VULNERABILITY SCAN REPORT

Scan ID: scan_20250714_103310
Target: 127.0.0.1
Scan Period: 2025-07-14T07:33:10.900271+00:00 to 2025-07-14T07:34:53.028437+00:00

Nmap Scan Results

Host: 127.0.0.1

Hostnames: localhost

Open Ports:

80/tcp: http 2.4.58

Script: vulners

cpe:/a:apache:http_server:2.4.58:
95499236-C9FE-56A6-9D7D-E943A24B633A 10.0 https://vulners.com/githubexploit/95499236-C9FE-56A6-9D7D-E943A24B633A *EXPLOIT*
2C119FFA-ECE0-5E14-A4A4-354A2C38071A 10.0 https://vulners.com/githubexploit/2C119FFA-ECE0-5E14-A4A4-354A2C38071A *EXPLOIT*
CVE-2024-38476 9.8 https://vulners.com/cve/CVE-2024-38476
CVE-2024-38474 9.8 https://vulners.com/cve/CVE-2024-38474
A5425A79-9D81-513A-9CC5-549D6321897C 9.8 https://vulners.com/githubexploit/A5425A79-9D81-513A-9CC5-549D6321897C *EXPLOIT*
FD2EE3A5-BAEA-5845-BA35-E6889992214F 9.1 https://vulners.com/githubexploit/FD2EE3A5-BAEA-5845-BA35-E6889992214F *EXPLOIT*
E606D7F4-5FA2-5907-B30E-367D6FFECD89 9.1 https://vulners.com/githubexploit/E606D7F4-5FA2-5907-B30E-367D6FFECD89 *EXPLOIT*
D8A19443-2A37-5592-8955-F614504AAF45 9.1 https://vulners.com/githubexploit/D8A19443-2A37-5592-8955-F614504AAF45 *EXPLOIT*
CVE-2024-40898 9.1 https://vulners.com/cve/CVE-2024-40898
CVE-2024-38475 9.1 https://vulners.com/cve/CVE-2024-38475
B5E74010-A082-5ECE-AB37-623A5B33FE7D 9.1 https://vulners.com/githubexploit/B5E74010-A082-5ECE-AB37-623A5B33FE7D *EXPLOIT*
5418A85B-F4B7-5BBD-B106-0800AC961C7A 9.1 https://vulners.com/githubexploit/5418A85B-F4B7-5BBD-B106-0800AC961C7A *EXPLOIT*
2EF14600-503F-53AF-BA24-683481265D30 9.1 https://vulners.com/githubexploit/2EF14600-503F-53AF-BA24-683481265D30 *EXPLOIT*
0486EBEE-F207-570A-9AD8-33269E72220A 9.1 https://vulners.com/githubexploit/0486EBEE-F207-570A-9AD8-33269E72220A *EXPLOIT*
B0A9E5E8-7CCC-5984-9922-A89F11D6BF38 8.2 https://vulners.com/githubexploit/B0A9E5E8-7CCC-5984-9922-A89F11D6BF38 *EXPLOIT*
CVE-2024-38473 8.1 https://vulners.com/cve/CVE-2024-38473
249A954E-0189-5182-AE95-31C866A057E1 8.1

https://vulners.com/githubexploit/249A954E-0189-5182-AE95-31C866A057E1 *EXPLOIT*

23079A70-8B37-56D2-9D37-F638EBF7F8B5 8.1

https://vulners.com/githubexploit/23079A70-8B37-56D2-9D37-F638EBF7F8B5 *EXPLOIT*

CVE-2024-39573 7.5 https://vulners.com/cve/CVE-2024-39573

CVE-2024-38477 7.5 https://vulners.com/cve/CVE-2024-38477

CVE-2024-38472 7.5 https://vulners.com/cve/CVE-2024-38472

CVE-2024-27316 7.5 https://vulners.com/cve/CVE-2024-27316

CNVD-2024-20839 7.5 https://vulners.com/cnvd/CNVD-2024-20839

CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 7.5

https://vulners.com/githubexploit/CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 *EXPLOIT*

