ZAP by Checkmarx Scanning Report

Site: https://aihmctbangalore.edu.in:4415

Generated on Thu, 8 May 2025 18:57:23

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	0
Informational	1

Alerts

Name	Risk Level	Number of Instances
CSP: Failure to Define Directive with No Fallback	Medium	3
CSP: script-src unsafe-eval	Medium	6
CSP: script-src unsafe-inline	Medium	6
CSP: style-src unsafe-inline	Medium	6
Re-examine Cache-control Directives	Informational	1

Alert Detail

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing /excluding them is the same as allowing anything.
URL	https://aihmctbangalore.edu.in:4415
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://aihmctbangalore.edu.in:4415/robots.txt

Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://aihmctbangalore.edu.in:4415/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: script-src unsafe-eval**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://aihmctbangalore.edu.in:4415
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	script-src includes unsafe-eval.
URL	https://aihmctbangalore.edu.in:4415
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com;

	connect-src 'self'; frame-src https://maps.google.com; object-src 'none'; frame-ancestors 'self'; form-action 'self';
Other Info	script-src includes unsafe-eval.
URL	https://aihmctbangalore.edu.in:4415/robots.txt
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	script-src includes unsafe-eval.
URL	https://aihmctbangalore.edu.in:4415/robots.txt
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none'; frame-ancestors 'self'; form-action 'self';
Other Info	script-src includes unsafe-eval.
URL	https://aihmctbangalore.edu.in:4415/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	script-src includes unsafe-eval.
URL	https://aihmctbangalore.edu.in:4415/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none'; frame-ancestors 'self'; form-action 'self';
Other Info	script-src includes unsafe-eval.
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693

WASC Id	15
Plugin Id	10055

Medium	CSP: script-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://aihmctbangalore.edu.in:4415
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	script-src includes unsafe-inline.
URL	https://aihmctbangalore.edu.in:4415
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none'; frame-ancestors 'self'; form-action 'self';
Other Info	script-src includes unsafe-inline.
URL	https://aihmctbangalore.edu.in:4415/robots.txt
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	script-src includes unsafe-inline.
URL	https://aihmctbangalore.edu.in:4415/robots.txt
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none'; frame-ancestors 'self'; form-action 'self';
Other Info	script-src includes unsafe-inline.
URL	https://aihmctbangalore.edu.in:4415/sitemap.xml
Method	GET

Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	script-src includes unsafe-inline.
URL	https://aihmctbangalore.edu.in:4415/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none'; frame-ancestors 'self'; form-action 'self';
Other Info	script-src includes unsafe-inline.
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	**CSP: style-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://aihmctbangalore.edu.in:4415
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	style-src includes unsafe-inline.
URL	https://aihmctbangalore.edu.in:4415
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com;

	connect-src 'self'; frame-src https://maps.google.com; object-src 'none'; frame-ancestors 'self'; form-action 'self';
Other Info	style-src includes unsafe-inline.
URL	https://aihmctbangalore.edu.in:4415/robots.txt
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	style-src includes unsafe-inline.
URL	https://aihmctbangalore.edu.in:4415/robots.txt
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none'; frame-ancestors 'self'; form-action 'self';
Other Info	style-src includes unsafe-inline.
URL	https://aihmctbangalore.edu.in:4415/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none';
Other Info	style-src includes unsafe-inline.
URL	https://aihmctbangalore.edu.in:4415/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval' https://fonts.googleapis.com https://s.w.org https://maps.google.com; style-src 'self' 'unsafe-inline' https://fonts.googleapis.com; img-src 'self' data: https://s.w.org; font-src 'self' https://fonts.gstatic.com; connect-src 'self'; frame-src https://maps.google.com; object-src 'none'; frame-ancestors 'self'; form-action 'self';
Other Info	style-src includes unsafe-inline.
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693

WASC Id	15
Plugin Id	10055

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://aihmctbangalore.edu.in:4415
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015