{ }

RP Web Scanning - TryHackMe

Ludovic COULON

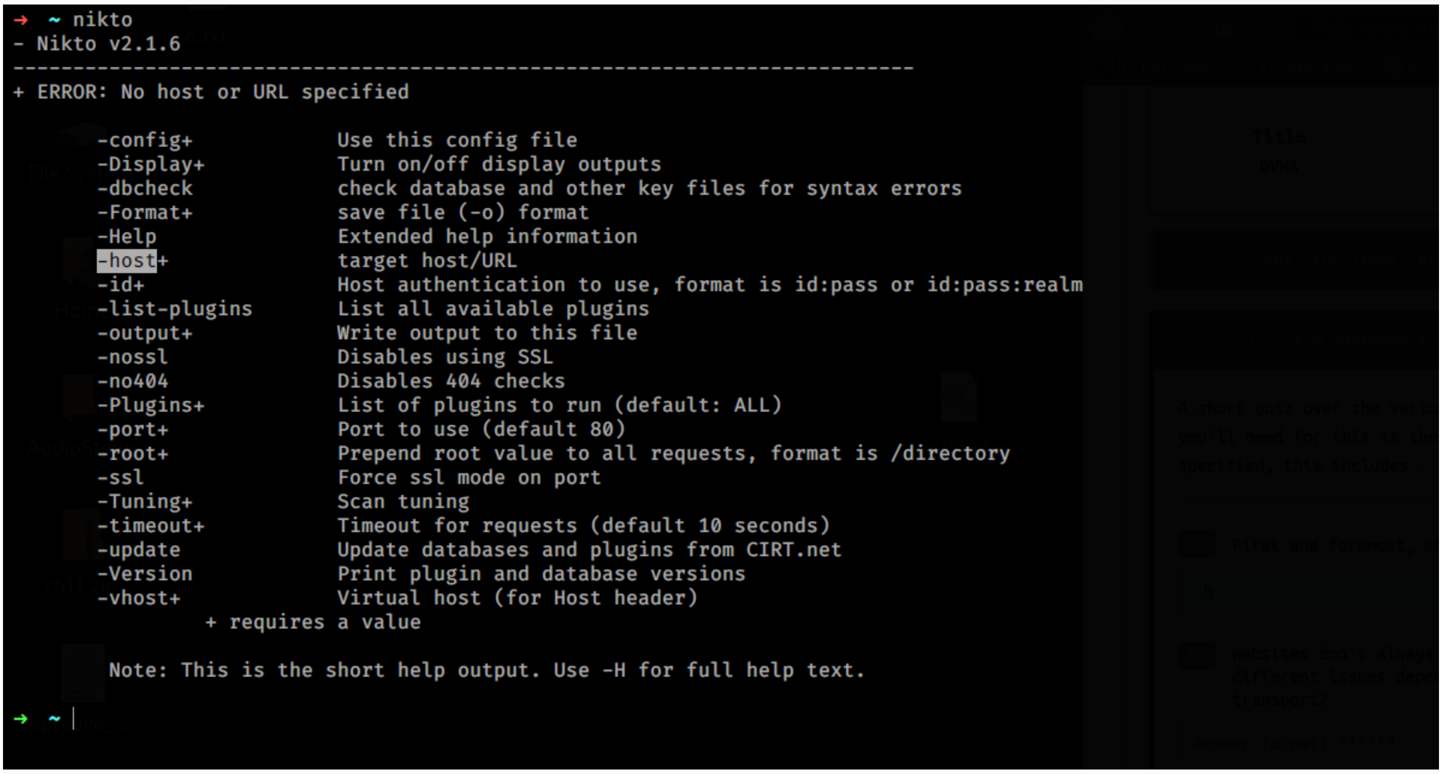
June 19th, 2020 · 3 min read

TryHackMe | RP: Web Scanning

A short quiz over the various switches used with Nikto as well as a quick scan against our target. All you'll need for this is the help menu for nikto. Include all parts of the switch unless otherwise specified.

#1 First and foremost, what switch do we use to set the target host?

```
-h
```

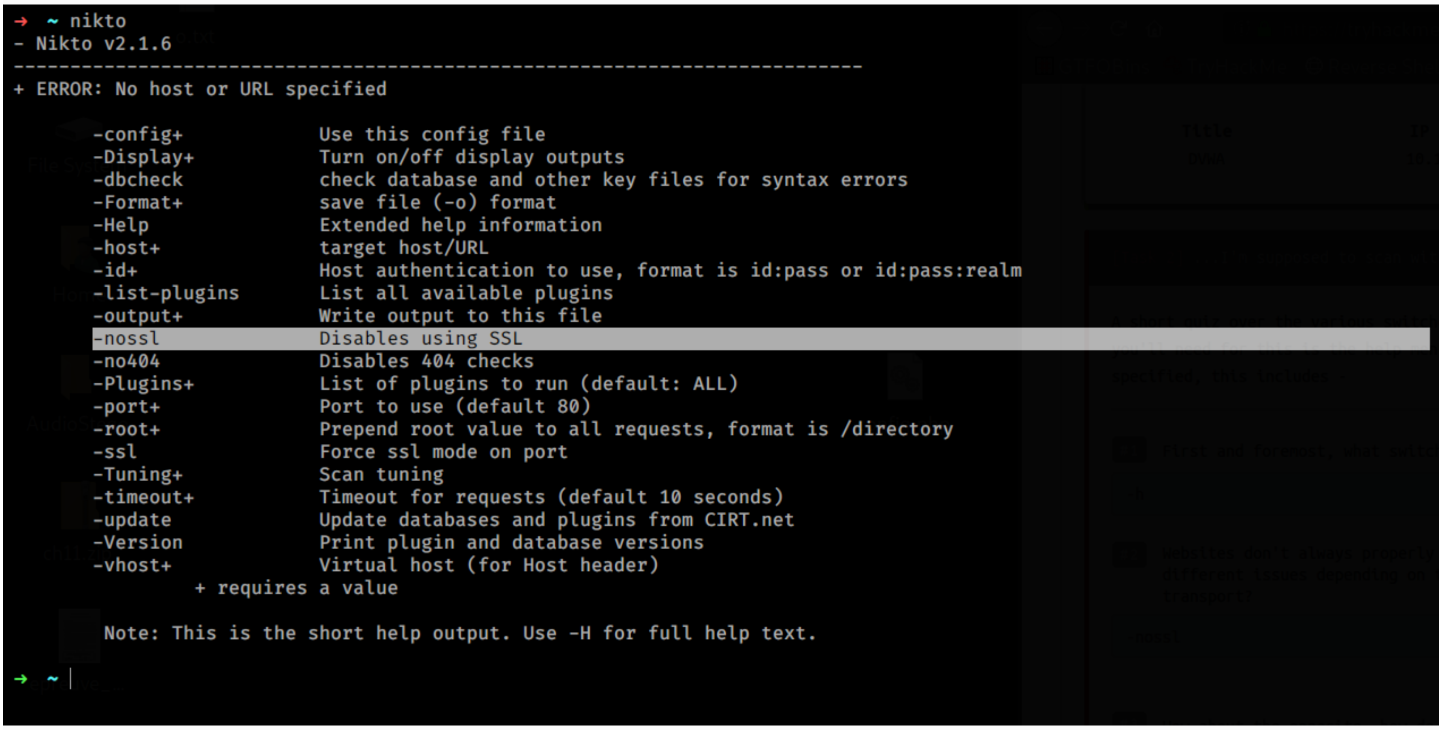


```
➜ ~ nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host or URL specified

       -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.

➜ ~ |
```

#2 Websites don’t always properly redirect to their secure transport port and can sometimes have different issues depending

on the manner in which they are scanned. How do we disable secure transport?

