Abatrades authentication ZAP scan

Site: https://mine-production-1f69.up.railway.app

Generated on Sun, 17 Aug 2025 17:02:23

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	3
Informational	3
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	5
Hidden File Found	Medium	4
Missing Anti-clickjacking Header	Medium	5
Strict-Transport-Security Header Not Set	Low	15
Timestamp Disclosure - Unix	Low	1
X-Content-Type-Options Header Missing	Low	15
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	5
Re-examine Cache-control Directives	Informational	5

Alert Detail

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including 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://mine-production-1f69.up.railway.app/

Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/privacy-policy
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/shop
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	Hidden File Found

Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	https://mine-production-1f69.up.railway.app/._darcs
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	https://mine-production-1f69.up.railway.app/.bzr
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	https://mine-production-1f69.up.railway.app/.hg
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	https://mine-production-1f69.up.railway.app/BitKeeper
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
Instances	4
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
CWE Id	538
WASC Id	13
Plugin Id	40035

Medium	**Missing Anti-clickjacking Header**
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://mine-production-1f69.up.railway.app/
Method	GET
Attack	
Evidence	
Other Info	

URL	https://mine-production-1f69.up.railway.app/privacy-policy
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/shop
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	5
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://mine-production-1f69.up.railway.app/
Method	GET
Attack	
Evidence	
Other Info	

URL	https://mine-production-1f69.up.railway.app/assets/1-BVcBmwPn.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/assets/abatrades-large-logo-CU7DyDI3.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/assets/abatrades-logo-C3DlW3kN.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/assets/abatrades-logo-other-BIqSh3Wd.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/assets/images1-Di9IrLYK.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/assets/images2-LjN6K-iw.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/assets/images4-BN-ha6US.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/assets/index-gGzm3YFI.js

Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/assets/index-WKikEGiP.css
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/assets/market-yHbBkQs5.jpg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/privacy-policy
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/shop
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	15
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://mine-production-1f69.up.railway.app/assets/index-gGzm3YFI.js
Method	GET
Attack	
Evidence	1540483477
Other Info	1540483477, which evaluates to: 2018-10-25 17:04:37.
Instances	1
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://mine-production-1f69.up.railway.app/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/assets/1-BVcBmwPn.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/assets/abatrades-large-logo-CU7DyDI3.png

Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/assets/abatrades-logo-C3DlW3kN.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/assets/abatrades-logo-other-BIqSh3Wd.png
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/assets/images1-Di9IrLYK.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/assets/images2-LjN6K-iw.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/assets/images4-BN-ha6US.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/assets/index-gGzm3YFI.js
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/assets/index-WKikEGiP.css
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/assets/market-yHbBkQs5.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/privacy-policy
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/robots.txt
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/shop
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://mine-production-1f69.up.railway.app/sitemap.xml
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	15
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://mine-production-1f69.up.railway.app/assets/index-gGzm3YFI.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "//popper.js.org)");let c=this._element;this._config.reference==="parent"?c=this._parent:u(this._config.reference)?c=l(this._conf", see evidence field for the suspicious comment/snippet.
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://mine-production-1f69.up.railway.app/
Method	GET
Attack	
Evidence	<script type="module" crossorigin src="/assets/index-gGzm3YFI.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://mine-production-1f69.up.railway.app/privacy-policy
Method	GET
Attack	

Evidence	<script type="module" crossorigin src="/assets/index-gGzm3YFI.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://mine-production-1f69.up.railway.app/robots.txt
Method	GET
Attack	
Evidence	<script type="module" crossorigin src="/assets/index-gGzm3YFI.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://mine-production-1f69.up.railway.app/shop
Method	GET
Attack	
Evidence	<script type="module" crossorigin src="/assets/index-gGzm3YFI.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://mine-production-1f69.up.railway.app/sitemap.xml
Method	GET
Attack	
Evidence	<script type="module" crossorigin src="/assets/index-gGzm3YFI.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	5
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	[10109](10109)

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://mine-production-1f69.up.railway.app/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/privacy-policy
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/robots.txt

Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/shop
Method	GET
Attack	
Evidence	
Other Info	
URL	https://mine-production-1f69.up.railway.app/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	5
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