Summary of **www.plexeltech.com** [Desktop version] Website Security Test

Provided "as is" without any warranty of any kind.

www.plexeltech.com was tested **9** times during the last **12** months.

Your final score:

A
B
C
F

A

Date/Time:	Nov 21st, 2026 11:31 GMT+0
Server IP:	172.64.80.1
Reverse DNS:	-
Location:	N/A
Version:	for desktop

Test Results Summary for www.plexeltech.com

One third-party web software dependancy was identified. It appears to be outdated, but no known vulnerabilities were detected. No Content Management System (CMS) was identified. One CMS component, JS-library or framework was identified: react. Show details.

No obvious GDPR-related compliance issues were detected across Privacy Policy, Website Security, TLS Encryption, Cookie Protection, Cookie Disclaimer. The following checks were not performed, as no corresponding cookies with personal or tracking information seem to be sent by the website: Cookie Protection, Cookie Disclaimer. Show details.

The website is compliant with PCI DSS Requirement 6.3, while being non-compliant with Requirement 6.4. Show details.

Issues were identified with key security header misconfigured Content-Security-Policy. Optional HTTP headers appear to be properly configured: Server, Permissions-Policy, Referrer-Policy, Cache-Control. Show details.

Full Test Results: https://www.immuniweb.com/websec/www.plexeltech.com/JCSjzCKM/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2026 ImmuniWeb SA

Content-Security-Policy is enforced and appears to be properly configured. A report-only Content-Security-Policy is not present. Show details.

No cookies were detected. Show details.

27 external requests detected; all requests completed successfully. SRI is correctly implemented for one third-party JavaScript or CSS file. Show details.

6 robots.txt rules and 6 bot protection mechanisms detected. No protection detected via User-Agent blocks or meta restrictions. Additional anti-scraping protection appears to be provided by external infrastructure. Show details.

Compliance Summary for www.plexeltech.com

PCI DSS Compliance Failed: The website is compliant with PCI DSS Requirement 6.3, while being non-compliant with Requirement 6.4.

Full Test - Table of Contents

- Web Server Configuration Test
- Web Software Security Test
- GDPR Compliance Test
- PCI DSS Compliance Test
- HTTP Headers Security Test
- Content Security Policy (CSP) Test
- Cookies Privacy and Security Test
- External Content Security Test
- Protection from Data Scraping Test

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

Upgrade to ImmuniWeb® AI Platform

Take Your Security Testing to the Next Level



Continuous Threat Exposure Management with ImmuniWeb® Discovery



Web Application Penetration Testing with ImmuniWeb® On-Demand



Continuous Web Scanning and Penetration Testing with ImmuniWeb® Continuous

FREE DEMO

Corporate Datasheet [PDF]

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

Web Server Configuration Test

HTTP RESPONSE

200

HTTP VERSIONS

HTTP/1.0 HTTP/1.1 HTTP/2 HTTP/3

NPN

H2 HTTP/1.1

ALPN

H2

CONTENT ENCODING

GZIP BR ZSTD

SERVER SIGNATURE

cloudflare

WAF

No WAF detected

LOCATION

N/A

HTTP METHODS ENABLED

✔ GET ✔ HEAD

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

Web Software Security Test

Web Software Found	Web Software Outdated	Web Software Vulnerabilities
1	1	0

The following security vulnerabilities are known to be present in the fingerprinted version of web software. To run a comprehensive vulnerability scan of your web application, please use ImmuniWeb® Neuron.

Fingerprinted Software & Vulnerabilities

No CMS were fingerprinted on the website.	Information

Fingerprinted Software Components & Vulnerabilities

React 19.3.0-canary-278794d7-20261002

The component is outdated. No known security vulnerabilities found. Update to the most recent version **19.3.1**.

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

GDPR Compliance Test

If the website processes or stores personal data of the EU residents, the following requirements of EU GDPR may apply:

PRIVACY POLICY

Privacy Policy was found on the website.	Good configuration

WEBSITE SECURITY

No publicly known vulnerabilities were found in the website CMS or its components.	Good configuration

TLS ENCRYPTION

HTTPS encryption is present on the web server.	Good configuration

COOKIE PROTECTION

No cookies with personal or tracking information seem to be sent.	Information

COOKIE DISCLAIMER

No third-party cookies or cookies with tracking information seem to be sent.	Information

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

PCI DSS Compliance Test

If the website falls into a CDE (Cardholder Data Environment) scope, the following Requirements of PCI DSS may apply:

REQUIREMENT 6.3

No publicly known vulnerabilities seem to be present in the fingerprinted versions of the website CMS and its components.	Good configuration

REQUIREMENT 6.4

No WAF was detected on the website. Implement a WAF to protect the website against common web attacks.	Misconfiguration or weakness

