STARTING NIKTO

Web server are a constant in our lifes now, and we need to be able to deal with them. And a useful first step is the ability to do a simple check against the web server in question to check for known 'bad things'. Now *Nikto* (see here) is a great tool, command line based, scriptable, no funny dependencies and does what it says on the tin. It has some useful options for IDS avoidance and can 'talk' SSL.

But at the simplest, you download the archive, unextract it and just point it at web server port and away you go. Here is an example..

```
# ./nikto.pl -h http://192.168.2.107:8080
- Nikto v2.1.1
---------------------------------------------------------------------------
+ Target IP:          192.168.2.107
+ Target Hostname:    192.168.2.107
+ Target Port:        8080
+ Start Time:         2010-06-13 22:13:31
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
- Root page / redirects to: http://dojo-vm.local:8080/index.html
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ETag header found on server, fields: 0xW/261 0x1114607402000
+ Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
+ OSVDB-397: HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ OSVDB-5646: HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ OSVDB-6659: /mjFX8brYX4XqE9G2BdzkDGJGyvcDzMQTShU3z5Cpdi4y8tcyQtA3CVVEfNrQQ9nhMJHe3xfEPehXTbNf2cWkbs
7JuVDsWBEbRlYkevS2iXw3BzH4oLs55NpPJP8bbmCUgcGWDkfaT60KyK1NU5Fo2RMBr6tGlptILvA3Lkh9441aY94UWxyDoXlTN
AaHYGkGUgepwTILhLWFGky2lVOGiOzlMR8zr2Y<font%20size=50>DEFACED<!--//--: MyWebServer 1.0.2 is vulnerable to
HTML injection. Upgrade to a later version.
+ ERROR: /phpinfo.php?cx[]=0wPWh8x1RITF6DMjETySQtsFqXJi0dHkZMlKCklXAfZuiuw9mVwUypCpsXIkOs0GxIgwBsQO8hcPRV0ior0q0Ui5
z8Mg5mAABeonchsulTrOMq2fnOj1U3LVFa6XjWS3yCiJty2K2oqWM0WzMDYnn7BxnH9t8giKw8SrF8TznhOesT3OWgDdBejRCxqXOBN3d2X
0IwkkChJmcP7mD7zugr63IcNFqNhCsHDCz6zZM4dbO59gI68RVL7xMr6AigWQ14TyUPCKU5R9Uce4mPyCeVH3NX9cgjzRliXbKw4X1Vu57cw
skaSu09lWP7VX9SGpxHLosC4vMUZRSPu6QmgbhjshZVqTVGCdaLhFzDglSe8zf4g9qtjI8mLpCZsJcYxksFYx62JvY9GnbI50vETypcRa0JdnwolTb
MXIzJ8kCYk2Og5KRqOroB3zvvLRKAoRXByyz3A9sX42gMXOJW61gHrfc4huoYpfjKje8oUavWkoqe8k8mchwwslPYiI1aSc8mugugGOU1r6kDL
EpVEIc4s0key0zDPGPD2IH4ogsY49mL9KcqHg3uMtFT3tNV50TD3LDcGxHBSl8I9ALcv1wLZOiYuBycNQekIVVWxyXN4BkOQjpz6KGms4Qh
2CkkwfSRCFfGx0MLk1VDhIxT44XGceqyx3ogF3r4GInWh2jLusBjuiIS4CRf0xeuUStYjfUhtBOBvK8YKXAOvAiEKCoGRyJ83LTEoTed49c6HB3
3uynAN7b4RHEFFH98Vc8wxSllcXZMixiLF0cftJ2MC0Tmavzjep9WYdQdbVg6i5G8STgD7qGpcuUZjcgf5dP25f3iZRHcB8cSSEGIiz0FyzUYHhCY
tVmyjiVO3Xu6CGyiVXf1IGUBn1AZA8tOALFvrnh3ntFsMgcqrYOZ4vSvo9NMOPTlWJOMidKEefiN7p8CyaFItOAfH8oMoUhptJsDXl6mer1pRIrr
WKmAFh39xSBv3kamicce7yvRX1vJbZp4BKBqJeVh5ODRprbfx97SfsQ2YDgcKUqJTRCuFxflGiV520EhMo5wLj6ap6lSzVzXuGuYo6oR1XnD9tx
hyxkLWVUIVfrmExNKzX5lFLp8PDkIp4QpxXKbW2Y4ivNtVPZw32U7nJFlAhIT1guJGwrjxzPGaRBiTus0WosHLkMxznH4a2Ch7p6L1lllIm70GX
qTIsFq7nRDYswNJthN5Cz0FSzTl8oYN7SuVlLIiScty22OcdHZlz8lssvOdZEF95r8KYazCe0J4DeX0gKyUo7Dsj0uYq8SWDCwPaUYPUOXlhul1ud
