

# VULNERABILITY SCAN REPORT

Scan ID: scan\_20250908\_130133

Target: 127.0.0.1

Scan Period: 2025-09-08T10:01:33.634542+00:00 to 2025-09-08T10:03:17.913742+00:00

## Nmap Scan Results

**Host: 127.0.0.1**

Hostnames: localhost

Open Ports:

80/tcp: http 2.4.58

*Script: http-stored-xss*

Couldn't find any stored XSS vulnerabilities.

*Script: http-dombased-xss*

Couldn't find any DOM based XSS.

*Script: vulners*

cpe:/a:apache:http\_server:2.4.58:

CVE-2024-38476 9.8 <https://vulners.com/cve/CVE-2024-38476>

CVE-2024-38474 9.8 <https://vulners.com/cve/CVE-2024-38474>

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-2025-23048 9.1 <https://vulners.com/cve/CVE-2025-23048>

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\*

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-2025-53020 7.5 <https://vulners.com/cve/CVE-2025-53020>

CVE-2025-49630 7.5 <https://vulners.com/cve/CVE-2025-49630>

CVE-2024-47252 7.5 <https://vulners.com/cve/CVE-2024-47252>

CVE-2024-43394 7.5 <https://vulners.com/cve/CVE-2024-43394>  
CVE-2024-43204 7.5 <https://vulners.com/cve/CVE-2024-43204>  
CVE-2024-42516 7.5 <https://vulners.com/cve/CVE-2024-42516>  
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\*

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

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

CVE-2025-49812 7.4 <https://vulners.com/cve/CVE-2025-49812>  
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-2025-54090 6.3 <https://vulners.com/cve/CVE-2025-54090>  
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>

CVEs: CVE-2024-39573, CVE-2024-27316, CVE-2024-24795, CVE-2023-38709, CVE-2024-38477, CVE-2024-42516, CVE-

*Script: http-csrf*

Couldn't find any CSRF vulnerabilities.

*Script: http-server-header*

Apache/2.4.58 (Ubuntu)

*Script: http-enum*

/server-status/: Potentially interesting folder

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://www.mkit.com.ar/labs/htexploit/>

<http://capec.mitre.org/data/definitions/274.html>

[https://www.owasp.org/index.php/Testing\\_for\\_HTTP\\_Methods\\_and\\_XST\\_%28OWASP-CM-008%29](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](http://www.imperva.com/resources/glossary/http_verb_tampering.html)

*Script: http-server-header*

CUPS/2.4 IPP/2.1

*Script: vulners*

CUPS 2.4:

1337DAY-ID-39819 9.0 <https://vulners.com/zdt/1337DAY-ID-39819> \*EXPLOIT\*

PACKETSTORM:182767 8.6 <https://vulners.com/packetstorm/PACKETSTORM:182767> \*EXPLOIT\*

MSF:EXPLOIT-MULTI-MISC-CUPS\_IPP\_REMOTE\_CODE\_EXECUTION- 8.6

[https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-MISC-CUPS\\_IPP\\_REMOTE\\_CODE\\_EXECUTION-](https://vulners.com/metasploit/MSF:EXPLOIT-MULTI-MISC-CUPS_IPP_REMOTE_CODE_EXECUTION-) \*EXPLOIT\*

6D7EB122-6604-5374-B851-DA56ABDA1F34 8.6

<https://vulners.com/githubexploit/6D7EB122-6604-5374-B851-DA56ABDA1F34> \*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\*

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\*

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

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

CVEs: CVE-2024-47850

*Script: http-aspnet-debug*

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

*Script: http-vuln-cve2014-3704*

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

*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/jsript/upload.php: Lizard Cart/Remote File upload (401 Unauthorized)  
/admin/jsript/upload.html: Lizard Cart/Remote File upload (401 Unauthorized)  
/admin/jsript/upload.pl: Lizard Cart/Remote File upload (401 Unauthorized)  
/admin/jsript/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

5432/tcp: postgresql 9.6.0 or later

*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

*Script: ssl-date*

TLS randomness does not represent time

*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: fingerprint-strings*

SMBProgNeg:

SFATAL

VFATAL

C0A000

Munsupported frontend protocol 65363.19778: server supports 3.0 to 3.0

Fpostmaster.c

L2147

RProcessStartupPacket