



WEBSITE & DATA EXPOSURE ASSESSMENT

Security Exposure Report

Everything connected to your company that the internet can see, and a 90-day plan to close the gaps.

CLIENT

Tallyfield, Inc.

DOMAINS

tallyfield.example ·
tallyfieldpayroll.example

REVIEW WINDOW

October 1-9, 2026

REPORT ID

NYX-SAMPLE-P-001

Confidential — prepared for the named client only. This sample uses a fictional business and the reserved .example domain; all findings are illustrative.

01 — EXECUTIVE SUMMARY

Where Tallyfield stands

Written for the founders and leadership team. Technical details for engineering start in section 05.

OVERALL RISK

CRITICAL

Customer data and a live payment key are reachable today (F-01, F-02). Expected to drop to **Medium** after the first 7 days of the roadmap, and to **Low** after 90 days.

What we looked at. Both brands (tallyfield.example and tallyfieldpayroll.example), 14 subdomains, the web app and public API, public code repositories, search engine results, 240 lookalike domain variations and the email security of both domains. Everything was reviewed from the outside.

What we found. The core product is well built: the app and API use modern TLS, strong headers and current software. The serious problems sit around it, in things the company has forgotten or no longer controls: a storage bucket with customer exports, a payment key in a former contractor's code, a build server open to the internet and old subdomains pointing at services that no longer exist.



What this means for the business

BUSINESS RISK	WHY IT APPLIES HERE	FINDINGS
Customer data breach	Bookkeeping exports for customer businesses can be listed by anyone. A breach like this may trigger notification duties under state law and customer contracts.	F-01
Direct financial loss	A live secret key for the payment provider is public. With it, someone could issue refunds or read payment data.	F-02
Supply chain compromise	The build server that ships code to customers is reachable from the internet and runs a version with a widely exploited vulnerability.	F-03
Phishing of customers	A lookalike domain was registered three weeks ago with email enabled, and the payroll brand has no email protection at all.	F-06, F-07
Brand content takeover	An old docs subdomain can be claimed by a stranger, who could publish anything under the Tallyfield name.	F-04

01 – EXECUTIVE SUMMARY (CONTINUED)

Three patterns behind the findings

Fixing individual findings closes today’s gaps. Addressing these patterns stops new ones from appearing.

14

subdomains found, 3 of them forgotten and exposed

9

outside vendors connected to public assets

240

lookalike domains checked, 3 registered by others

1. Forgotten assets

Development and old documentation hosts, a storage bucket and the build server were set up for a project and never retired. None of them are in the main product, so they missed the security work the product received. **F-01, F-03, F-04, F-05**
2. Secrets outside your control

A former contractor’s public repository and a shared document indexed by search engines contain information that should only exist internally. Once something is public, deleting it at the source is not enough; keys must be replaced. **F-02, F-08**
3. Two brands, one standard

The main brand’s email and web settings are mostly in good shape; the payroll brand, launched later, has none of them. Attackers go for the weaker brand because customers trust both equally. **F-06, F-07, F-12**

Recommended order of work

PHASE	GOAL	FINDINGS
First 7 days	Close every path to customer data, money and the build pipeline; protect the payroll brand from impersonation	F-01 – F-07
Days 8–30	Tighten the API, stop internal information leaks, secure shared accounts	F-08 – F-10, F-12, F-13
Days 31–60	Finish email enforcement and DNS hardening	F-11, F-14, F-15
Days 61–90	Build habits so this does not recur: asset inventory, secret scanning, contractor offboarding	Process

The full 30/60/90-day roadmap with owners is in section 09.

02 — ACTION LIST

What to fix in the next 7 days

One page for the engineering lead. Tick each box when done. Items 1–3 should start today.

- ☐ **Make the export bucket private** CRITICAL
Block public access on the storage bucket, then review its access logs for the last 90 days. **F-01**
- ☐ **Replace the leaked payment key** CRITICAL
Roll the live secret key in the payment provider's dashboard, update the app, and review recent refunds and API activity. **F-02**
- ☐ **Take the build server off the internet** CRITICAL
Restrict ci. to VPN or office addresses and update Jenkins to the current LTS release. **F-03**
- ☐ **Delete the dangling docs record** HIGH
Remove the old-docs CNAME record from DNS. **F-04**
- ☐ **Put the development app behind a login** HIGH
Require SSO or VPN for dev-app. and confirm it holds no copy of customer data. **F-05**
- ☐ **Report the lookalike domain** HIGH
Send an abuse report to the registrar and warn customer support about emails from tallyfie1d.example. **F-06**
- ☐ **Protect the payroll brand's email** HIGH
Publish SPF and a DMARC record for tallyfieldpayroll.example. **F-07**
- ☐ **Confirm the payroll domain will renew** CHECK
It expires on December 2, 2026. Check auto-renew and the card on file at the registrar. **Section 07**

02 — ACTION LIST (CONTINUED)

All findings at a glance

Fifteen findings, sorted by severity. Section 09 turns them into a 30/60/90-day plan.

