Plugin ID	CVE	CVSS v2.0	Risk	Host	Protocol	Port	Name	Synopsis	Description	Solution	See Also	Plugin Output
10107			None	13.229.233.16	tcp	80	HTTP Server Type and Version	A web server is running on the remote host.	This plugin attempts to determine the type and the version of the remote web server.	n/a		The remote web server type is : nginx/1.24.0 (Ubuntu)
10107			None	13.229.233.16	tcp	443	HTTP Server Type and Version	A web server is running on the remote host.	This plugin attempts to determine the type and the version of the remote web server.	n/a		The remote web server type is : nginx/1.24.0 (Ubuntu)
10386			None	13.229.233.16	tcp	80	Web Server No 404 Error Code Check	The remote web server does not return 404 error codes.	Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.	n/a		The following title tag will be used : SpaceShareUI
10386			None	13.229.233.16	tcp	443	Web Server No 404 Error Code Check	The remote web server does not return 404 error codes.	The remote web server is configured such that it does not return '404	n/a		The following title tag will be used :
11219			None	13.229.233.16	tcp	22	Nessus SYN scanner	It is possible to determine which TCP ports are open.	This plugin is a SYN 'half-open' port scanner. It shall be reasonably	Protect your target with an IP filter.		Port 22/tcp was found to be open
11219			None	13.229.233.16	tcp	80	Nessus SYN scanner	It is possible to determine which TCP ports are open.	This plugin is a SYN 'half-open' port scanner. It shall be reasonably	Protect your target with an IP filter.		Port 80/tcp was found to be open
11219			None	13.229.233.16	tcp	443	Nessus SYN scanner	It is possible to determine which TCP ports are open.	This plugin is a SYN 'half-open' port scanner. It shall be reasonably	Protect your target with an IP filter.		Port 443/tcp was found to be open
11219			None	13.229.233.16	tcp	3000	Nessus SYN scanner	It is possible to determine which TCP ports are open.	This plugin is a SYN 'half-open' port scanner. It shall be reasonably	Protect your target with an IP filter.		Port 3000/tcp was found to be open
19506			None	13.229.233.16	tcp	0	Nessus Scan Information	This plugin displays information about the Nessus scan.		n/a		
24260			None	13.229.233.16	tcp	80	HyperText Transfer Protocol (HTTP) Information	Some information about the remote HTTP configuration can be extracted.	This test gives some information about the remote HTTP protocol - the	n/a		
24260			None	13.229.233.16	tcp	443	HyperText Transfer Protocol (HTTP) Information	Some information about the remote HTTP configuration can be extracted.	This test gives some information about the remote HTTP protocol - the	n/a		
24260			None	13.229.233.16	tcp	3000	HyperText Transfer Protocol (HTTP) Information	Some information about the remote HTTP configuration can be extracted.	This test gives some information about the remote HTTP protocol - the	n/a		
43111			None	13.229.233.16	tcp	80	HTTP Methods Allowed (per directory)	This plugin determines which HTTP methods are allowed on various CGI	By calling the OPTIONS method, it is possible to determine which HTTP	n/a	http://www.nessus.org/u?d9c03a9a	
43111			None	13.229.233.16	tcp	443	HTTP Methods Allowed (per directory)	This plugin determines which HTTP methods are allowed on various CGI	By calling the OPTIONS method, it is possible to determine which HTTP	n/a	http://www.nessus.org/u?d9c03a9a	
43111			None	13.229.233.16	tcp	3000	HTTP Methods Allowed (per directory)	This plugin determines which HTTP methods are allowed on various CGI	By calling the OPTIONS method, it is possible to determine which HTTP	n/a	http://www.nessus.org/u?d9c03a9a	
50344			None	13.229.233.16	tcp	80	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	The remote web server does not take steps to mitigate a class of web	The remote web server in some responses sets a permissive	Set a non-permissive Content-Security-Policy frame-	http://www.nessus.org/u?55aa8f57	
50344			None	13.229.233.16	tcp	443	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header	The remote web server does not take steps to mitigate a class of web	The remote web server in some responses sets a permissive	Set a non-permissive Content-Security-Policy frame-	http://www.nessus.org/u?55aa8f57	
50345			None	13.229.233.16	tcp	80	Missing or Permissive X-Frame-Options HTTP Response Header	The remote web server does not take steps to mitigate a class of web	The remote web server in some responses sets a permissive	Set a properly configured X-Frame-Options header	https://en.wikipedia.org/wiki/Clickjacking	
50345			None	13.229.233.16	tcp	443	Missing or Permissive X-Frame-Options HTTP Response Header	The remote web server does not take steps to mitigate a class of web	The remote web server in some responses sets a permissive	Set a properly configured X-Frame-Options header	https://en.wikipedia.org/wiki/Clickjacking	
84502			None	13.229.233.16	tcp	443	HSTS Missing From HTTPS Server	The remote web server is not enforcing HSTS.	The remote HTTPS server is not enforcing HTTP Strict Transport	Configure the remote web server to use HSTS.	https://tools.ietf.org/html/rfc6797	
91815			None	13.229.233.16	tcp	80	Web Application Sitemap	The remote web server hosts linkable content that can be crawled by	The remote web server contains linkable content that can be used to	n/a	http://www.nessus.org/u?5496c8d9	
91815			None	13.229.233.16	tcp	443	Web Application Sitemap	The remote web server hosts linkable content that can be crawled by	The remote web server contains linkable content that can be used to	n/a	http://www.nessus.org/u?5496c8d9	
106375			None	13.229.233.16	tcp	80	nginx HTTP Server Detection	The nginx HTTP server was detected on the remote host.	Nessus was able to detect the nginx HTTP server by looking at	n/a	https://nginx.org/	
106375			None	13.229.233.16	tcp	443	nginx HTTP Server Detection	The nginx HTTP server was detected on the remote host.	Nessus was able to detect the nginx HTTP server by looking at	n/a	https://nginx.org/	
142960		5.8	Medium	13.229.233.16	tcp	443	HSTS Missing From HTTPS Server (RFC 6797)	The remote web server is not enforcing HSTS, as defined by RFC 6797.	The remote web server is not enforcing HSTS, as defined by RFC 6797.	Configure the remote web server to use HSTS.	https://tools.ietf.org/html/rfc6797	

Information about this scan :

Nessus version : 10.7.3
Nessus build : 20038
Plugin feed version : 202405212255
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : SPACE SHARE PROD
Scan policy used : Web Application Tests
Scanner IP : 192.168.45.100
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 42.702 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : no
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests - Test mode : single
Web app tests - Try all HTTP methods : no
Web app tests - Maximum run time : 5 minutes.
Web app tests - Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2024/5/22 12:12 W. Australia Standard Time
Scan duration : 1459 sec
Scan for malware : no