4B14D194-BDE3-5D7F-A262-A701F90DE667 7.5

https://vulners.com/githubexploit/4B14D194-BDE3-5D7F-A262-A701F90DE667 *EXPLOIT*

45D138AD-BEC6-552A-91EA-8816914CA7F4 7.5

https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914CA7F4 *EXPLOIT*

CVE-2023-38709 7.3 https://vulners.com/cve/CVE-2023-38709

CNVD-2024-36395 7.3 https://vulners.com/cnvd/CNVD-2024-36395

CVE-2024-24795 6.3 https://vulners.com/cve/CVE-2024-24795

CVE-2024-39884 6.2 https://vulners.com/cve/CVE-2024-39884

CVE-2024-36387 5.4 https://vulners.com/cve/CVE-2024-36387

CVE-2025-53020 0.0 https://vulners.com/cve/CVE-2025-53020

CVE-2025-49812 0.0 https://vulners.com/cve/CVE-2025-49812

CVE-2025-49630 0.0 https://vulners.com/cve/CVE-2025-49630

CVE-2025-23048 0.0 https://vulners.com/cve/CVE-2025-23048

CVE-2024-47252 0.0 https://vulners.com/cve/CVE-2024-47252

CVE-2024-43394 0.0 https://vulners.com/cve/CVE-2024-43394

CVE-2024-43204 0.0 https://vulners.com/cve/CVE-2024-43204

CVE-2024-42516 0.0 https://vulners.com/cve/CVE-2024-42516

CVEs: CVE-2024-27316, CVE-2023-38709, CVE-2024-43394, CVE-2024-42516, CVE-2024-38474, CVE-2024-43204, CVE

Script: http-server-header

Apache/2.4.58 (Ubuntu)

Script: http-csrf

Couldn't find any CSRF vulnerabilities.

Script: http-stored-xss

Couldn't find any stored XSS vulnerabilities.

Script: http-enum

/server-status/: Potentially interesting folder

Script: http-dombased-xss

Couldn't find any DOM based XSS.

631/tcp: ipp 2.4

Script: http-method-tamper

VULNERABLE:
Authentication bypass by HTTP verb tampering
State: VULNERABLE (Exploitable)
This web server contains password protected resources vulnerable to authentication bypass vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to the common HTTP methods and in misconfigured .htaccess files.

Extra information:

URIs suspected to be vulnerable to HTTP verb tampering:
/admin [GENERIC]

References:
http://capec.mitre.org/data/definitions/274.html
http://www.mkit.com.ar/labs/htexploit/
https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_%28OWASP-CM-008%29
http://www.imperva.com/resources/glossary/http_verb_tampering.html

Script: vulners

CUPS 2.4:
MSF:EXPLOIT-MULTI-MISC-CUPS_IPP_REMOTE_CODE_EXECUTION- 9.0 https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-MISC-CUPS_IPP_REMOTE_CODE_EXECUTION- *EXPLOIT*
1337DAY-ID-39819 9.0 https://vulners.com/zdt/1337DAY-ID-39819 *EXPLOIT*
PACKETSTORM:182767 8.6 https://vulners.com/packetstorm/PACKETSTORM:182767 *EXPLOIT*
FF9C732B-4CA6-5152-9A4F-FF2F80A6C2D7 8.6 https://vulners.com/githubexploit/FF9C732B-4CA6-5152-9A4F-FF2F80A6C2D7 *EXPLOIT*
E609D4C4-3620-555A-8EF9-5338C47C582A 8.6 https://vulners.com/githubexploit/E609D4C4-3620-555A-8EF9-5338C47C582A *EXPLOIT*
6D7EB122-6604-5374-B851-DA56ABDA1F34 8.6 https://vulners.com/githubexploit/6D7EB122-6604-5374-B851-DA56ABDA1F34 *EXPLOIT*
5A844916-7D1B-5CCE-BD42-04F500FF436F 8.6 https://vulners.com/githubexploit/5A844916-7D1B-5CCE-BD42-04F500FF436F *EXPLOIT*
34D7D370-3683-5358-9692-BB0B5AF7F412 8.6 https://vulners.com/githubexploit/34D7D370-3683-5358-9692-BB0B5AF7F412 *EXPLOIT*
CVE-2024-47850 7.5 https://vulners.com/cve/CVE-2024-47850
F5502B30-710E-5D69-B67C-937F75899289 5.3 https://vulners.com/githubexploit/F5502B30-710E-5D69-B67C-937F75899289 *EXPLOIT*
EA20CCC7-E73D-5A9D-AF80-6634C5E3191F 5.3 https://vulners.com/githubexploit/EA20CCC7-E73D-5A9D-AF80-6634C5E3191F *EXPLOIT*
D0B85558-0ED9-5259-A56D-4C807CC07FCF 5.3