ID	FINDING	SEVERITY	WHERE IT'S FIXED
F-01	Storage bucket lists customer data exports publicly	CRITICAL	Cloud console (S3)
F-02	Live payment API key in a public code repository	CRITICAL	Payment dashboard + app config
F-03	Build server reachable from the internet, outdated version	CRITICAL	Firewall + Jenkins
F-04	Old docs subdomain can be taken over	HIGH	DNS settings
F-05	Development app publicly reachable	HIGH	Hosting / access policy
F-06	Lookalike domain registered with email enabled	HIGH	Registrar abuse report
F-07	Payroll brand has no SPF or DMARC	HIGH	DNS settings
F-08	Internal onboarding document indexed by search engines	MEDIUM	Google Drive sharing
F-09	API accepts requests from any website with credentials	MEDIUM	API code (CORS)
F-10	GraphQL schema open to anyone on production	MEDIUM	API configuration
F-11	Full source code readable through source maps	MEDIUM	Build configuration
F-12	Main domain DMARC applies to only 25% of mail	MEDIUM	DNS settings
F-13	Checkout email in 2 breaches, one with passwords	MEDIUM	Your own accounts
F-14	No CAA records limiting who can issue certificates	LOW	DNS settings
F-15	Marketing site missing two security headers	LOW	CDN / site settings

03 — SCOPE AND METHOD

What we checked, and how

An external, non-intrusive assessment of everything connected to the company's domains that is visible from the internet.

ITEM	DETAILS
Client	Tallyfield, Inc. (fictional), Dallas, Texas — bookkeeping software for small businesses
Domains in scope	tallyfield.example, tallyfieldpayroll.example and all their subdomains
Applications	Marketing sites, app. (web app, login page only) and api. (public behavior only, no account)
Third-party services	Help desk, status page, payment provider and email: configuration visible from outside only
Checkout email	ops@tallyfield.example (breach lookup only)
Review window	October 1–9, 2026
Report ID	NYX-SAMPLE-P-001

What we did

- Everything in the External Website Security Review, for both brands
- Found subdomains through certificate logs, DNS and search engines, and checked each for exposure and takeover risk
- Searched public code repositories and paste sites for the company's domains, keys and internal hostnames
- Searched engines for indexed internal pages and publicly shared documents
- Checked 240 lookalike domain variations for registration, websites and email
- Reviewed DNS, email and certificate settings for both domains

What we did not do

- No login attempts, no account creation and no password guessing
- No use of any key, token or credential we found
- No downloading or opening of customer files
- No exploitation of any vulnerability, including the build server
- No testing of vendor platforms beyond their public settings
- No load testing and no social engineering of staff

How we rate severity

SEVERITY	MEANING	SUGGESTED TIMING
CRITICAL	Directly exposes sensitive data, money or systems, or is known to be exploited in the wild.	Same day
HIGH	A realistic path to compromise or fraud that needs little skill to use.	Within 7 days
MEDIUM	Weakens defenses or makes other attacks easier.	Within 30–60 days
LOW	Good-practice improvements that reduce what attackers can learn.	Within 90 days

03 — SCOPE AND METHOD (CONTINUED)

Terms used in this report

For readers outside engineering.

Subdomain	An address under your main domain, such as <code>app.tallyfield.example</code> . Each one is a separate door into the company.
Subdomain takeover	When a subdomain still points to an outside service you no longer use, someone else can sign up for that service and control what the subdomain shows.
Storage bucket	A folder in cloud storage (here Amazon S3). It can be private or open to the world.
API key / secret key	A password that lets software act on your behalf, for example to issue refunds through your payment provider.
Build server (CI)	The system that turns your code into the product customers use. Whoever controls it controls what customers receive.
Development app	A version of the product used by engineers for testing, usually with weaker protections.
Lookalike domain	A domain that is easy to mistake for yours, like <code>tallyfie1d</code> with the number 1 instead of the letter l.
CORS	A setting that tells browsers which other websites may read data from your API.
GraphQL schema	The full list of data and actions an API offers, like a map of the API.
Source maps	Files that turn the compressed code browsers download back into the original, readable source code.
SPF, DKIM, DMARC	Three DNS records that together stop strangers from sending email in your name.
CAA record	A DNS record that lists which companies may issue HTTPS certificates for your domain.
Certificate logs	Public records of every HTTPS certificate issued. They reveal subdomains a company may have forgotten.

