VULNERABILITY SCAN REPORT

Scan ID: scan_20250714_120224
Target: mmu.ac.ke
Scan Period: 2025-07-14T09:02:25.110908+00:00 to 2025-07-14T09:13:55.568509+00:00

Nmap Scan Results

Host: 41.204.160.15

Hostnames: mmu.ac.ke, cp-uon.kenet.or.ke

Open Ports:

80/tcp: http

Script: http-stored-xss

Couldn't find any stored XSS vulnerabilities.

Script: http-csrf

Couldn't find any CSRF vulnerabilities.

Script: http-slowloris-check

VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE
IDs: CVE:CVE-2007-6750
Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service.

Disclosure date: 2009-09-17
References:
http://ha.ckers.org/slowloris/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750

CVEs: CVE-2007-6750

Script: http-aspnet-debug

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

Script: http-dombased-xss

Couldn't find any DOM based XSS.

Script: http-vuln-cve2014-3704

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

443/tcp: http

Script: http-stored-xss

Couldn't find any stored XSS vulnerabilities.

Script: http-aspnet-debug

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

Script: http-csrf

Couldn't find any CSRF vulnerabilities.

Script: http-dombased-xss

Couldn't find any DOM based XSS.

Script: ssl-cert

Subject: commonName=*.mmu.ac.ke

Subject Alternative Name: DNS:*.mmu.ac.ke, DNS:mmu.ac.ke

Issuer: commonName=Sectigo RSA Domain Validation Secure Server CA/organizationName=Sectigo Limited/stateOrProvinceName=Greater Manchester/countryName=GB

Public Key type: rsa

Public Key bits: 2048

Signature Algorithm: sha256WithRSAEncryption

Not valid before: 2024-08-14T00:00:00

Not valid after: 2025-08-14T23:59:59

MD5: f6d9:d031:080a:4bbc:3637:dfc8:62ef:3d90

SHA-1: fb2f:f895:a3d1:45b0:91ba:d1a1:812b:b7fc:8dc8:44d1

DNS Records

A: 41.204.160.15

MX: 2 alt2.aspmx.l.google.com., 3 alt3.aspmx.l.google.com., 2 alt1.aspmx.l.google.com., 1 aspmx.l.google.com., 3 alt4.aspmx.l.google.com.

TXT: "v=spf1 include:_spf.google.com -all", "google-site-verification=P1XOE0WV_i7tum8MQ0boxbpOFuH8jMKgxPdDrWaKMe0"