altaShop ZAP Report

Sites: https://altashop-api.fly.dev https://alta-shop.vercel.app

Generated on Wed, 18 Jan 2023 16:11:15

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	3
Low	5
Informational	4

Alerts

Name	Risk Level	Number of Instances
Cloud Metadata Potentially Exposed	High	1
Content Security Policy (CSP) Header Not Set	Medium	1
Cross-Domain Misconfiguration	Medium	15
Missing Anti-clickjacking Header	Medium	1
Application Error Disclosure	Low	1
Private IP Disclosure	Low	2
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	18
Strict-Transport-Security Header Not Set	Low	31
X-Content-Type-Options Header Missing	Low	30
Information Disclosure - Suspicious Comments	Informational	8
Modern Web Application	Informational	1
Re-examine Cache-control Directives	Informational	16
Retrieved from Cache	Informational	16

Alert Detail

High	Cloud Metadata Potentially Exposed
Description	The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure. All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.
URL	https://alta-shop.vercel.app/latest/meta-data/
Method	GET
Attack	169.154.169.254

Evidence	
Instances	1
Solution	Do not trust any user data in NGINX configs. In this case it is probably the use of the $host variable which is set from the 'Host' header and can be controlled by an attacker.
Reference	https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/
CWE Id	
WASC Id	
Plugin Id	90034

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://alta-shop.vercel.app/
Method	GET
Attack	
Evidence	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
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 http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://alta-shop.vercel.app/
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/css/chunk-vendors.4ee89b31.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/css/products.9499f8c8.css

Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/css/transaction.d253099c.css
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/favicon.ico
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/fonts/fa-solid-900.55b416a8.woff2
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/js/about.2dfb0e5b.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/js/app.7d529d6c.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/js/auth-login.3f381918.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/js/auth-register.6346cfe3.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/js/auth.1e4c9cfd.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/js/chunk-vendors.c9f64bfb.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/js/order.6fab8a7d.js
Method	GET

Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/js/products.ddc11296.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://alta-shop.vercel.app/js/transaction.0141ad0b.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Instances	15
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Medium	Missing Anti-clickjacking Header
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	https://alta-shop.vercel.app/
Method	GET
Attack	
Evidence	
Instances	1
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	Application Error Disclosure
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	https://altashop-api.fly.dev/api/products/1/ratings

Method	POST
Attack	
Evidence	HTTP/1.1 500 Internal Server Error
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	90022

Low	**Private IP Disclosure**
Description	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	https://altashop-api.fly.dev/api/categories
Method	GET
Attack	
Evidence	10.0.0.1
URL	https://altashop-api.fly.dev/api/products
Method	GET
Attack	
Evidence	10.0.0.1
Instances	2
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP /PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Plugin Id	2

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://altashop-api.fly.dev/api/products/1
Method	DELETE
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/auth/info
Method	GET
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/categories
Method	GET

Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/categories/1
Method	GET
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/hello
Method	GET
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/orders
Method	GET
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/orders/1
Method	GET
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/products
Method	GET
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/products/1
Method	GET
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/products/1/comments
Method	GET
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/products/1/ratings
Method	GET
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/auth/login
Method	POST
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/auth/register
Method	POST
Attack	

Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/categories
Method	POST
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/orders
Method	POST
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/products
Method	POST
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/products/1/comments
Method	POST
Attack	
Evidence	Fly/e78c172f (2023-01-10)
URL	https://altashop-api.fly.dev/api/products/1/ratings
Method	POST
Attack	
Evidence	Fly/e78c172f (2023-01-10)
Instances	18
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10036

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://altashop-api.fly.dev/api/products/1
Method	DELETE
Attack	
Evidence	
URL	https://alta-shop.vercel.app/
Method	GET
Attack	

Evidence	
URL	https://alta-shop.vercel.app/css/chunk-vendors.4ee89b31.css
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/css/products.9499f8c8.css
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/css/transaction.d253099c.css
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/about.2dfb0e5b.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/app.7d529d6c.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/auth-login.3f381918.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/auth-register.6346cfe3.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/auth.1e4c9cfd.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/chunk-vendors.c9f64bfb.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/order.6fab8a7d.js
Method	GET
Attack	
Evidence	

URL	https://alta-shop.vercel.app/js/products.ddc11296.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/transaction.0141ad0b.js
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/auth/info
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/categories
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/categories/1
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/hello
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/orders
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/orders/1
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1/comments

Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1/ratings
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/auth/login
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/auth/register
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/categories
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/orders
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1/comments
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1/ratings
Method	POST
Attack	
Evidence	
Instances	31
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

	http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

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://altashop-api.fly.dev/api/products/1
Method	DELETE
Attack	
Evidence	
URL	https://alta-shop.vercel.app/
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/css/chunk-vendors.4ee89b31.css
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/css/products.9499f8c8.css
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/css/transaction.d253099c.css
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/favicon.ico
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/fonts/fa-solid-900.55b416a8.woff2
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/about.2dfb0e5b.js
Method	GET
Attack	

