

SECURITY REPORT



SCAN TARGET

https://x.com/home

Open ports detected: 0 · Public IP: **162.159.140.229**

A risk score of 10/10 (CRITICAL) 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 x.com found 104 issues including 1 high-risk and 34 medium-risk findings. The most critical issue is 'Sensitive Path Publicly Accessible — /.aws/credentials' 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 Sensitive Path Publicly Accessible — /.aws/credentials: Remove or block public access to /.
- 2 Environment Secrets Exposed (Unconfirmed): 1.
- 3 Exposed .git Directory (Unconfirmed): Block public access to /.

DETAILED FINDINGS

Sensitive Path Publicly Accessible — /.aws/credentials

Port PATH · Content Discovery

HIGH

WHAT IT IS	/.aws/credentials returned HTTP 200 — a real, distinct response, not the site's soft-404 page. No specific secret pattern was matched in this response, but this path is normally never meant to be public.
BUSINESS RISK	/.aws/credentials returned HTTP 200 — a real, distinct response, not the site's soft-404 page. No specific secret pattern was matched in this response, but this path is normally never meant to be public.
HOW TO FIX	Remove or block public access to /.aws/credentials immediately, and rotate any credentials it may have contained.
URGENCY	Fix immediately
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.

Environment Secrets Exposed (Unconfirmed)

Port HTTPS · Environment
Secrets Exposed

MEDIUM

WHAT IT IS	The path <code>/.env</code> returns a restricted-access response (401/403) that is genuinely distinct from how this site handles random nonexistent paths — this confirms <i>something</i> is being specially handled at this path, but the response contains no content confirming what it actually is — this exposes credentials or sensitive configuration that should never be public
BUSINESS RISK	Exposed credentials in <code>/.env</code> (API keys, database passwords, AWS access keys) give an attacker direct access to your critical systems — databases, cloud infrastructure, third-party APIs, and internal tools. A single exposed credential can lead to total infrastructure compromise.
REAL-WORLD EXAMPLE	Example: An AWS credentials file exposed at <code>/.env</code> contained a key with full EC2/RDS access. An attacker used it to launch crypto miners on the account, incurring \$50k in charges within 72 hours before discovery. The attacker also captured all database dumps and sold them on underground forums.
HOW TO FIX	1. IMMEDIATELY rotate all exposed credentials (API keys, database passwords, SSH keys). Treat them as fully compromised. 2. Block public access to <code>/.env</code> via web server rules (Nginx: <code>location ~ /\.env { deny all; }</code>). 3. Never commit secrets to version control — use <code>.gitignore</code> and environment variable loaders (python-dotenv, Node's dotenv). 4. Use a secrets manager (AWS Secrets Manager, HashiCorp Vault, Doppler) for production credentials.
URGENCY	Fix within 1 week
REFERENCE	CWE-798 — Use of Hard-coded Credentials A username, password, or key is built directly into the code or configuration, where it can be found and reused by an attacker.

Exposed .git Directory (Unconfirmed)

Port HTTPS · Exposed .git
Directory

MEDIUM

WHAT IT IS	The path <code>/.git/HEAD</code> returns a restricted-access response (401/403) that is genuinely distinct from how this site handles random nonexistent paths — this confirms <i>*something*</i> is being specially handled at this path, but the response contains no content confirming what it actually is — this exposes the site's Git repository metadata, not an admin login
BUSINESS RISK	This is not a login page to brute-force — a publicly accessible <code>/.git/HEAD</code> can let an attacker reconstruct this site's Git repository: full source code, configuration files, commit history, internal file paths, and any secrets that were ever committed, even ones later removed from the latest version but never rotated.
REAL-WORLD EXAMPLE	Example: A free, widely available tool rebuilds this site's entire source code and commit history from the exposed <code>.git</code> folder within minutes — sometimes turning up a hardcoded API key or password that was deleted from the current code but never actually rotated.
HOW TO FIX	Block public access to <code>/.git/HEAD</code> entirely — it should never be servable. Nginx: <code>'location ~ /\.git { deny all; }'</code> . Apache: <code>'<DirectoryMatch "\.git"> Require all denied </DirectoryMatch>'</code> . Better yet, don't deploy the <code>.git</code> folder to the live server at all. If any credentials were ever committed to this repo, rotate them — treat them as compromised.
URGENCY	Fix within 1 week
REFERENCE	CWE-527