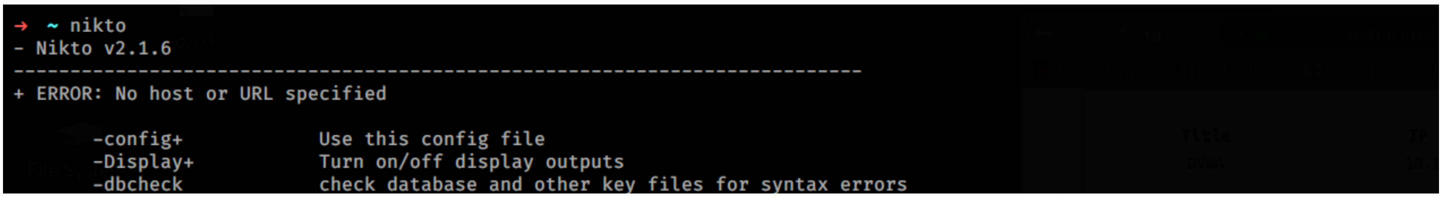
```
-nossl
```



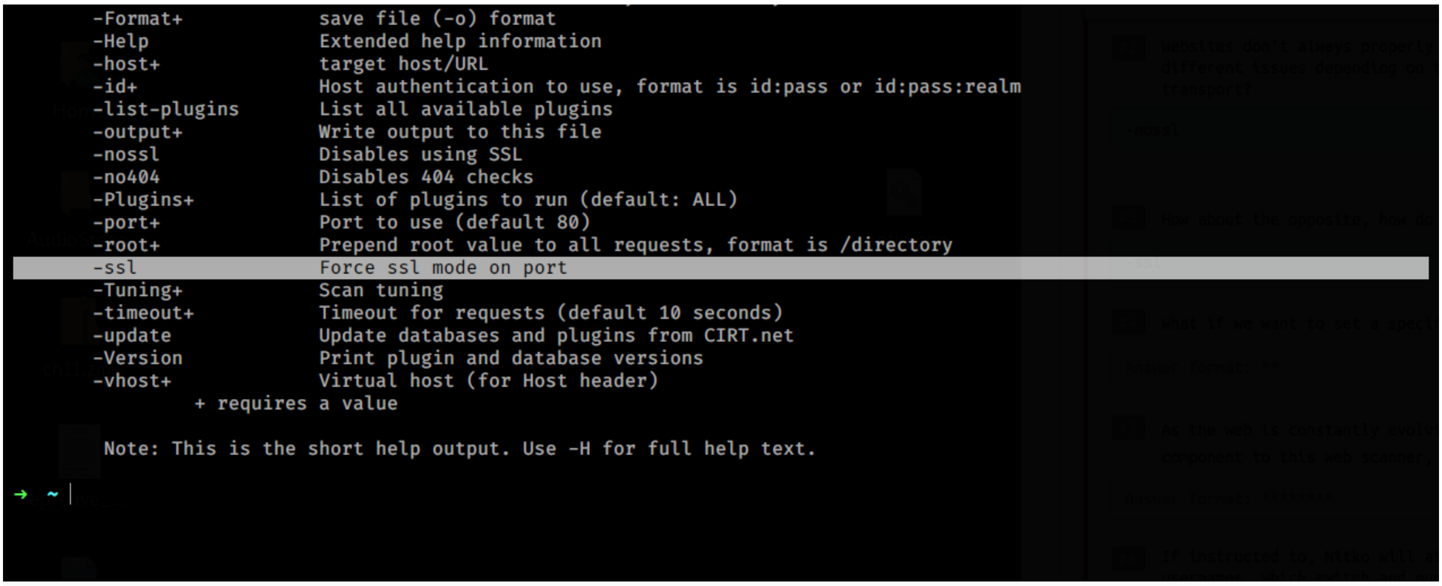
```
➜ ~ nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host or URL specified

       -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.

➜ ~
```

#3 How about the opposite, how do we force secure transport?

```
-ssl
```



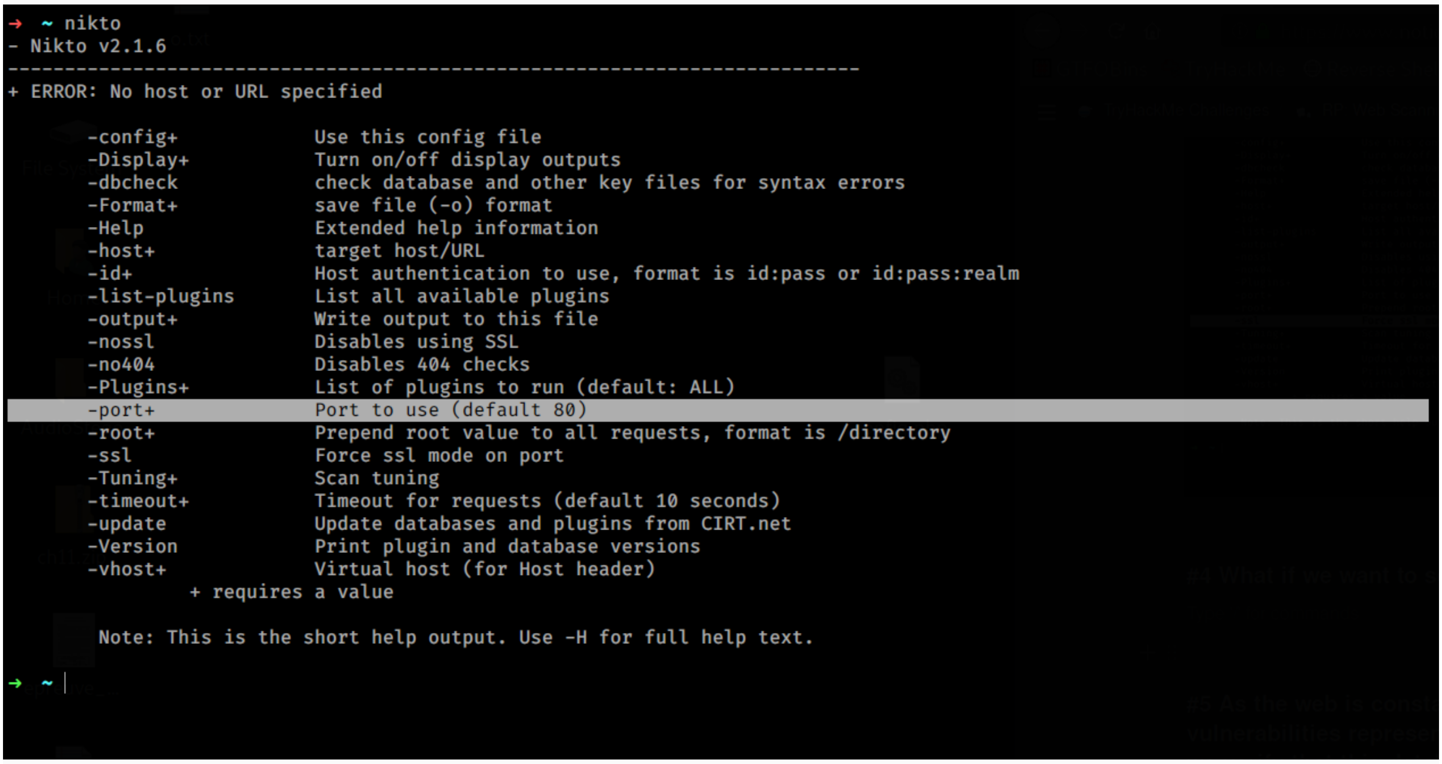
```
➜ ~ nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host or URL specified

       -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.

➜ ~ |
```

