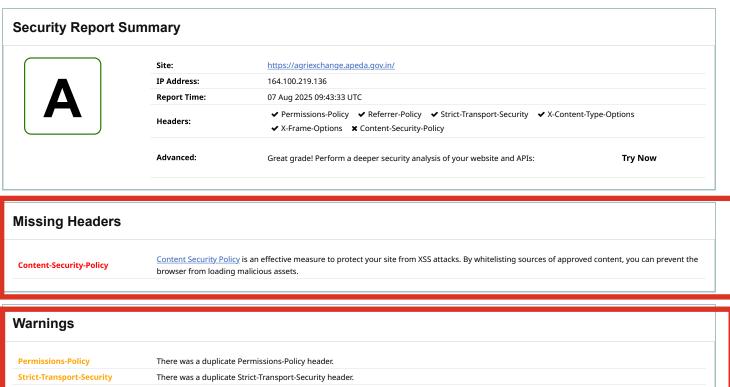
Home About API

Scan your site now

https://agriexchange.apeda.gov.in Scan ☐ Hide results ✓ Follow redirects



warmigo	
Permissions-Policy	There was a duplicate Permissions-Policy header.
Strict-Transport-Security	There was a duplicate Strict-Transport-Security header.
X-Content-Type-Options	There was a duplicate X-Content-Type-Options header.
X-Frame-Options	There was a duplicate X-Frame-Options header.

HTTP/1.1	200 OK
Access-Control-Allow-Headers	Content-Type, Authorization
Access-Control-Allow-Methods	GET, POST
Access-Control-Allow-Origin	*
Cache-Control	no-cache,no-store
Content-Encoding	gzip
Content-Type	text/html; charset=utf-8
Date	Thu, 07 Aug 2025 09:43:33 GMT
Expires	-1
Permissions-Policy	accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Permissions-Policy	geolocation=(), microphone=(), camera=()
Pragma	no-cache
Referrer-Policy	no-referrer
Referrer-Policy	no-referrer-when-downgrade
Set-Cookie	.AspNetCore.Session=CfDJ8A49gPZ2JjdPvfL4HnYGxta5NNJQchDZLRsbM%2Fg1pYrnILlCB0ZCTFEXRcuYROmDqbu7nXvNfOFvI9qovTvdGwQI9mvCYRKTT wi3p2XHCTDWycYqRcaaWi31ZWDvUh5avT6Gl%2FFaN48C3LjCvvM0vx6AUy4UAI3IAvZdErgfh%2BQl; path=/; secure; samesite=strict; httponly

1 of 2 07-08-2025, 15:14

Strict-Transport-Security	max-age=2592000
Strict-Transport-Security	max-age=63072000; includeSubDomains; preload
Vary	Accept-Encoding
X-Content-Type-Options	nosniff
X-Content-Type-Options	nosniff
X-Frame-Options	DENY
X-Frame-Options	SAMEORIGIN
X-Permitted-Cross-Domain- Policies	none
X-Xss-Protection	1; mode=block
X-Xss-Protection	1; mode=block
Transfer-Encoding	chunked

Upcoming Headers	
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.	
Permissions-Policy	<u>Permissions Policy</u> is a new header that allows a site to control which features and APIs can be used in the browser.	
Permissions-Policy	<u>Permissions Policy</u> is a new header that allows a site to control which features and APIs can be used in the browser.	
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 an should be set by all sites.	
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 an should be set by all sites.	
Set-Cookie	There is no <u>Cookie Prefix</u> on this cookie.	
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.	
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.	
K-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".	
K-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".	
K-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 car defend against attacks like clickjacking.	
(-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.	
(-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.	
(-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.	

2 of 2