CSP script-src Too Permissive

Port HTTPS · Content Security
Policy

MEDIUM

WHAT IT IS	CSP <code>script-src</code> allows <code>'unsafe-inline'</code> — an injected or hijacked script can still run freely
BUSINESS RISK	This setting defeats most of the protection CSP is meant to provide. If a third-party script you rely on is ever compromised — the exact mechanism behind most 'watering hole' attacks — it will execute without restriction and with no warning.
REAL-WORLD EXAMPLE	Example: A vendor's analytics or chat-widget script gets compromised at the source; because the policy still allows it (or allows <code>inline/eval</code> scripts generally), the malicious code runs exactly as if it belonged on the site, with no warning to anyone.
HOW TO FIX	Tighten <code>script-src</code> to an explicit allowlist of trusted domains and drop <code>'unsafe-inline'/'unsafe-eval'/wildcards</code> . Move inline scripts to external files or use a nonce/hash. Test changes with https://csp-evaluator.withgoogle.com before deploying.
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	1 third-party script source(s) loaded without Subresource Integrity (SRI): abs.twimg.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.

API Documentation Exposed — /swagger-ui/

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/swagger-ui/ returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, parameters, or authentication schemes that weren't otherwise easy to find. Review its contents manually to judge how sensitive it actually is.
BUSINESS RISK	/swagger-ui/ returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, parameters, or authentication schemes that weren't otherwise easy to find. Review its contents manually to judge how sensitive it actually is.
HOW TO FIX	If this API is internal-only, restrict access to this documentation endpoint. If it's meant to be public, no action needed.
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.

API Documentation Exposed — /openapi.json

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/openapi.json returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, parameters, or authentication schemes that weren't otherwise easy to find. Review its contents manually to judge how sensitive it actually is.
BUSINESS RISK	/openapi.json returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, parameters, or authentication schemes that weren't otherwise easy to find. Review its contents manually to judge how sensitive it actually is.
HOW TO FIX	If this API is internal-only, restrict access to this documentation endpoint. If it's meant to be public, no action needed.
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.

API Documentation Exposed — /swagger.json

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/swagger.json returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, parameters, or authentication schemes that weren't otherwise easy to find. Review its contents manually to judge how sensitive it actually is.
BUSINESS RISK	/swagger.json returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, parameters, or authentication schemes that weren't otherwise easy to find. Review its contents manually to judge how sensitive it actually is.
HOW TO FIX	If this API is internal-only, restrict access to this documentation endpoint. If it's meant to be public, no action needed.
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.

API Documentation Exposed — /graphql

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/graphql returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, parameters, or authentication schemes that weren't otherwise easy to find. Review its contents manually to judge how sensitive it actually is.
BUSINESS RISK	/graphql returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, parameters, or authentication schemes that weren't otherwise easy to find. Review its contents manually to judge how sensitive it actually is.
HOW TO FIX	If this API is internal-only, restrict access to this documentation endpoint. If it's meant to be public, no action needed.
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.

Sensitive Path Publicly Accessible — /info.php

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/info.php 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	/info.php 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 /info.php 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 — /adminer.php

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/adminer.php 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	/adminer.php 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 /adminer.php 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 — /backup.backup

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/backup.backup 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	/backup.backup 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 /backup.backup 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 — /backup.zip

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/backup.zip 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	/backup.zip 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 /backup.zip 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 — /backup.tar.gz

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/backup.tar.gz 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	/backup.tar.gz 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 /backup.tar.gz 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 — /site.tar.gz

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/site.tar.gz 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	/site.tar.gz 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 /site.tar.gz 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 — /site.zip

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/site.zip 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	/site.zip 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 /site.zip 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 — /site.backup