#4 What if we want to set a specific port to scan?

-p

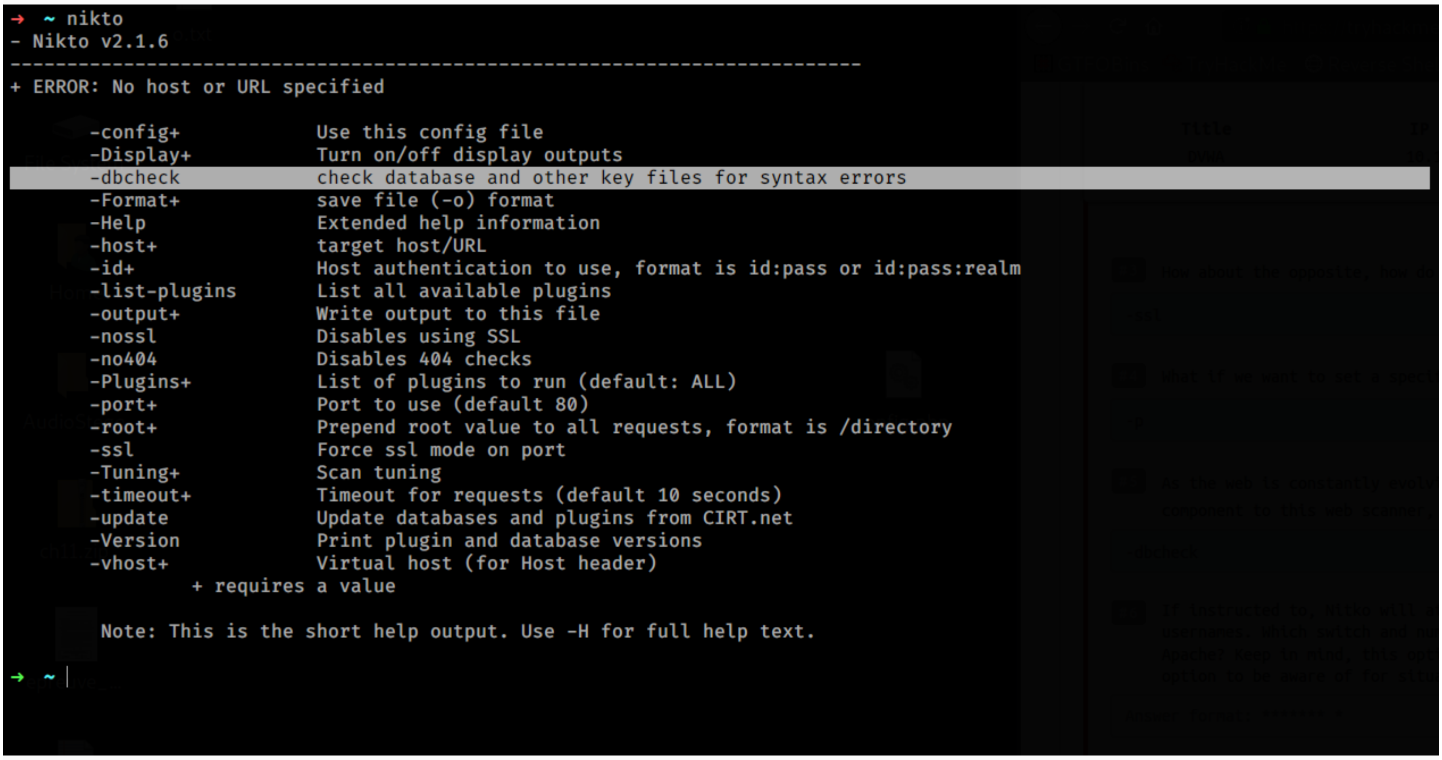


```
➜ ~ nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host or URL specified

       -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.

➜ ~ |
```

#5 As the web is constantly evolving, so is Nikto. A database of

vulnerabilities represents a core component to this web scanner, how do we verify that this database is working and free from error?

```
-dbcheck
```



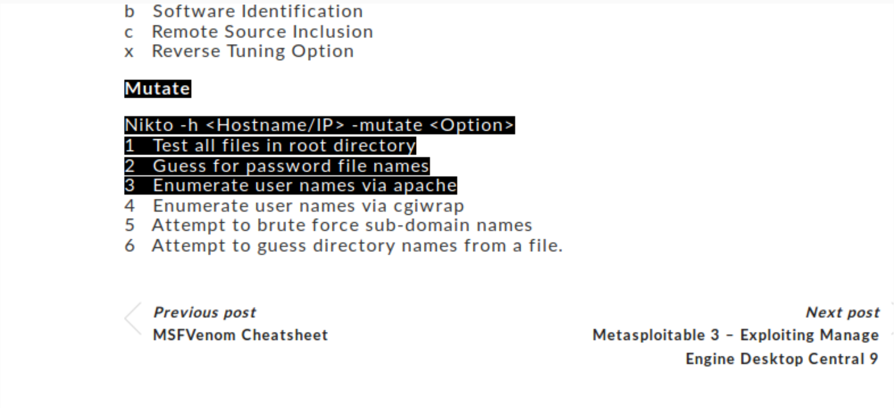
```
➜ ~ nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host or URL specified

       -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.

➜ ~ |
```