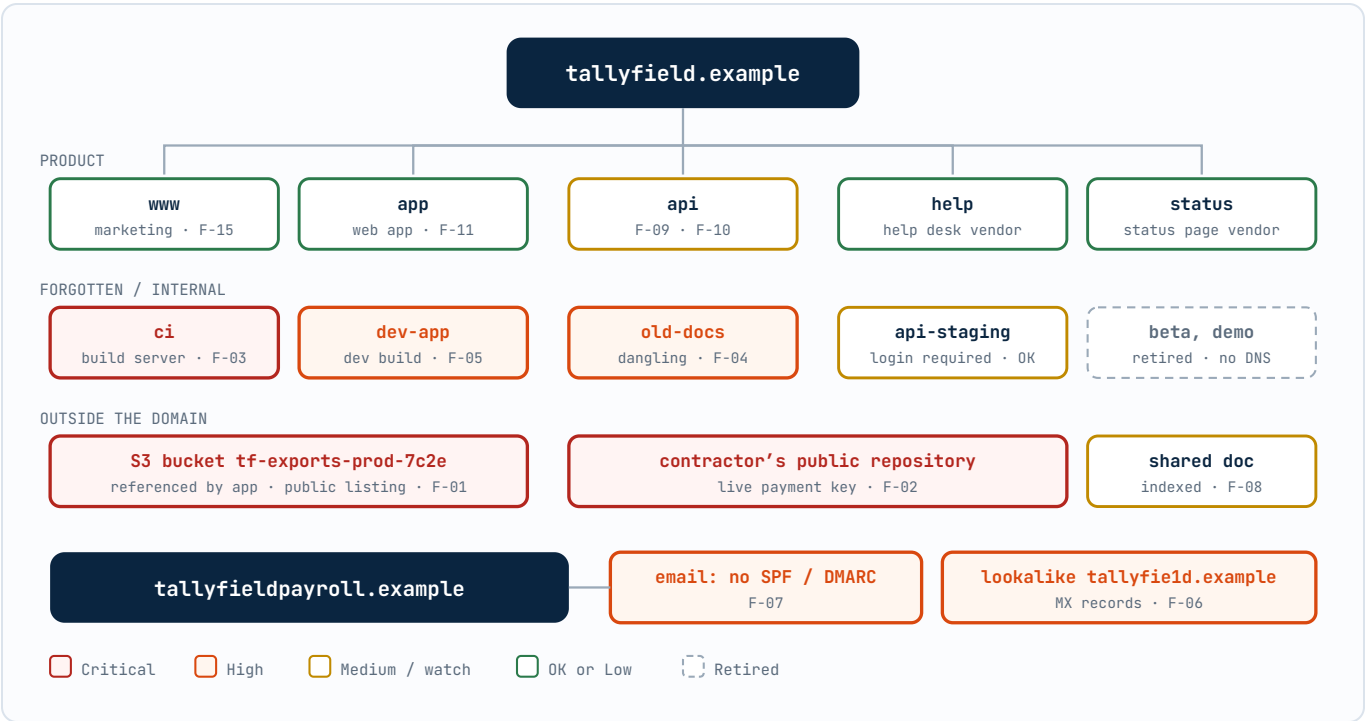
Sources and tools

AREA	SOURCES USED
Subdomain discovery	Certificate transparency logs (crt.sh), public DNS, search engine results, web archive snapshots
Code and leak search	Public code repositories, public gists and paste sites, search engine operators
Lookalike domains	Typo, character-swap, homoglyph and TLD variations, checked against DNS, WHOIS and mail records
Breach lookup	Have I Been Pwned
Web and TLS checks	Standard open-source scanners, verified manually in a browser

04 – ATTACK SURFACE

Subdomain exposure map

Every address we found under both domains, colored by what we found there.



