EXTERNAL ATTACK SURFACE ASSESSMENT

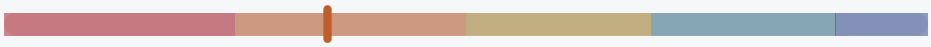
harbourstreetbakery.example

PREPARED FOR	Harbour Street Bakery (Sam Okafor, Owner)
PREPARED BY	Frontage Security
ENGAGEMENT DATE	October 9, 2026
SCAN STARTED	2026-10-09T06:00:00+00:00
REPORT GENERATED	2026-10-13 18:31 UTC
FINDINGS	11 total (2 high, 3 medium, 4 low, 2 info)
CLASSIFICATION	Sample report, fictional client

SECURITY POSTURE

35 out of 100 At risk

At least one issue offers a credible route for an attacker and should be addressed within days.



URGENT | AT RISK | NEEDS ATTENTION | REASONABLE | STRONG

CONTRIBUTING FACTORS

HIGH	2 findings	-40.0
MEDIUM	3 findings	-15.5
LOW	5 findings, of which 1 accepted and weighted at one quarter	-4.9

Scored from 100 by deducting for each finding according to its severity, in steps of 5 and rounded down. One critical finding carries roughly the weight of three high findings, and additional findings of the same severity carry progressively less weight, since a single point of entry is sufficient for an attacker. Accepted risks are counted at one quarter of their weight. Findings recorded as false positives are excluded.

Executive summary

This assessment of harbourstreetbakery.example identified 11 findings (2 high, 3 medium, 4 low, 2 info). The high-severity item(s) should be prioritized for prompt remediation; none rise to an immediate critical exposure.

0	2	3	4	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Priority items

HIGH Missing DMARC record (harbourstreetbakery.example)

HIGH TLS certificate expires in 9 days (shop.harbourstreetbakery.example)

Changes since the previous assessment

3 new findings, 2 resolved, 8 unchanged since the last completed scan of this target.

New

SEVERITY	CATEGORY	FINDING
High	SSL/TLS	TLS certificate expires in 9 days
Info	Open Ports	Open port: 443 (https)
Info	Open Ports	Open port: 80 (http)

Resolved

- Critical: High-risk service exposed: Remote Desktop (port 3389) (203.0.113.24)
- Medium: Missing SPF record (harbourstreetbakery.example)

Findings at a glance

#	SEVERITY	CATEGORY	FINDING	ASSET
1	High	Email Security	Missing DMARC record	harbourstreetbakery.example
2	High	SSL/TLS	TLS certificate expires in 9 days	shop.harbourstreetbakery.example
3	Medium	DNS	Only one working nameserver is published for this domain	harbourstreetbakery.example
4	Medium	Email Security	No DKIM record found at common selectors	harbourstreetbakery.example

#	SEVERITY	CATEGORY	FINDING	ASSET
5	Medium	SSL/TLS	Obsolete protocol supported: TLS 1.0	shop.harbourstreetbakery.example
6	Low	DNS	No CAA record, any certificate authority may issue for this domain	harbourstreetbakery.example
7	Low	Open Ports	Service banner exposes version info: nginx 1.18.0	203.0.113.24
8	Low	Web	No Content-Security-Policy header	www.harbourstreetbakery.example
9	Low	Web	No X-Content-Type-Options: nosniff header	www.harbourstreetbakery.example
10	Info	Open Ports	Open port: 443 (https)	203.0.113.24
11	Info	Open Ports	Open port: 80 (http)	203.0.113.24

