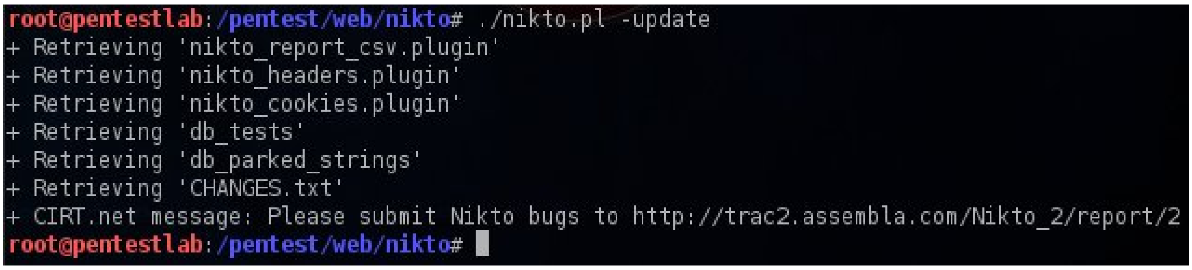
Scanning Web Servers With Nikto

pentestlab.blog/category/web-application/page/9

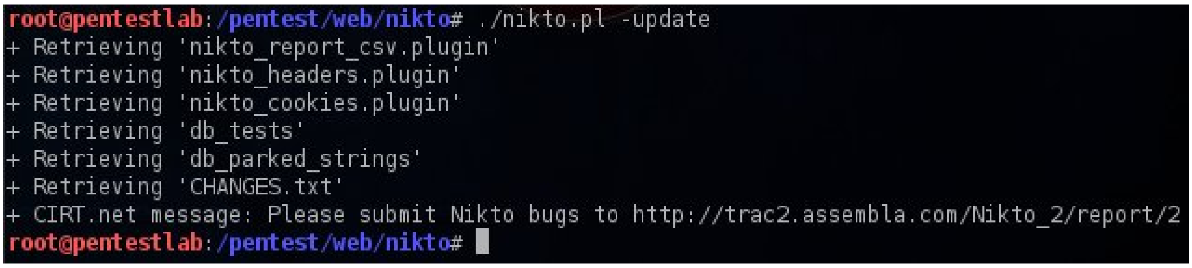
December 6, 2012



```
root@pentestlab:/pentest/web/nikto# ./nikto.pl -update
+ Retrieving 'nikto_report_csv.plugin'
+ Retrieving 'nikto_headers.plugin'
+ Retrieving 'nikto_cookies.plugin'
+ Retrieving 'db_tests'
+ Retrieving 'db_parked_strings'
+ Retrieving 'CHANGES.txt'
+ CIRT.net message: Please submit Nikto bugs to http://trac2.assembla.com/Nikto_2/report/2
root@pentestlab:/pentest/web/nikto#
```

Nikto is a tool that it has been written in Perl and it can perform tests against web servers in order to identify potential vulnerabilities.Nikto can be used in web application penetration tests and in some cases can produce juicy results.Specifically if a system administrator has not configured very well his web server and the web server is out of date or there is a misconfiguration Nikto is capable to find them.

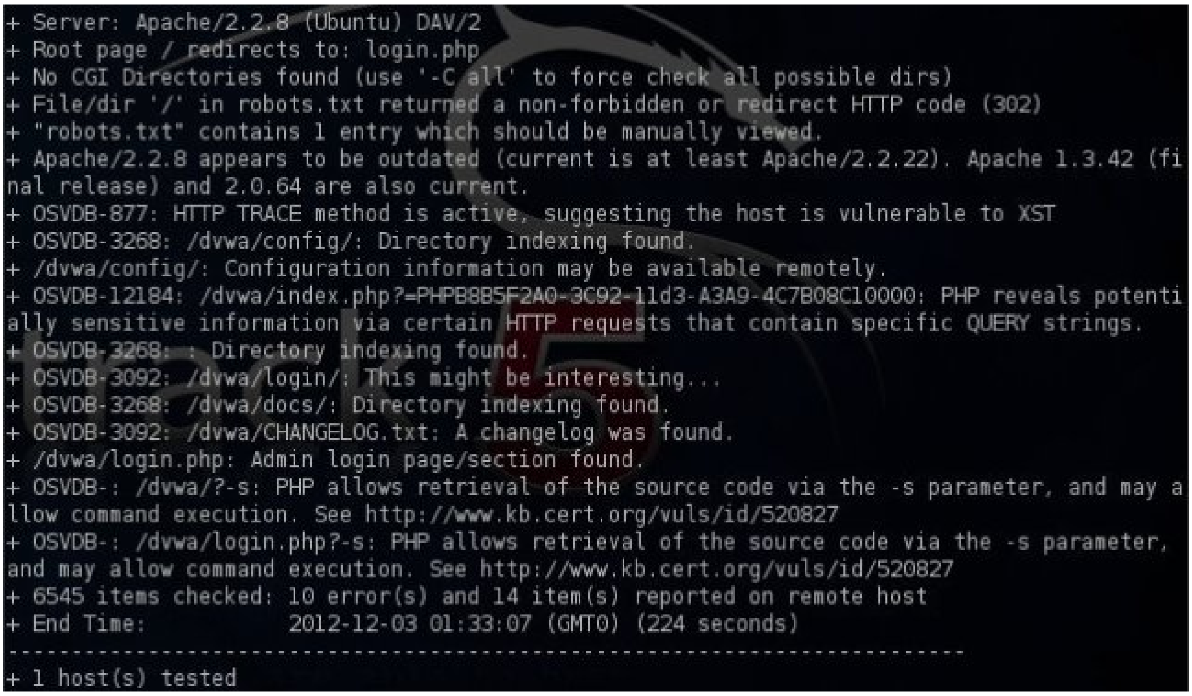
For the needs of the article we will use Nikto in order to scan the web server where the DVWA (Damn Vulnerable Web Application) is hosted.Before we start the scan it is always a good practice to perform an update for obtaining the latest plugins.This can be achieved with the **-update** parameter.



```
root@pentestlab:/pentest/web/nikto# ./nikto.pl -update
+ Retrieving 'nikto_report_csv.plugin'
+ Retrieving 'nikto_headers.plugin'
+ Retrieving 'nikto_cookies.plugin'
+ Retrieving 'db_tests'
+ Retrieving 'db_parked_strings'
+ Retrieving 'CHANGES.txt'
+ CIRT.net message: Please submit Nikto bugs to http://trac2.assembla.com/Nikto_2/report/2
root@pentestlab:/pentest/web/nikto#
```