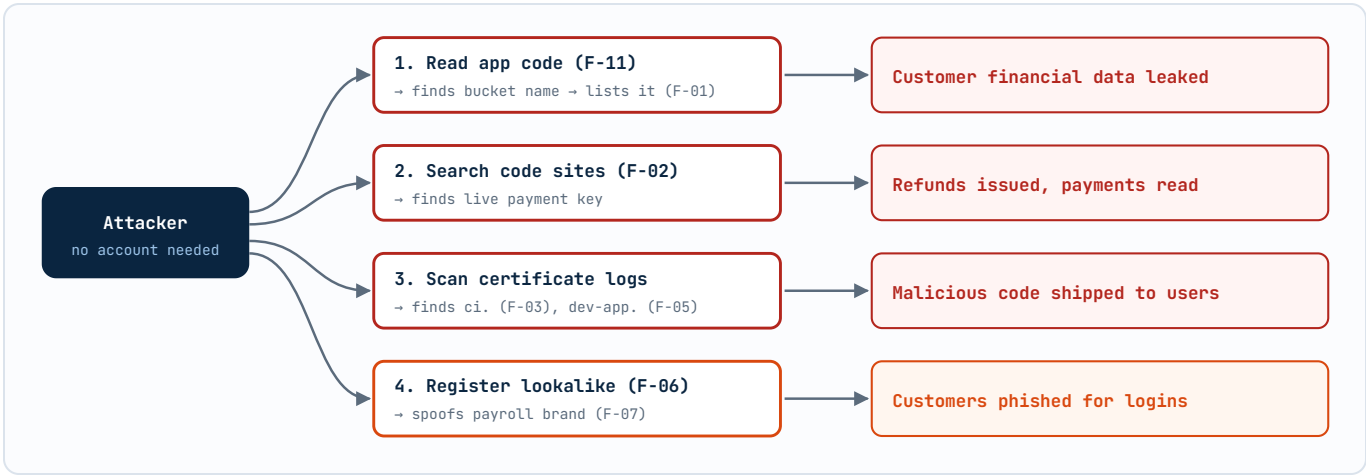
All subdomains found

ADDRESS	WHAT IT IS	FOUND VIA	STATUS
www, apex	Marketing site (hosted website builder)	DNS	OK (F-15)
app.	Customer web app	DNS	F-11
api.	Public REST and GraphQL API	DNS, app code	F-09, F-10
help.	Help desk (vendor)	DNS	OK
status.	Status page (vendor)	DNS	OK
ci.	Jenkins build server	Certificate logs	F-03
dev-app.	Development build of the app	Certificate logs	F-05
old-docs.	CNAME to a deleted docs hosting project	Web archive	F-04
api-staging.	Staging API, requires login	App code	OK
mail., autodiscover.	Email (Google Workspace)	DNS	OK
beta., demo.	Appear in 2024 certificate logs, no DNS today	Certificate logs	Retired
payroll brand www	WordPress marketing site	DNS	F-07

04 – ATTACK SURFACE (CONTINUED)

How an attacker would approach Tallyfield

The most likely attack paths, combining several findings. Each one is closed by fixing the findings listed.



Why these paths matter

None of the four paths requires breaking into the main product. Each starts with information that is already public and needs only basic tools. Automated services continuously scan certificate logs, code repositories and newly registered domains, so the realistic question is not whether these exposures will be found, but when.

Third-party services connected to public assets

VENDOR ROLE	WHERE IT APPEARS	NOTE
Website builder	www (main brand)	Limited header control (F-15)
Help desk	help.	HTTPS, SSO for agents
Status page	status.	OK
Payment provider	app., checkout	Key leaked (F-02)
Cloud storage (Amazon S3)	Referenced in app code	Public bucket (F-01)
Error monitoring	app., dev-app.	Public DSN, expected and low risk
Product analytics	app.	Masks form inputs: OK
Email (Google Workspace)	MX for both domains	Payroll brand unprotected (F-07)
Docs hosting (former)	old-docs.	Project deleted (F-04)

05 — TECHNICAL FINDINGS

Detailed findings

Each finding explains what we saw, why it matters, and what engineering should do. Critical and High findings come first.

F-01 Storage bucket lists customer data exports publicly

CRITICAL

Asset: **S3 bucket tf-exports-prod-7c2e** Category: **Data exposure**

WHAT WE SAW

The web app's code contains the name of a storage bucket used for "Export to CSV". Requesting the bucket address without any credentials returns a full list of its files.

```
app.tallyfield.example/static/js/main.4f1a.js → "exportBucket":"tf-exports-prod-7c2e"
GET https://tf-exports-prod-7c2e.s3.amazonaws.com/ → 200 OK <ListBucketResult>
  exports/2026/09/[customer-id]/general-ledger_2026-Q3.csv
  exports/2026/09/[customer-id]/payroll-summary_2026-09.csv
  ... (about 18,400 objects; newest from October 8, 2026)
# listing only — no file was downloaded
```

WHY IT MATTERS

File names show these are complete ledgers and payroll summaries of customer businesses. Anyone with the bucket name, which is in code every visitor downloads, can list and very likely download them. This is the most serious finding in the report.

HOW TO FIX

- Turn on "Block all public access" for the bucket and at the account level in the AWS console today.
- Serve exports through short-lived pre-signed URLs created by the API after the user is authenticated.
- Review S3 server access logs or CloudTrail data events for the past 90 days for list and download requests from unknown sources, and involve legal counsel on notification duties.

F-02 Live payment API key in a public code repository

CRITICAL

Location: **public repository of a former contractor** Category: **Leaked secrets**

WHAT WE SAW

A public repository named `tallyfield-invoice-sync`, owned by a personal account, contains a configuration file with a live secret key for the payment provider. It was committed in June 2025 and is still present in the repository history.

```
github.com/[redacted]/tallyfield-invoice-sync · config/settings.py · commit 3e9a1c2 (2025-06-17)
PAYMENT_SECRET_KEY = "sk_live_51N...[redacted by Nyorsoft]"
WEBHOOK_URL = "https://api.tallyfield.example/hooks/payments"
```

WHY IT MATTERS

A live secret key gives full access to the payment account: issuing refunds, reading customer payment details and changing settings. Bots scan public repositories for keys like this within minutes of publication. We did not use or test the key.

HOW TO FIX

- Roll (replace) the secret key in the payment provider's dashboard today and deploy the new key. Deleting the repository alone does not help, because copies may exist.
- Review the payment account's API logs and refunds since June 2025.

- Ask the repository owner to delete it, and use restricted keys with only the permissions each integration needs.