Detailed findings

HIGH

Missing DMARC record

EMAIL SECURITY

ASSET	`harbourstreetbakery.example`
DESCRIPTION	No DMARC record found. DMARC tells receiving mail servers what to do with mail that fails SPF/DKIM checks, and gives the domain owner visibility into spoofing attempts via aggregate reports. Without it, spoofed mail impersonating this domain may be delivered normally.
EVIDENCE	`TXT _dmarc.harbourstreetbakery.example -> NXDOMAIN (no record)`
REMEDIATION	Publish a DMARC record starting at policy 'p=none' with reporting enabled to monitor, e.g. 'v=DMARC1; p=none; rua=mailto:dmarc-reports@harbourstreetbakery.example'. After reviewing reports for false positives, move to 'p=quarantine' then 'p=reject'.
FORWARD TO	your email provider or IT support provider (for example Microsoft 365, Google Workspace, or whoever configured your email)
SUGGESTED MESSAGE	`A security check found that our domain has no DMARC record, so nothing tells Gmail or Outlook what to do with email that fails our checks, and forged mail in our name is usually delivered. Please publish a monitor-only record to begin with: a TXT record at '_dmarc' in our domain reading 'v=DMARC1; p=none; rua=mailto:' followed by a mailbox we can use for the reports. We would like to stay in monitor-only mode until we have seen a few weeks of those reports.`
ESTIMATED EFFORT	A few minutes to publish, then a few weeks of watching the reports before anything is tightened.
RISK OF THE CHANGE	Monitor-only mode changes nothing about how your mail is delivered, so this first step is safe. The later step of moving the policy to quarantine or reject is the one that can affect real mail, and it should wait until the reports show every legitimate sender passing.

ref 78fb72cde0a6

HIGH

TLS certificate expires in 9 days

SSL/TLS

ASSET	`shop.harbourstreetbakery.example`
DESCRIPTION	The certificate served for this hostname expires in 9 days. When it does, browsers will show a full-page security warning in place of the site, and anything that validates the certificate, such as a payment widget or an integration, will stop working.
EVIDENCE	`shop.harbourstreetbakery.example:443 notAfter=2026-10-18 issuer=Let's Encrypt`
REMEDIATION	Renew the certificate now. If renewal was meant to be automatic, check why it has not run, and confirm the renewal job is still working before the next expiry.
FORWARD TO	whoever manages your website, typically your web designer, developer or hosting provider
SUGGESTED MESSAGE	`The HTTPS certificate on our site expires shortly. If it lapses, visitors will be shown a browser warning telling them the site is not safe, and most will leave rather than click past it. Please renew it now, and if renewal is supposed to be automatic, please confirm it has actually run.`
ESTIMATED EFFORT	Normally under an hour, and much better now than on the day.
RISK OF THE CHANGE	Low. Reissuing a certificate does not change the site, although some setups need a brief web server restart to pick the new one up.

ref 1827cf1ea3bf

MEDIUM

Only one working nameserver is published for this domain

DNS

ASSET	`harbourstreetbakery.example`
DESCRIPTION	This domain resolves through a single nameserver. Whenever that one server is unreachable, for maintenance, a fault, a network problem at its host or a denial of service attack aimed at it, the whole domain stops resolving. Everything that depends on the domain goes with it: the website, inbound mail, and any integration a partner points at a name here.
EVIDENCE	`NS harbourstreetbakery.example -> ns1.example-dns.test (1 record)`
REMEDIATION	Add at least one more authoritative nameserver, hosted separately from the first. With a managed DNS provider this is usually already included and only needs the extra nameserver names added at the registrar.
FORWARD TO	whoever manages your DNS records, typically your web designer, IT support provider or domain registrar
SUGGESTED MESSAGE	`A security check found that only one working nameserver is published for our domain, so if that single server has a problem our website and our email both stop being reachable until it comes back. Please add at least one more authoritative nameserver, hosted separately from the first. With a managed DNS provider this is usually already included and only needs the extra names added at the registrar.`
ESTIMATED EFFORT	Usually minutes if the provider already runs more than one, then a wait for it to spread.
RISK OF THE CHANGE	Adding a nameserver is safe, but the new one has to be serving the same records before it is listed, otherwise some lookups start failing.