Updating Nikto

Now we can scan the URL of the web application with the command **./nikto.pl -host IP**.You can see the results of Nikto in the next image:



```
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ File/dir '/' in robots.txt returned a non-forbidden or redirect HTTP code (302)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (fi
nal release) and 2.0.64 are also current.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /dvwa/config/: Directory indexing found.
+ /dvwa/config/: Configuration information may be available remotely.
+ OSVDB-12184: /dvwa/index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potenti
ally sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: : Directory indexing found.
+ OSVDB-3092: /dvwa/login/: This might be interesting...
+ OSVDB-3268: /dvwa/docs/: Directory indexing found.
+ OSVDB-3092: /dvwa/CHANGELOG.txt: A changelog was found.
+ /dvwa/login.php: Admin login page/section found.
+ OSVDB-: /dvwa/?-s: PHP allows retrieval of the source code via the -s parameter, and may a
llow command execution. See http://www.kb.cert.org/vuls/id/520827
+ OSVDB-: /dvwa/login.php?-s: PHP allows retrieval of the source code via the -s parameter,
and may allow command execution. See http://www.kb.cert.org/vuls/id/520827
+ 6545 items checked: 10 error(s) and 14 item(s) reported on remote host
+ End Time:           2012-12-03 01:33:07 (GMT0) (224 seconds)
---------------------------------------------------------------------
+ 1 host(s) tested
```

Nikto results

Analyzing The Output

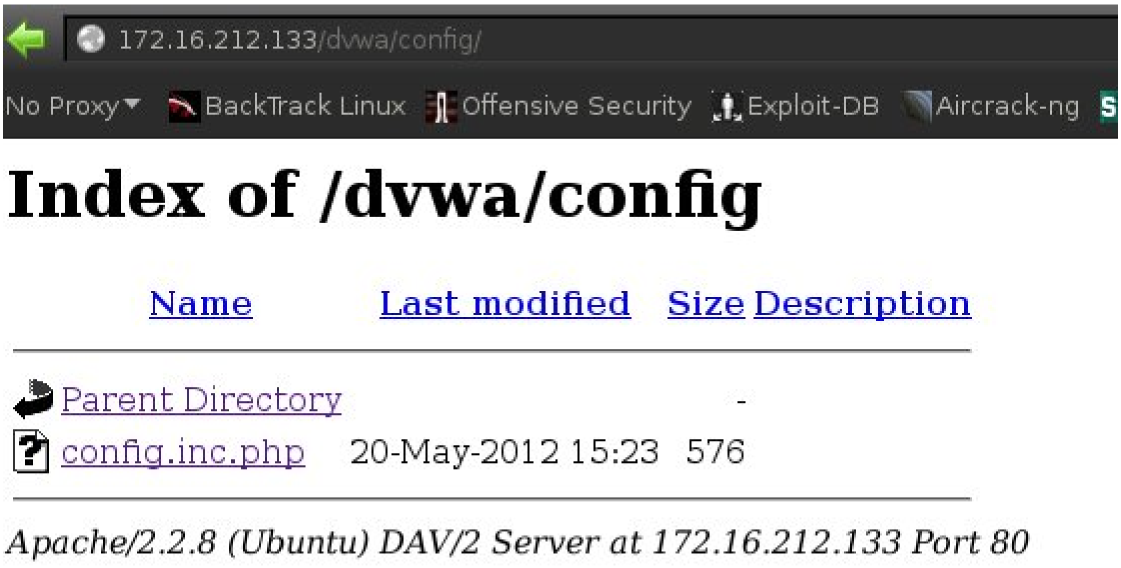
The first information that we have is the version of the Apache which is 2.2.8.So we can check on the web in order to see what kind of vulnerabilities exist for this version.Also Nikto discovered the robots.txt file which in many cases can contain sensitive directories and it must always be checked.In this case the robots.txt contained the following entry:

