



EXTERNAL WEBSITE SECURITY REVIEW

Website Security Report

What an outsider can see about your firm online, and what to fix first.

CLIENT

Mesa Ridge Legal Group

WEBSITE

www.mesaridgelegal.example

REVIEW WINDOW

October 5-9, 2026

REPORT ID

NYX-SAMPLE-S-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 the firm stands

Written for the managing partner and office manager. Technical details for whoever manages the website start in section 05.

OVERALL RISK

HIGH

Driven by client documents being publicly listed (F-01). Expected to drop to **Medium** once the “fix this week” list is done, and to **Low** once all findings are fixed.

What we looked at. The firm’s website, its intake and contact forms, login pages, visible API endpoints, every third-party script the site loads, the cookies it sets, its email domain records and all subdomains listed in public certificate logs. Everything was reviewed from the outside, the way anyone on the internet could see it.

What we found. The biggest risk is not a hacker breaking in. It is that confidential material is already reachable without breaking anything: documents clients upload through the case-review form are listed in a public folder, and a forgotten staging copy of the site is open and indexed by Google.



What this means for the firm

BUSINESS RISK	WHY IT APPLIES HERE	FINDINGS
Client confidentiality	File names of uploaded client documents are visible to anyone, and an advertising pixel receives the type of legal matter a visitor selects on the intake form.	F-01, F-04
Website takeover	A chat script comes from a domain that has expired. Whoever registers it could run their own code on every page, including the intake form.	F-03
Reputation and search results	An outdated staging copy of the site appears in Google next to the real one and shows technical error messages.	F-02
Email fraud	The domain’s email settings still allow messages that pretend to come from the firm, for example fake trust-account payment instructions.	F-07

Professional obligations: F-01 and F-04 may be relevant to the firm’s duty to protect client information (for example ABA Model Rule 1.6(c) and the Texas Disciplinary Rules). We are not lawyers advising on that question; we recommend the firm’s ethics or compliance contact reviews both findings.

02 — ACTION LIST

What to fix this week

One page to forward to whoever manages the website. Tick each box when done. Everything else in this report can follow over the next month.

- ☐ **Close the public folder with client uploads** CRITICAL
 Turn off directory listing and move form uploads out of the public web folder. Then check the server logs for who opened the folder. **F-01**
- ☐ **Remove the expired chat widget** HIGH
 Delete the Chatperch script from the website and Google Tag Manager today, before someone registers the domain. **F-03**
- ☐ **Take the staging site offline** HIGH
 Password-protect or delete staging.mesaridgelegal.example and ask Google to remove its pages. **F-02**
- ☐ **Stop the advertising pixel on the intake page** MEDIUM
 Exclude the case-review page from the Meta Pixel in Google Tag Manager. **F-04**
- ☐ **Limit what clients can upload** MEDIUM
 Allow only PDF, Word and image files, with a 10 MB limit. **F-09**
- ☐ **Turn on two-factor login for all WordPress accounts** MEDIUM
 Applies to every attorney and staff account that can log in to the website. **F-10**

All findings

ID	FINDING	SEVERITY	WHERE IT'S FIXED
F-01	Documents uploaded by clients are listed in a public folder	CRITICAL	Website files / form settings
F-02	Staging copy of the website is public and indexed by Google	HIGH	Hosting control panel
F-03	Chat script loaded from an expired domain anyone can register	HIGH	Google Tag Manager / theme
F-04	Advertising pixel receives the legal matter type from the intake form	MEDIUM	Google Tag Manager
F-05	Session cookie set without Secure, HttpOnly or SameSite flags	MEDIUM	Hosting control panel (PHP)
F-06	Outdated jQuery 1.12.4 with published vulnerabilities	MEDIUM	WordPress theme
F-07	Email domain still open to spoofing (DMARC p=none, SPF ?all)	MEDIUM	DNS settings
F-08	No Content-Security-Policy despite 11 third-party scripts	MEDIUM	Website files (.htaccess)
F-09	Upload field accepts any file type up to 50 MB	MEDIUM	Form plugin settings
F-10	Username exposed and login page without extra protection	MEDIUM	WordPress dashboard
F-11	Checkout email address appears in 1 known data breach	LOW	Your own accounts
F-12	No security.txt file for reporting problems	LOW	Website files

03 — SCOPE AND METHOD

What we checked, and how

An external, non-intrusive review combining automated checks with manual review of every public page, form and script.