ref 524ccac0c2b6

MEDIUM

No DKIM record found at common selectors

EMAIL SECURITY

ASSET	`harbourstreetbakery.example`
DESCRIPTION	No DKIM record was found at any of the 12 commonly used selector names. This does not conclusively mean DKIM is not configured, because DKIM selectors are arbitrary and cannot be discovered through DNS, but if this domain does not use DKIM then outbound mail is not cryptographically signed and is easier to spoof or tamper with in transit.
EVIDENCE	`Selectors checked: default, google, selector1, selector2, k1, k2, mail, dkim, s1, s2, smtp, mandrill. No TXT record returned for any.`
REMEDIATION	Confirm with the mail provider (Google Workspace, Microsoft 365, etc.) which DKIM selector is in use and verify the record is published. If DKIM is not yet configured, enable it through the mail provider's admin console.
FORWARD TO	your email provider or IT support provider (for example Microsoft 365, Google Workspace, or whoever configured your email)
SUGGESTED MESSAGE	`A security check could not find a DKIM signature for our outgoing mail at any of the usual names. That is not conclusive, because DKIM is only visible if you know the name it was published under, so please confirm whether it is switched on for our domain and switch it on if it is not. We do not know what the record should contain: the name and the key come from the mail platform itself.`
ESTIMATED EFFORT	A couple of clicks in most providers' admin console, plus one DNS entry they will give you.
RISK OF THE CHANGE	Turning DKIM on through your mail provider is routine and safe. A hand-built setup left half finished can cause your own mail to fail checks, which is why it is worth letting the provider do it.

ref e3555cdf3368

MEDIUM

Obsolete protocol supported: TLS 1.0

SSL/TLS

ASSET	`shop.harbourstreetbakery.example`
DESCRIPTION	The server still accepts TLS 1.0, a protocol version the IETF formally deprecated in 2021 (RFC 8996). It has known weaknesses, and its presence lets an attacker able to interfere with a connection try to push a visitor onto the weakest option offered. The card industry's security standard also prohibits it for systems that take payments.
EVIDENCE	`shop.harbourstreetbakery.example:443 TLS 1.0: accepted TLS 1.1: accepted TLS 1.2: accepted TLS 1.3: not offered`
REMEDIATION	Disable TLS 1.0 and 1.1 on the web server and allow only TLS 1.2 and TLS 1.3.
FORWARD TO	whoever manages your website, typically your web designer, developer or hosting provider
SUGGESTED MESSAGE	`A security check found that our site still accepts an obsolete version of the encryption that protects web traffic. Somebody able to interfere with a connection can try to push a visitor onto the weakest option offered, so every option offered is a real option. Please turn it off and allow only TLS 1.2 and TLS 1.3.`
ESTIMATED EFFORT	A configuration change on the web server, so a short job.
RISK OF THE CHANGE	Worth one check first. If anything unusual connects to this site, an old payment terminal or a program written in-house, it may only speak the older version and would stop working. On an ordinary website that is unlikely, but it is the question to ask before the change.

ref 4ef3814c359c

LOW

No CAA record, any certificate authority may issue for this domain

DNS

ASSET	`harbourstreetbakery.example`
DESCRIPTION	The domain publishes no CAA record. A CAA record is the domain owner's instruction to the certificate authorities of the world saying which of them are allowed to issue certificates for the domain. With no record, all of them are permitted. CAA will not stop an attacker who already controls the DNS, but it removes the easiest route in.
EVIDENCE	`CAA harbourstreetbakery.example -> no records`
REMEDIATION	Publish a CAA record at the domain root naming only the certificate authorities actually in use, for example '0 issue "letsencrypt.org"', and add an '0 iodef' entry so an authority can tell you when something asks for a certificate it is not allowed to issue.
FORWARD TO	whoever manages your DNS records, typically your web designer, IT support provider or domain registrar
SUGGESTED MESSAGE	`A security check noted that we publish no CAA record, which means any certificate authority in the world may issue an HTTPS certificate for our domain. A CAA record limits that to the ones we actually use. Please publish one at the root of our domain naming only those authorities, and add a reporting address so an authority can tell us when something asks for a certificate it is not allowed to issue. We do not know which authorities to name: that depends on who issues the certificates for our website, our email, and anything sitting behind a content delivery network, so please check that before publishing it.`
ESTIMATED EFFORT	A few minutes once the list of authorities is confirmed.
RISK OF THE CHANGE	The risk is leaving one out. An authority missing from the list stops being able to renew, which can mean a certificate quietly expiring and browsers warning visitors away from your site. The list needs checking before it is published.

