Scan Target: testphp.vulnweb.com
Scanner Source IP: 66.175.214.247
User Agent: Nikto 2.1.5

- Nikto v2.1.5

+ Target IP: 176.28.50.165
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2019-01-17 11:13:43 (GMT0)

+ Server: nginx/1.4.1
+ Retrieved x-powered-by header: PHP/5.3.10-1~lucid+2uwsgi2
+ The anti-clickjacking X-Frame-Options header is not present.
+ Server leaks inodes via ETags, header found with file /clientaccesspolicy.xml, fields: 0x5049b03d 0x133
+ /clientaccesspolicy.xml contains a full wildcard entry. See http://msdn.microsoft.com/en-us/library/cc197955(v=vs.95).aspx
+ lines
+ /crossdomain.xml contains a full wildcard entry.
See http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ /crossdomain.xml contains 0 line which should be manually viewed for improper domains or wildcards.
+ /CVS/Entries: CVS Entries file may contain directory listing information.
+ OSVDB-3268: /admin/: Directory indexing found.
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ /login.php: Admin login page/section found.
+ 5567 items checked: 6 error(s) and 13 item(s) reported on remote host
+ End Time: 2019-01-17 11:22:39 (GMT0) (536 seconds)

+ 1 host(s) tested