https://vulners.com/githubexploit/D0B85558-0ED9-5259-A56D-4C807CC07FCF *EXPLOIT*

ADDB422D-CF88-55B8-BA36-EC2BAC7507A0 5.3

https://vulners.com/githubexploit/ADDB422D-CF88-55B8-BA36-EC2BAC7507A0 *EXPLOIT*

9DB4B6B1-3FB0-5827-B554-3F3779D23B09 5.3

https://vulners.com/githubexploit/9DB4B6B1-3FB0-5827-B554-3F3779D23B09 *EXPLOIT*

62F720CF-C08E-5ED1-91ED-CEE3A133F124 5.3

https://vulners.com/githubexploit/62F720CF-C08E-5ED1-91ED-CEE3A133F124 *EXPLOIT*

48FAED93-C711-59A0-B81E-A65D4463C7F0 5.3

https://vulners.com/githubexploit/48FAED93-C711-59A0-B81E-A65D4463C7F0 *EXPLOIT*

3951C81B-06CE-5CA8-B97C-F2F1D450E85F 5.3

https://vulners.com/githubexploit/3951C81B-06CE-5CA8-B97C-F2F1D450E85F *EXPLOIT*

CVEs: CVE-2024-47850

Script: http-aspnet-debug

ERROR: Script execution failed (use -d to debug)

Script: http-server-header

CUPS/2.4 IPP/2.1

Script: http-enum

/admin.php: Possible admin folder (401 Unauthorized)
/admin/: Possible admin folder (401 Unauthorized)
/admin/admin/: Possible admin folder (401 Unauthorized)
/administrator/: Possible admin folder (401 Unauthorized)
/adminarea/: Possible admin folder (401 Unauthorized)
/adminLogin/: Possible admin folder (401 Unauthorized)
/admin_area/: Possible admin folder (401 Unauthorized)
/administratorlogin/: Possible admin folder (401 Unauthorized)
/admin/account.php: Possible admin folder (401 Unauthorized)
/admin/index.php: Possible admin folder (401 Unauthorized)
/admin/login.php: Possible admin folder (401 Unauthorized)
/admin/admin.php: Possible admin folder (401 Unauthorized)
/admin_area/admin.php: Possible admin folder (401 Unauthorized)
/admin_area/login.php: Possible admin folder (401 Unauthorized)
/admin/index.html: Possible admin folder (401 Unauthorized)
/admin/login.html: Possible admin folder (401 Unauthorized)
/admin/admin.html: Possible admin folder (401 Unauthorized)
/admin_area/index.php: Possible admin folder (401 Unauthorized)
/admin/home.php: Possible admin folder (401 Unauthorized)
/admin_area/login.html: Possible admin folder (401 Unauthorized)
/admin_area/index.html: Possible admin folder (401 Unauthorized)
/admin/controlpanel.php: Possible admin folder (401 Unauthorized)
/admincp/: Possible admin folder (401 Unauthorized)
/admincp/index.asp: Possible admin folder (401 Unauthorized)
/admincp/index.html: Possible admin folder (401 Unauthorized)

