

Lab 6-5-1 Scanning Using Nikto

```
File Actions Edit View Help
(kali@kali)~$ nikto -h 192.168.111.131
- Nikto v2.1.6

+ Target IP: 192.168.111.131
+ Target Hostname: 192.168.111.131
+ Target Port: 80
+ Start Time: 2022-01-13 07:18:08 (GMT-5)

+ Server: Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090
110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1
+ Cookie PHPSESSID created without the httponly flag
+ Cookie security created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.3.1
+ 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 prote
ct 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 different fashion to the MIME type
+ Root page / redirects to: login.php
+ Server may leak inodes via ETags, header found with file /robots.txt, inode: 2207, size: 26
, mtime: Tue Aug 24 15:45:32 2010
+ mod_apreq2-20090110/2.7.1 appears to be outdated (current is at least 2.8.0)
+ PHP/5.3.1 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13,
7.2.1 may also current release for each branch.
+ Apache/2.2.14 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is
the EOL for the 2.x branch.
+ OpenSSL/0.9.8l appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0o and 0.9.8
zc are also current.
+ mod_perl/2.0.4 appears to be outdated (current is at least 2.0.8)
+ mod_ssl/2.2.14 appears to be outdated (current is at least 2.8.31) (may depend on server ve
rsion)
+ Perl/v5.10.1 appears to be outdated (current is at least v5.20.0)
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute f
orce file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternati
ves for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.
html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT
_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, H
TTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html
.var, HTTP_NOT_FOUND.html.var
+ OSVDB-112004: /cgi-bin/printenv: Site appears vulnerable to the 'shellshock' vulnerability
```

File Edit View History Bookmarks Tools Help

Index of /config

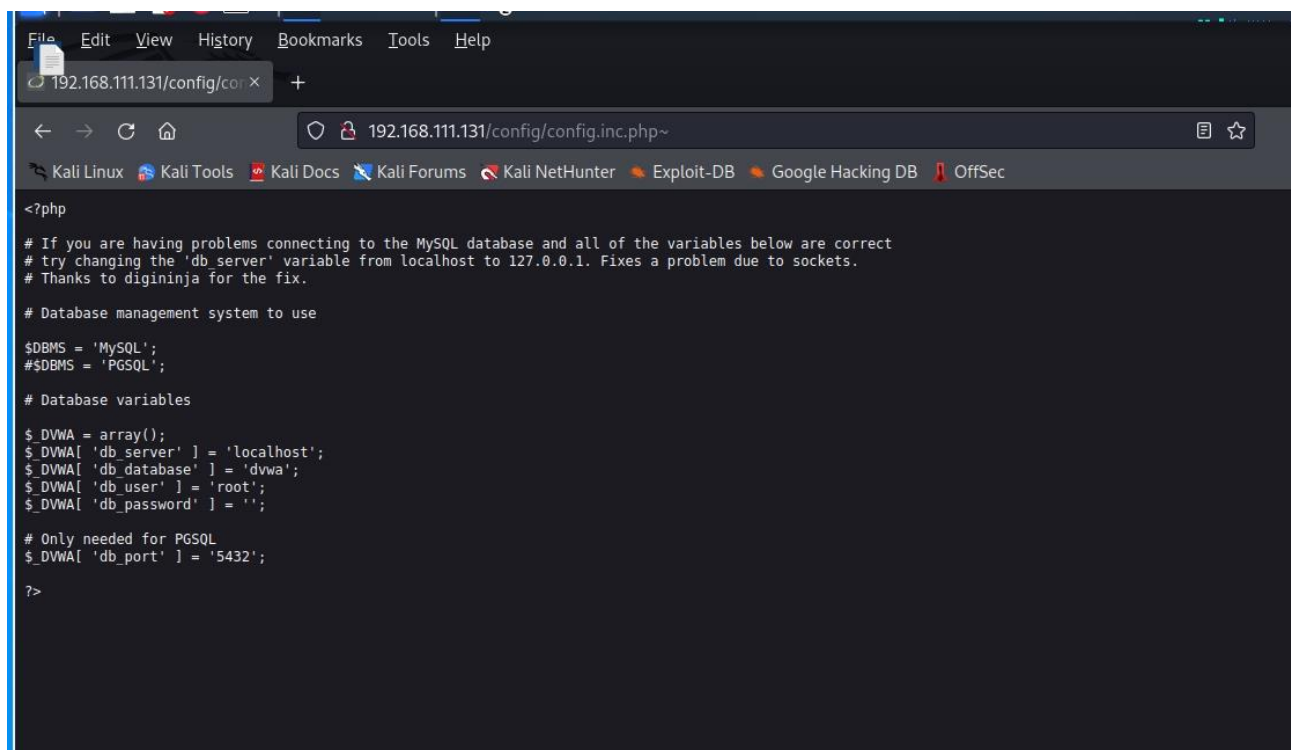
192.168.111.131/config/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Index of /config

Name	Last modified	Size	Description
Parent Directory	-	-	-
config.inc.php	24-Aug-2010 20:45	576	

Apache/2.2.14 (Unix) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1 St
Port 80



```
<?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';

?>
```