Escaner de vulnerabilidades nikto2

descarga

```
$ wget https://cirt.net/nikto/nikto-2.1.4.tar.gz –no-check-certificate
```

ejecución

parámetros:

- -h : host a escanear
- -port: puerto a escanear, por defecto el 80

ejemplo de salida

```
#./nikto.pl -h cau.eurocity.es
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          192.168.3.164
+ Target Hostname:    cau.eurocity.es
+ Target Port:        80
+ Start Time:         2012-02-15 09:34:11
---------------------------------------------------------------------------
+ Server: Apache/2.2.16 (Debian)
+ Retrieved x-powered-by header: PHP/5.3.3-7+squeeze3
+ ETag header found on server, inode: 1287121, size: 17, mtime: 0x4b77f1ad8fb80
+ Apache/2.2.16 appears to be outdated (current is at least Apache/2.2.17). Apache
1.3.42 (final release) and 2.0.64 are also current.
+ Multiple index files found: index.php, index.html,
+ DEBUG HTTP verb may show server debugging information. See
http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ 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: /install/: This might be interesting...
+ OSVDB-3092: /lib/: This might be interesting...
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3268: /manual/images/: Directory indexing found.
+ OSVDB-3092: /install/install.php: Install file found.
+ OSVDB-3092: /CHANGELOG.txt: A changelog was found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 6448 items checked: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2012-02-15 09:37:58 (227 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```