Generated on : DD-MM--YYYY

Report

Website Security Audit

https://abccorp.com/

Generated By White Label IQ

INDEX

Executive Summary

This audit was conducted to review the security of the WordPress site, identify risks, and suggest improvements to strengthen protection.

The site has several strong protections already in place:

- SSL certificate is active and HTTPS enforced.
- Daily backups configured via WPEngine (30-day retention).
- Wordfence firewall and malware scanning enabled.
- Login protection, XML-RPC disabled, and strong passwords enforced.
- Logging and monitoring configured (login attempts, file changes, suspicious activity alerts).

⚠️ However, there are areas needing improvement:

- 2FA (Two-Factor Authentication) not enabled for admin accounts.
- Admin login access not restricted by IP.
- Database prefix still using default wp_.
- Missing key security headers (e.g., CSP, Referrer-Policy).
- Outdated plugins (e.g., Elementor, Yoast SEO).
- Unused themes should be removed.

By resolving these issues, the site will be much harder to exploit and better prepared against attacks.

Core Findings Overview

Category	Status	What We Found
WordPress Version	Updated	Site is running v6.8.2 (latest).
Theme Editing	Enabled	WP theme editor is active – should be disabled.
WordPress Version Exposure	Hidden	Version is not publicly visible.
Debug Mode	Off	Debugging correctly disabled.
Strong Passwords	Enforced	All users must use strong passwords.
Admin URL	Changed	Default login URL is hidden (WPS Hide Login active).
2FA (Admin)	Disabled	2FA not enabled for admin accounts.
Admin IP Restriction	Not Set	Admin access not locked to IP addresses.
Login Attempts	Limited	Brute force protection is active.
XML-RPC	Disabled	XML-RPC disabled to prevent attacks.

Category	Status	What We Found
DB Prefix	Default	Using default wp_ prefix. Vulnerable to attacks.
DB Backups	Configured	30-day daily backups active.
DB Access	Restricted	Access locked via hosting, secure.
Security Headers	Missing	Content-Security-Policy and Referrer-Policy missing.
Firewall	Active	Wordfence installed and configured.
Directory Listing	Disabled	Properly disabled on server.
File Monitoring	Enabled	Alerts active, need target email configured.

Section Summary: Most protections are in place, but missing 2FA, default DB prefix, and missing security headers remain the main risks

Plugin & Theme Inventory

Plugins

Plugin Name	Current Version	Recommended Version	Status	Notes
Elementor	3.31.2	3.31.3	Outdated	Update required
Yoast SEO	25.7	25.8	Outdated	Update required
Gravity Forms	2.9.17.1 / 2.9.16 / 2.9.15 / 2.9.14 / 2.9.13	Latest	Up-to-date	Multiple versions active – consolidate to latest stable version
Wordfence Security	8.1.0 / 8.0.5	Latest	Up-to-date	Ensure only latest version is active
WPS Hide Login	1.9.17.2	Latest	Up-to-date	Login URL hidden
Max Mega Menu	3.6.2	Latest	Up-to-date	No issues
Genesis Blocks	3.1.7	Latest	Up-to-date	No issues
Duplicate Page	4.5.5	Latest	Up-to-date	No issues
Disable Comments	2.5.2	Latest	Up-to-date	No issues
Contact Form 7	6.1.1	Latest	Up-to-date	No issues
Redirection	5.5.2	Latest	Up-to-date	No issues

Theme

Theme Name	Version	Status	Severity	Notes
Texam	1.4.0	Up-to-date	Up-to-date ⌄	Texam
Texam Child	1.4.0	Up-to-date	Up-to-date ⌄	Texam Child
Other Themes	–	Should be removed	Can be removed ⌄	Other Themes

Section Summary: Most plugins and themes are current, but Elementor and Yoast SEO need updates. Multiple old versions of Gravity Forms and Wordfence should be cleaned up.

Recommendations

Below are our recommendations, grouped by urgency.

🔴 Critical (Immediate Action)

These are the most serious issues and must be fixed right away. If not, hackers could break into the site, steal information, or even take control of it.

- Enable Two-Factor Authentication (2FA) for all Admin accounts.
- Restrict Admin access by IP to trusted networks.
- Update Elementor → 3.31.3 and Yoast SEO → 25.8.
- Address default database prefix (wp_) in future builds or development.

🟠 High Priority (Within 1 Week)

These issues aren't as urgent as critical ones but can still cause problems if ignored.Old plugins are easy targets for hackers, and broken backups mean the site may not be recoverable.

- Remove unused/abandoned plugins and themes.

🟡 Medium Priority (Within 2–3 Weeks)

These are improvements that make the site stronger and safer for the future. While not an immediate danger, delaying them makes the site more open to risks over time.

- Consolidate Gravity Forms versions to latest stable.
- Configure file change monitoring alerts in Wordfence.
- Monitor access logs and block suspicious/spam requests.

🔵 Ongoing Maintenance

Website security is not a one-time fix – it needs constant care. Without regular updates, even a secure site can become unsafe.

- Keep backups running and stored in a safe place.
- Review and update plugins and themes regularly.
- Check admin accounts often and remove unused ones.
- Keep firewall and malware tools updated.

Section Summary: Fix plugin issues immediately, enable 2FA and secure database within a week, and complete server/IP restrictions within 2–3 weeks.

Implementation Roadmap

Timeline	Action Items
Immediate	Update Elementor & Yoast SEO. Remove duplicate plugin versions.
1 Week	Enable 2FA, change DB prefix, remove unused themes.
2–3 Weeks	Restrict admin logins by IP, add missing security headers, set file change alert emails.
Ongoing	Quarterly audits, keep plugins/themes updated, test backups, monitor Wordfence alerts.

Section Summary: The roadmap shows what needs fixing first and what can wait a bit. Critical issues should be solved right away, while other improvements can be scheduled over the next few weeks.

Conclusion

The website has a solid security foundation, but urgent fixes (2FA, admin IP restriction, outdated plugins, DB prefix) are needed.

By implementing these recommendations and following the roadmap:

✅ Reduce risk of hacks and malware
✅ Protect data and customer information
✅ Ensure site restorability via backups
✅ Build long-term trust with visitors

WHITE LABEL IQ

Security Audit Report

https://abccorp.com/

This comprehensive security audit has identified key areas for improvement to ensure your website maintains a strong security posture. The findings presented in this report provide a clear roadmap for enhancing security and protecting against potential cyber threats.

We recommend prioritizing the critical and high-risk issues identified, as these pose the most significant security risks. The implementation of the recommended security measures will significantly improve your website's security profile and reduce exposure to potential attacks.

Thank you for choosing White Label IQ for your security needs. We're committed to helping you maintain a secure and protected digital presence.