#6 If instructed to, Nitko will attempt to guess and test both files within

directories as well as usernames. Which switch and numerical value do we use to set Nikto to enumerate usernames in Apache? Keep in mind, this option is

deprecated in favor of plugins, however, it’s still a great option to be aware of for situational usage.

```
-mutate 3
```



b Software Identification
c Remote Source Inclusion
x Reverse Tuning Option

Mutate

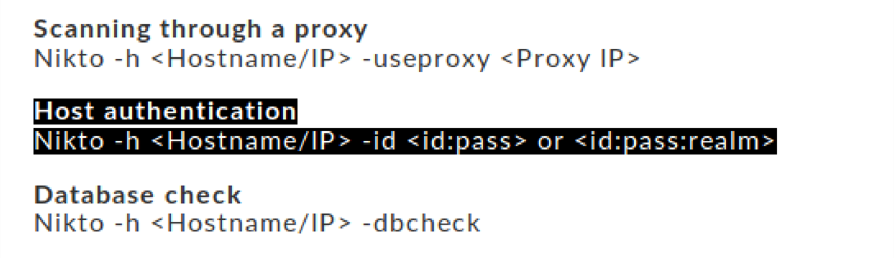
Nikto -h <Hostname/IP> -mutate <Option>
1 Test all files in root directory
2 Guess for password file names
3 Enumerate user names via apache
4 Enumerate user names via cgiwrap
5 Attempt to brute force sub-domain names
6 Attempt to guess directory names from a file.

Previous post
MSFVenom Cheatsheet
Next post
Metasploitable 3 – Exploiting Manage Engine Desktop Central 9

#7 Suppose we know the username and password for a web forum, how do we set Nikto to do a credentialed check? Suppose

the username is admin and the password is PrettyAwesomePassword1234

```
-i admin:PrettyAwesomePassword1234
```



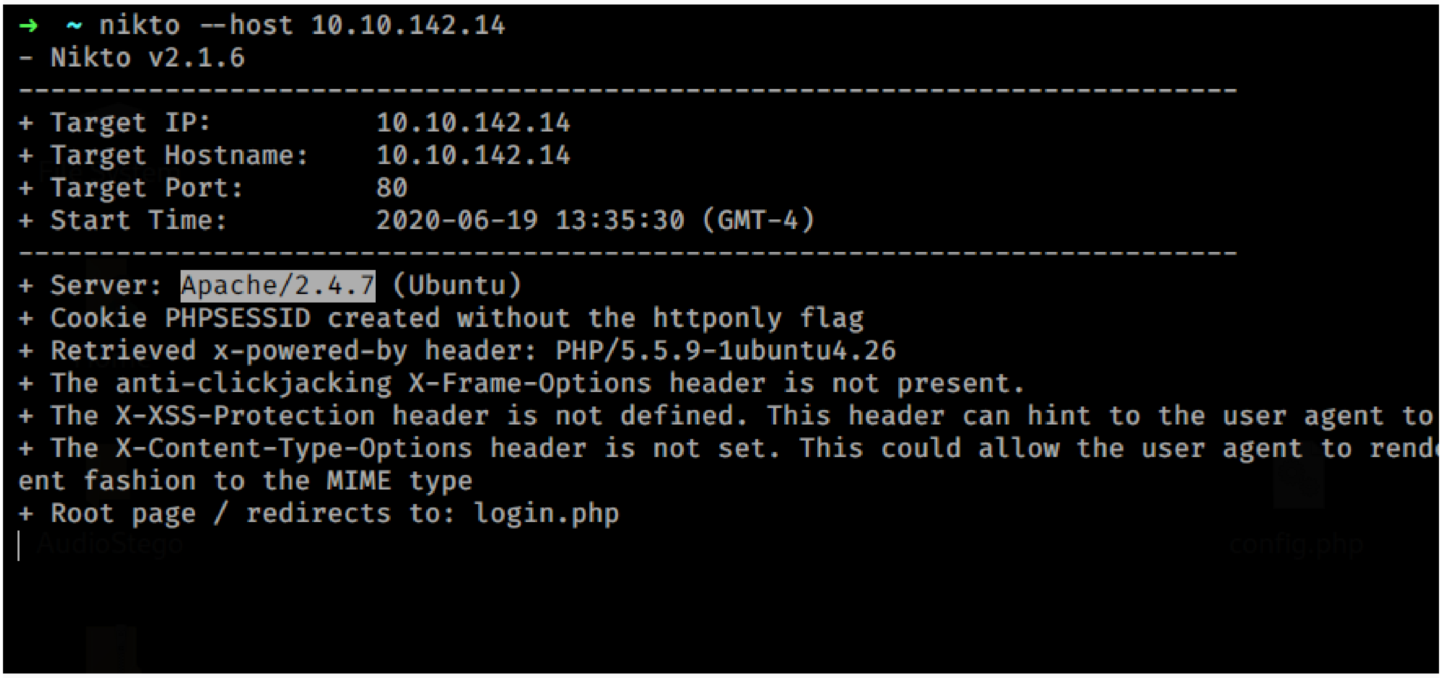
Scanning through a proxy
Nikto -h <Hostname/IP> -useproxy <Proxy IP>

Host authentication
Nikto -h <Hostname/IP> -id <id:pass> or <id:pass:realm>

Database check
Nikto -h <Hostname/IP> -dbcheck

#8 Let’s scan our target machine, what web server do we discover and what version is it?