Geif4hdEh8hSMMz5LX10MnANwj4XPsI4esHfIiUOgPOPbBRfF9bowuEQvnbvPSkDvqpaaXdEN9lKHSETjwGMyUmwNU2TlJtMDAqXYKVnFIo
Iby6i7xq9ikaJObOrrWYTBGZT5oeha8meSn23e6h9FkQlDb6WOXB2Qob78F3cMnHV1VqGa1VWHcHsI03bRV6KtEJ2QkTEFeG48XKP3d8emcEJ
UctwXmK6c6sUZMBpNHwoDv5eWs0EqHichvBd2OspCZLgLQAP1cgUhlbjNMxaMIWf3HHLrbw8ujYtCe2vA9S1Sacuvl26zqD7lNmTbUVufyy9
m9BLGXdyR0qhB55XP0YsaeENnQ9crngMYBTrwyda3BHQ2MfY0sau6FWP46L3u497uLEthpKzkRPwBPewZOJbiwErgnjum2uPG7GSFXYfyiB
MqDX2Wbr46bvJrr83BQDQMGoroAd0gwS98t04EmY107W261mSaqA11YeO7VjMNKlv17VBMbKHloOlSRTXHPOBf2ujvTyxZtco2T1GwstZ8il
zLbCCzaxOgagdAT4qsWAJCtZeeBV6MkuIKhwCqXgeiSGJhKRLnQWtndS9pVrAUcf0Ez5ruQZAblafhW6wS16LL04HGzw4YkFHqOvpbEs0LfeB
0oiFV7jTkVy298jXaeH0yDiKOH8QQ02p1JEKMl0RgeccJY6KXwJFTlICnDiZrtCqpYcx3irLieg3PZHpZHWFL8s7nqKBDXW8DJcZbDaHYrZP4rT
hxApxokh50WLwEKq3wRpZGaoAkGrCiYE7sF1LwbQ56xyZzZvBwBqCDtZlNqiiDFBDBO4XvKx3xkX3eXxu5dZd42BbJ23FRw58I9L0xgr9tAN
eOPJJwYsQA2haYq5QQNyIRhhTlvjlWFg4CIx9RR1DQriR2m8QfJzygvVIZKO4j16JsiYv5okscZrhxnCwhh3IKuEg8OtJ4SPujGnewkIAlisU3kvHQ9
h4w1HIyufhCXAsANewAsNF8Q23dqPAyPYJC2N2U8BycSh3x8hmycQvcfRflYRodWdCDRhpRLaJTt8GwWMIUmkoTilYjEYgiDzz9FMow65BS
WGe8MZBvGl95fkpPq1rJfKsuaV85nKSxV3NoyStoygD9ZpD31zHDXGW4xAfVQlh1eM9JQ4twr89RpnHG3uTBPeh5u3PO8LTyHStVORTVFq9w
yca7Fw7IM2HZJU1EtlYezqT7jFw0FlST74FtRbB8V8N0pIRduQgx6t7rGojdLMpsH5KmlynySOxF2kAzYoGoyl3YBnQIqAsvkZPA3uN7p8mhpgbon
HtSxnsbG47yOuKsMtqPaMCb3BMpXuwW66RtK1uJfs7TcA3YcDxTUz0B7G3o3iE1tV29VotOG9Myj9PutSc7DKdUBpvKVIEAKHFFl1lL4bGOLa
uqW1gwUN4SvJPDmRHeyJMWoowfgC9lkejJNYlNNr3365VkXRJrstdESnjLrC2wfcZhSqXa5GtGxF0BqPaI6djJbuLE0wZSBVLteaWdONVDpSX9
ehrkeEhfjiaqRpoOr6gKPvQmCJ0ELy41lDp9lGN6NiPJfsJA73SiidNwBjhBUk4WidFWtfcakcAoL1HtpsPEGDicJSv7KHvOmdJMggZctzEi2oCeKlQy
dfpWUU98ZmpUaj03nwWbTT5kAcKKiNvydt0bJT2YGecnd9Tl7RsuP1F1iIR0bX73STkjxcqbPD8wXsq7oiyp10no5yB8qNk0gLyntg8ZefLaO87b0f6
```

```
DOpetfugVbbgZ7OLNKKerob1SDPmW3SJUQNQUSvfjADs7ZrXOR6ufHTlq8C5zStVMOTcq620pZtb86hlX5RIkDclXWaSKYXMvTYigiuzqGBD
qwWJaOyHTlZAllPnszs0X9ETp4LEa5Hxh6he1kmYp5eVpMocn7WEQF460pkpwu0CVLM1Ahfn37CRgaP3elYQOHCdpq6uk6ArXszqmHSgXwsw
sGpsOosrPqNjnlW4mMd5pwo3SF4y5pdIiB4yWqGKARJ314U1L1xlkMfkkq5tP1ms1y6EZm5V4fPiRUdYmD7BYRaTUof96gMG4L0NA0yGfG7WD
6WJIEAhrrnAdoxPvaxpdJJYGlnvPgHuajfuP1IZWDNheOzWDHh7PZ4wQjzg4kOW3SFgGmEeBgV9x9rRyAOxZbq9TC8jZj5nmgFftEZPPoSVZhW
wAouAIiNZS5uYeHuPc5lvxX2R8z1ABcPC5HEQ482ng3VzvDfPhloo80YlIsHV3xbJywUck1lJue7INrEpehgkPVarhfqGeq16KIEO6Ja7PMOiVZJAbt
voLIgnOgkrrgZdcQ1ruE7NvFzA0ZSiMvjeuVCYpq6dLOd2FQu977tx7is8eVk2GNpPI6sJeXXFV3jd1bK7l0G0ox1NB8vHteOsCqjGrYj3owsLYS31d
DiPiLduTmlfUIhE72bJ9erYYoMKlXbyFF3EbBu3DzoBLCtgDG4GzGJwD0GvdQGkrsn2HtPVhhZfScJzM08Z1p7tQ7xRt6D6kv0jwU5WpV4cVRKs
D0jUaiVS6CgOl6Rj0dY5GG6NaVayenHG0quxbRXz1ZighaJRdJP06FhNDP1upWnc266h273ayfxeNx5pG98WsAR9z0nT3iGsYgs3IvO0Ryx7NK3G
dRfxiqDDXrlfgxbZmRk7KGNoalMmK3Vpxfk9vHmNVe0j634O9OhtrGZ1rd7dj3LjuhC82uFrB2x51d55rhiTtHBFYalYQnmHLR8zZhEMhbGpc4SD3
OcJhiaPKGZctMCZ6LliUyWHoXBVITn<script>alert(foo)</script> returned an error: error reading HTTP response