F-03 Build server reachable from the internet, outdated version

CRITICAL

Host: **ci.tallyfield.example** Category: **Exposed infrastructure**

WHAT WE SAW

```
GET https://ci.tallyfield.example/login → 200 OK "Sign in to Jenkins"
X-Jenkins: 2.387.1
```

Jenkins 2.387.1 is an LTS release from March 2023. Versions up to 2.426.2 LTS are affected by CVE-2024-23897, which lets an unauthenticated attacker read parts of files on the server (whole files in some configurations) and which has been widely exploited.

WHY IT MATTERS

The build server holds deployment credentials and produces the code customers run. If an attacker reads its files or takes it over, they can steal secrets or insert malicious code into the product.

HOW TO FIX

- Restrict access to VPN or office IP addresses at the firewall or load balancer today.
- Upgrade Jenkins and all plugins to the current LTS release.
- Because the server was exposed while vulnerable, rotate the credentials stored in Jenkins (cloud, registry, deployment keys).

We identified the version from the response header only. We did not test whether the vulnerability can be exploited on this server.

F-04 Old docs subdomain can be taken over

HIGH

Host: **old-docs.tallyfield.example** Category: **Subdomain takeover**

WHAT WE SAW

```
old-docs.tallyfield.example CNAME tallyfield-docs.pagehost.example
GET https://old-docs.tallyfield.example/ → 404 "There isn't a site here. Claim this name in your dashboard."
```

WHY IT MATTERS

The DNS record still points to a documentation hosting project that was deleted. On this kind of service, anyone can create a new project with the same name and publish content on `old-docs.tallyfield.example`: a fake login page, malware or false statements in the company's name.

HOW TO FIX

- Delete the CNAME record today.
- Add a step to vendor offboarding: remove DNS records before cancelling the service.

We did not claim the name. The vendor's message confirms it is available.

F-05 Development app publicly reachable

HIGH

Host: **dev-app.tallyfield.example** Category: **Forgotten assets**

WHAT WE SAW

```
GET https://dev-app.tallyfield.example/ → 200 OK <title>Tallyfield (DEV)</title>
window.__CONFIG__ = {"env":"development","apiBase":"https://api-staging.tallyfield.example","debug":true, ...}
```

A development build of the app is open to the internet with debug mode on. It shows the normal login page and a developer toolbar.

WHY IT MATTERS

Development environments often have test accounts with simple passwords, relaxed checks and copies of real data. They are usually updated less often than production. Search engines and attackers find them through certificate logs, as we did.

HOW TO FIX

- Put dev-app behind company SSO or VPN.
- Confirm the staging database contains no real customer data. If it does, replace it with generated test data.

F-06 Lookalike domain registered with email enabled

HIGH

Domain: **tallyfie1d.example** (number 1 instead of letter l) Category: **Brand impersonation**

WHAT WE SAW

```
WHOIS  created 2026-09-20 · registrant privacy service
MX     tallyfie1d.example → mail server configured
A      no website
```

WHY IT MATTERS

A domain registered three weeks ago, set up to send and receive email but with no website, is a typical sign of a phishing campaign in preparation. In emails, tallyfie1d is very hard to tell apart from tallyfield. Likely targets are customers (fake invoices or login pages) and staff (fake payment requests).

HOW TO FIX

- Report the domain to the registrar's abuse contact as likely phishing preparation.
- Warn customer support and finance, and add the domain to the email blocklist in Google Workspace.
- Consider registering the remaining high-risk variations listed in section 06.

F-07 Payroll brand has no SPF or DMARC

HIGH

Domain: **tallyfieldpayroll.example** Category: **Email security**

WHAT WE SAW

tallyfieldpayroll.example	TXT	(no SPF record)
_dmarc.tallyfieldpayroll.example	TXT	(no record)
google._domainkey	TXT	(no DKIM key)
MX		Google Workspace

WHY IT MATTERS

Nothing stops anyone from sending email as payroll@tallyfieldpayroll.example. Payroll emails are a favorite phishing theme because recipients expect them to ask for bank details.

HOW TO FIX

tallyfieldpayroll.example	TXT	"v=spf1 include:_spf.google.com ~all"
_dmarc	TXT	"v=DMARC1; p=quarantine; rua=mailto:dmarc@tallyfield.example"

- Turn on DKIM signing in Google Workspace for this domain and publish the key.
- The DMARC record above sends reports to the main domain. Authorize that by adding a record on the main domain: `tallyfieldpayroll.example._report._dmarc.tallyfield.example` TXT `"v=DMARC1"`.

F-08 Internal onboarding document indexed by search engines

MEDIUM

Location: **Google Docs**, shared "anyone with the link" Category: **Information leak**

WHAT WE SAW

```
search: site:docs.google.com "tallyfield.example" "staging"
→ "Engineering onboarding – Tallyfield" docs.google.com/document/d/[redacted]
```

The document lists internal tools, the names of the build and staging hosts, and the team's on-call process. It contains no passwords.