ITEM	DETAILS
Client	Mesa Ridge Legal Group (fictional), Austin, Texas
In scope	<code>https://www.mesaridgelegal.example</code> , the apex domain and subdomains found in public certificate logs
Out of scope	The client portal run by a third-party vendor (portal.): headers and TLS only, no testing of the vendor's application
Checkout email	<code>office@mesaridgelegal.example</code> (breach lookup only)
Review window	October 5–9, 2026
Report ID	NYX-SAMPLE-S-001

What we did

- Everything in the Public Website Security Check: headers, TLS, SPF/DKIM/DMARC, software versions, breach lookup, exposed files
- Manually reviewed every public form, upload field, login page and the WordPress REST API
- Listed every third-party script and where it loads
- Recorded every cookie the site sets and its security flags
- Searched certificate transparency logs for subdomains

What we did not do

- No login attempts and no password guessing
- No form submissions and no file uploads
- No exploitation of any vulnerability
- No opening or downloading of client files we found listed
- No testing of the vendor's client portal application
- No load testing and no access to internal systems

How we rate severity

SEVERITY	MEANING	SUGGESTED TIMING
CRITICAL	Directly exposes sensitive data or gives an attacker an easy way in.	Same day
HIGH	A known, realistic path to compromise or fraud that needs little skill to use.	Within 7 days
MEDIUM	Weakens defenses or makes other attacks easier. Not an emergency on its own.	Within 30 days
LOW	Good-practice improvements that reduce what attackers can learn.	Next maintenance