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/site.backup 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	/site.backup 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 /site.backup 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 — /www.backup

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/www.backup 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	/www.backup 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 /www.backup 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 — /www.zip

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/www.zip 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	/www.zip 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 /www.zip 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 — /www.tar.gz

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/www.tar.gz 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	/www.tar.gz 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 /www.tar.gz 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 — /database.tar.gz

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/database.tar.gz 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	/database.tar.gz 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 /database.tar.gz 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 — /database.backup

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/database.backup 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	/database.backup 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 /database.backup 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 — /database.zip

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/database.zip 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	/database.zip 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 /database.zip 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 — /db.zip

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/db.zip 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	/db.zip 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 /db.zip 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 — /db.backup

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/db.backup 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	/db.backup 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 /db.backup 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 — /db.tar.gz

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/db.tar.gz 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	/db.tar.gz 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 /db.tar.gz 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 — /config.backup

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/config.backup 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	/config.backup 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 /config.backup 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 — /config.zip

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/config.zip 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	/config.zip 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 /config.zip 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 — /config.tar.gz

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/config.tar.gz 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	/config.tar.gz 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 /config.tar.gz 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 — /app.zip

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/app.zip 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	/app.zip 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 /app.zip 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 — /app.tar.gz

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/app.tar.gz 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	/app.tar.gz 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 /app.tar.gz 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 — /app.backup

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/app.backup 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	/app.backup 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 /app.backup 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.tar.gz

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/old.tar.gz 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.tar.gz 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.tar.gz 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.backup

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/old.backup 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.backup 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.backup 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.zip

Port PATH · Content Discovery

MEDIUM

WHAT IT IS	/old.zip 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.zip 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.zip 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.

Public IP Flagged for Abuse — 162.159.140.229

Port HTTPS · IP Reputation

LOW

WHAT IT IS	Public IP 162.159.140.229 (hosted by Cloudflare, Inc.) has an abuse confidence score of 0/100 from 6 report(s) in the last 90 days on AbuseIPDB.
BUSINESS RISK	A flagged IP usually means one of two things: this server has already been compromised and is being used to send spam or attack other systems, or this is a shared-hosting IP where a different customer on the same server is doing something malicious — either way, some mail providers and firewalls will treat traffic from this IP with extra suspicion, which can affect email deliverability and how visitors' security software treats your site.
HOW TO FIX	If this is a dedicated server, check for signs of compromise (unexpected processes, outbound traffic, unfamiliar scheduled tasks) and consider a malware scan. If this is shared hosting, contact your hosting provider — ask whether the IP is shared and whether they can move you to a clean one. You can see the specific reports at https://www.abuseipdb.com/check/162.159.140.229 .
URGENCY	Monitor

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 (guest_id_marketing)

Port HTTPS · Cookie Security

LOW

WHAT IT IS	Cookie 'guest_id_marketing' is missing the HttpOnly flag(s). Observed attributes: Max-Age=63072000, Expires=Thu, 14 Sep 2028 05:46:26 GMT, Path=/, Domain=.x.com, Secure, SameSite=None.
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 'guest_id_marketing' 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: <code>app.config['SESSION_COOKIE_SECURE']=True, SESSION_COOKIE_HTTPONLY=True, SESSION_COOKIE_SAMESITE='Lax'.</code>
URGENCY	Fix within 1 month
REFERENCE	CWE-1004 — Sensitive Cookie Without 'HttpOnly' Flag The cookie isn't marked HttpOnly, so a malicious script on the page (such as one injected via XSS) can read and steal it.

Insecure Cookie Flags (guest_id_ads)

Port HTTPS · Cookie Security

LOW

WHAT IT IS	Cookie 'guest_id_ads' is missing the HttpOnly flag(s). Observed attributes: Max-Age=63072000, Expires=Thu, 14 Sep 2028 05:46:26 GMT, Path=/, Domain=.x.com, Secure, SameSite=None.
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 'guest_id_ads' 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: <code>app.config['SESSION_COOKIE_SECURE']=True, SESSION_COOKIE_HTTPONLY=True, SESSION_COOKIE_SAMESITE='Lax'.</code>
URGENCY	Fix within 1 month
REFERENCE	CWE-1004 — Sensitive Cookie Without 'HttpOnly' Flag The cookie isn't marked HttpOnly, so a malicious script on the page (such as one injected via XSS) can read and steal it.