/admincp/login.php: Possible admin folder (401 Unauthorized)
/admin/account.html: Possible admin folder (401 Unauthorized)
/adminpanel.html: Possible admin folder (401 Unauthorized)
/admin/admin_login.html: Possible admin folder (401 Unauthorized)
/admin_login.html: Possible admin folder (401 Unauthorized)
/admin/cp.php: Possible admin folder (401 Unauthorized)
/administrator/index.php: Possible admin folder (401 Unauthorized)
/administrator/login.php: Possible admin folder (401 Unauthorized)
/admin/admin_login.php: Possible admin folder (401 Unauthorized)
/admin_login.php: Possible admin folder (401 Unauthorized)
/administrator/account.php: Possible admin folder (401 Unauthorized)
/administrator.php: Possible admin folder (401 Unauthorized)
/admin_area/admin.html: Possible admin folder (401 Unauthorized)
/admin/admin-login.php: Possible admin folder (401 Unauthorized)
/admin-login.php: Possible admin folder (401 Unauthorized)
/admin/home.html: Possible admin folder (401 Unauthorized)
/admin/admin-login.html: Possible admin folder (401 Unauthorized)
/admin-login.html: Possible admin folder (401 Unauthorized)
/admincontrol.php: Possible admin folder (401 Unauthorized)
/admin/adminLogin.html: Possible admin folder (401 Unauthorized)
/adminLogin.html: Possible admin folder (401 Unauthorized)
/adminarea/index.html: Possible admin folder (401 Unauthorized)
/adminarea/admin.html: Possible admin folder (401 Unauthorized)
/admin/controlpanel.html: Possible admin folder (401 Unauthorized)
/admin.html: Possible admin folder (401 Unauthorized)
/admin/cp.html: Possible admin folder (401 Unauthorized)
/adminpanel.php: Possible admin folder (401 Unauthorized)
/administrator/index.html: Possible admin folder (401 Unauthorized)
/administrator/login.html: Possible admin folder (401 Unauthorized)
/administrator/account.html: Possible admin folder (401 Unauthorized)
/administrator.html: Possible admin folder (401 Unauthorized)
/adminarea/login.html: Possible admin folder (401 Unauthorized)
/admincontrol/login.html: Possible admin folder (401 Unauthorized)
/admincontrol.html: Possible admin folder (401 Unauthorized)
/adminLogin.php: Possible admin folder (401 Unauthorized)
/admin/adminLogin.php: Possible admin folder (401 Unauthorized)
/adminarea/index.php: Possible admin folder (401 Unauthorized)
/adminarea/admin.php: Possible admin folder (401 Unauthorized)
/adminarea/login.php: Possible admin folder (401 Unauthorized)
/admincontrol/login.php: Possible admin folder (401 Unauthorized)
/admin2.php: Possible admin folder (401 Unauthorized)
/admin2/login.php: Possible admin folder (401 Unauthorized)
/admin2/index.php: Possible admin folder (401 Unauthorized)
/administratorlogin.php: Possible admin folder (401 Unauthorized)

/admin/account.cfm: Possible admin folder (401 Unauthorized)
/admin/index.cfm: Possible admin folder (401 Unauthorized)
/admin/login.cfm: Possible admin folder (401 Unauthorized)
/admin/admin.cfm: Possible admin folder (401 Unauthorized)
/admin.cfm: Possible admin folder (401 Unauthorized)
/admin/admin_login.cfm: Possible admin folder (401 Unauthorized)
/admin_login.cfm: Possible admin folder (401 Unauthorized)
/adminpanel.cfm: Possible admin folder (401 Unauthorized)
/admin/controlpanel.cfm: Possible admin folder (401 Unauthorized)
/admincontrol.cfm: Possible admin folder (401 Unauthorized)
/admin/cp.cfm: Possible admin folder (401 Unauthorized)
/admincp/index.cfm: Possible admin folder (401 Unauthorized)
/admincp/login.cfm: Possible admin folder (401 Unauthorized)
/admin_area/admin.cfm: Possible admin folder (401 Unauthorized)
/admin_area/login.cfm: Possible admin folder (401 Unauthorized)
/administrator/login.cfm: Possible admin folder (401 Unauthorized)
/administratorlogin.cfm: Possible admin folder (401 Unauthorized)
/administrator.cfm: Possible admin folder (401 Unauthorized)
/administrator/account.cfm: Possible admin folder (401 Unauthorized)
/adminLogin.cfm: Possible admin folder (401 Unauthorized)
/admin2/index.cfm: Possible admin folder (401 Unauthorized)
/admin_area/index.cfm: Possible admin folder (401 Unauthorized)
/admin2/login.cfm: Possible admin folder (401 Unauthorized)
/admincontrol/login.cfm: Possible admin folder (401 Unauthorized)
/administrator/index.cfm: Possible admin folder (401 Unauthorized)
/adminarea/login.cfm: Possible admin folder (401 Unauthorized)
/adminarea/admin.cfm: Possible admin folder (401 Unauthorized)
/adminarea/index.cfm: Possible admin folder (401 Unauthorized)
/admin/adminLogin.cfm: Possible admin folder (401 Unauthorized)
/admin-login.cfm: Possible admin folder (401 Unauthorized)
/admin/admin-login.cfm: Possible admin folder (401 Unauthorized)
/admin/home.cfm: Possible admin folder (401 Unauthorized)
/admin/account.asp: Possible admin folder (401 Unauthorized)
/admin/index.asp: Possible admin folder (401 Unauthorized)
/admin/login.asp: Possible admin folder (401 Unauthorized)
/admin/admin.asp: Possible admin folder (401 Unauthorized)
/admin_area/admin.asp: Possible admin folder (401 Unauthorized)
/admin_area/login.asp: Possible admin folder (401 Unauthorized)
/admin_area/index.asp: Possible admin folder (401 Unauthorized)
/admin/home.asp: Possible admin folder (401 Unauthorized)
/admin/controlpanel.asp: Possible admin folder (401 Unauthorized)
/admin.asp: Possible admin folder (401 Unauthorized)
/admin/admin-login.asp: Possible admin folder (401 Unauthorized)
/admin-login.asp: Possible admin folder (401 Unauthorized)