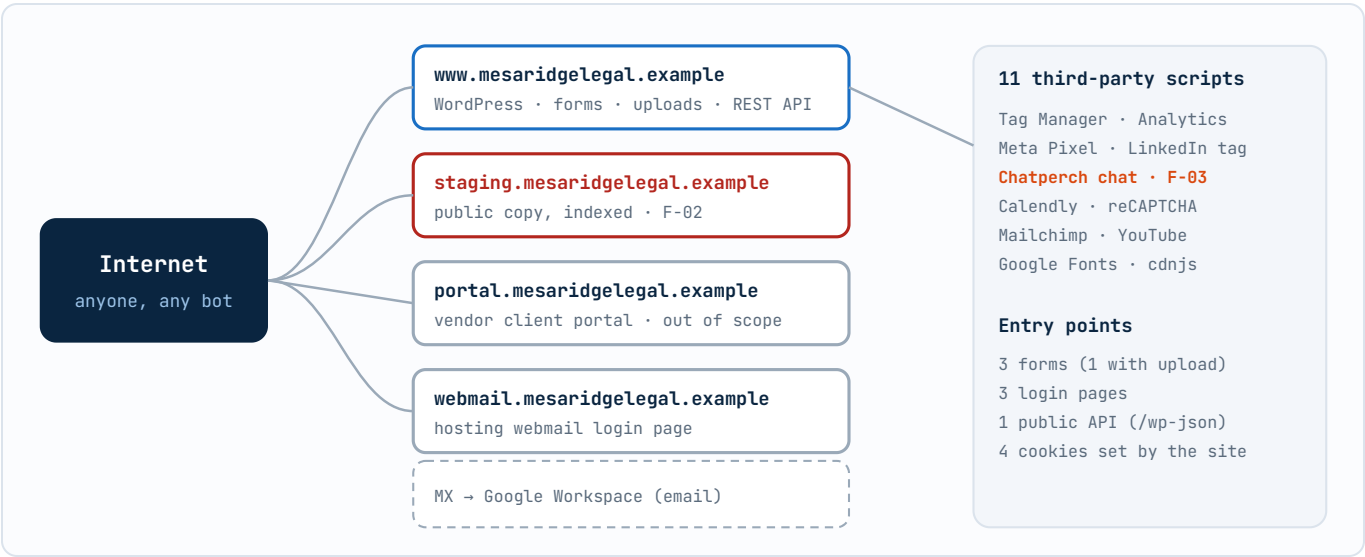
Terms used in this report

Staging site	A test copy of a website used while building or changing it. It should never be public.
Third-party script	Code from another company that runs on your pages, such as analytics or a chat box. It can see what visitors do on the page.
Cookie flags	Settings that decide whether a browser cookie can be stolen by scripts or sent over unencrypted connections.
Certificate logs	Public records of every HTTPS certificate issued. They reveal subdomains a company may have forgotten.
API endpoint	An address that returns data to programs instead of showing a page to people.

04 – ATTACK SURFACE SNAPSHOT

What an outsider can see

Every address, entry point and outside service connected to the firm’s website that we found from the internet.



Hosts and subdomains

ADDRESS	WHAT IT IS	SOURCE	STATUS
www / apex	Main website, WordPress on shared hosting	DNS	Reviewed
staging.	Full copy of the website from a 2025 redesign	Certificate logs	Exposed (F-02)
portal.	Client portal hosted by a third-party vendor	DNS (CNAME)	Headers and TLS OK
webmail.	Hosting provider’s webmail login	Certificate logs	Login page only
old.	Appears in 2023 certificate logs, no longer in DNS	Certificate logs	Retired

Entry points

ENTRY POINT	WHAT IT ACCEPTS	PROTECTION SEEN
/contact/	Name, email, phone, message	reCAPTCHA
/free-case-review/	Contact details, matter type, description, file upload	None visible (F-09)
Newsletter (footer)	Email address, sent to Mailchimp	Double opt-in
/wp-login.php	WordPress staff login	None visible (F-10)
/wp-json/	Public REST API, read-only	Lists users (F-10)
webmail. / portal.	Email and client portal logins	Vendor-managed

05 — TECHNICAL FINDINGS

Detailed findings

Each finding explains what we saw, why it matters for the firm, and what the person who manages the website should do.

F-01 Documents uploaded by clients are listed in a public folder**CRITICAL**Location: `/wp-content/uploads/case-review/` Category: **Data exposure****WHAT WE SAW**

Files sent through the “Free case review” form are saved in a folder that lists its contents to anyone. On October 6 it showed 214 files. Their names alone reveal client matters.

```
# folder listing only — no file was opened or downloaded
GET /wp-content/uploads/case-review/2026/09/ → 200 OK "Index of /.../2026/09"
  custody-agreement-draft-[name].pdf          412K
  termination-letter-[employer].pdf          188K
  medical-bills-accident-0814.pdf             2.1M
  ... (214 files across 14 monthly folders)
```

WHY IT MATTERS

Anyone who finds this folder, including automated scanners that look for open folders, can download documents clients sent in confidence. Each file is an individual record of a person’s legal situation.

HOW TO FIX

- Add Options -Indexes to the main `.htaccess` file today. This hides the listing immediately.
- In the form plugin settings, store uploads outside the public web folder (most form plugins offer a “protected uploads” option) and move the existing files there.
- Check the server access logs (cPanel → “Raw Access”) for requests to `/case-review/` from unknown addresses, and involve the firm’s ethics contact in deciding on notification.

F-02 Staging copy of the website is public and indexed by Google**HIGH**Host: `staging.mesaridgelegal.example` Category: **Forgotten assets****WHAT WE SAW**

The subdomain appears in public certificate logs and serves a full copy of the website from the 2025 redesign. It has no password, debug messages are switched on, and Google has indexed it.

```
crt.sh → staging.mesaridgelegal.example (certificate issued 2025-03-11, renewed automatically)
GET https://staging.mesaridgelegal.example/ → 200 OK, no login required
Warning: Undefined variable $matter in /home/mrlg/staging/wp-content/themes/mesa/intake.php on line 8
8
Google: site:staging.mesaridgelegal.example → about 37 results
```

WHY IT MATTERS

Staging copies are rarely updated, so their plugins become outdated first and are an easy way into the same hosting account. The error messages reveal server folder names, and people searching for the firm may land on an old version with outdated attorney information.