Evidence	
URL	https://alta-shop.vercel.app/js/app.7d529d6c.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/auth-login.3f381918.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/auth-register.6346cfe3.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/auth.1e4c9cfd.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/chunk-vendors.c9f64bfb.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/order.6fab8a7d.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/products.ddc11296.js
Method	GET
Attack	
Evidence	
URL	https://alta-shop.vercel.app/js/transaction.0141ad0b.js
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/auth/info
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/categories
Method	GET
Attack	
Evidence	

URL	https://altashop-api.fly.dev/api/categories/1
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/hello
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/orders
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/orders/1
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1/comments
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1/ratings
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/auth/login
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/categories
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/orders
Method	POST
Attack	
Evidence	

URL	https://altashop-api.fly.dev/api/products
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1/comments
Method	POST
Attack	
Evidence	
Instances	30
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	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx 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. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://alta-shop.vercel.app/js/app.7d529d6c.js
Method	GET
Attack	
Evidence	user
URL	https://alta-shop.vercel.app/js/auth-login.3f381918.js
Method	GET
Attack	
Evidence	query
URL	https://alta-shop.vercel.app/js/auth-register.6346cfe3.js
Method	GET
Attack	
Evidence	user
URL	https://alta-shop.vercel.app/js/chunk-vendors.c9f64bfb.js
Method	GET
Attack	
Evidence	from
URL	https://alta-shop.vercel.app/js/chunk-vendors.c9f64bfb.js
Method	GET
Attack	
Evidence	query
URL	https://alta-shop.vercel.app/js/chunk-vendors.c9f64bfb.js

Method	GET
Attack	
Evidence	user
URL	https://alta-shop.vercel.app/js/order.6fab8a7d.js
Method	GET
Attack	
Evidence	query
URL	https://alta-shop.vercel.app/js/transaction.0141ad0b.js
Method	GET
Attack	
Evidence	query
Instances	8
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	[200](200)
WASC Id	13
Plugin Id	[10027](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://alta-shop.vercel.app/
Method	GET
Attack	
Evidence	<script src="/js/chunk-vendors.c9f64bfb.js"></script>
Instances	1
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://altashop-api.fly.dev/api/products/1
Method	DELETE
Attack	
Evidence	
URL	https://alta-shop.vercel.app/
Method	GET
Attack	

Evidence	public, max-age=0, must-revalidate
URL	https://altashop-api.fly.dev/api/auth/info
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/categories
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/categories/1
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/hello
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/orders
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/orders/1
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1/comments
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1/ratings
Method	GET
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/auth/login
Method	POST
Attack	
Evidence	

URL	https://altashop-api.fly.dev/api/categories
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/orders
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products
Method	POST
Attack	
Evidence	
URL	https://altashop-api.fly.dev/api/products/1/comments
Method	POST
Attack	
Evidence	
Instances	16
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

Informational	Retrieved from Cache
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://alta-shop.vercel.app/
Method	GET
Attack	
Evidence	Age: 414
URL	https://alta-shop.vercel.app/
Method	GET
Attack	
Evidence	Age: 92484
URL	https://alta-shop.vercel.app/css/chunk-vendors.4ee89b31.css
Method	GET

Attack	
Evidence	Age: 4951711
URL	https://alta-shop.vercel.app/css/products.9499f8c8.css
Method	GET
Attack	
Evidence	Age: 0
URL	https://alta-shop.vercel.app/css/transaction.d253099c.css
Method	GET
Attack	
Evidence	Age: 4890239
URL	https://alta-shop.vercel.app/favicon.ico
Method	GET
Attack	
Evidence	Age: 4904663
URL	https://alta-shop.vercel.app/fonts/fa-solid-900.55b416a8.woff2
Method	GET
Attack	
Evidence	Age: 4904667
URL	https://alta-shop.vercel.app/js/about.2dfb0e5b.js
Method	GET
Attack	
Evidence	Age: 4886739
URL	https://alta-shop.vercel.app/js/app.7d529d6c.js
Method	GET
Attack	
Evidence	Age: 4947756
URL	https://alta-shop.vercel.app/js/auth-login.3f381918.js
Method	GET
Attack	
Evidence	Age: 17988
URL	https://alta-shop.vercel.app/js/auth-register.6346cfe3.js
Method	GET
Attack	
Evidence	Age: 4904668
URL	https://alta-shop.vercel.app/js/auth.1e4c9cfd.js
Method	GET
Attack	
Evidence	Age: 4900139
URL	https://alta-shop.vercel.app/js/chunk-vendors.c9f64bfb.js
Method	GET
Attack	

Evidence	Age: 4947775
URL	https://alta-shop.vercel.app/js/order.6fab8a7d.js
Method	GET
Attack	
Evidence	Age: 4904668
URL	https://alta-shop.vercel.app/js/products.ddc11296.js
Method	GET
Attack	
Evidence	Age: 4841676
URL	https://alta-shop.vercel.app/js/transaction.0141ad0b.js
Method	GET
Attack	
Evidence	Age: 4900780
Instances	16
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	
WASC Id	
Plugin Id	10050