+ 3818 items checked: 5 item(s) reported on remote host
+ End Time:           2010-06-13 22:14:53 (82 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

..and lets try it against something else..

```
# ./nikto.pl -h http://192.168.2.107:3000
- Nikto v2.1.1
---------------------------------------------------------------------------
+ Target IP:          192.168.2.107
+ Target Hostname:    dojo-vm.local
+ Target Port:        3000
+ Start Time:         2010-06-13 22:22:44
---------------------------------------------------------------------------
+ Server: WEBrick/1.3.1 (Ruby/1.8.7/2009-06-12)
+ robots.txt retrieved but it does not contain any 'disallow' entries (which is odd).
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ETag header found on server, inode: 187690, size: 99, mtime: 0x461bf506
+ Number of sections in the version string differ from those in the database, the server reports:
webrick/1.3.1(ruby/1.8.7/2009-06-12)
while the database has: 1.3.1. This may cause false positives.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ /search.php?searchfor=\"><script>alert('Vulnerable');</script>: Siteframe 2.2.4 is vulnerable to Cross
Site Scripting
(XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /members.asp?SF=%22;}alert('Vulnerable');function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and below is
vulnerable to
Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /forum_members.asp?find=%22;}alert('Vulnerable');function%20x(){v%20=%22: Web Wiz Forums ver. 7.01 and
below is vulnerable
to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ OSVDB-3268: /docs/: Directory indexing is enabled: /docs
+ OSVDB-6659: /
lQXd3Xte8ytxtKwsZl5HZEsNVjrcrGg2Tuh8iyrbE3Wr1Hg7WLpzu6Y7BQTexRmBYz5spzE2WKqTiT4tzP3LUPwDwj0yHANw7
e5wYw8Y9sBEVCPt3o0VCrzSUqfwVG2SD3NWHjP0sAeAw84tDUMrbWeGkx40UJFfGPohCSKdznThS0p3gnaA5NBFnoLurmXDA9CssltWwCa
7J0AwHeuF11UNJwNDtdE<font%20size=50>DEFACED<!--//--: MyWebServer 1.0.2 is vulnerable to HTML injection.
Upgrade to a later version.
Nested quantifiers in regex; marked by <-- HERE in m/^//pls/portal/owa_util.cellsprint?p_theQuery=select+*
<-- HERE +from+sys.dba_users\??/ at /admin/tools/web/nikto-2.1.1/plugins/nikto_core.plugin line 332, <IN>
line 451.
```

Now bear in mind, this is not exactly a stealthy tool, anyone who even vaguely watches the logs will see these scans without too much trouble. But for the purposes of checking whether there is a glaring problem on your site, it does exactly what you want it to.

Final Words

Another great feature about *nikto* is that it is able to be scripted, and as such you can set it up in cron and let it check at regular intervals. The trick is, as with all such things, to run it yourself before someone else does it for you. It also goes without saying that when it does find something, you should check it out. As always, have fun and learn.