HOW TO FIX

- Delete the staging site, or protect it with a password in the hosting control panel (“Directory Privacy”).
- Once it is password-protected, its pages drop out of Google over the following weeks. To speed this up, verify the subdomain in Google Search Console and use Removals → New request.

- Make sure the staging database does not contain real client form submissions. If it does, treat it like F-01.

F-03 Chat script loaded from an expired domain anyone can register

HIGH

Script: `widget.chatperch.example/loader.js` Category: Third-party risk

WHAT WE SAW

Every page, including the intake form, still tries to load a chat widget from `chatperch.example`. The vendor appears to have shut down: the script no longer loads, historical registration records show the domain expired on August 14, 2026, and it is now listed as available.

```
<script src="https://widget.chatperch.example/loader.js" async></script> (via Google Tag Manager, a
ll pages)
WHOIS chatperch.example → no match / domain available
DNS widget.chatperch.example → NXDOMAIN
```

WHY IT MATTERS

Whoever registers this domain next can serve any code they like, and the website will run it on every page. That code could read what visitors type into the intake form or redirect them to a fake page. Expired script domains are actively bought for this purpose.

HOW TO FIX

- Remove the Chatperch tag in Google Tag Manager and publish the container today. Check the theme files for a second copy of the script.
- Review the full script inventory in section 06 at least twice a year and remove anything no longer used.

F-04 Advertising pixel receives the legal matter type from the intake form

MEDIUM

Location: `/free-case-review/` Category: Privacy / confidentiality

WHAT WE SAW

The “Practice areas” pages link to the intake form with the matter type in the page address, for example `?matter=divorce`. When the intake page opens, the Meta Pixel sends that full address to Meta as part of its normal page-view tracking. We observed this in the browser’s network log without submitting the form.

```
https://www.mesaridgelegal.example/free-case-review/?matter=divorce
→ facebook.com/tr/?id=...&ev=PageView&dl=https%3A%2F%2Fwww.mesaridgelegal.example%2Ffree-case-review%2
F%3Fmatter%3Ddivorce
```

WHY IT MATTERS

Combined with Meta’s own data about the visitor, this tells an advertising company that a specific person is looking for a divorce or criminal defense lawyer. Clients would not expect that, and regulators have taken action against similar tracking on sensitive forms.

HOW TO FIX

- In Google Tag Manager, add an exception so the Meta Pixel and LinkedIn tag do not fire on `/free-case-review/`.
- Change the links so the matter type is not added to the page address (the form can pre-select it another way).

F-05 Session cookie set without Secure, HttpOnly or SameSite flags

MEDIUM

Location: `/free-case-review/` Category: Cookie security

WHAT WE SAW

```
Set-Cookie: PHPSESSID=8f3c...; path=/
```

The form plugin starts a PHP session to remember a partly completed intake form. The cookie that identifies this session has none of the three protective flags (see the full cookie table in section 06).

WHY IT MATTERS

Without `HttpOnly`, any script on the page, including a compromised third-party script like the one in F-03, can read the cookie and continue someone's half-finished intake form. Without `Secure`, the cookie may be sent over an unencrypted connection.

HOW TO FIX

- In the hosting control panel's PHP options, set `session.cookie_secure = 0n`, `session.cookie_httponly = 0n` and `session.cookie_samesite = Lax`.

F-06 Outdated jQuery 1.12.4 with published vulnerabilities

MEDIUM

Component: **jQuery 1.12.4 (bundled in theme)** Category: **Outdated software**

WHAT WE SAW

```
<script src="/wp-content/themes/mesa/js/jquery-1.12.4.min.js"></script>
```

The theme loads its own old copy of jQuery instead of the current version that comes with WordPress. Versions below 3.5.0 are affected by published cross-site scripting issues (CVE-2020-11022 and CVE-2020-11023).