/admin/cp.asp: Possible admin folder (401 Unauthorized)
/administrator/account.asp: Possible admin folder (401 Unauthorized)
/administrator.asp: Possible admin folder (401 Unauthorized)
/administrator/login.asp: Possible admin folder (401 Unauthorized)
/admincp/login.asp: Possible admin folder (401 Unauthorized)
/admincontrol.asp: Possible admin folder (401 Unauthorized)
/adminpanel.asp: Possible admin folder (401 Unauthorized)
/admin/admin_login.asp: Possible admin folder (401 Unauthorized)
/admin_login.asp: Possible admin folder (401 Unauthorized)
/adminLogin.asp: Possible admin folder (401 Unauthorized)
/admin/adminLogin.asp: Possible admin folder (401 Unauthorized)
/adminarea/index.asp: Possible admin folder (401 Unauthorized)
/adminarea/admin.asp: Possible admin folder (401 Unauthorized)
/adminarea/login.asp: Possible admin folder (401 Unauthorized)
/administrator/index.asp: Possible admin folder (401 Unauthorized)
/admincontrol/login.asp: Possible admin folder (401 Unauthorized)
/admin2.asp: Possible admin folder (401 Unauthorized)
/admin2/login.asp: Possible admin folder (401 Unauthorized)
/admin2/index.asp: Possible admin folder (401 Unauthorized)
/administratorlogin.asp: Possible admin folder (401 Unauthorized)
/admin/account.aspx: Possible admin folder (401 Unauthorized)
/admin/index.aspx: Possible admin folder (401 Unauthorized)
/admin/login.aspx: Possible admin folder (401 Unauthorized)
/admin/admin.aspx: Possible admin folder (401 Unauthorized)
/admin_area/admin.aspx: Possible admin folder (401 Unauthorized)
/admin_area/login.aspx: Possible admin folder (401 Unauthorized)
/admin_area/index.aspx: Possible admin folder (401 Unauthorized)
/admin/home.aspx: Possible admin folder (401 Unauthorized)
/admin/controlpanel.aspx: Possible admin folder (401 Unauthorized)
/admin.aspx: Possible admin folder (401 Unauthorized)
/admin/admin-login.aspx: Possible admin folder (401 Unauthorized)
/admin-login.aspx: Possible admin folder (401 Unauthorized)
/admin/cp.aspx: Possible admin folder (401 Unauthorized)
/administrator/account.aspx: Possible admin folder (401 Unauthorized)
/administrator.aspx: Possible admin folder (401 Unauthorized)
/administrator/login.aspx: Possible admin folder (401 Unauthorized)
/admincp/index.aspx: Possible admin folder (401 Unauthorized)
/admincp/login.aspx: Possible admin folder (401 Unauthorized)
/admincontrol.aspx: Possible admin folder (401 Unauthorized)
/adminpanel.aspx: Possible admin folder (401 Unauthorized)
/admin/admin_login.aspx: Possible admin folder (401 Unauthorized)
/admin_login.aspx: Possible admin folder (401 Unauthorized)
/adminLogin.aspx: Possible admin folder (401 Unauthorized)
/admin/adminLogin.aspx: Possible admin folder (401 Unauthorized)

