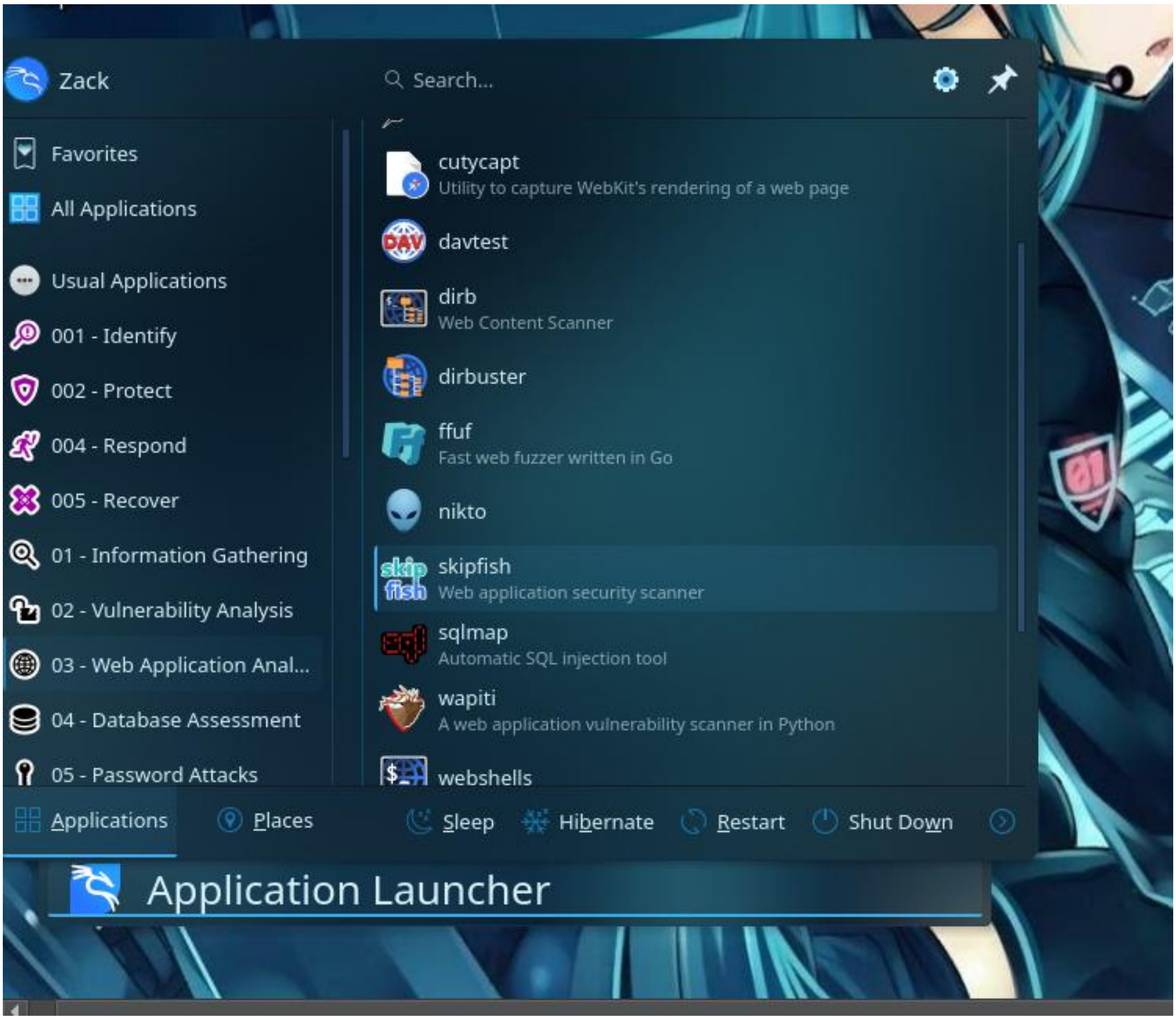
Skipfish

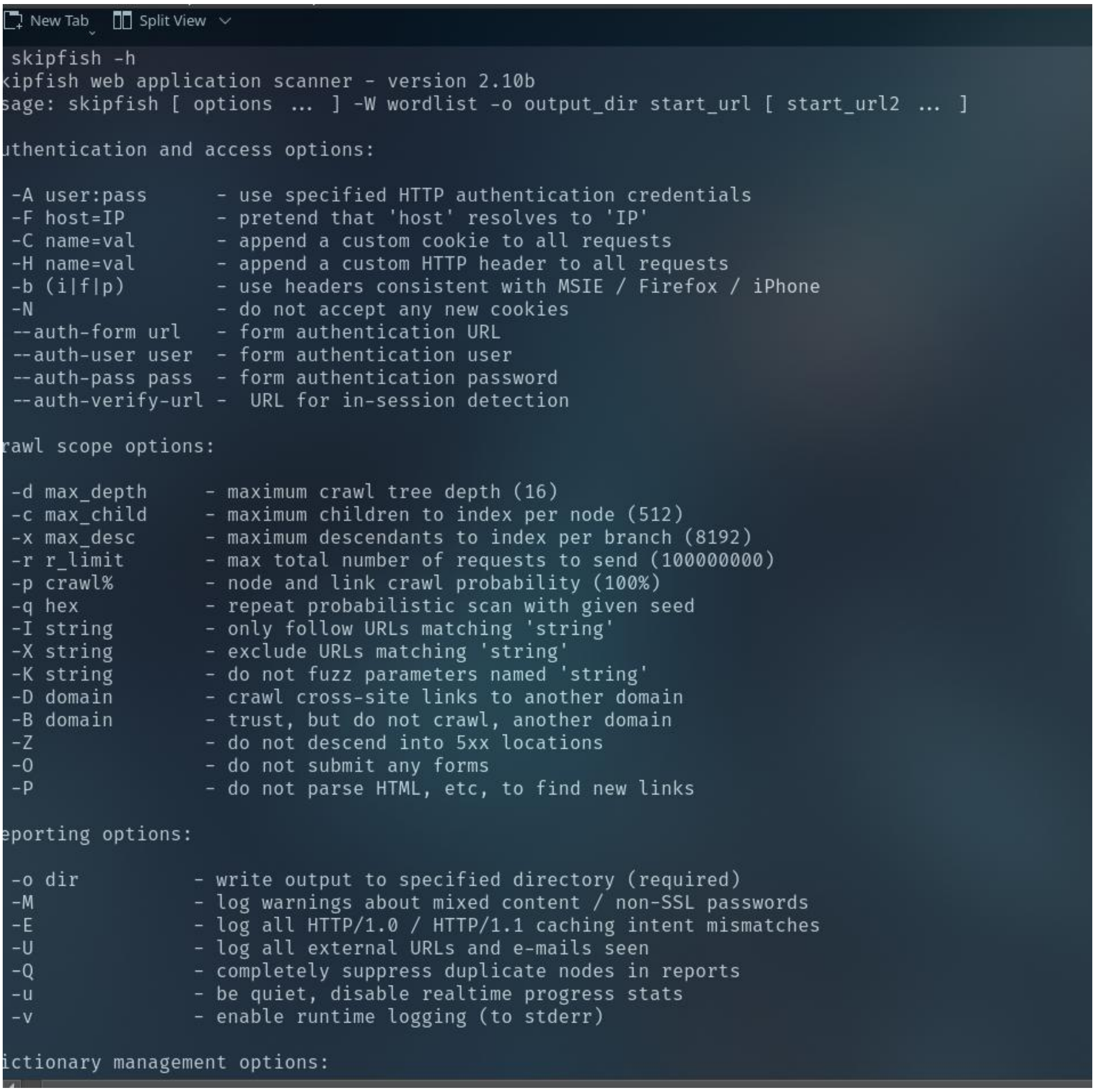
Skipfish application

1) Launch Kali from VMWare Workstation. Enter root/toor as username and password.
2) Skipfish is applicable on cross platform includes Linux, BSD, MAC and windows. It is a power full scanner that crawls targeted website and fully scanned all the pages. It is readily available on Kali Linux. You can access it by selecting Applications-->Web Application Analysis--> skipfish.