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

HTTP Headers Security Test

Some HTTP headers related to security and privacy are missing or misconfigured.	Misconfiguration or weakness

MISSING OPTIONAL HTTP HEADERS

Access-Control-Allow-Origin

SERVER

Web server does not disclose its version.	Good configuration

Raw HTTP Header

```
Server: cloudflare
```

STRICT-TRANSPORT-SECURITY (HSTS)

The header is properly set.	Good configuration

Raw HTTP Header

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

Directives

Name	Description	Alerts
max-age	Sets the time browsers must enforce the use of HTTPS to browse the website.	No problems found

X-FRAME-OPTIONS

The header is properly set.	Good configuration
The header value is not consistent with Content-Security-Policy.	Information

Full Test Results: https://www.immuniweb.com/websec/www.plexeltech.com/JCSjzCKM/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2026 ImmuniWeb SA

Raw HTTP Header

```
X-Frame-Options: DENY
```

X-CONTENT-TYPE-OPTIONS

The header is properly set.	Good configuration

Raw HTTP Header

```
X-Content-Type-Options: nosniff
```

PERMISSIONS-POLICY

The header is properly set.	Good configuration

Raw HTTP Header

```
Permissions-Policy: camera=(), microphone=(), geolocation=(), payment=()
```

REFERRER-POLICY

The header is properly set.	Good configuration

Raw HTTP Header

```
Referrer-Policy: strict-origin-when-cross-origin
```

CACHE-CONTROL

The header is properly set.	Good configuration

Raw HTTP Header

```
Cache-Control: no-cache, no-store, must-revalidate
```


This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

Content Security Policy (CSP) Test

CONTENT-SECURITY-POLICY (CSP)

Content-Security Policy is enforced.	Good configuration

Raw HTTP Header

```
Content-Security-Policy: default-src 'self'; script-src 'nonce-AKhJF1C+fTi0cXkYrvJYew==' 'strict-dynamic' 'self' https://challenges.cloudflare.com https://static.cloudflareinsights.com; style-src 'self' 'unsafe-inline'; img-src 'self' data: https://assets.plexeltech.com; media-src https://assets.plexeltech.com; font-src 'self'; connect-src 'self' https://api.plexeltech.com https://cloudflareinsights.com; frame-src https://challenges.cloudflare.com; object-src 'none'; base-uri 'self'; form-action 'self'; frame-ancestors 'none'; upgrade-insecure-requests ;
```

Directives

Name	Description	Alerts
default-src	The default-src directive serves as a fallback for the other fetch directives. 'self' - Keyword is OK	No problems found
script-src	Restricts the locations from which scripts may be executed. 'nonce-AKhJF1C+fTi0cXkYrvJYew==' - Nonce is OK 'strict-dynamic' - Keyword is OK 'self' - Keyword is OK https://challenges.cloudflare.com - URL is OK. https://static.cloudflareinsights.com - URL is OK.	No problems found

Full Test Results: https://www.immuniweb.com/websec/www.plexeltech.com/JCSjzCKM/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2026 ImmuniWeb SA

Name	Description	Alerts
style-src	Restricts the locations from which style may be applied to a Document. 'self' - Keyword is OK 'unsafe-inline' - Keyword is OK	No problems found
img-src	Restricts the URLs from which image resources may be loaded. 'self' - Keyword is OK data: - Scheme is OK https://assets.plexeltech.com - URL is OK.	No problems found
media-src	Restricts the URLs from which video, audio, and associated text track resources may be loaded. https://assets.plexeltech.com - URL is OK.	No problems found
font-src	Restricts the URLs from which font resources may be loaded. 'self' - Keyword is OK	No problems found
connect-src	Controls requests which transmit or receive data from other origins using script interfaces. 'self' - Keyword is OK https://api.plexeltech.com - URL is OK. https://cloudflareinsights.com - URL is OK.	No problems found
frame-src	Restricts the URLs which may be loaded into nested browsing contexts (frames).	No problems found

Full Test Results: https://www.immuniweb.com/websec/www.plexeltech.com/JCSjzCKM/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2026 ImmuniWeb SA

Name	Description	Alerts
	https://challenges.cloudflare.com - URL is OK.	
object-src	Restricts the URLs from which plugin content may be loaded. 'none' - Keyword is OK	No problems found
base-uri	Restricts the URLs which can be used in a Document's base element. 'self' - Keyword is OK	No problems found
form-action	Restricts the URLs which can be used as the target of a form submissions from a given context. 'self' - Keyword is OK	No problems found
frame-ancestors	Restricts the URLs which can embed the resource using frame, iframe, object, or embed. 'none' - Keyword is OK	No problems found
require-trusted-types-for	MISSING: The HTTP Content-Security-Policy (CSP) require-trusted-types-for Experimental directive instructs user agents to control the data passed to DOM XSS sink functions, like Element.innerHTML setter. Consider requiring Trusted Types for scripts to lock down DOM XSS injection sinks. You can do this by adding "require-trusted-types-for 'script'" to your policy.	Information

CONTENT-SECURITY-POLICY-REPORT-ONLY

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

The header was not sent by the server.	Information

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

Cookies Privacy and Security Test

No cookies were sent by the web application.	Good configuration

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

External Content Security Test

SUBRESOURCE INTEGRITY

Subresource Integrity (SRI) is a security feature that allows browsers to verify that fetched resources (scripts and stylesheets) are delivered without unexpected alterations. The integrity of third-party resources is ensured by validating their cryptographic hashes.