/adminarea/index.aspx: Possible admin folder (401 Unauthorized)
/adminarea/admin.aspx: Possible admin folder (401 Unauthorized)
/adminarea/login.aspx: Possible admin folder (401 Unauthorized)
/administrator/index.aspx: Possible admin folder (401 Unauthorized)
/admincontrol/login.aspx: Possible admin folder (401 Unauthorized)
/admin2.aspx: Possible admin folder (401 Unauthorized)
/admin2/login.aspx: Possible admin folder (401 Unauthorized)
/admin2/index.aspx: Possible admin folder (401 Unauthorized)
/administratorlogin.aspx: Possible admin folder (401 Unauthorized)
/admin/index.jsp: Possible admin folder (401 Unauthorized)
/admin/login.jsp: Possible admin folder (401 Unauthorized)
/admin/admin.jsp: Possible admin folder (401 Unauthorized)
/admin_area/admin.jsp: Possible admin folder (401 Unauthorized)
/admin_area/login.jsp: Possible admin folder (401 Unauthorized)
/admin_area/index.jsp: Possible admin folder (401 Unauthorized)
/admin/home.jsp: Possible admin folder (401 Unauthorized)
/admin/controlpanel.jsp: Possible admin folder (401 Unauthorized)
/admin.jsp: Possible admin folder (401 Unauthorized)
/admin/admin-login.jsp: Possible admin folder (401 Unauthorized)
/admin-login.jsp: Possible admin folder (401 Unauthorized)
/admin/cp.jsp: Possible admin folder (401 Unauthorized)
/administrator/account.jsp: Possible admin folder (401 Unauthorized)
/administrator.jsp: Possible admin folder (401 Unauthorized)
/administrator/login.jsp: Possible admin folder (401 Unauthorized)
/admincp/index.jsp: Possible admin folder (401 Unauthorized)
/admincp/login.jsp: Possible admin folder (401 Unauthorized)
/admincontrol.jsp: Possible admin folder (401 Unauthorized)
/admin/account.jsp: Possible admin folder (401 Unauthorized)
/adminpanel.jsp: Possible admin folder (401 Unauthorized)
/admin/admin_login.jsp: Possible admin folder (401 Unauthorized)
/admin_login.jsp: Possible admin folder (401 Unauthorized)
/adminLogin.jsp: Possible admin folder (401 Unauthorized)
/admin/adminLogin.jsp: Possible admin folder (401 Unauthorized)
/adminarea/index.jsp: Possible admin folder (401 Unauthorized)
/adminarea/admin.jsp: Possible admin folder (401 Unauthorized)
/adminarea/login.jsp: Possible admin folder (401 Unauthorized)
/administrator/index.jsp: Possible admin folder (401 Unauthorized)
/admincontrol/login.jsp: Possible admin folder (401 Unauthorized)
/admin2.jsp: Possible admin folder (401 Unauthorized)
/admin2/login.jsp: Possible admin folder (401 Unauthorized)
/admin2/index.jsp: Possible admin folder (401 Unauthorized)
/administratorlogin.jsp: Possible admin folder (401 Unauthorized)
/admin1.php: Possible admin folder (401 Unauthorized)
/administr8.asp: Possible admin folder (401 Unauthorized)

/administr8.php: Possible admin folder (401 Unauthorized)
/administr8.jsp: Possible admin folder (401 Unauthorized)
/administr8.aspx: Possible admin folder (401 Unauthorized)
/administr8.cfm: Possible admin folder (401 Unauthorized)
/administr8/: Possible admin folder (401 Unauthorized)
/administer/: Possible admin folder (401 Unauthorized)
/administracao.php: Possible admin folder (401 Unauthorized)
/administracao.asp: Possible admin folder (401 Unauthorized)
/administracao.aspx: Possible admin folder (401 Unauthorized)
/administracao.cfm: Possible admin folder (401 Unauthorized)
/administracao.jsp: Possible admin folder (401 Unauthorized)
/administracion.php: Possible admin folder (401 Unauthorized)
/administracion.asp: Possible admin folder (401 Unauthorized)
/administracion.aspx: Possible admin folder (401 Unauthorized)
/administracion.jsp: Possible admin folder (401 Unauthorized)
/administracion.cfm: Possible admin folder (401 Unauthorized)
/administrators/: Possible admin folder (401 Unauthorized)
/adminpro/: Possible admin folder (401 Unauthorized)
/admins/: Possible admin folder (401 Unauthorized)
/admins.cfm: Possible admin folder (401 Unauthorized)
/admins.php: Possible admin folder (401 Unauthorized)
/admins.jsp: Possible admin folder (401 Unauthorized)
/admins.asp: Possible admin folder (401 Unauthorized)
/admins.aspx: Possible admin folder (401 Unauthorized)
/administracion-sistema/: Possible admin folder (401 Unauthorized)
/admin108/: Possible admin folder (401 Unauthorized)
/admin_cp.asp: Possible admin folder (401 Unauthorized)
/admin/backup/: Possible backup (401 Unauthorized)
/admin/download/backup.sql: Possible database backup (401 Unauthorized)
/robots.txt: Robots file
/admin/upload.php: Admin File Upload (401 Unauthorized)
/admin/CiscoAdmin.jhtml: Cisco Collaboration Server (401 Unauthorized)
/admin-console/: JBoss Console (401 Unauthorized)
/admin4.nsf: Lotus Domino (401 Unauthorized)
/admin5.nsf: Lotus Domino (401 Unauthorized)
/admin.nsf: Lotus Domino (401 Unauthorized)
/administrator/wp-login.php: Wordpress login page. (401 Unauthorized)
/admin/libraries/ajaxfilemanager/ajaxfilemanager.php: Log1 CMS (401 Unauthorized)
/admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload (401 Unauthorized)
/admin/includes/tiny_mce/plugins/tinybrowser/upload.php: CompactCMS or B-Hind CMS/FCKeditor File upload (401 Unauthorized)
/admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload (401 Unauthorized)