ref b940fa3657b4

LOW

Service banner exposes version info: nginx 1.18.0

OPEN PORTS

ASSET	`203.0.113.24`
DESCRIPTION	A service announces its exact software version to anyone who connects. That makes it easy to look up known weaknesses in that version. The important part is confirming the software is on a currently supported and patched version.
EVIDENCE	`203.0.113.24:80/tcp Server: nginx/1.18.0`
REMEDIATION	Confirm the software is up to date and, where it is easy to do, stop it announcing the version (for nginx, 'server_tokens off').
FORWARD TO	whoever manages that server and its firewall, typically your IT support provider or hosting provider
SUGGESTED MESSAGE	`A security check noted that a service on our server announces its exact software version to anyone who connects, which makes it easy to look up known weaknesses in that version. The important part is confirming the software is on a currently supported and patched version. Where it is easy to do, please also stop it announcing the version.`
ESTIMATED EFFORT	The version check is the real work. Hiding the version is usually a small configuration change.
RISK OF THE CHANGE	Hiding a version banner changes nothing about what the service does. Updating the software itself needs the usual care and a sensible time to do it.

ref 5879f21c449e

LOW

No Content-Security-Policy header

WEB

ASSET	`www.harbourstreetbakery.example`
DESCRIPTION	The site sends no Content-Security-Policy. A CSP is a list, enforced by the browser, of where the page is allowed to load scripts, styles, frames and other content from. It limits the damage when something goes wrong, such as a cross-site scripting bug or a compromised third party script. It is a mitigation and not a fix, so this is graded low on its own.
EVIDENCE	`GET https://www.harbourstreetbakery.example/ -> 200; no Content-Security-Policy response header`
REMEDIATION	Start with Content-Security-Policy-Report-Only and a reporting endpoint so you can see what a policy would break before it breaks it, then move to the enforcing header once the reports are quiet.
FORWARD TO	whoever manages your website, typically your web designer, developer or hosting provider
SUGGESTED MESSAGE	`A security check noted that our site sends no Content Security Policy, which is the instruction limiting what code a browser will run on our pages and one of the better defenses against an injected script. Please start with the report-only version of the header and a reporting address, so we can see what a policy would break before it breaks anything, and switch to the enforcing version once the reports are quiet.`
ESTIMATED EFFORT	A project rather than a quick change, especially on a site with plugins. Report-only mode first is the honest way to find out how big.
RISK OF THE CHANGE	Enforcing a policy that is too strict breaks parts of the site, most often forms, embedded maps and payment widgets. Report-only mode has no effect on visitors at all, which is why it comes first.

ref 77b8dcd18f45

LOW

No X-Content-Type-Options: nosniff header

WEB

ASSET	`www.harbourstreetbakery.example`
DESCRIPTION	The site does not send 'X-Content-Type-Options: nosniff'. Without it a browser is free to ignore the content type the server declared and guess from the bytes instead, which can turn a harmless-looking file into something the browser runs as a script.
EVIDENCE	`GET https://www.harbourstreetbakery.example/ -> 200; no X-Content-Type-Options response header`
REMEDIATION	Send 'X-Content-Type-Options: nosniff' on every response, at the web server or the CDN so it applies to static files too.
FORWARD TO	whoever manages your website, typically your web designer, developer or hosting provider
SUGGESTED MESSAGE	`A security check noted that our site does not send the X-Content-Type-Options header, so a browser may guess at the type of a file we serve and in some cases run it as code. Please send 'X-Content-Type-Options: nosniff' on every response, set at the web server or the CDN so it covers static files too.`
ESTIMATED EFFORT	One line of configuration, so minutes.
RISK OF THE CHANGE	Very low. Occasionally a file that was being served with the wrong type stops working as it did, which is itself worth knowing about.