WHY IT MATTERS

These issues can let injected content run as code in a visitor's browser if the site passes untrusted text to certain jQuery functions. Old libraries are also the first thing automated scanners flag.

HOW TO FIX

- Remove the bundled file from the theme and use the jQuery version shipped with WordPress. Test the menu and forms afterwards.

F-07 Email domain still open to spoofing (DMARC p=none, SPF ?all)

MEDIUM

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

WHAT WE SAW

mesaridgelegal.example	TXT	"v=spf1 include:_spf.google.com include:servers.mcsv.net ?all"
_dmarc.mesaridgelegal.example	TXT	"v=DMARC1; p=none"
google._domainkey	TXT	DKIM key present (2048-bit)

WHY IT MATTERS

DMARC exists but is set to monitoring only, with no address to receive reports, so nobody sees spoofing attempts and nothing is blocked. The SPF record ends in `?all`, which tells receiving servers to treat unknown senders as neutral. Law firms are frequent targets of fake payment-instruction emails.

HOW TO FIX

- Change the end of the SPF record from `?all` to `~all`.
- Add a report address: `"v=DMARC1; p=none; rua=mailto:dmarc@mesaridgelegal.example"`, ideally pointed at a free DMARC report service.
- After 2–4 weeks of clean reports, move to `p=quarantine` and then `p=reject`.

F-08 No Content-Security-Policy despite 11 third-party scripts**MEDIUM**Location: **all pages** Category: **Browser protections**

The site sends HSTS, X-Frame-Options, X-Content-Type-Options and Referrer-Policy correctly, but no Content-Security-Policy (CSP). A CSP is the browser's list of places the page may load scripts from. With 11 outside services on the site, it is the main safety net if one of them is compromised.

HOW TO FIX

- Start with a report-only policy, so nothing breaks while you see what the site actually loads:

```
Header always set Content-Security-Policy-Report-Only "default-src 'self'; script-src 'self' 'unsafe-inline' https://www.googletagmanager.com https://connect.facebook.net https://snap.licdn.com https://assets.calendly.com https://www.google.com https://www.gstatic.com https://cdnjs.cloudflare.com; frame-ancestors 'self'; report-uri https://[your-report-service]/csp"
```

- This is a starting point. The reports (sent to a free CSP reporting service) will list every other address the site uses, such as fonts, Mailchimp and YouTube. Add those to the policy.
- Once two weeks pass without unexpected reports, switch the header name to Content-Security-Policy to enforce it.

F-09 Upload field accepts any file type up to 50 MB**MEDIUM**Location: **/free-case-review/** Category: **File uploads****WHAT WE SAW**

```
<input type="file" name="input_7" multiple> # no "accept" restriction
formSettings = {"allowedExtensions":"","maxFileSize":52428800} # 50 MB, all types
```

We read these settings from the page source. We did not upload any file.

WHY IT MATTERS

Anyone can send the firm executable files or macro-enabled documents that look like evidence. Staff open uploads as part of normal work, which makes this a convenient way to deliver malware. Combined with F-01, uploaded files would also be served from the firm's own domain.

HOW TO FIX

- In the form settings, allow only pdf, doc, docx, jpg, png, heic and set the limit to 10 MB per file.

F-10 Usernames exposed and login page without extra protection**MEDIUM**Location: **/wp-json/wp/v2/users, /wp-login.php** Category: **Login entry points**

```
GET /wp-json/wp/v2/users → 200 OK slugs: "jmesa", "rortega-admin", "frontdesk"
GET /wp-login.php → 200 OK (no CAPTCHA, no visible two-factor prompt)
```

The public API lists three user slugs, which normally match login names. The login page shows no sign of attempt limits or two-factor authentication. We did not attempt to log in.

HOW TO FIX

- Turn on two-factor authentication for every account and install a plugin that limits failed login attempts.
- Hide the user list in the REST API (available in most security plugins).

