O exemplo abaixo mostra a saída de um scaner-geral feito com a ferramenta Nikto:

nikto -host 10.10.131.39

- Nikto v2.1.6

---------------------------------------------------------------------------

+ Target IP: 10.10.131.39

+ Target Hostname: 10.10.131.39

+ Target Port: 80

+ Start Time: 2023-03-01 11:06:37 (GMT-3)

---------------------------------------------------------------------------

+ Server: Apache/2.4.29 (Ubuntu)

+ The anti-clickjacking X-Frame-Options header is not present.

+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS

+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diffe rent fashion to the MIME type

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ Apache/2.4.29 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.

+ Server may leak inodes via ETags, header found with file /, inode: 2aa6, size: 5c2d54e72ade1, mtime: gzip

+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS

+ Cookie PHPSESSID created without the httponly flag

+ OSVDB-3233: /icons/README: Apache default file found.

Repare que ele lista “possíveis” vulnerabilidade a serem exploradas, como por exemplo o não uso de X-XSS-Protection que esta listado como não definido.