User-agent: *

Disallow: /

This actually means that all the robots should not visit any pages on this site.The next information that we have from Nikto is that the version of the web server is out of date which can be considered as an issue.Additionally Nikto has identified that the TRACE method is allowed.This method is used to debug web server connections and can be abused in order to disclose sensitive information configuration.

If we rate these issues so far we can say that the impact is low.However Nikto has discovered other issues which seems to be most interesting.Lets examine the directory indexing in the **dvwa/config/**.



Index of /dvwa/config

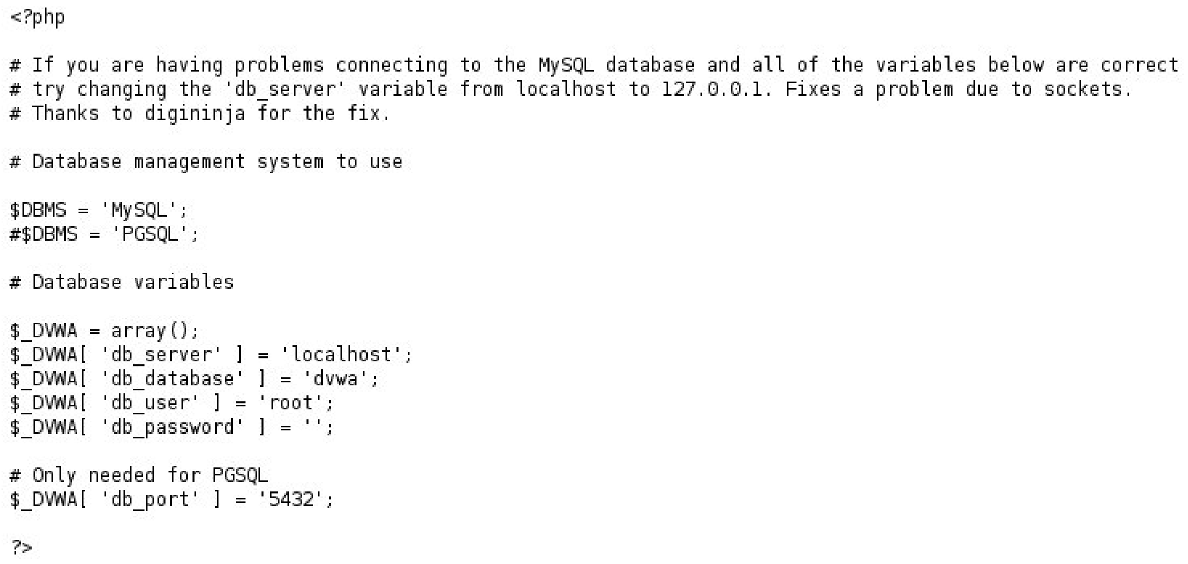
Name	Last modified	Size	Description
Parent Directory		-	
config.inc.php	20-May-2012 15:23	576	

Apache/2.2.8 (Ubuntu) DAV/2 Server at 172.16.212.133 Port 80

Directory Indexing – DVWA

We can see that there is a PHP file which probably contains the configuration details of the application.In order to see what this file contains we will put the ~ after the config.inc.php file so the URL will be:

http://172.16.212.133/dvwa/config/config.inc.php~



```
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
# Thanks to digininja for the fix.

# Database management system to use

$DBMS = 'MySQL';
#$DBMS = 'PGSQL';

# Database variables

$_DVWA = array();
$_DVWA[ 'db_server' ] = 'localhost';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ] = 'root';
$_DVWA[ 'db_password' ] = '';

# Only needed for PGSQL
$_DVWA[ 'db_port' ] = '5432';

?>
```

Discover credentials on the config.php file

As we can see from the config file we obtained the following information:

- Application Database (dvwa)
- Database User (root)
- Database Password (null)

We can now use these credentials in order to connect and to own the database of the application.We can of course check and the other issues but from the moment that we have valid credentials for the database the goal has achieved.

Conclusion

This was just a simple demonstration of the capabilities of Nikto against a web server that was intentionally vulnerable.Also from this tutorial we saw that it is always a good practice to check the config files as they might contain plain text credentials and the major effectiveness of Nikto to discover misconfiguration on the web server.However this doesn’t mean that this amount of vulnerabilities will be discovered in real world scenarios as in nowadays most administrators have the knowledge to avoid that kind of mistakes when configuring their web servers.