WHY IT MATTERS

It gives an attacker a ready-made map of internal systems and the names of people to target with phishing.

HOW TO FIX

- Change sharing to "Restricted" (company only), and in the Google Workspace admin console limit link sharing outside the organization.
- Request removal of the cached result through Google's "Remove outdated content" tool.

F-09 API accepts requests from any website with credentials

MEDIUM

Host: **api.tallyfield.example** Category: **API configuration**

WHAT WE SAW

```
GET /v2/me Origin: https://unrelated-site.example
→ 401 Unauthorized
Access-Control-Allow-Origin: https://unrelated-site.example
Access-Control-Allow-Credentials: true
```

The API copies whatever website is asking into its CORS answer and allows credentials.

WHY IT MATTERS

If the API accepts session cookies, any website a logged-in customer visits could read that customer's data from the API in the background. We could not confirm without an account whether the API uses cookies or tokens. If it uses cookies, treat this as High.

HOW TO FIX

- Replace the reflected origin with a fixed allow-list: `https://app.tallyfield.example` and any other first-party front ends.

F-10 GraphQL schema open to anyone on production

MEDIUM

Location: **api.tallyfield.example/graphql** Category: **API configuration**

```
POST /graphql {"query":"{ __schema { types { name } } }"} → 200 OK (312 types, no login)
... "AdminImpersonateUserInput", "InternalBillingOverride", "FeatureFlagMutation" ...
```

The full API schema, including internal and admin operations, is available without logging in. It does not by itself give access, but it shows an attacker exactly which operations to target.

HOW TO FIX

- Disable introspection in production, and confirm that admin operations check permissions on the server for every request.

F-11 Full source code readable through source maps

MEDIUM

Host: **app.tallyfield.example** Category: **Information leak**

```
GET /static/js/main.4f1a.js.map → 200 OK (14.2 MB, 1,206 original source files)
```

Anyone can rebuild the app's original front-end source code, including comments and internal names. This is how the bucket name in F-01 is easiest to find.

HOW TO FIX

- Stop publishing .map files in production builds, or upload them only to the error monitoring service.

F-12 Main domain DMARC applies to only 25% of mail

MEDIUM

Domain: **tallyfield.example** Category: **Email security**

```
_dmarc.tallyfield.example TXT "v=DMARC1; p=quarantine; pct=25; rua=mailto:dmarc@tallyfield.example"
```

The policy is correct, but pct=25 means only one in four spoofed messages is quarantined. The rest are delivered normally. If your DMARC reports show that all legitimate senders pass, the rollout can be completed.

HOW TO FIX

- Remove pct=25, then after two weeks change to p=reject.

F-13 Checkout email in 2 breaches, one with passwords

MEDIUM

Address: **ops@tallyfield.example** Source: **Have I Been Pwned**

BREACH (ILLUSTRATIVE)	YEAR	DATA EXPOSED
Developer forum	2020	Email addresses, usernames, hashed passwords
SaaS marketing tool	2023	Email addresses, company names

This shared operations mailbox is likely tied to admin accounts at several vendors. If the forum password was reused anywhere, those accounts are at risk.

HOW TO FIX

- Change any reused passwords, move shared vendor logins to a password manager, and require two-step verification on this mailbox.

Breach data provided by Have I Been Pwned (haveibeenpwned.com). Breach names in this sample are illustrative.

F-14 No CAA records limiting who can issue certificates

LOW

Domains: **both** Category: **DNS hardening**

Without CAA records, any public certificate authority may issue certificates for the domains. A CAA record limits this to the providers you actually use.

```
tallyfield.example  CAA  0 issue "letsencrypt.org"
tallyfield.example  CAA  0 issue "amazon.com"
```

F-15 Marketing site missing two security headers

LOW

Host: **www.tallyfield.example** Category: **Browser protections**

The marketing site sends HSTS and X-Content-Type-Options but no Content-Security-Policy or Permissions-Policy. The website builder limits custom headers; the CDN in front of it can add them. Risk is low because the site has no logins or forms that handle sensitive data.

06 – BRAND AND LEAK MONITORING

Lookalike domains and public leak search

Results of the searches outside your own infrastructure.

Lookalike domains

We generated 240 variations of both brand names (typos, swapped and missing letters, look-alike characters and other domain endings) and checked each one. Three are registered by someone other than Tallyfield.

DOMAIN	REGISTERED	EMAIL	WEBSITE	ASSESSMENT
tallyfie1d.example	2026-09-20	Yes	None	Phishing risk (F-06)
tallyfield-app.example	2024-02-11	No	"For sale"	Watch, consider buying
tallyfeildpayroll.example	2025-11-03	No	Parked ads	Watch
tallyfeild.example	2023-05-30	No	Redirects to you	Appears to be yours

Unregistered high-risk variations worth registering defensively: tallyfie1d.example, tally-field.example, tallyfielddpayrol.example.

