Scan your site now

lixt-ws.z01.azurefd.net **Scan**

☐ Hide results ☑ Follow redirects

Security Report Summary

A

Site:	https://lixt-ws.z01.azurefd.net/
IP Address:	2620:1ec:46::69
Report Time:	17 Nov 2021 13:11:54 UTC
Headers:	✓ X-Content-Type-Options ✓ X-Frame-Options ✓ Content-Security-Policy ✓ Referrer-Policy ✓ Strict-Transport-Security ✗ Permissions-Policy

Raw Headers

HTTP/1.1	401
Cache-Control	no-store
Keep-Alive	timeout=60
Pragma	no-cache
Content-Length	102
Content-Type	application/json
Set-Cookie	ARRAffinity=a7ddb0ec2e2faaf6f2acfc91e17093ad766adb7e8c28eb6e3d180f7c0861f8bd;Path=/;**HttpOnly**;**Secure**;Domain=lixt-ws.azurewebsites.net
Set-Cookie	ARRAffinity**SameSite**=a7ddb0ec2e2faaf6f2acfc91e17093ad766adb7e8c28eb6e3d180f7c0861f8bd;Path=/;**HttpOnly**;**SameSite**=None;**Secure**; Domain=lixt-ws.azurewebsites.net
WWW-Authenticate	Bearer realm="null", error="unauthorized", error_description="Full authentication is required to access this resource"
Access-Control-Allow-Origin	*
Access-Control-Allow-Methods	*
Access-Control-Max-Age	3600
Access-Control-Allow-Headers	*
X-Content-Type-Options	**nosniff**
X-XSS-Protection	**1**; **mode**=block
X-Frame-Options	**DENY**
X-Cache	CONFIG_NOCACHE
Content-Security-Policy	**script-src** *'self'* https://lixt-ws.azurewebsites.net
Referrer-Policy	**same-origin**
Strict-Transport-Security	**max-age**=31536000; **includeSubDomains**
X-Azure-Ref	0mv+UYQAAAAA5Wdgq4uEMSZygnjTSo7V+U0pDRURHRTA1MTEANjc4NGExMWMtN2ZhOS00MzI1LWJiMTYtZThmNmI5N2UwN2Zm
Date	Wed, 17 Nov 2021 13:11:54 GMT

Missing Headers

Permissions-Policy	Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser.

Upcoming Headers

Expect-CT	Expect-CT allows a site to determine if they are ready for the upcoming Chrome requirements and/or enforce their CT policy.

Cross-Origin-Embedder-Policy	Cross-Origin Embedder Policy allows a site to prevent assets being loaded that do not grant permission to load them via CORS or CORP.
Cross-Origin-Opener-Policy	Cross-Origin Opener Policy allows a site to opt-in to Cross-Origin Isolation in the browser.
Cross-Origin-Resource-Policy	Cross-Origin Resource Policy allows a resource owner to specify who can load the resource.

Additional Information

Access-Control-Allow-Origin	This is a very lax CORS policy. Such a policy should only be used on a public CDN.
X-Content-Type-Options	X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".
X-XSS-Protection	X-XSS-Protection sets the configuration for the XSS Auditor built into older browsers. The recommended value was "X-XSS-Protection: 1; mode=block" but you should now look at Content Security Policy instead.
X-Frame-Options	X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking.
Content-Security-Policy	Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. Analyse this policy in more detail. You can sign up for a free account on Report URI to collect reports about problems on your site.
Referrer-Policy	Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.
Strict-Transport-Security	HTTP Strict Transport Security is an excellent feature to support on your site and strengthens your implementation of TLS by getting the User Agent to enforce the use of HTTPS.