

R V COLLEGE OF ENGINEERING

Name: ANKIT KUMAR USN: 1RV18IS007 Dept/Lab: ISE/CSDF Expt No.: 08 a
Date: 14/12/2021 Title: INFORMATION GATHERING TOOL

a. SKIPFISH

INTRODUCTION

Skipfish is an active web application security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes.

The resulting map is then annotated with the output from a number of active (but hopefully non-disruptive) security checks. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

Objectives - To perform a security scan of a web application using SkipFish.

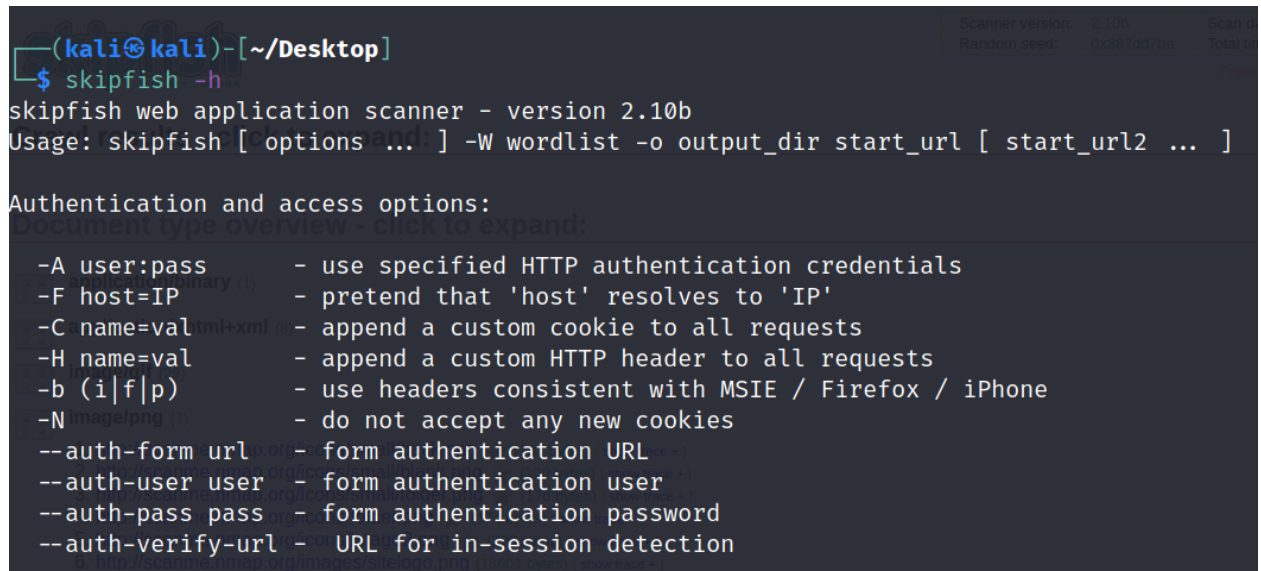
EXECUTION STEPS

1. Installing Skipfish from a package

Command - `sudo apt install skipfish`

2. To get all the parameters in Skipfish

Command - `skipfish -h`



```
(kali㉿kali)-[~/Desktop]
$ skipfish -h
skipfish web application scanner - version 2.10b
Usage: skipfish [options...] -W wordlist -o output_dir start_url [ start_url2 ... ]

Authentication and access options:
-A user:pass      - use specified HTTP authentication credentials
-F host=IP        - pretend that 'host' resolves to 'IP'
-C name=val       - append a custom cookie to all requests
-H name=val       - append a custom HTTP header to all requests
-b (i|f|p)        - use headers consistent with MSIE / Firefox / iPhone
-N               - do not accept any new cookies
--auth-form url   - form authentication URL
--auth-user user  - form authentication user
--auth-pass pass  - form authentication password
--auth-verify-url - URL for in-session detection
```

Example case

1. To scan the target and to write the output in the directory -

Using the given directory for output (-o skip), scan the web application URL (<http://scanme.nmap.org>):