Insecure Cookie Flags (gt)

Port HTTPS · Cookie Security

LOW

WHAT IT IS	Cookie 'gt' is missing the HttpOnly flag(s). Observed attributes: Max-Age=9000, Expires=Tue, 15 Sep 2026 08:16:26 GMT, Path=/, Domain=.x.com, Secure, SameSite=Lax.
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 'gt' 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: <code>app.config['SESSION_COOKIE_SECURE']=True, SESSION_COOKIE_HTTPONLY=True, SESSION_COOKIE_SAMESITE='Lax'.</code>
URGENCY	Fix within 1 month
REFERENCE	CWE-1004 — Sensitive Cookie Without 'HttpOnly' Flag The cookie isn't marked HttpOnly, so a malicious script on the page (such as one injected via XSS) can read and steal it.

Insecure Cookie Flags (personalization_id)

Port HTTPS · Cookie Security

LOW

WHAT IT IS	Cookie 'personalization_id' is missing the HttpOnly flag(s). Observed attributes: Max-Age=63072000, Expires=Thu, 14 Sep 2028 05:46:26 GMT, Path=/, Domain=.x.com, Secure, SameSite=None.
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 'personalization_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: <code>app.config['SESSION_COOKIE_SECURE']=True, SESSION_COOKIE_HTTPONLY=True, SESSION_COOKIE_SAMESITE='Lax'.</code>
URGENCY	Fix within 1 month
REFERENCE	CWE-1004 — Sensitive Cookie Without 'HttpOnly' Flag The cookie isn't marked HttpOnly, so a malicious script on the page (such as one injected via XSS) can read and steal it.

Insecure Cookie Flags (guest_id)

Port HTTPS · Cookie Security

LOW

WHAT IT IS	Cookie 'guest_id' is missing the HttpOnly flag(s). Observed attributes: Max-Age=63072000, Expires=Thu, 14 Sep 2028 05:46:26 GMT, Path=/, Domain=.x.com, Secure, SameSite=None.
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 'guest_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: <code>app.config['SESSION_COOKIE_SECURE']=True, SESSION_COOKIE_HTTPONLY=True, SESSION_COOKIE_SAMESITE='Lax'.</code>
URGENCY	Fix within 1 month
REFERENCE	CWE-1004 — Sensitive Cookie Without 'HttpOnly' Flag The cookie isn't marked HttpOnly, so a malicious script on the page (such as one injected via XSS) can read and steal it.

Insecure Cookie Flags (ct0)

Port HTTPS · Cookie Security

LOW

WHAT IT IS	Cookie 'ct0' is missing the HttpOnly flag(s). Observed attributes: Max-Age=-1789451185, Expires=Thu, 01 Jan 1970 00:00:01 GMT, Path=/, Domain=.x.com, Secure, SameSite=Lax.
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 'ct0' 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: <code>app.config['SESSION_COOKIE_SECURE']=True, SESSION_COOKIE_HTTPONLY=True, SESSION_COOKIE_SAMESITE='Lax'.</code>
URGENCY	Fix within 1 month
REFERENCE	CWE-1004 — Sensitive Cookie Without 'HttpOnly' Flag The cookie isn't marked HttpOnly, so a malicious script on the page (such as one injected via XSS) can read and steal it.

