LEAKTRACE EVIDENCE PACKAGE

Harbourview Law LLP

Auditor-ready evidence bundle for **harbourview-llp.example**. Every finding ships with the observed output, a reproduction command, methodology citation and remediation timeline.

CUSTOMER	**Harbourview Law LLP**
DOMAIN	**harbourview-llp.example**
REGION	**CA**
REPORT ID	**LT-BIZ-2026-7098**
SCAN ID	**00000000-0000-0000-0000-000000000004**
SCANNED AT	**2026-09-30T02:57:33Z**
RISK SCORE	**66 / 100 (High)**
GENERATED AT	**2026-10-31T03:18:09Z**
SCHEMA VERSION	**1**

This document is auditor-grade evidence. The accompanying machine-readable JSON (evidence_package.json) contains the same data structure for ingestion into GRC platforms. Methodology and reproduction notes are detailed in the Methodology section. — LeakTrace Inc.

SUMMARY

23 total findings across infrastructure and credential sources. Severity breakdown:

0	2	6	10	5
CRITICAL	HIGH	MEDIUM	LOW	INFO

FINDINGS & EVIDENCE

HIGH

BEC Risk 60/100: spoofed mail can reach your clients

`finding_key: bec_score::5034d928b7 · category: bec_score`

`observed at 2026-09-30T02:57:33Z`

OBSERVED OUTPUT

```
Email authentication posture for harbourview-llp.example, as published in public DNS:

SPF strict mode (-all)
DMARC: p=missing pct=0
DKIM couldn't be confirmed from outside
MTA-STS: dns=False mode=none
BIMI not configured
TLS-RPT not configured
DNSSEC not enabled
```

REPRODUCE YOURSELF

```
dig TXT harbourview-llp.example +short @1.1.1.1 ; dig TXT _dmarc.harbourview-llp.example
+short @1.1.1.1
```

METHODOLOGY

Industry-standard email authentication checks across all six layers (SPF, DMARC, DKIM, MTA-STS, TLS-RPT, BIMI), plus DNSSEC

HIGH

No DMARC record: attackers can send fake invoices and emails from your domain and recipients have no authoritative way to reject them

finding_key: email_security::3830b490a6 · category: email_security

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
;; status: NXDOMAIN (answered by 1.1.1.1): _dmarc.harbourview-llp.example does not exist
```

REPRODUCE YOURSELF

```
dig TXT _dmarc.harbourview-llp.example +short @1.1.1.1
```

METHODOLOGY

DMARC enforcement check: is the rule on monitor mode, quarantine, or full reject

MEDIUM

WordPress detected: this is the most targeted website platform in the world. Any outdated plugin or theme is an entry point for attackers

finding_key: cms::cba57a59e8 · category: cms

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
robots.txt for harbourview-llp.example references WordPress paths (wp-admin / wp-login).
```

REPRODUCE YOURSELF

```
curl -s https://harbourview-llp.example/robots.txt | grep -i wp-
```

METHODOLOGY

Public fingerprinting of your content management system from response headers and HTML

MEDIUM

No content security policy: attackers can inject fake content, forms, or payment fields into your website

finding_key: header::784b0ea935 · category: header

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
HTTP/1.1 200 OK
Date: Wed, 30 Sep 2026 02:57:33 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
X-Powered-By: PHP/8.2
```

REPRODUCE YOURSELF

```
curl -sI https://harbourview-llp.example/
```

METHODOLOGY

HTTP response headers your website sends to every visitor's browser

MEDIUM

HSTS not enforced: your site does not send the header that tells a browser to use only its secure address. Most current browsers try the secure address first; an older browser, or a link that names the insecure address, can still start there

finding_key: header::81db7711b1 · category: header

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
HTTP/1.1 200 OK
Date: Wed, 30 Sep 2026 02:57:33 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
X-Powered-By: PHP/8.2
```

REPRODUCE YOURSELF

```
curl -sI https://harbourview-llp.example/
```

METHODOLOGY

HTTP response headers your website sends to every visitor's browser

MEDIUM

MIME-sniffing not blocked: uploaded files can be reinterpreted by browsers as executable scripts

finding_key: header::cb5b7f54c3 · category: header

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
HTTP/1.1 200 OK
Date: Wed, 30 Sep 2026 02:57:33 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
X-Powered-By: PHP/8.2
```

REPRODUCE YOURSELF

```
curl -sI https://harbourview-llp.example/
```

METHODOLOGY

HTTP response headers your website sends to every visitor's browser

MEDIUM

No clickjacking protection: your website can be embedded inside a fake page to trick your clients into clicking the wrong thing

finding_key: header::f1abd00937 · category: header

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
HTTP/1.1 200 OK
Date: Wed, 30 Sep 2026 02:57:33 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
X-Powered-By: PHP/8.2
```