Execute Test with Skipfish:

3) When you open Skipfish for the first time, a Terminal window will pop up displaying the Skipfish commands. Skipfish can use built-in or customizable dictionaries for vulnerability assessment. Skipfish should look like this when opened:



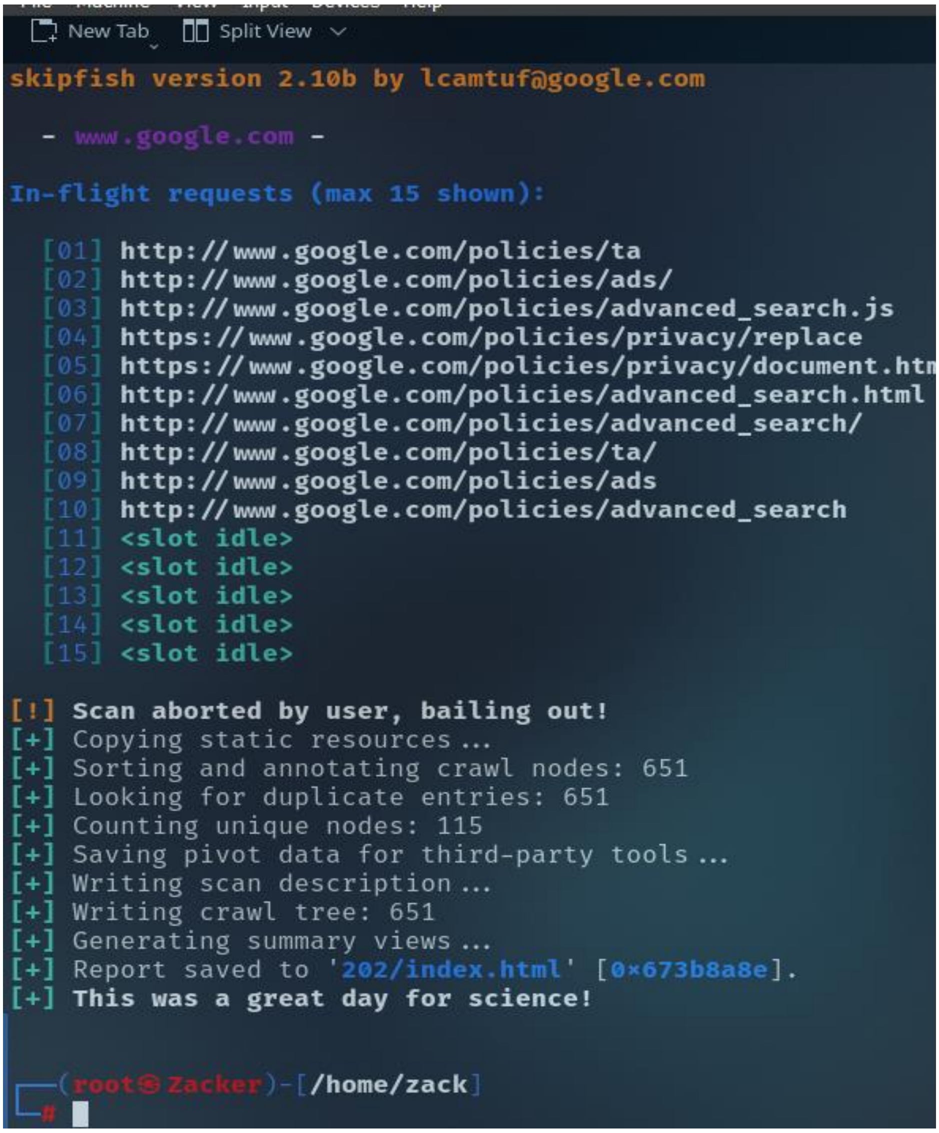
```
 skipfish -h
kipfish web application scanner - version 2.10b
sage: skipfish [ options ... ] -W wordlist -o output_dir start_url [ start_url2 ... ]

uthentication 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

rawl scope options:

 -d max_depth     - maximum crawl tree depth (16)
 -c max_child     - maximum children to index per node (512)
 -x max_desc      - maximum descendants to index per branch (8192)
 -r r_limit       - max total number of requests to send (100000000)
 -p crawl%        - node and link crawl probability (100%)
 -q hex           - repeat probabilistic scan with given seed
 -I string        - only follow URLs matching 'string'
 -X string        - exclude URLs matching 'string'
 -K string        - do not fuzz parameters named 'string'
 -D domain        - crawl cross-site links to another domain
 -B domain        - trust, but do not crawl, another domain
 -Z               - do not descend into 5xx locations
 -O               - do not submit any forms
 -P               - do not parse HTML, etc, to find new links

eporting options:

 -o dir          - write output to specified directory (required)
 -M              - log warnings about mixed content / non-SSL passwords
 -E              - log all HTTP/1.0 / HTTP/1.1 caching intent mismatches
 -U              - log all external URLs and e-mails seen
 -Q              - completely suppress duplicate nodes in reports
 -u              - be quiet, disable realtime progress stats
 -v              - enable runtime logging (to stderr)

ictionary management options:
```