Code repositories, paste sites and search engines

SEARCH	RESULT	OUTCOME
Code repositories for both domains and internal hostnames	1 repository with a live key, 3 forks of an old open-source SDK (no secrets)	F-02
Code repositories for key patterns tied to your webhooks	Same repository as above	F-02
Public paste sites	No results	Clear
Indexed documents (docs.google.com, file types pdf, xlsx, docx)	1 internal onboarding document, 2 public marketing PDFs	F-08
Indexed internal pages (dev, staging, admin paths)	dev-app . login page indexed	F-05
Web archive snapshots of both domains	Revealed old-docs .; no archived pages with sensitive data	F-04

07 — DOMAIN AND EMAIL SECURITY

Both domains side by side

Domain-level settings that protect against spoofing, hijacking and certificate misuse.

CONTROL	TALLYFIELD.EXAMPLE	TALLYFIELDPAYROLL.EXAMPLE
SPF	Present, ~all	Missing (F-07)
DKIM	2048-bit key	Missing (F-07)
DMARC	quarantine, pct=25 (F-12)	Missing (F-07)
MTA-STS (encrypted mail delivery)	Not set	Not set
TLS-RPT (delivery problem reports)	Not set	Not set
DNSSEC	Enabled	Not enabled
CAA records	None (F-14)	None (F-14)
Registrar transfer lock	On	On
Domain expiry	March 2028	December 2, 2026
DNS provider	Managed DNS with CDN	Registrar default DNS

Observations

Payroll domain expires in under two months

Registration data shows tallyfieldpayroll.example expires on December 2, 2026. We cannot see from the outside whether auto-renew is on. If it lapses, someone else can register it and receive email sent to the payroll brand. Confirm auto-renew and the payment card on file at the registrar this week.

Two brands, two standards

The main domain uses a managed DNS provider with DNSSEC; the payroll domain still sits on the registrar's default DNS. Moving it to the same provider makes it easier to keep both domains on one standard.

Mail transport encryption

MTA-STS and TLS-RPT make sure email sent to your domains is encrypted in transit and tell you when it is not. They are not urgent, but they are part of finishing email security once DMARC is at p=reject.

Target configuration after the roadmap

```
# both domains
TXT      "v=spf1 include:_spf.google.com ~all"
_dmarc TXT "v=DMARC1; p=reject; rua=mailto:dmarc@tallyfield.example"
CAA      0 issue "letsencrypt.org"      CAA 0 issue "amazon.com"
_mta-sts TXT "v=STSV1; id=20261101"      _smtp._tls TXT "v=TLSRPTv1; rua=mailto:tlsrpt@tallyfield.example"
# MTA-STS also needs a policy file at https://mta-sts.<domain>/.well-known/mta-sts.txt
```

08 — INVENTORY

Third-party scripts and cookies

What outside companies can run on your pages, and the cookies your sites set.

Third-party scripts

SERVICE	PURPOSE	LOADED ON	NOTE
Payment provider (JS)	Card entry and checkout	app.	Loaded from vendor, OK
Error monitoring	Crash reports	app., dev-app.	Public DSN is expected
Product analytics	Usage statistics	app.	Form inputs masked
Help desk widget	In-app support chat	app., www	OK
Google Tag Manager	Marketing tags	www (both brands)	Keep off app.
Google Analytics 4	Visitor statistics	www (both brands)	OK
LinkedIn Insight Tag	Ads	www (main brand)	OK
Marketing forms	Demo requests, newsletter	www (both brands)	OK
jsDelivr (library CDN)	Slider library	payroll www	No integrity check (SRI)

The app loads no advertising or marketing tags, which is the right separation for a product handling financial data. Keep it that way as marketing tools are added.

Cookies set by your sites

COOKIE	SITE	SECURE	HTTPONLY	SAMESITE	ASSESSMENT
__Host-tf_session	app.	Yes	Yes	Lax	Good
tf_csrf	app.	Yes	No (by design)	Strict	Good
tf_dev_session	dev-app.	No	Yes	Not set	Fix with F-05
_ga, _ga_*	www (both)	Yes	n/a	Lax	Expected
wordpress_test_cookie	payroll www	Yes	No	Not set	Harmless

"n/a": cookies created by analytics scripts are meant to be readable by those scripts, so HttpOnly does not apply. The __Host- prefix on the app session cookie is a strong practice: browsers refuse it unless it is Secure and tied to one exact host.

09 — REMEDIATION ROADMAP

30/60/90-day plan

A phased plan that fixes the findings in order of risk and then builds the habits that prevent them from coming back.