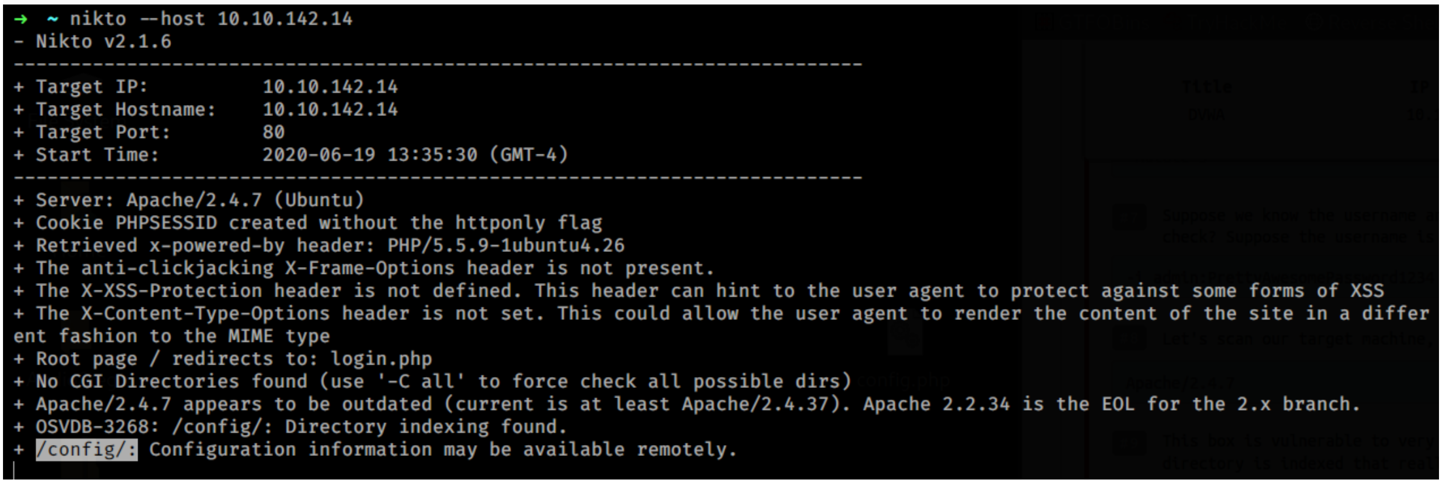
```
Apache/2.4.7
```



```
➜  ~ nikto --host 10.10.142.14
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.142.14
+ Target Hostname:    10.10.142.14
+ Target Port:        80
+ Start Time:         2020-06-19 13:35:30 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26
+ 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
+ The X-Content-Type-Options header is not set. This could allow the user agent to rend
ent fashion to the MIME type
+ Root page / redirects to: login.php
```

#9 This box is vulnerable to very poor directory control due to it’s web server version, what directory is indexed that really shouldn’t be?

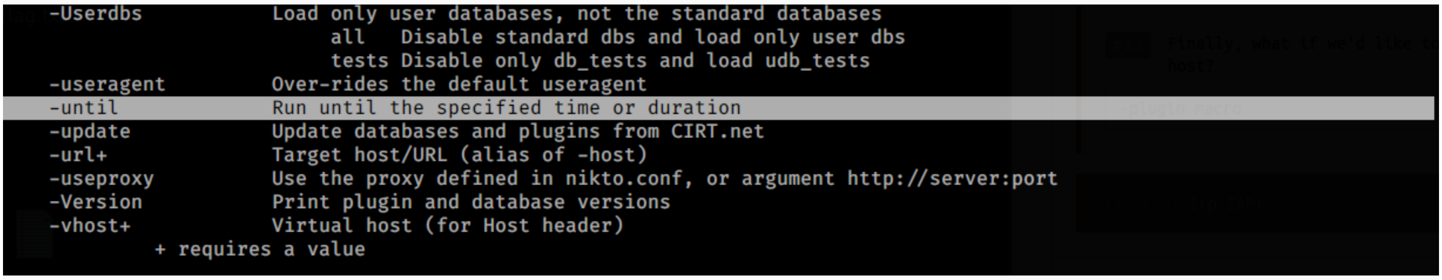
```
config
```



```
➜  ~ nikto --host 10.10.142.14
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.142.14
+ Target Hostname:    10.10.142.14
+ Target Port:        80
+ Start Time:         2020-06-19 13:35:30 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Cookie PHPSESSID created without the httponly flag
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26
+ 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 protect 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 differ
ent fashion to the MIME type
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 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.
+ OSVDB-3268: /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
```

#10 Nikto scans can take a while to fully complete, which switch do we set in order to limit the scan to end at a certain time?

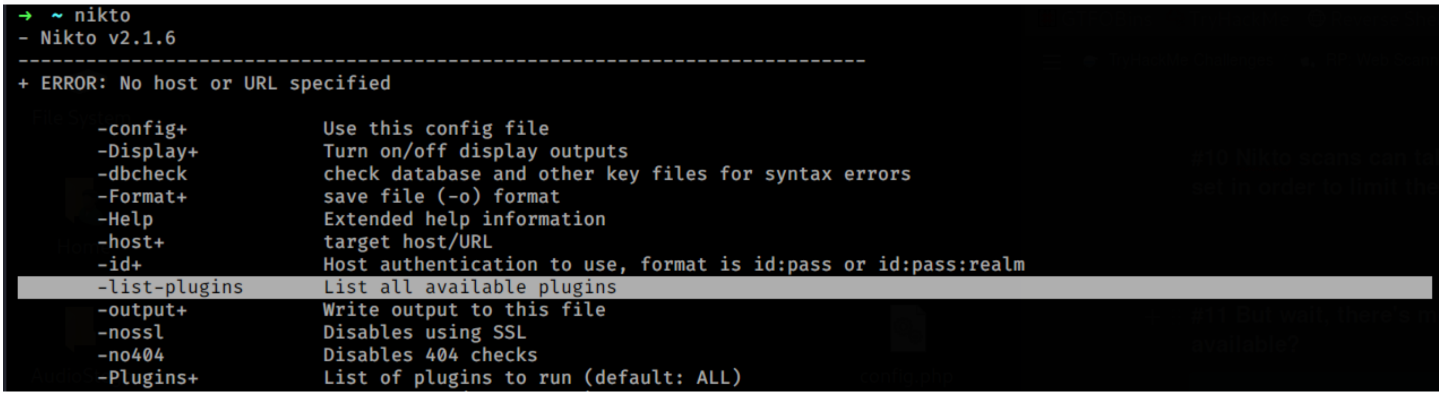
```
-until
```



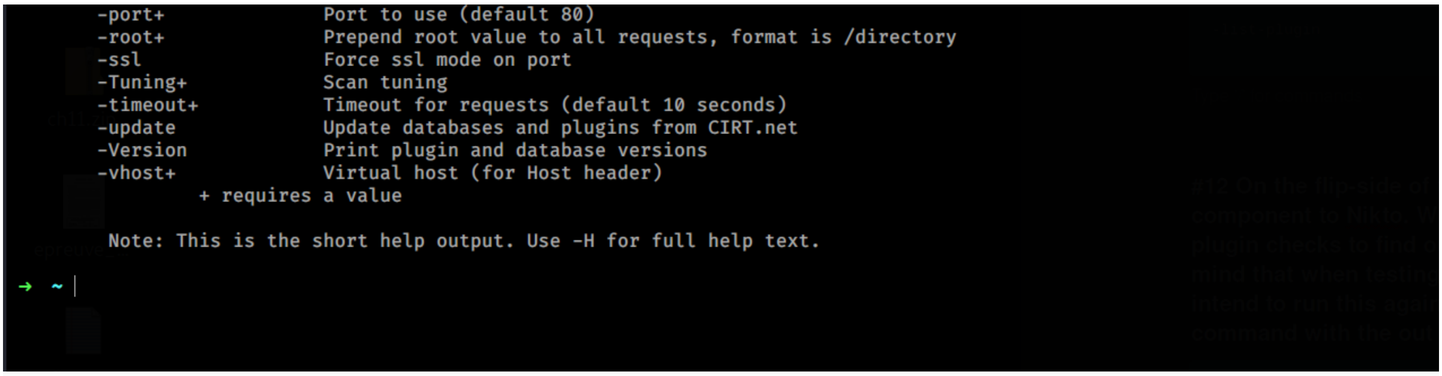
```
   -Userdbs            Load only user databases, not the standard databases
                            all   Disable standard dbs and load only user dbs
                            tests Disable only db_tests and load udb_tests
   -useragent          Over-rides the default useragent
   -until              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
```