/admin/jscript/upload.php: Lizard Cart/Remote File upload (401 Unauthorized)
/admin/jscript/upload.html: Lizard Cart/Remote File upload (401 Unauthorized)
/admin/jscript/upload.pl: Lizard Cart/Remote File upload (401 Unauthorized)
/admin/jscript/upload.asp: Lizard Cart/Remote File upload (401 Unauthorized)
/admin/environment.xml: Moodle files (401 Unauthorized)
/classes/: Potentially interesting folder
/es/: Potentially interesting folder
/help/: Potentially interesting folder
/printers/: Potentially interesting folder

Script: http-vuln-cve2014-3704

ERROR: Script execution failed (use -d to debug)

5432/tcp: postgresql 9.6.0 or later

Script: ssl-cert

Subject: commonName=g-100HP
Subject Alternative Name: DNS:g-100HP
Issuer: commonName=g-100HP
Public Key type: rsa
Public Key bits: 2048
Signature Algorithm: sha256WithRSAEncryption
Not valid before: 2024-08-08T14:51:25
Not valid after: 2034-08-06T14:51:25
MD5: ccf8:fa91:0c85:d0df:fe11:61ef:2e4c:c5cd
SHA-1: c7c1:bec8:284c:884d:49ed:0cf9:09c8:7da4:5e31:2b2a

Script: ssl-date

TLS randomness does not represent time

Script: fingerprint-strings

SMBProgNeg:
SFATAL
VFATAL
C0A000
Munsupported frontend protocol 65363.19778: server supports 3.0 to 3.0
Fpostmaster.c
L2147
RProcessStartupPacket

Script: ssl-enum-ciphers

TLSv1.2:
ciphers:
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (dh 2048) - A
TLS_DHE_RSA_WITH_AES_256_CCM_8 (dh 2048) - A
TLS_DHE_RSA_WITH_AES_256_CCM (dh 2048) - A
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (secp256r1) - A
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 (dh 2048) - A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
TLS_DHE_RSA_WITH_AES_128_CCM_8 (dh 2048) - A
TLS_DHE_RSA_WITH_AES_128_CCM (dh 2048) - A
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (secp256r1) - A
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 (dh 2048) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (secp256r1) - A
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 (dh 2048) - A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A
TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (secp256r1) - A
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 (dh 2048) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (dh 2048) - A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (dh 2048) - A
TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
TLS_RSA_WITH_AES_256_CCM_8 (rsa 2048) - A
TLS_RSA_WITH_AES_256_CCM (rsa 2048) - A
TLS_RSA_WITH_ARIA_256_GCM_SHA384 (rsa 2048) - A
TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_128_CCM_8 (rsa 2048) - A
TLS_RSA_WITH_AES_128_CCM (rsa 2048) - A
TLS_RSA_WITH_ARIA_128_GCM_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
compressors:
NULL

cipher preference: server
TLSv1.3:
ciphers:
TLS_AKE_WITH_AES_256_GCM_SHA384 (secp256r1) - A
TLS_AKE_WITH_CHACHA20_POLY1305_SHA256 (secp256r1) - A
TLS_AKE_WITH_AES_128_GCM_SHA256 (secp256r1) - A
cipher preference: server
least strength: A

OpenVAS Scan Results

Scan ID: N/A

Total Findings: 0

Critical: 0

High: 0

Medium: 0

Low: 0

DNS Records

A: 127.0.0.1