Immediate — days 1-7

- Block public access to the export bucket and review access logs (F-01) — *Engineering + legal*
- Roll the payment key and audit the payment account (F-02) — *Engineering + finance*
- Restrict and upgrade the build server, rotate its credentials (F-03) — *Engineering*
- Delete the dangling DNS record (F-04) and protect dev-app (F-05) — *Engineering*
- Report the lookalike domain and brief support (F-06) — *Operations*
- Publish SPF and DMARC for the payroll brand (F-07) — *Operations*
- Confirm auto-renew for the payroll domain before December 2 (section 07) — *Operations*

Short term — days 8-30

- Fix the API CORS allow-list (F-09) and disable GraphQL introspection (F-10) — *Engineering*
- Restrict document sharing in Google Workspace (F-08) — *Operations*
- Change shared vendor passwords, move them to a password manager (F-13) — *Operations*
- Turn on DKIM for the payroll brand and remove pct=25 on the main domain (F-07, F-12) — *Operations*

Medium term — days 31-60

- Stop publishing source maps (F-11) — *Engineering*
- Move both domains to DMARC p=reject — *Operations*
- Add CAA records (F-14) and the missing marketing site headers at the CDN (F-15) — *Engineering*
- Register the three defensive domain variations — *Operations*

Long term — days 61-90: make it stick

- **Asset inventory:** one owner-maintained list of every domain, subdomain, bucket and vendor, reviewed quarterly.
- **Secret scanning:** enable it on all company repositories and in the build pipeline; require restricted keys.
- **Contractor offboarding:** a checklist covering repositories, keys, shared documents and DNS records.
- **Environment rule:** no development or staging system is reachable without SSO or VPN.
- **Monitoring:** alerts for new certificates and newly registered lookalike domains.

10 — WHAT IS ALREADY IN GOOD SHAPE

Checks that passed

The core product shows good engineering practice. These were checked and found in order.

CHECK	RESULT	NOTES
HTTPS on all live hosts	Pass	All hosts redirect to HTTPS; HSTS with preload on app. and api.
TLS configuration	Pass	TLS 1.2 and 1.3 only, strong ciphers, valid certificates on all hosts
App security headers	Pass	Strict CSP, X-Frame-Options, Referrer-Policy and Permissions-Policy on app.
App cookies	Pass	Session cookie is Secure, HttpOnly, SameSite=Lax
Login page	Pass	Offers two-factor authentication and SSO, generic error messages
API authentication	Pass	All REST endpoints we called returned 401 without a token
Staging API	Pass	Requires authentication
Main domain SPF and DKIM	Pass	Correct, 2048-bit DKIM key
Retired subdomains	Pass	beta. and demo. removed from DNS, so they cannot be taken over
Vendor subdomains	Pass	Help desk and status page correctly claimed and configured
Exposed files	Pass	No .git, .env, backups or config files on any host
Software versions (except CI)	Pass	No outdated components with published vulnerabilities on app., api. or either marketing site
Paste sites	Pass	No company data found
security.txt	Pass	Present and current, with a working contact address

11 — WRITTEN FOLLOW-UP (EXAMPLE)

What the follow-up after your fixes looks like

Included in this package. Once you tell us the Critical and High findings are fixed, we re-check them from the outside and send a short written confirmation like this one.

ID	FINDING	STATUS	HOW WE VERIFIED
F-01	Public export bucket	Fixed	Bucket address returns 403 AccessDenied without credentials
F-02	Leaked payment key	Fixed	Repository removed; key rotation confirmed by you in writing (we never test keys)
F-03	Exposed build server	Fixed	ci. no longer reachable from the internet
F-04	Dangling docs subdomain	Fixed	CNAME record removed from DNS
F-05	Public development app	Partly fixed	Now behind SSO; its login page is still indexed by search engines — request removal
F-06	Lookalike domain	In progress	Abuse report filed by you; registrar has not acted yet. We recommend checking again in 30 days.
F-07	Payroll brand email	Fixed	SPF, DKIM and DMARC p=quarantine published and valid

Updated overall risk after follow-up: **Medium**. Remaining items are on the 30–60 day roadmap.

The follow-up is limited to light validation of the Critical and High findings from the outside. Medium and Low findings can be re-checked with the Retest of Key Fixes add-on or the Quarterly Re-Check.

12 — NEXT STEPS

What happens now

1. Start with section 02

The 7-day action list covers everything urgent and is written for the engineering lead.

2. Ask us anything by email

Questions about a finding? Write to info@nyorsoft.com and quote the finding ID (e.g. F-09). We reply in writing.

3. Tell us when Critical and High are fixed

We re-check them and send the written follow-up shown above, with an updated certificate.

4. Stay on top of it

New subdomains and lookalike domains appear all the time. The **Quarterly Re-Check** repeats these checks four times a year.

Limitations

This assessment covers only what was visible from the public internet during the review window. It is not a penetration test, a code review or a legal or compliance opinion, and it does not guarantee that the systems are free of other vulnerabilities. Version-based findings rely on information the systems reveal and on public advisories. Nyorsoft did not use any credential it found and did not access, download or modify any non-public data.

This is a sample report. Tallyfield, Inc., the domains tallyfield.example and tallyfieldpayroll.example, the repository and all findings are fictional and were created to show the format and depth of a Nyorsoft Website & Data Exposure Assessment. Any resemblance to a real business is unintended.