REPRODUCE YOURSELF

```
curl -sI https://harbourview-llp.example/
```

METHODOLOGY

HTTP response headers your website sends to every visitor's browser

MEDIUM

Your business name is registered on 6 other endings besides your own and we cannot tell from outside whether those are yours or somebody else's

finding_key: typosquat::374b1b4734 · category: typosquat

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
Your business name is registered on 6 other endings besides your own and we cannot tell from outside whether those are yours or somebody else's
```

REPRODUCE YOURSELF

```
dig +short harbourview-llp.example && whois harbourview-llp.example
```

METHODOLOGY

Registration lookup of domains spelled a character or two away from yours

LOW

An online storage folder with your firm's name exists. We could not open it and cannot tell whose it is. Azure Blob bucket 'harbourview-llp'

finding_key: cloud_bucket::5011ad9d62 · category: cloud_bucket

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
provider: Azure Blob
bucket: harbourview-llp
url: https://harbourview-llp.blob.storage.example/?comp=list
access_level: exists_protected
approximate_object_count: 0
```

REPRODUCE YOURSELF

```
curl -sI https://harbourview-llp.blob.storage.example/?comp=list
```

METHODOLOGY

Public-bucket enumeration across AWS, Google Cloud and Azure storage

LOW

DNSSEC not enabled: your domain's traffic can be redirected to a fake version of your website without detection

finding_key: dns::ba6a30ced3 · category: dns

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
*** Can't find harbourview-llp.example: No answer
Authoritative answers can be found from:
harbourview-llp.example
origin = ns1.harbourview-llp.example
mail addr = hostmaster.harbourview-llp.example
serial = 2026100101
refresh = 10000
retry = 2400
expire = 604800
minimum = 1800
```

REPRODUCE YOURSELF

```
dig DNSKEY harbourview-llp.example @1.1.1.1 +dnssec
```

METHODOLOGY

DNSSEC check: is your domain's DNS cryptographically signed so attackers can't redirect visitors

LOW

TLS-RPT reporting not configured: you have no visibility into email-in-transit security failures (downgrade attempts, certificate issues, etc.)

finding_key: email_security::0e507a7ca0 · category: email_security

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
;; status: NXDOMAIN (answered by 1.1.1.1): _smtp._tls.harbourview-llp.example does not exist
```

REPRODUCE YOURSELF

```
dig TXT _smtp._tls.harbourview-llp.example +short @1.1.1.1
```

METHODOLOGY

TLS-RPT check: your published address for receiving encryption-failure reports

LOW

MTA-STS not configured: email-in-transit to your domain can be silently downgraded to plaintext by a network attacker. Both the _mta-sts TXT record and the policy file are missing

`finding_key: email_security::3cc992cc46 · category: email_security`

`observed at 2026-09-30T02:57:33Z`

OBSERVED OUTPUT

```
DNS record: (none)
Policy URL: https://mta-sts.harbourview-llp.example/.well-known/mta-sts.txt (HTTP n/a)
Policy text:
(no policy file fetched)
```

REPRODUCE YOURSELF

```
dig TXT _mta-sts.harbourview-llp.example +short @1.1.1.1 ; curl -s https://mta-sts.harbourview-llp.example/.well-known/mta-sts.txt
```

METHODOLOGY

MTA-STS check: your published policy for forcing encrypted email delivery

LOW

No referrer policy: visitor URLs and search-result paths are leaked to every third-party resource your site loads

`finding_key: header::6560b8ed45 · category: header`

`observed at 2026-09-30T02:57:33Z`

OBSERVED OUTPUT

```
HTTP/1.1 200 OK
Date: Wed, 30 Sep 2026 02:57:33 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
X-Powered-By: PHP/8.2
```

REPRODUCE YOURSELF

```
curl -sI https://harbourview-llp.example/
```

METHODOLOGY

HTTP response headers your website sends to every visitor's browser

LOW

No permissions policy: third-party scripts can request camera, microphone, geolocation and payment access without restriction

finding_key: header::ad396e80f2 · category: header

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
HTTP/1.1 200 OK
Date: Wed, 30 Sep 2026 02:57:33 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
X-Powered-By: PHP/8.2
```

REPRODUCE YOURSELF

```
curl -sI https://harbourview-llp.example/
```

METHODOLOGY

HTTP response headers your website sends to every visitor's browser

LOW

Your server is advertising its software version (nginx): attackers use this to find known vulnerabilities specific to that version

finding_key: header::adc708bb1e · category: header

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
HTTP/1.1 200 OK
Date: Wed, 30 Sep 2026 02:57:33 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx
X-Powered-By: PHP/8.2
```