#11 But wait, there’s more! How do we list all of the plugins are available?

```
-list-plugin
```



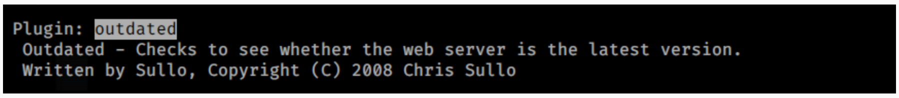
```
➜  ~ nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host or URL specified

       -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.

➜ ~ |
```

#12 On the flip-side of the database, plugins represent another core component to Nikto. Which switch do we use to instruct Nikto to use plugin checks to find out of date software on the target host? Keep in mind that when testing this command we need to specify the host we intend to run this against. For submitting your answer, use only the base command with the out of date option.

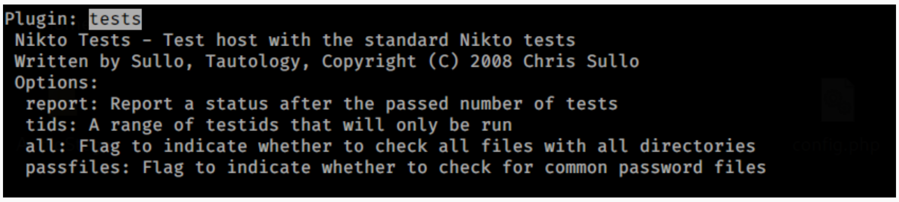
```
-plugin outated
```



```
Plugin: outdated
 Outdated - Checks to see whether the web server is the latest version.
 Written by Sullo, Copyright (C) 2008 Chris Sullo
```

#13 Finally, what if we'd like to use our plugins to run a series of standard tests against the target host?

```
-plugin tests
```



```
Plugin: tests
 Nikto Tests - Test host with the standard Nikto tests
 Written by Sullo, Tautology, Copyright (C) 2008 Chris Sullo
 Options:
  report: Report a status after the passed number of tests
  tids: A range of testids that will only be run
  all: Flag to indicate whether to check all files with all directories
  passfiles: Flag to indicate whether to check for common password files
```

A brief quiz and tutorial over using the OWASP Zap Scanner

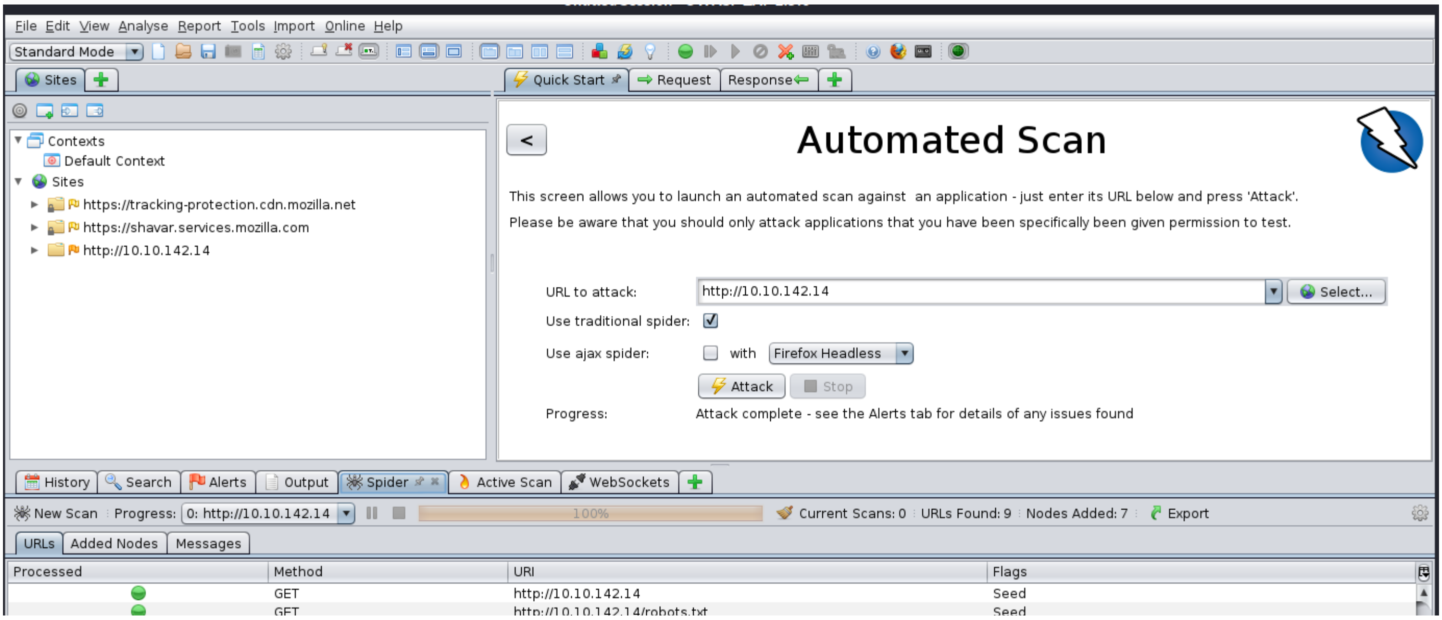
#1 Let's start simple and launch zap. This can be done in a number of ways

(Commands: owasp-zap, zaproxy) or through launching it in the Kali GUI.

```
No awnser needed
```

#2 Launch ZAP, what option to we set in order to specify what we are attacking?

```
Url to attack
```



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://10.10.142.14

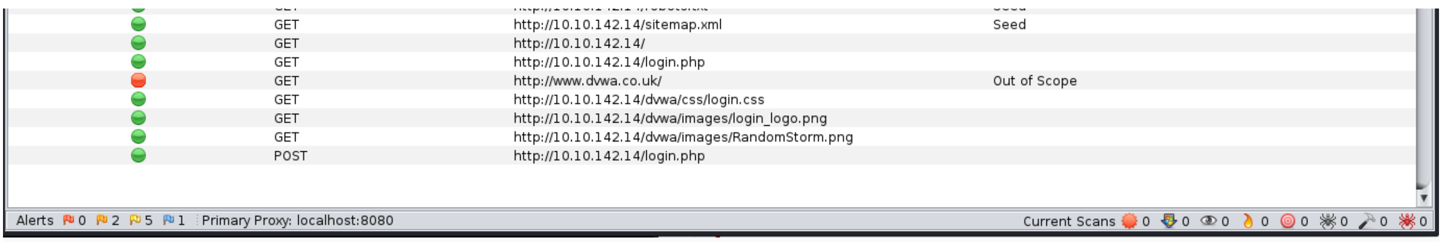
Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Attack complete - see the Alerts tab for details of any issues found

