameSite Attribute The cookie isn't marked Secure, so a browser could send it over an unencrypted connection where it can be intercepted. The cookie isn't marked HttpOnly, so a malicious script on the page (such as one injected via XSS) can read and steal it. The cookie's SameSite attribute isn't set to a safe value, making it easier for other sites to trick a visitor's browser into sending it in cross-site requests.

Insecure Cookie Flags (player)

Port HTTPS · Cookie Security — LOW

WHAT IT IS	Cookie 'player' is missing the Secure, HttpOnly, SameSite flag(s). Observed attributes: domain=.myspace.com, path=/, expires=Fri, 04 Sep 2026 07:04:07 GMT.
BUSINESS RISK	This cookie's name doesn't clearly indicate it holds session or authentication data, so the practical impact depends on what value it actually stores — anywhere from low-stakes (a UI preference) to more sensitive (tracking or personalization data). Missing these flags means whatever the cookie does hold is more exposed than it needs to be to interception or script access.
REAL-WORLD EXAMPLE	Example: whatever value 'player' holds could be read by an injected script (no HttpOnly) or intercepted on an unencrypted connection (no Secure) — the actual severity depends on how sensitive that value turns out to be.
HOW TO FIX	Add the missing flag(s) when setting this cookie: Secure (only send over HTTPS), HttpOnly (block JavaScript access), SameSite=Lax or Strict (limit cross-site sending). Most frameworks expose this as a one-line config option — e.g. Flask: app.config['SESSION_COOKIE_SECURE']=True, SESSION_COOKIE_HTTPONLY=True, SESSION_COOKIE_SAMESITE='Lax'.
URGENCY	**Fix within 1 month**
REFERENCE	CWE-614, CWE-1004, CWE-1275 — Sensitive Cookie in HTTPS Session Without 'Secure' Attribute; Sensitive Cookie Without 'HttpOnly' Flag; Sensitive Cookie with Improper SameSite Attribute The cookie isn't marked Secure, so a browser could send it over an unencrypted connection where it can be intercepted. The cookie isn't marked HttpOnly, so a malicious script on the page (such as one injected via XSS) can read and steal it. The cookie's SameSite attribute isn't set to a safe value, making it easier for other sites to trick a visitor's browser into sending it in cross-site requests.

Login/Admin Path Discovered — /login/

Port PATH · Content Discovery — LOW

WHAT IT IS	/login/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry point exists at this path.
BUSINESS RISK	/login/ 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

Hosting Network Identified

Port HTTPS · IP WHOIS / Network Ownership

INFO

WHAT IT IS	Public IP 34.111.176.156 is registered to Google LLC — network: GOOGL-2 — block: 34.64.0.0 – 34.127.255.255.
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 — /config/

Port PATH · Content Discovery

INFO

WHAT IT IS	/config/ 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	/config/ 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 — /backups/

Port PATH · Content Discovery

INFO

WHAT IT IS	/backups/ 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	/backups/ 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 — /backup/

Port PATH · Content Discovery

INFO

WHAT IT IS	/backup/ 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	/backup/ 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 — /debug/

Port PATH · Content Discovery

INFO

WHAT IT IS	/debug/ 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	/debug/ 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 — /api/

Port PATH · Content Discovery

INFO

WHAT IT IS	/api/ 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	/api/ 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 — /staging/

Port PATH · Content Discovery

INFO

WHAT IT IS	/staging/ 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	/staging/ 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 — /old/

Port PATH · Content Discovery

INFO

WHAT IT IS	/old/ 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	/old/ 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

Path Discovered — /hidden/

Port PATH · Content Discovery

INFO

WHAT IT IS	/hidden/ 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	/hidden/ 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 — /tmp/

Port PATH · Content Discovery

INFO

WHAT IT IS	/tmp/ 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	/tmp/ 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 — /secret/

Port PATH · Content Discovery

INFO

WHAT IT IS	/secret/ 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	/secret/ 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 — /private/

Port PATH · Content Discovery

INFO

WHAT IT IS	/private/ 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	/private/ 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 — /actuator

Port PATH · Content Discovery

INFO

WHAT IT IS	/actuator 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	/actuator 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 — /status

Port PATH · Content Discovery

INFO

WHAT IT IS	/status 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	/status 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 — /metrics

Port PATH · Content Discovery — INFO

WHAT IT IS	/metrics 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	/metrics 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

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

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

PORT REFERENCE TABLE

PORT	SERVICE	RISK	DESCRIPTION
SSL	SSL Certificate	HIGH	SSL certificate error ([SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: unable to get loc

DNS	DKIM Key Strength	**MEDIUM**	DKIM key for selector 'default' appears to be approximately 1024 bits — 1024-bit RSA keys are consid
HTTPS	Content Security Policy	**MEDIUM**	CSP is set but has no script-src or default-src directive — script execution isn't restricted at all
HTTPS	Third-Party Script Loading	**MEDIUM**	5 third-party script source(s) loaded without Subresource Integrity (SRI): aim.loc.kr, ajax.googleap
PATH	Content Discovery	**MEDIUM**	/server-status returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (b
PATH	Content Discovery	**MEDIUM**	/old.old returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup/
HTTPS	MIME Sniffing	**LOW**	Missing X-Content-Type-Options — browsers may guess file types incorrectly, which can enable content
HTTPS	Referrer Policy	**LOW**	Missing Referrer-Policy — page URLs (which may include sensitive data) are shared with third-party s
HTTPS	Permissions Policy	**LOW**	Missing Permissions-Policy — browser features like camera, microphone, and location aren't restricte
HTTPS	Cookie Security	**LOW**	Cookie 'persistent_id' is missing the Secure, SameSite flag(s). Observed attributes: domain=.myspace
HTTPS	Cookie Security	**LOW**	Cookie 'visit_id' is missing the Secure, SameSite flag(s). Observed attributes: domain=.myspace.com,
HTTPS	Cookie Security	**LOW**	Cookie 'beacons_enabled' is missing the Secure, HttpOnly, SameSite flag(s). Observed attributes: dom
HTTPS	Cookie Security	**LOW**	Cookie 'player' is missing the Secure, HttpOnly, SameSite flag(s). Observed attributes: domain=.mysp
PATH	Content Discovery	**LOW**	/login/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry poi
HTTPS	IP WHOIS / Network Ownership	**INFO**	Public IP 34.111.176.156 is registered to Google LLC — network: GOOGL-2 — block: 34.64.0.0 – 34.127.
PATH	Content Discovery	**INFO**	/config/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	**INFO**	/backups/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pat
PATH	Content Discovery	**INFO**	/backup/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	**INFO**	/debug/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path

PATH	Content Discovery	**INFO**	/api/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path is
PATH	Content Discovery	**INFO**	/staging/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pat
PATH	Content Discovery	**INFO**	/old/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path is
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**	/hidden/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	**INFO**	/tmp/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path is
PATH	Content Discovery	**INFO**	/secret/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	**INFO**	/private/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pat
PATH	Content Discovery	**INFO**	/actuator returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pat
PATH	Content Discovery	**INFO**	/status returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	**INFO**	/metrics returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	**INFO**	/sitemap.xml is present and was used to seed additional path checks.
PATH	Content Discovery	**INFO**	/robots.txt is present and was used to seed additional path checks.

NEXT STEPS

→ Start with the 1 HIGH risk finding(s) today — these are your most urgent risks. First, address 'SSL Certificate Error': Contact your hosting provider or IT team to inspect and replace the SSL certificate. Then work through the remaining findings in order of severity.