F-11 Checkout email address appears in 1 known data breach

LOW

Address: **office@mesaridgelegal.example** Source: **Have I Been Pwned**

The address appears in one breach of a legal-directory website (2021, illustrative), which exposed email addresses and firm names but no passwords. The main effect is more targeted phishing. Keep two-step verification on for this mailbox.

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

F-12 No security.txt file for reporting problems

LOW

Location: **/.well-known/security.txt** Category: **Good practice**

Researchers who notice a problem like F-01 look for this small file to know whom to tell. Without it, reports may never reach the firm.

Contact: **mailto:security@mesaridgelegal.example**
Expires: **2027-10-31T00:00:00Z**
Preferred-Languages: **en**

06 — INVENTORY

Third-party scripts and cookies

Everything outside companies can run on the firm's pages, and every cookie the site itself sets.

Third-party scripts

SERVICE	PURPOSE	LOADED ON	NOTE
Google Tag Manager	Loads the other marketing tags	All pages	Loads most of the marketing scripts below
Google Analytics 4	Visitor statistics	All pages	OK
Meta Pixel	Facebook / Instagram ads	All pages	Remove from intake (F-04)
LinkedIn Insight Tag	LinkedIn ads	All pages	Remove from intake (F-04)
Chatperch	Live chat (vendor defunct)	All pages	Expired domain (F-03)
Calendly	Consultation booking	/contact/	OK
Google reCAPTCHA	Spam protection	/contact/	Missing on intake form
Mailchimp	Newsletter signup	Footer	OK
YouTube	Embedded videos	/about/	Use youtube-nocookie.com
Google Fonts	Web fonts	All pages	OK
cdnjs (Font Awesome)	Icons	All pages	No integrity check (SRI)

Cookies set by the website

COOKIE	SET BY	SECURE	HTTPONLY	SAMESITE	ASSESSMENT
PHPSESSID	Intake form plugin	No	No	Not set	Fix (F-05)
wordpress_test_cookie	WordPress login page	Yes	No	Not set	Harmless
_ga, _ga_*	Google Analytics (script)	Yes	n/a	Lax	Expected
_fbp	Meta Pixel (script)	Yes	n/a	Lax	Expected

"n/a": cookies created by analytics scripts are meant to be readable by those scripts, so HttpOnly does not apply.

07 — WHAT IS ALREADY IN GOOD SHAPE

Checks that passed

CHECK	RESULT	NOTES
HTTPS enforced	Pass	All HTTP requests redirect to HTTPS (301)
TLS configuration	Pass	Only TLS 1.2 and 1.3, strong ciphers, valid certificate
HSTS, X-Frame-Options, Referrer-Policy	Pass	Present on all pages
PHP version	Pass	PHP 8.3, supported with security fixes
WordPress core and plugins	Pass	Current versions, no published vulnerabilities
DKIM signing	Pass	2048-bit key for Google Workspace
Exposed source code, backups or secrets	Pass	No .git, .env, backups or config copies found
Contact form spam protection	Pass	reCAPTCHA on /contact/
Client portal transport	Pass	Vendor portal enforces HTTPS and HSTS
Retired subdomains	Pass	old. no longer resolves, so it cannot be taken over

08 — NEXT STEPS

What happens now

1. Forward section 02

The one-page action list is written for whoever manages the website and covers everything urgent.

2. Ask us anything by email

Questions about a finding? Write to info@nyorsoft.com and quote the finding ID (e.g. F-04). We reply in writing.

3. Optional: confirm the fixes

With the **Retest of Key Fixes** add-on we re-check the Critical and High findings and issue an updated certificate.

4. Stay on top of it

Scripts and subdomains change over time. The **Quarterly Re-Check** repeats these checks four times a year.

Limitations

This review 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 website is free of other vulnerabilities. Version-based findings rely on information the website reveals and on public advisories. Nyorsoft did not access, download or modify any non-public data.

This is a sample report. Mesa Ridge Legal Group, the domain mesaridgelegal.example, Chatperch and all findings are fictional and were created to show the format and depth of a Nyorsoft External Website Security Review. Any resemblance to a real business is unintended.