4) There are various command options available in Skipfish. To run Skipfish against a target website using a custom wordlist, enter skipfish, select your wordlist using the -W option followed by the location of the wordlist, select your output directory using -o followed by the location, and finally the target website.

   Using the given directory for output ***(-o 202)***, scan the web application URL ***(http://www.google.com)***
   Command:
   ```
   skipfish -o 202 http://www.google.com
   ```

   If there are no compiling errors, you will be presented with a launch screen that states the will start in 60 seconds or on pressing any key.

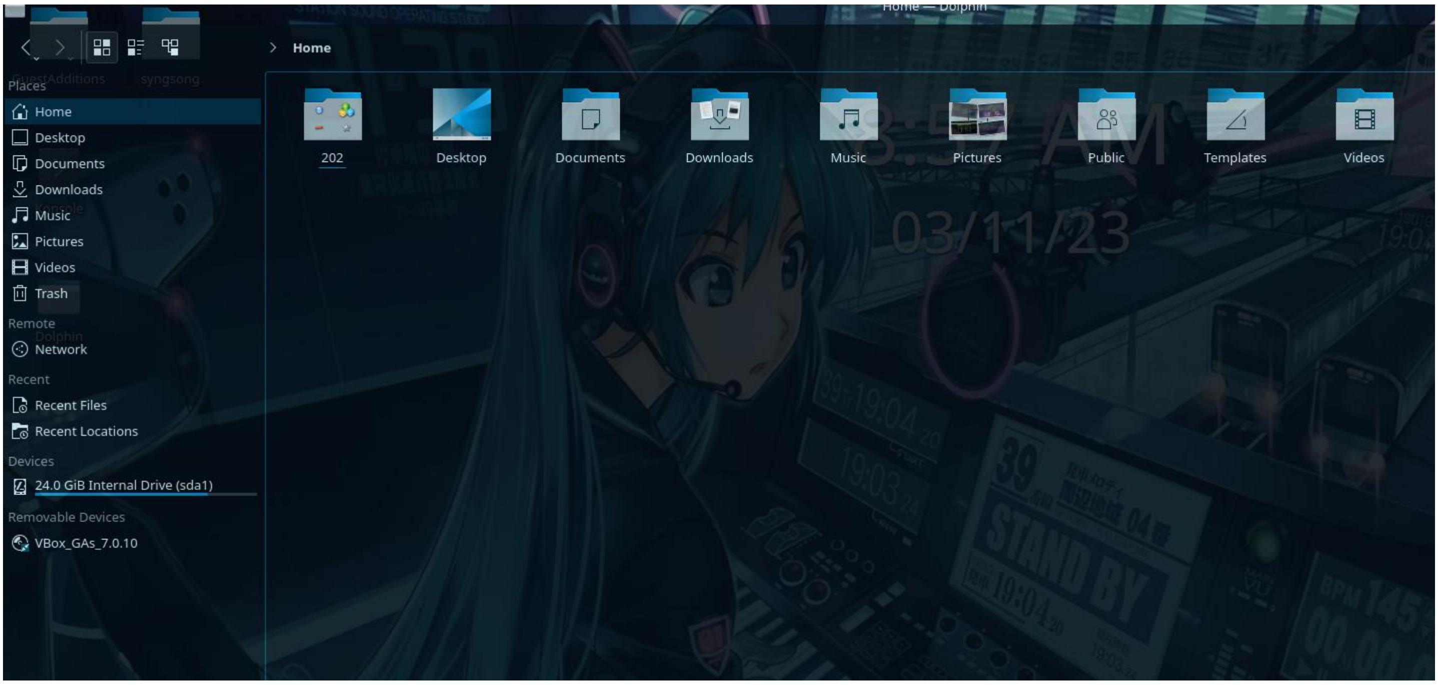
5) You can press the Spacebar to see the details on the scan or watch the default numbers run. Scanning a target can take anywhere from **30 seconds to a few hours** to complete the process. You can end a scan early by typing Ctrl + C. For this test, if scan exceeds 15 minutes, press Ctrl + C.

