Nikto Web Server Vulnerability Scan Report

Scan Date: 2025-08-10 17:49:59 (GMT+5.5)
Tool Version: Nikto v2.5.0

Target Information

Target IP: 192.168.243.87

Hostname: 192.168.243.87

Port: 80

Web Server: Apache/2.4.63 (Debian)

Vulnerabilities Found

1. Missing Anti-Clickjacking Header

Description: The X-Frame-Options header is not present.

Impact: Could allow Clickjacking attacks.

Reference: MDN - X-Frame-Options

2. Missing X-Content-Type-Options Header

Description: The X-Content-Type-Options header is not set.

Impact: The browser might render content in an unintended MIME type, leading to possible XSS or content-sniffing attacks.

Reference: Netsparker Article

3. ETag Inode Leak

Description: The server may leak inode numbers via ETags.

Details: inode: 29cf, size: 63bdba3d90b74, mtime: gzip.

CVE: CVE-2003-1418

4. HTTP Methods Allowed

Description: The following HTTP methods are enabled: HEAD, GET, POST, OPTIONS.

Impact: Some methods (like OPTIONS) can reveal unnecessary information about the server.

5. Apache Server-Status Exposure

Description: /server-status page is accessible, revealing Apache internal information.

Recommendation: Restrict access to trusted IPs or disable it.

Reference: OSVDB-561

Additional Notes

No CGI directories were found.

Total Requests Made: 8102

Errors: 0

Findings: 5

Recommendations

Add X-Frame-Options header to prevent clickjacking.

Add X-Content-Type-Options: nosniff to mitigate content-sniffing risks.

Disable ETag inode exposure.

Restrict HTTP methods to only what is necessary (e.g., GET and POST).

Restrict or disable /server-status in Apache configuration

```
nikto -h http://192.168.243.87
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.243.87
+ Target Hostname:    192.168.243.87
+ Target Port:        80
+ Start Time:         2025-08-10 17:49:59 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.63 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not
present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Head
ers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This
could allow the user agent to render the content of the site
in a different fashion to the MIME type. See:
https://www.netsparker.com/web-vulnerability-scanner/vuln
erabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all
possible dirs)
+ /: Server may leak inodes via ETags, header found with
file /, inode: 29cf, size: 63bdba3d90b74, mtime: gzip. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-
1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST,
OPTIONS .
```

```
+ /server-status: This reveals Apache information.
Comment out appropriate line in the Apache conf file or
restrict access to allowed sources. See: OSVDB-561
+ 8102 requests: 0 error(s) and 5 item(s) reported on
remote host
+ End Time:           2025-08-10 17:50:20 (GMT5.5) (21
seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested



******************************************************************
***
      Portions of the server's headers (Apache/2.4.63) are
not in
      the Nikto 2.5.0 database or are newer than the known
string. Would you like
```