Progress: 0: http://10.10.142.14 100% Current Scans: 0 URLs Found: 9 Nodes Added: 7

Processed	Method	URI	Flags
●	GET	http://10.10.142.14	Seed
●	GET	http://10.10.142.14/robots.txt	Seed



●	GET	http://10.10.142.14/robots.txt	Seed
●	GET	http://10.10.142.14/sitemap.xml	Seed
●	GET	http://10.10.142.14/	
●	GET	http://10.10.142.14/login.php	
●	GET	http://www.dvwa.co.uk/	Out of Scope
●	GET	http://10.10.142.14/dvwa/css/login.css	
●	GET	http://10.10.142.14/dvwa/images/login_logo.png	
●	GET	http://10.10.142.14/dvwa/images/RandomStorm.png	
●	POST	http://10.10.142.14/login.php	

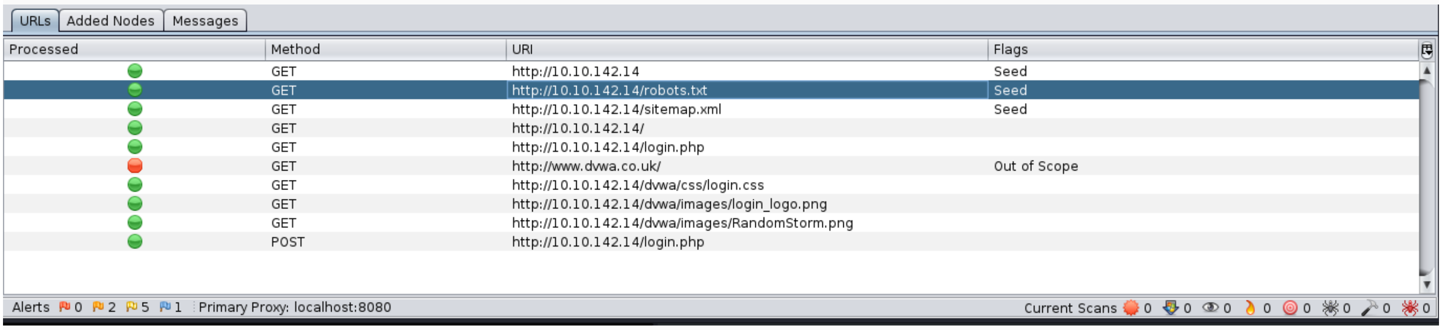
#3 Launch the attack against our target! Throughout the course of this attack you may notice this is very similar to Nikto. Similar to Nessus vs.

OpenVAS, Nikto and ZAP and both offer different perspectives on a host and, as such, it’s useful to know how to leverage both scanning tools in order to maximize your own visibility in a situation wherein ‘noise’ doesn’t particularly matter.

```
No awnser needed
```

#4 ZAP will discover a file that typically contains pages which well-behaved web indexing engines will read in order to know which sections of a site to avoid. What is the name of this file? (Lucky for us, our scanner isn’t what we would call ‘well-behaved’!)

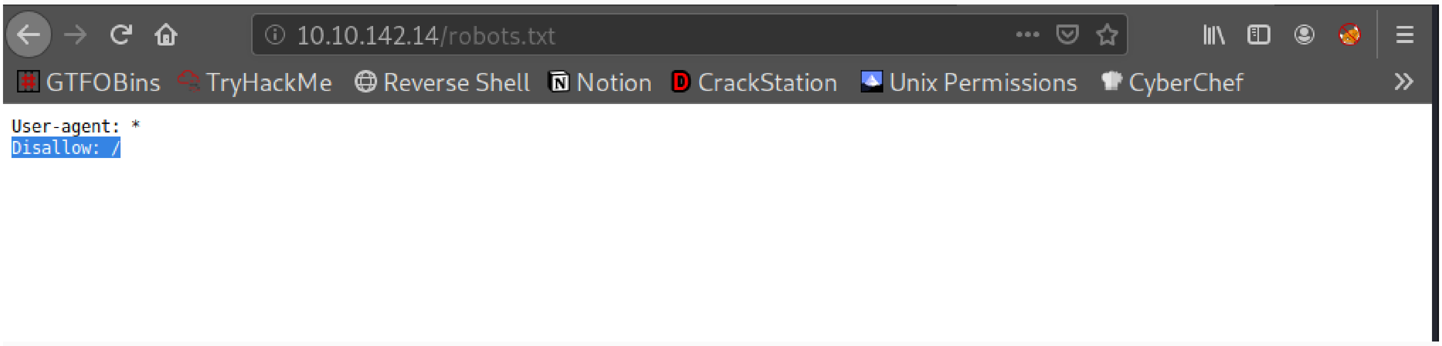
```
/robots.txt
```



Processed	Method	URI	Flags
🟢	GET	http://10.10.142.14	Seed
🟢	GET	http://10.10.142.14/robots.txt	Seed
🟢	GET	http://10.10.142.14/sitemap.xml	Seed
🟢	GET	http://10.10.142.14/	
🟢	GET	http://10.10.142.14/login.php	
🔴	GET	http://www.dvwa.co.uk/	Out of Scope
🟢	GET	http://10.10.142.14/dvwa/css/login.css	
🟢	GET	http://10.10.142.14/dvwa/images/login_logo.png	
🟢	GET	http://10.10.142.14/dvwa/images/RandomStorm.png	
🟢	POST	http://10.10.142.14/login.php	

#5 One entry is included in the disallow section of this file, what is it?

