ZAP Scanning Report

Site: https://vpntest2023.blob.core.windows.net

Generated on Wed, 9 Oct 2024 03:02:20

ZAP Version: 2.15.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	2
Informational	1
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	3
Strict-Transport-Security Header Not Set	Low	3
Non-Storable Content	Informational	3

Alert Detail

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://vpntest2023.blob.core.windows.net
Method	GET
Parameter	
Attack	
Evidence	Microsoft-HTTPAPI/2.0
Other Info	
URL	https://vpntest2023.blob.core.windows.net/robots.txt
Method	GET

Parameter	
Attack	
Evidence	Blob Service Version 1.0 Microsoft-HTTPAPI/2.0
Other Info	
URL	https://vpntest2023.blob.core.windows.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Blob Service Version 1.0 Microsoft-HTTPAPI/2.0
Other Info	
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
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://vpntest2023.blob.core.windows.net
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vpntest2023.blob.core.windows.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://vpntest2023.blob.core.windows.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	

Other Info	
Instances	3
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

Informational	**Non-Storable Content**
Description	The response contents are not storable by caching components such as proxy servers. If the response does not contain sensitive, personal or user-specific information, it may benefit from being stored and cached, to improve performance.
URL	https://vpntest2023.blob.core.windows.net
Method	GET
Parameter	
Attack	
Evidence	400
Other Info	
URL	https://vpntest2023.blob.core.windows.net/robots.txt
Method	GET
Parameter	
Attack	
Evidence	400
Other Info	
URL	https://vpntest2023.blob.core.windows.net/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	400
Other Info	
Instances	3
Solution	The content may be marked as storable by ensuring that the following conditions are satisfied: The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable) The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood) The "no-store" cache directive must not appear in the request or response header fields

	For caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the response For caching by "shared" caches such as "proxy" caches, the "Authorization" header field must not appear in the request, unless the response explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control response directives) In addition to the conditions above, at least one of the following conditions must also be satisfied by the response: It must contain an "Expires" header field It must contain a "max-age" response directive For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive It must contain a "Cache Control Extension" that allows it to be cached It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049