REPRODUCE YOURSELF

```
curl -sI https://harbourview-llp.example/
```

METHODOLOGY

HTTP response headers your website sends to every visitor's browser

LOW

Your website shares an IP address with 500+ other sites: if any of them get blacklisted, your site can be blocked too

finding_key: neighbors::012d0fbf9c · category: neighbors

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
Your website shares an IP address with 500+ other sites: if any of them get blacklisted,
your site can be blocked too
```

REPRODUCE YOURSELF

```
curl -s 'https://reverse-ip.example/?q=harbourview-llp.example'
```

METHODOLOGY

Reverse IP lookup listing the other domains served from your address

LOW

Your robots.txt file publicly lists internal paths (/wp-admin/): this tells attackers exactly where to look for admin panels and private areas

finding_key: robots::3abdc7edb2 · category: robots

observed at 2026-09-30T02:57:33Z

OBSERVED OUTPUT

```
Disallow: /wp-admin/
```

REPRODUCE YOURSELF

```
curl -s https://harbourview-llp.example/robots.txt
```

METHODOLOGY

robots.txt check for leakage of internal paths

LOW

WordPress publishes its author list: the display names and URL slugs of accounts that have posted content are readable without logging in, via 1 endpoint(s)

`finding_key: wp_user_enum::7951480fa2 · category: wp_user_enum`

`observed at 2026-09-30T02:57:33Z`

OBSERVED OUTPUT

```
GET https://harbourview-llp.example/wp-json/wp/v2/users
Response: 200 OK (application/json)
[
  {
    "id": 2,
    "name": "Jordan Wexley",
    "slug": "jordan-wexley"
  },
  {
    "id": 3,
    "name": "Harbourview Law LLP",
    "slug": "front-desk"
  }
]
```

REPRODUCE YOURSELF

```
curl -s https://harbourview-llp.example/wp-json/wp/v2/users | jq
```

METHODOLOGY

WordPress public author-list endpoint check

INFO

Certificate Transparency footprint mapped: 1 unique subdomain(s) seen in CT logs, 1 currently resolving

`finding_key: cert_transparency::41ffb2c24d · category: cert_transparency`

`observed at 2026-09-30T02:57:33Z`

OBSERVED OUTPUT

```
www.harbourview-llp.example
```

REPRODUCE YOURSELF

```
curl -s 'https://ct-log.example/?q=%25.harbourview-llp.example&output=json' | jq -r '.
[].name_value' | sort -u
```

METHODOLOGY

Certificate Transparency log check: every SSL certificate ever issued for your domain

INFO

BIMI not configured: your brand logo does not appear next to mail your domain sends in supported clients. This weakens visual brand-protection against spoofers

`finding_key: email_security::334b47c7b4 · category: email_security`

`observed at 2026-09-30T02:57:33Z`

OBSERVED OUTPUT

```
;; status: NXDOMAIN (answered by 1.1.1.1): default._bimi.harbourview-llp.example does not exist
```

REPRODUCE YOURSELF

```
dig TXT default._bimi.harbourview-llp.example +short @1.1.1.1
```

METHODOLOGY

BIMI check: your published record for showing a verified logo next to your emails

INFO

No /.well-known/security.txt published: researchers reporting vulnerabilities have no documented contact path

`finding_key: exposed_endpoint::37abc86e69 · category: exposed_endpoint`

`observed at 2026-09-30T02:57:33Z`

OBSERVED OUTPUT

```
GET https://harbourview-llp.example/.well-known/security.txt did not return 200.
```

REPRODUCE YOURSELF

```
curl -sI https://harbourview-llp.example/.well-known/security.txt
```

METHODOLOGY

RFC 9116: A File Format to Aid in Security Vulnerability Disclosure

INFO

Overall security grade: F: your website failed 5 out of 12 standard security tests, leaving your clients' data at risk

`finding_key: observatory::f75b0cd881 · category: observatory`

INFO

SaaS platform in use: Microsoft 365 / Entra ID: this is where your credential and OAuth attack surface lives, so tenant hardening and multi-factor enforcement here protect the most

`finding_key: saas_vendor::e73b54f04d · category: saas_vendor`

METHODOLOGY

LeakTrace EASM v2 — passive attack-surface review

All findings are derived from passive reconnaissance of public-facing infrastructure and breach-database correlation. No private systems were accessed. Each finding includes the observed output, a reproduction command the auditor can run independently and the methodology citation for that check.

DATA SOURCES

- DNS / SSL / HTTP header inspection of public endpoints
- Mozilla Observatory grading
- Have I Been Pwned breach correlation
- Subdomain enumeration via passive sources
- Public typosquat registry monitoring

REPRODUCTION

Every infrastructure finding ships with a reproduction_command field. Running it from any internet-connected host should reproduce the observed output exactly, modulo the upstream service's state at the time of execution.