SSH Private Key Exposed (Unconfirmed)

Port HTTPS · SSH Private Key
Exposed

LOW

WHAT IT IS	The path <code>/.id_rsa</code> returns a restricted-access response (401/403) that is genuinely distinct from how this site handles random nonexistent paths — this confirms <i>something</i> is being specially handled at this path, but the response contains no content confirming what it actually is — this exposes credentials or sensitive configuration that should never be public
BUSINESS RISK	Exposed credentials in <code>/.id_rsa</code> (API keys, database passwords, AWS access keys) give an attacker direct access to your critical systems — databases, cloud infrastructure, third-party APIs, and internal tools. A single exposed credential can lead to total infrastructure compromise.
REAL-WORLD EXAMPLE	Example: An AWS credentials file exposed at <code>/.id_rsa</code> contained a key with full EC2/RDS access. An attacker used it to launch crypto miners on the account, incurring \$50k in charges within 72 hours before discovery. The attacker also captured all database dumps and sold them on underground forums.
HOW TO FIX	1. IMMEDIATELY rotate all exposed credentials (API keys, database passwords, SSH keys). Treat them as fully compromised. 2. Block public access to <code>/.id_rsa</code> via web server rules (Nginx: <code>location ~ /\.env { deny all; }</code>). 3. Never commit secrets to version control — use <code>.gitignore</code> and environment variable loaders (python-dotenv, Node's dotenv). 4. Use a secrets manager (AWS Secrets Manager, HashiCorp Vault, Doppler) for production credentials.
URGENCY	Fix within 1 month
REFERENCE	CWE-798 — Use of Hard-coded Credentials A username, password, or key is built directly into the code or configuration, where it can be found and reused by an attacker.

Protected Path — `/.env`

Port PATH · Content Discovery

LOW

WHAT IT IS	<code>/.env</code> returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	<code>/.env</code> 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

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

Protected Path — /.git/HEAD

Port PATH · Content Discovery

LOW

WHAT IT IS	/.git/HEAD returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/.git/HEAD 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

Protected Path — /.git/config

Port PATH · Content Discovery

LOW

WHAT IT IS	/.git/config returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/.git/config 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

Protected Path — /.svn/entries

Port PATH · Content Discovery

LOW

WHAT IT IS	/.svn/entries returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/.svn/entries 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

Protected Path — /.htpasswd

Port PATH · Content Discovery

LOW

WHAT IT IS	/.htpasswd returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/.htpasswd 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

Protected Path — /id_rsa

Port PATH · Content Discovery

LOW

WHAT IT IS	/id_rsa returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/id_rsa 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

Protected Path — /phpinfo.php

Port PATH · Content Discovery

LOW

WHAT IT IS	/phpinfo.php returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/phpinfo.php 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 — /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

Login/Admin Path Discovered — /administrator/

Port PATH · Content Discovery

LOW

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

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

Protected Path — /web.config

Port PATH · Content Discovery

LOW

WHAT IT IS	/web.config returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/web.config 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

Protected Path — /web.config.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/web.config.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/web.config.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 — /wp-admin/

Port PATH · Content Discovery

LOW

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

Protected Path — /.DS_Store

Port PATH · Content Discovery

LOW

WHAT IT IS	/.DS_Store returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/.DS_Store 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

Protected Path — /.idea/workspace.xml

Port PATH · Content Discovery

LOW

WHAT IT IS	/.idea/workspace.xml returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/.idea/workspace.xml 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

Protected Path — /error_log

Port PATH · Content Discovery

LOW

WHAT IT IS	/error_log returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/error_log 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

Protected Path — /backup.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/backup.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/backup.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

Protected Path — /backup.old

Port PATH · Content Discovery

LOW

WHAT IT IS	/backup.old returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/backup.old 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

Protected Path — /site.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/site.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/site.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

Protected Path — /site.old

Port PATH · Content Discovery

LOW

WHAT IT IS	/site.old returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/site.old 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

Protected Path — /www.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/www.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/www.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

Protected Path — /www.old

Port PATH · Content Discovery

LOW

WHAT IT IS	/www.old returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/www.old 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

Protected Path — /database.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/database.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/database.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

Protected Path — /database.old

Port PATH · Content Discovery

LOW

WHAT IT IS	/database.old returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/database.old 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

Protected Path — /db.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/db.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/db.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

Protected Path — /db.old

Port PATH · Content Discovery

LOW

WHAT IT IS	/db.old returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/db.old 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

