SAMPLE REPORT · ILLUSTRATIVE ONLY · NOT AN ACTUAL SCAN

Website Security Report

Sample report · prepared for Riverside Family Law, PLLC

PREPARED FOR	**Riverside Family Law, PLLC**
TARGET	**https://www.riversidefamilylaw.com**
SCAN TYPE	**Full Scan**
SCAN STARTED	**Apr 15, 2026, 9:42:18 AM PDT**
SCAN DURATION	**22 minutes, 18 seconds**
GENERATED	**Apr 15, 2026**
GENERATED BY	**RiskMeter Cybersecurity**

This is a sample document. Findings, target, and metadata are fabricated for demonstration purposes. Real RiskMeter reports describe actual scans of explicitly authorized assets.

SAMPLE · ILLUSTRATIVE

Threat level

High

One or more high-severity vulnerabilities were discovered. A malicious user can exploit these issues to obtain credentials, deface the site, or intercept client communication. Address the High-severity findings first.

Scan detail

Target	https://www.riversidefamilylaw.com
Scan type	Full Scan
Start time	Apr 15, 2026, 9:42:18 AM PDT
Scan duration	22 minutes, 18 seconds
Authentication profile	—

SAMPLE · ILLUSTRATIVE

Vulnerabilities found in this scan

Severity	Vulnerabilities	Instances
Critical	1	1
High	3	3
Medium	5	5
Low	4	4
Informational	4	4
Total	**17**	**17**

SAMPLE · ILLUSTRATIVE

Executive summary

The table below lists every vulnerability group found in this scan, ordered by severity. Each entry counts the number of distinct instances discovered against the target. For full evidence and remediation guidance, see the corresponding RiskMeter Technical Report.

Vulnerability group	Severity	Count
Backup file exposed (wp-config.php.bak)	Critical	1
.git repository exposed on web root	High	1
WordPress core is outdated (5.8.x — multiple known CVEs)	High	1
WordPress login page lacks rate limiting	High	1
Outdated jQuery 1.7.2 — multiple known XSS vulnerabilities	Medium	1
Directory listing enabled on /wp-content/uploads/	Medium	1
TLS/SSL weak cipher suites enabled	Medium	1
Contact form lacks CSRF protection	Medium	1
SSL certificate expires within 30 days	Medium	1
Cookies not marked as Secure	Low	1
Cookies not marked as HttpOnly	Low	1
HSTS header missing	Low	1
X-Frame-Options header missing (clickjacking)	Low	1
Server version disclosed in HTTP header	Informational	1
WordPress version disclosed in generator meta tag	Informational	1
Email address disclosure in page source	Informational	1

SAMPLE · ILLUSTRATIVE

Vulnerability group	Severity	Count
Permissions-Policy header not implemented	Informational	1