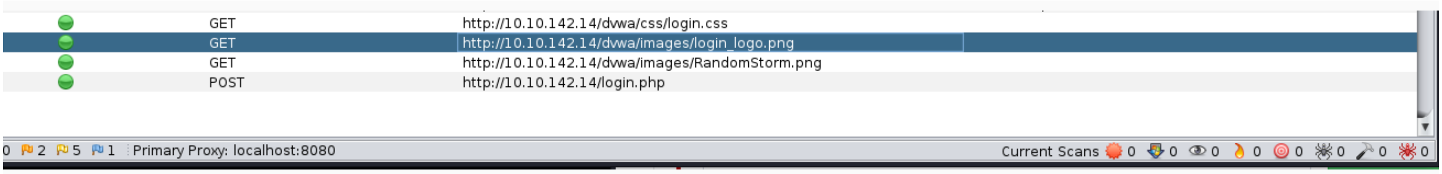
```
/
```



```
User-agent: *
Disallow: /
```

#6 ZAP will find a directory that contains images for our application, what is the path for that directory? (This is what will follows the name/ip of the website)

```
/dvwa/images
```



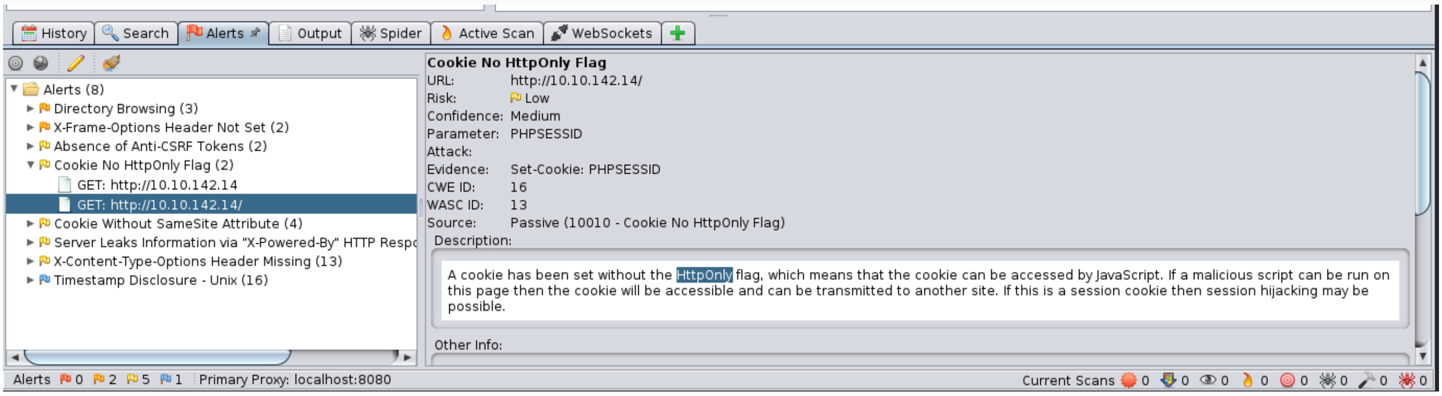
```
GET     http://10.10.142.14/dvwa/css/login.css
GET     http://10.10.142.14/dvwa/images/login_logo.png
GET     http://10.10.142.14/dvwa/images/RandomStorm.png
POST    http://10.10.142.14/login.php
```

0 2 5 1 Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

#7 This website doesn’t force a secure connection by default and ZAP isn’t pleased

with it. Which related cookie is ZAP upset about?

```
httpOnly
```



- Alerts (8)
  - Directory Browsing (3)
  - X-Frame-Options Header Not Set (2)
  - Absence of Anti-CSRF Tokens (2)
  - Cookie No HttpOnly Flag (2)
    - GET: http://10.10.142.14
    - GET: http://10.10.142.14/
  - Cookie Without SameSite Attribute (4)
  - Server Leaks Information via "X-Powered-By" HTTP Respo
  - X-Content-Type-Options Header Missing (13)
  - Timestamp Disclosure - Unix (16)

Cookie No HttpOnly Flag
URL: http://10.10.142.14/
Risk: Low
Confidence: Medium
Parameter: PHPSESSID
Attack:
Evidence: Set-Cookie: PHPSESSID
CWE ID: 16
WASC ID: 13
Source: Passive (10010 - Cookie No HttpOnly Flag)
Description:

A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

Other Info:

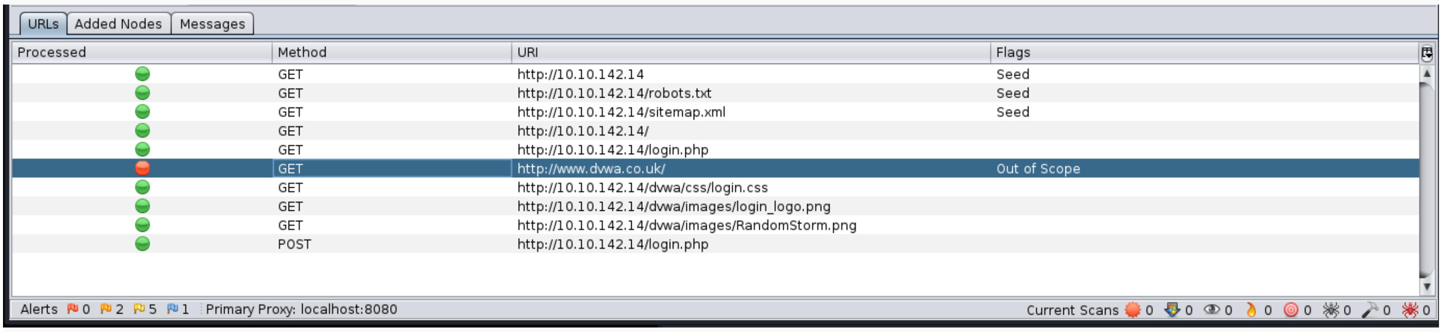
Alerts 0 2 5 1 Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

#8 Featured in various rooms on TryHackMe, Cross-Site Scripting is a vicious attack that is becoming ever more

common on the open web. What Alert does ZAP produce to let us know that this site is vulnerable to XSS? Note, there are often a couple warnings produced for this, look for one more so directly related to the web client.

```
Web Browser XSS Protection Not Enabled
```

#9 The ZAP proxy spider represents the component responsible for ‘crawling’ the site. What site is found to be out of scope?



Processed	Method	URI	Flags
🟢	GET	http://10.10.142.14	Seed
🟢	GET	http://10.10.142.14/robots.txt	Seed
🟢	GET	http://10.10.142.14/sitemap.xml	Seed
🟢	GET	http://10.10.142.14/	
🟢	GET	http://10.10.142.14/login.php	
🔴	GET	http://www.dvwa.co.uk/	Out of Scope
🟢	GET	http://10.10.142.14/dvwa/css/login.css	
🟢	GET	http://10.10.142.14/dvwa/images/login_logo.png	
🟢	GET	http://10.10.142.14/dvwa/images/RandomStorm.png	
🟢	POST	http://10.10.142.14/login.php	

Alerts 0 2 5 1 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

```
http://www.dvwa.co.uk/
```

#10 ZAP will use primarily two methods in order to scan a website, which of these two HTTP methods requests content?

```
GET (logic)
```

#11 Which option attempts to submit content to the website?

```
POST
```

More articles from Ludovic COULON

Break Out The Cage - TryHackMe

Writeup for the Break Out The Cage room on TryHackMe

June 18th, 2020 · 1 min read