SRI is correctly implemented for all third-party JavaScripts and CSS.	Good configuration

EXTERNAL CONTENT

External web content (e.g. images, video, CSS or JavaScript) can improve website loading time. However, the external content can also put privacy of website visitors at risk given that some information about them is transmitted to the third parties operating the external resources, sometimes even without proper HTTPS encryption or user consent.

External HTTP Requests	Failed HTTP Requests
27	0

assets.plexeltech.com

- https://assets.plexeltech.com/v/stack/openai.98480cb4.svg
- https://assets.plexeltech.com/v/stack/microsoft365.064e7297.svg
- https://assets.plexeltech.com/v/social/linkedin.50df151a.svg
- https://assets.plexeltech.com/v/stack/googleworkspace.437e4866.svg
- https://assets.plexeltech.com/v/stack/anthropic.1a77aaf9.svg
- https://assets.plexeltech.com/v/stack/cloudflare.6b3490a3.svg
- https://assets.plexeltech.com/v/stack/python.5b00bca1.svg
- https://assets.plexeltech.com/v/stack/swift.7e903c52.svg

Full Test Results: https://www.immuniweb.com/websec/www.plexeltech.com/JCSjzCKM/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2026 ImmuniWeb SA

https://assets.plexeltech.com/v/stack/react.f2cadfd0.svg

https://assets.plexeltech.com/v/stack/slack.c3cb1240.svg

https://assets.plexeltech.com/v/stack/kubernetes.845f6768.svg

https://assets.plexeltech.com/v/stack/jira.7cc5c9b0.svg

https://assets.plexeltech.com/v/stack/elasticsearch.a343a64f.svg

https://assets.plexeltech.com/v/stack/rust.ea9dec17.svg

https://assets.plexeltech.com/v/stack/postgresql.f1b685de.svg

https://assets.plexeltech.com/v/stack/kotlin.c14d02fb.svg

https://assets.plexeltech.com/v/stack/qdrant.e620b073.svg

https://assets.plexeltech.com/v/stack/clickhouse.0738f531.svg

https://assets.plexeltech.com/v/stack/huggingface.9eecf74e.svg

https://assets.plexeltech.com/brand/favicon.ico

https://assets.plexeltech.com/v/rail/quickbooks.2b15f324.svg

https://assets.plexeltech.com/v/rail/zoho.5a5d454a.svg

https://assets.plexeltech.com/v/rail/sap.0a4475a6.svg

https://assets.plexeltech.com/v/rail/xero.a871c564.svg

https://assets.plexeltech.com/v/rail/sage.bbdd25e0.svg

https://assets.plexeltech.com/v/rail/json.8cbb06b0.svg

static.cloudflareinsights.com

https://static.cloudflareinsights.com/beacon.min.js/vce701823e78c4301a35b7e07294d87301792088814092 SRI

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

Protection from Data Scraping Test

Many companies rely on AI bots to scrape website content, using the collected data to train their machine learning models. To safeguard information, website owners can apply different techniques to detect, limit, or block scraping activities carried out by these bots.

Robots.txt Rules	User-Agent Blocks	Meta Tags	Protection vs. Bots
6	0	0	6

This site is behind Cloudflare: AI crawlers are blocked by default unless explicitly allowed in the domain's AI Crawl Control settings.	Good configuration

Default Rules

The website has the following default access rules for all crawlers defined in robots.txt, unless overridden by more specific rules below.

```
User-agent: *
Allow: /
Disallow: /logo-preview.html
```

Raw Value

GPTBot by OpenAI

Robots.txt Directives

Rule found for GPTBot User-Agent in robots.txt.	Good configuration

```
User-agent: GPTBot
Disallow: /
```

Raw Value

Full Test Results: https://www.immuniweb.com/websec/www.plexeltech.com/JCSjzCKM/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2026 ImmuniWeb SA

Server-side Blocking

No server-side User-Agent-based blocking detected for GPTBot.	Information

Gemini by Google

To control whether your website's content can be used to train Google's AI models (such as Gemini), Google follows the special Google-Extended User-Agent directive in your robots.txt file.