Syntax - skipfish -o <Filename> <URL>

Command - skipfish -o skip http://scanme.nmap.org

```
Welcome to skipfish. Here are some useful tips:

1) To abort the scan at any time, press Ctrl-C. A partial report will be written
   to the specified location. To view a list of currently scanned URLs, you can
   press space at any time during the scan.

2) Watch the number requests per second shown on the main screen. If this figure
   drops below 100-200, the scan will likely take a very long time.

3) The scanner does not auto-limit the scope of the scan; on complex sites, you
   may need to specify locations to exclude, or limit brute-force steps.

4) There are several new releases of the scanner every month. If you run into
   trouble, check for a newer version first, let the author know next.

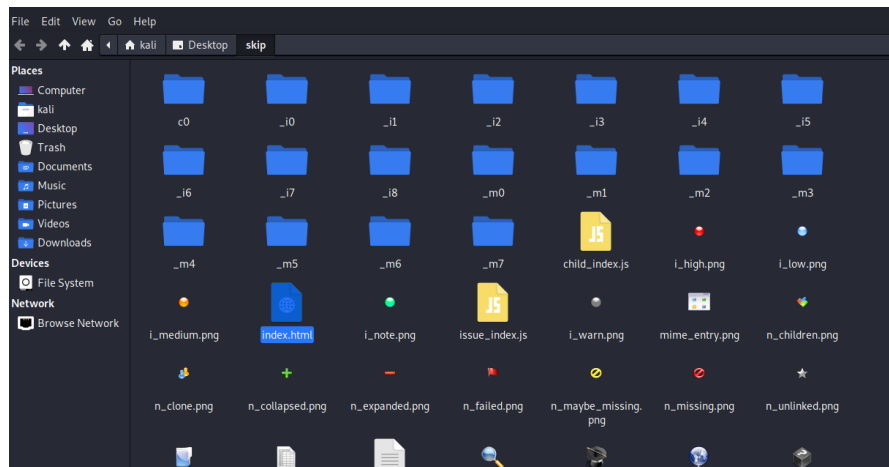
More info: http://code.google.com/p/skipfish/wiki/KnownIssues

Press any key to continue (or wait 60 seconds)...
```

- After some time, depending on the size of the website, the scan will complete and it will create a professional web application security assessment.

```
- scanme.nmap.org -0:53.726/s), 40170 kB in, 4906 kB out (69.1 kB/s) al
- scanme.nmap.org -0:55.062/s), 40212 kB in, 4916 kB out (69.0 kB/s) al
Scan statistics: 0:10:56.301/s), 40255 kB in, 4926 kB out (69.0 kB/s) al
Scan statistics: 0:10:57.540/s), 40293 kB in, 4935 kB out (68.9 kB/s) al
  Scan time : 0:10:58.773/s), 40333 kB in, 4945 kB out (68.9 kB/s) al
  Scan time : 0:11:00.407/s), 40369 kB in, 4955 kB out (68.8 kB/s) al
  HTTP requests : 24052 (36.4/s), 40393 kB in, 4963 kB out (68.7 kB/s) al
  Compression : 3670 kB in, 14221 kB out (59.0% gain) 0 drops, 0 val
  HTTP faults : 1 net errors, 0 proto errors, 66 retried, 0 drops, 0 val
  TCP handshakes : 384 total (62.6 req/conn) urged dict , 14 par, 0 val
  TCP faults : 0 failures, 0 timeouts, 6 purged dict , 14 par, 0 val
  External links : 1600 skipped 06 done (83.46%) dict , 14 par, 0 val
  Reqs pending : 0 , 106 done (83.46%) dict , 14 par, 0 val
Database statistics: 7 total, 106 done (83.46%) dict , 14 par, 0 val
Database statistics: 7 total, 106 done (83.46%) dict , 14 par, 0 val
  Pivots : 127 total, 106 done (83.46%) dict , 14 par, 0 val
  Pivots : 127 total, 108 done (85.04%) dict , 14 par, 0 val
  In progress : 12 pending, 0 init, 0 attacks, 7 dict , 14 par, 0 val
  Missing nodes : 11 spotted dir, 78 file, 0 pininfo, 19 unkn, 14 par, 0 val
  Node types : 1 serv, 15 dir, 78 file, 0 pininfo, 19 unkn, 14 par, 0 val
  Issues found : 39 info, 1 warn, 0 low, 10 medium, 0 high impact
  Dict size : 71 words (71 new), 7 extensions, 256 candidates
  Signatures : 77 total
```

- The output folder will look something like this:



- Click on the index.html file in the above folder to open the assessment. It will look like this:



- Different types of documents scanned can be viewed in the “Document Type Overview Panel”.

Document type overview - click to expand:



- Similarly, different types of issues can be viewed in the following manner:

Issue type overview - click to expand:

- 🟡 **Interesting server message** (3)
 - 1. <http://scanme.nmap.org/shared/error/includes/bottom.html> [show trace +]
Memo: SHTML error (sig: 22003)
 - 2. http://scanme.nmap.org/shared/templates/nmap_header.html [show trace +]
Memo: SHTML error (sig: 22003)
 - 3. http://scanme.nmap.org/shared/templates/nmap_pagemap.html [show trace +]
Memo: SHTML error (sig: 22003)
- 🟡 **External content embedded on a page (higher risk)** (5)
- ⬛ **Resource fetch failed** (1)
- 🟢 **Incorrect or missing charset (low risk)** (12)
- 🟢 **Incorrect or missing MIME type (low risk)** (3)
- 🟢 **Hidden files / directories** (10)
- 🟢 **Directory listing enabled** (21)
- 🟢 **New 404 signature seen** (1)
- 🟢 **New 'Server' header value seen** (1)

NOTE: 100 samples maximum per issue or document type.

CONCLUSION

1. Skipfish provides the summary overviews of document types and issue types found, and an interactive sitemap, with nodes discovered through brute-force, denoted in a distinctive way.
2. The final report generated by the tool is meant to serve as a foundation for professional web application security assessments.

REFERENCES

1. Skipfish - <https://www.kali.org/tools/skipfish/>
2. Skipfish - <https://gbhackers.com/skipfish-web-application-security-scanner/>