Protected Path — /config.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/config.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/config.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

Protected Path — /config.old

Port PATH · Content Discovery

LOW

WHAT IT IS	/config.old returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/config.old 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

Protected Path — /app.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/app.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/app.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

Protected Path — /app.old

Port PATH · Content Discovery

LOW

WHAT IT IS	/app.old returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/app.old 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

Protected Path — /old.bak

Port PATH · Content Discovery

LOW

WHAT IT IS	/old.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/old.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

Protected Path — /old.old

Port PATH · Content Discovery

LOW

WHAT IT IS	/old.old returned HTTP 403. This confirms the path exists, but access control prevented access — it was not accessed.
BUSINESS RISK	/old.old 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

Hosting Network Identified

Port HTTPS · IP WHOIS /
Network Ownership

INFO

WHAT IT IS	Public IP 162.159.140.229 is registered to Cloudflare, Inc. — network: CLOUDFLARENET — block: 162.158.0.0 – 162.159.255.255.
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 — /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 — /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 — /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 — /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 — /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 — /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 — /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 — /uploads/

Port PATH · Content Discovery

INFO

WHAT IT IS	/uploads/ 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	/uploads/ 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 — /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 — /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 — /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 — /api/v1/

Port PATH · Content Discovery

INFO

WHAT IT IS	/api/v1/ 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/v1/ 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/v2/

Port PATH · Content Discovery

INFO

WHAT IT IS	/api/v2/ 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/v2/ 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 — /.well-known/security.txt

Port PATH · Content Discovery

INFO

WHAT IT IS	/.well-known/security.txt 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	/.well-known/security.txt 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/health

Port PATH · Content Discovery

INFO

WHAT IT IS	/actuator/health 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/health 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 — /composer.json

Port PATH · Content Discovery

INFO

WHAT IT IS	/composer.json 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	/composer.json 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 — /package.json

Port PATH · Content Discovery

INFO

WHAT IT IS	/package.json 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	/package.json 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 — /.vscode/settings.json

Port PATH · Content Discovery

INFO

WHAT IT IS	/.vscode/settings.json 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	/.vscode/settings.json 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 — /debug.log

Port PATH · Content Discovery

INFO

WHAT IT IS	/debug.log 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.log 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 — /*?lang=en-ss

Port PATH · Content Discovery

INFO

WHAT IT IS	/*?lang=en-ss 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	/*?lang=en-ss 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
PATH	Content Discovery	HIGH	/aws/credentials returned HTTP 200 — a real, distinct response, not the site's soft-404 page. No sp
HTTPS	Environment Secrets Exposed	MEDIUM	The path /.env returns a restricted-access response (401/403) that is genuinely distinct from how th
HTTPS	Exposed .git Directory	MEDIUM	The path /.git/HEAD returns a restricted-access response (401/403) that is genuinely distinct from h

HTTPS	Content Security Policy	MEDIUM	CSP script-src allows 'unsafe-inline' — an injected or hijacked script can still run freely
HTTPS	Third-Party Script Loading	MEDIUM	1 third-party script source(s) loaded without Subresource Integrity (SRI): abs.twimg.com
PATH	Content Discovery	MEDIUM	/swagger-ui/ returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, pa
PATH	Content Discovery	MEDIUM	/openapi.json returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, p
PATH	Content Discovery	MEDIUM	/swagger.json returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, p
PATH	Content Discovery	MEDIUM	/graphql returned HTTP 200. Publicly exposed API documentation can reveal internal endpoints, parame
PATH	Content Discovery	MEDIUM	/info.php returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup
PATH	Content Discovery	MEDIUM	/adminer.php returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (bac
PATH	Content Discovery	MEDIUM	/backup.backup returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (b
PATH	Content Discovery	MEDIUM	/backup.zip returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (back
PATH	Content Discovery	MEDIUM	/backup.tar.gz returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (b
PATH	Content Discovery	MEDIUM	/site.tar.gz returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (bac
PATH	Content Discovery	MEDIUM	/site.zip returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup
PATH	Content Discovery	MEDIUM	/site.backup returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (bac
PATH	Content Discovery	MEDIUM	/www.backup returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (back
PATH	Content Discovery	MEDIUM	/www.zip returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup/
PATH	Content Discovery	MEDIUM	/www.tar.gz returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (back
PATH	Content Discovery	MEDIUM	/database.tar.gz returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path