Robots.txt Directives

Rule found for Google-Extended User-Agent in robots.txt.	Good configuration
`User-agent: Google-Extended` `Disallow: /`	Raw Value

However, Google-Extended does not crawl your site directly. Instead, it respects the access granted to other Google crawlers: Googlebot, Googlebot-Image, Googlebot-Video, Googlebot-News, GoogleOther, GoogleOther-Image, GoogleOther-Video.

No rule is specified for Google in robots.txt; default rules apply.	Information

Claude by Anthropic

Robots.txt Directives

Rule found for ClaudeBot User-Agent in robots.txt.	Good configuration
`User-agent: ClaudeBot` `Disallow: /`	Raw Value
No specific rule for Claude-User, Claude-SearchBot User-Agent(s) was found in robots.txt; default rules apply.	Information

Server-side Blocking

Full Test Results: https://www.immuniweb.com/websec/www.plexeltech.com/JCSjzCKM/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2026 ImmuniWeb SA

No server-side User-Agent-based blocking detected for ClaudeBot, Claude-User, Claude-SearchBot.	Information

Perplexity by Perplexity AI

Robots.txt Directives

No specific rule for PerplexityBot User-Agent(s) was found in robots.txt; default rules apply.	Information

Server-side Blocking

No server-side User-Agent-based blocking detected for PerplexityBot, Perplexity-User.	Information

Copilot by Microsoft

Robots.txt Directives

No specific rule for bingbot User-Agent(s) was found in robots.txt; default rules apply.	Information

Meta Tag Restrictions

No meta tag restricting usage of website's content found.	Information

Server-side Blocking

No server-side User-Agent-based blocking detected for Bingbot, BingPreview.	Information

DeepSeek by Hangzhou DeepSeek Artificial Intelligence

DeepSeek does not have public policy confirming that it will follow rules as defined in robots.txt. Use server-side blocking based on User-Agent to restrict access.

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

Server-side Blocking

No server-side User-Agent-based blocking detected for DeepSeekBot.	Information

Meta AI by Meta

Robots.txt Directives

Rule found for Meta-ExternalAgent User-Agent in robots.txt.	Good configuration
`User-agent: Meta-ExternalAgent` `Disallow: /`	Raw Value

Server-side Blocking

No server-side User-Agent-based blocking detected for Meta AI Crawler.	Information

AmazonBot by Amazon

Robots.txt Directives

Rule found for AmazonBot User-Agent in robots.txt.	Good configuration
`User-agent: AmazonBot` `Disallow: /`	Raw Value

Meta Tag Restrictions

No meta tag restricting usage of website's content found.	Information

Server-side Blocking

No server-side User-Agent-based blocking detected for Amazonbot.	Information

Full Test Results: https://www.immuniweb.com/websec/www.plexeltech.com/JCSjzCKM/

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com

Copyright © 2026 ImmuniWeb SA

Apple Intelligence by Apple

To control whether your website's content can be used to train Apple's AI models (Apple Intelligence), Apple follows the special Applebot-Extended User-Agent directive in your robots.txt file.

Robots.txt Directives

Rule found for AppleBot-Extended User-Agent in robots.txt.	Good configuration

`User-agent: AppleBot-Extended` `Disallow: /`	Raw Value

Applebot-Extended does not crawl your site directly. Instead, it respects the access granted to other Apple crawlers: Applebot. If no Applebot rule is present, Applebot follows the rules defined for Googlebot.

No rule is specified for Apple was found in robots.txt; general rules apply.	Information

Server-side Blocking

No server-side User-Agent-based blocking detected for Applebot.	Information

Doubao by ByteDance

Doubao is an AI chatbot developed by ByteDance, the company behind TikTok. ByteDance operates the Bytespider web crawler, which may collect website content — potentially for training Doubao and other AI models. ByteDance does not have a public policy confirming that Bytespider will follow robots.txt rules. Use server-side blocking based on User-Agent to restrict access.

Server-side Blocking

No server-side User-Agent-based blocking detected for Bytespider.	Information

Custom Bot

A custom test crawler User-Agent used to check for simple keyword-based User-Agent blocks. Not associated with any real service and does not actually crawl the content on websites.

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

Server-side Blocking

No server-side User-Agent-based blocking detected for Custom Bot.	Information

This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA

Upgrade to ImmuniWeb® AI Platform

Take Your Security Testing to the Next Level

Continuous Threat Exposure Management with ImmuniWeb® Discovery

Web Application Penetration Testing with ImmuniWeb® On-Demand

Continuous Web Scanning and Penetration Testing with ImmuniWeb® Continuous

FREE DEMO

Corporate Datasheet [PDF]

The End of Report

Upgrade from Free Community Edition to ImmuniWeb® AI Platform



This document is intellectual property of ImmuniWeb SA and must never be used for any commercial purposes without express written permission. Please report any violations to info@immuniweb.com
Copyright © 2026 ImmuniWeb SA