ref f7cab63374f0

INFO

Open port: 443 (https)

OPEN PORTS

ASSET	`203.0.113.24`
DESCRIPTION	Port 443 accepts connections (https).
EVIDENCE	`203.0.113.24:443/tcp open https`
REMEDIATION	No action required.

ref 27476a01ff82

INFO

Open port: 80 (http)

OPEN PORTS

ASSET	`203.0.113.24`
DESCRIPTION	Port 80 accepts connections (http).
EVIDENCE	`203.0.113.24:80/tcp open http`
REMEDIATION	No action required.

ref 46a061f65bd8

Remediation roadmap

Indicative grouping. “Quick wins” are typically DNS or TLS configuration changes that can be made in hours; “projects” usually involve firewall changes, software upgrades, or architectural work. Order within each group is by severity.

Quick wins 8

HIGH **Missing DMARC record** (harbourstreetbakery.example)

Publish a DMARC record starting at policy 'p=none' with reporting enabled to monitor, e.g. 'v=DMARC1; p=none; rua=mailto:dmarc-reports@harbourstreetbakery.example'. After reviewing reports for false positives, move to 'p=quarantine' then 'p=reject'.

HIGH **TLS certificate expires in 9 days** (shop.harbourstreetbakery.example)

Renew the certificate now. If renewal was meant to be automatic, check why it has not run, and confirm the renewal job is still working before the next expiry.

MEDIUM **Only one working nameserver is published for this domain** (harbourstreetbakery.example)

Add at least one more authoritative nameserver, hosted separately from the first. With a managed DNS provider this is usually already included and only needs the extra nameserver names added at the registrar.

MEDIUM **No DKIM record found at common selectors** (harbourstreetbakery.example)

Confirm with the mail provider (Google Workspace, Microsoft 365, etc.) which DKIM selector is in use and verify the record is published. If DKIM is not yet configured, enable it through the mail provider's admin console.

MEDIUM **Obsolete protocol supported: TLS 1.0** (shop.harbourstreetbakery.example)

Disable TLS 1.0 and 1.1 on the web server and allow only TLS 1.2 and TLS 1.3.

LOW **No CAA record, any certificate authority may issue for this domain** (harbourstreetbakery.example)

Publish a CAA record at the domain root naming only the certificate authorities actually in use, for example '0 issue "letsencrypt.org"', and add an '0 iodef' entry so an authority can tell you when something asks for a certificate it is not allowed to issue.

LOW **No Content-Security-Policy header** (www.harbourstreetbakery.example)

Start with Content-Security-Policy-Report-Only and a reporting endpoint so you can see what a policy would break before it breaks it, then move to the enforcing header once the reports are quiet.

LOW **No X-Content-Type-Options: nosniff header** (www.harbourstreetbakery.example)

Send 'X-Content-Type-Options: nosniff' on every response, at the web server or the CDN so it applies to static files too.

Projects 1

LOW **Service banner exposes version info: nginx 1.18.0** (203.0.113.24)

Confirm the software is up to date and, where it is easy to do, stop it announcing the version (for nginx, 'server_tokens off').

Informational 2

- Open port: 443 (https) (203.0.113.24)
- Open port: 80 (http) (203.0.113.24)

Accepted and excluded items

The items below continue to be detected on every scan. They are excluded from the summary and the remediation roadmap because they have been accepted as a known risk or recorded as a false positive. They are listed here so that the decision remains visible and can be revisited.

SEVERITY	CATEGORY	FINDING	ASSET
Low	Web	No HSTS header, so the first request to this site is unprotected	www.harbourstreetbakery.example