PATH	Content Discovery	MEDIUM	/database.backup returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path
PATH	Content Discovery	MEDIUM	/database.zip returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (ba
PATH	Content Discovery	MEDIUM	/db.zip returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup/d
PATH	Content Discovery	MEDIUM	/db.backup returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backu
PATH	Content Discovery	MEDIUM	/db.tar.gz returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backu
PATH	Content Discovery	MEDIUM	/config.backup returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (b
PATH	Content Discovery	MEDIUM	/config.zip returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (back
PATH	Content Discovery	MEDIUM	/config.tar.gz returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (b
PATH	Content Discovery	MEDIUM	/app.zip returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup/
PATH	Content Discovery	MEDIUM	/app.tar.gz returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (back
PATH	Content Discovery	MEDIUM	/app.backup returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (back
PATH	Content Discovery	MEDIUM	/old.tar.gz returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (back
PATH	Content Discovery	MEDIUM	/old.backup returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (back
PATH	Content Discovery	MEDIUM	/old.zip returned HTTP 200, a real distinct page rather than a soft-404 — this kind of path (backup/
HTTPS	IP Reputation	LOW	Public IP 162.159.140.229 (hosted by Cloudflare, Inc.) has an abuse confidence score of 0/100 from 6
HTTPS	Permissions Policy	LOW	Missing Permissions-Policy — browser features like camera, microphone, and location aren't restricte
HTTPS	Cookie Security	LOW	Cookie 'guest_id_marketing' is missing the HttpOnly flag(s). Observed attributes: Max-Age=63072000,
HTTPS	Cookie Security	LOW	Cookie 'guest_id_ads' is missing the HttpOnly flag(s). Observed attributes: Max-Age=63072000, Expire

HTTPS	Cookie Security	LOW	Cookie 'gt' is missing the HttpOnly flag(s). Observed attributes: Max-Age=9000, Expires=Tue, 15 Sep
HTTPS	Cookie Security	LOW	Cookie 'personalization_id' is missing the HttpOnly flag(s). Observed attributes: Max-Age=63072000,
HTTPS	Cookie Security	LOW	Cookie 'guest_id' is missing the HttpOnly flag(s). Observed attributes: Max-Age=63072000, Expires=Th
HTTPS	Cookie Security	LOW	Cookie 'ct0' is missing the HttpOnly flag(s). Observed attributes: Max-Age=-1789451185, Expires=Thu,
HTTPS	SSH Private Key Exposed	LOW	The path /.id_rsa returns a restricted-access response (401/403) that is genuinely distinct from how
PATH	Content Discovery	LOW	/.env returned HTTP 403. This confirms the path exists, but access control prevented access — it was
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	/.git/HEAD returned HTTP 403. This confirms the path exists, but access control prevented access — i
PATH	Content Discovery	LOW	/.git/config returned HTTP 403. This confirms the path exists, but access control prevented access —
PATH	Content Discovery	LOW	/.svn/entries returned HTTP 403. This confirms the path exists, but access control prevented access
PATH	Content Discovery	LOW	/.htpasswd returned HTTP 403. This confirms the path exists, but access control prevented access — i
PATH	Content Discovery	LOW	/id_rsa returned HTTP 403. This confirms the path exists, but access control prevented access — it w
PATH	Content Discovery	LOW	/phpinfo.php returned HTTP 403. This confirms the path exists, but access control prevented access —
PATH	Content Discovery	LOW	/admin/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry poi
PATH	Content Discovery	LOW	/administrator/ returned HTTP 200 with no authentication challenge. This confirms a login or admin e
PATH	Content Discovery	LOW	/login/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry poi
PATH	Content Discovery	LOW	/dashboard/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry
PATH	Content Discovery	LOW	/web.config returned HTTP 403. This confirms the path exists, but access control prevented access —

PATH	Content Discovery	LOW	/web.config.bak returned HTTP 403. This confirms the path exists, but access control prevented access
PATH	Content Discovery	LOW	/wp-admin/ returned HTTP 200 with no authentication challenge. This confirms a login or admin entry
PATH	Content Discovery	LOW	/.DS_Store returned HTTP 403. This confirms the path exists, but access control prevented access — i
PATH	Content Discovery	LOW	/.idea/workspace.xml returned HTTP 403. This confirms the path exists, but access control prevented
PATH	Content Discovery	LOW	/error_log returned HTTP 403. This confirms the path exists, but access control prevented access — i
PATH	Content Discovery	LOW	/backup.bak returned HTTP 403. This confirms the path exists, but access control prevented access —
PATH	Content Discovery	LOW	/backup.old returned HTTP 403. This confirms the path exists, but access control prevented access —
PATH	Content Discovery	LOW	/site.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it
PATH	Content Discovery	LOW	/site.old returned HTTP 403. This confirms the path exists, but access control prevented access — it
PATH	Content Discovery	LOW	/www.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it
PATH	Content Discovery	LOW	/www.old returned HTTP 403. This confirms the path exists, but access control prevented access — it
PATH	Content Discovery	LOW	/database.bak returned HTTP 403. This confirms the path exists, but access control prevented access
PATH	Content Discovery	LOW	/database.old returned HTTP 403. This confirms the path exists, but access control prevented access
PATH	Content Discovery	LOW	/db.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it w
PATH	Content Discovery	LOW	/db.old returned HTTP 403. This confirms the path exists, but access control prevented access — it w
PATH	Content Discovery	LOW	/config.bak returned HTTP 403. This confirms the path exists, but access control prevented access —
PATH	Content Discovery	LOW	/config.old returned HTTP 403. This confirms the path exists, but access control prevented access —
PATH	Content Discovery	LOW	/app.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it

PATH	Content Discovery	LOW	/app.old returned HTTP 403. This confirms the path exists, but access control prevented access — it
PATH	Content Discovery	LOW	/old.bak returned HTTP 403. This confirms the path exists, but access control prevented access — it
PATH	Content Discovery	LOW	/old.old returned HTTP 403. This confirms the path exists, but access control prevented access — it
HTTPS	IP WHOIS / Network Ownership	INFO	Public IP 162.159.140.229 is registered to Cloudflare, Inc. — network: CLOUDFLARENET — block: 162.15
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	/backups/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pat
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	/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	/old/ 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	/dev/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path is
PATH	Content Discovery	INFO	/uploads/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pat
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	/tmp/ 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	/secret/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
PATH	Content Discovery	INFO	/api/v1/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path

PATH	Content Discovery	INFO	/api/v2/ returned HTTP 200, a real distinct response rather than the site's soft-404 page. This path
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	/.well-known/security.txt returned HTTP 200, a real distinct response rather than the site's soft-40
PATH	Content Discovery	INFO	/actuator/health returned HTTP 200, a real distinct response rather than the site's soft-404 page. T
PATH	Content Discovery	INFO	/composer.json returned HTTP 200, a real distinct response rather than the site's soft-404 page. Thi
PATH	Content Discovery	INFO	/package.json returned HTTP 200, a real distinct response rather than the site's soft-404 page. This
PATH	Content Discovery	INFO	/.vscode/settings.json returned HTTP 200, a real distinct response rather than the site's soft-404 p
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	/debug.log returned HTTP 200, a real distinct response rather than the site's soft-404 page. This pa
PATH	Content Discovery	INFO	/*?lang=en-ss returned HTTP 200, a real distinct response rather than the site's soft-404 page. This

NEXT STEPS

→ Start with the 1 HIGH risk finding(s) today — these are your most urgent risks. First, address 'Sensitive Path Publicly Accessible — /.aws/credentials': Remove or block public access to /. 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.