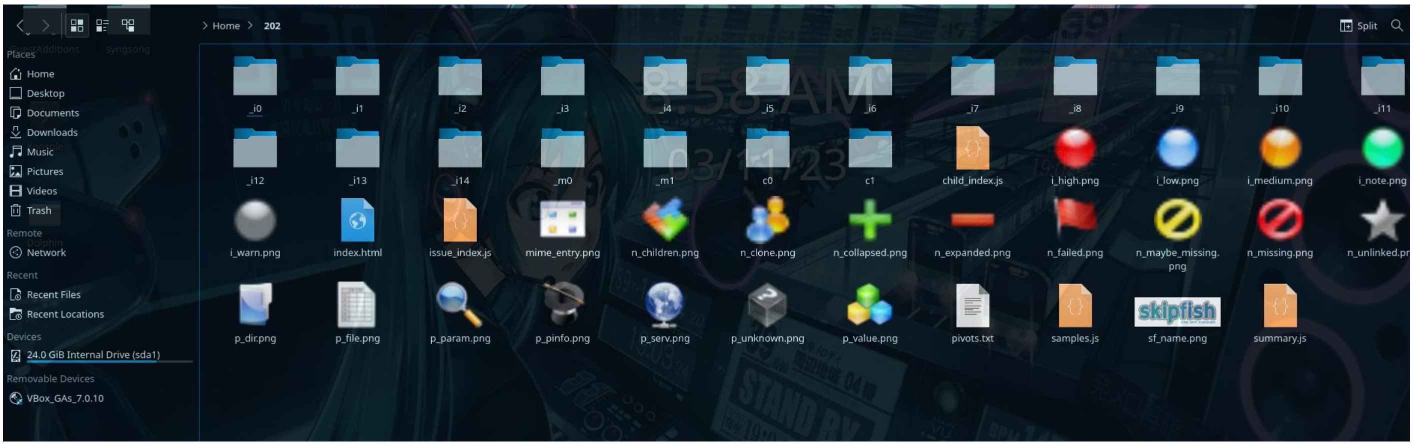


```
skipfish version 2.10b by lcamtuf@google.com

  - www.google.com -

In-flight requests (max 15 shown):

  [01] http://www.google.com/policies/ta
  [02] http://www.google.com/policies/ads/
  [03] http://www.google.com/policies/advanced_search.js
  [04] https://www.google.com/policies/privacy/replace
  [05] https://www.google.com/policies/privacy/document.htm
  [06] http://www.google.com/policies/advanced_search.html
  [07] http://www.google.com/policies/advanced_search/
  [08] http://www.google.com/policies/ta/
  [09] http://www.google.com/policies/ads
  [10] http://www.google.com/policies/advanced_search
  [11] <slot idle>
  [12] <slot idle>
  [13] <slot idle>
  [14] <slot idle>
  [15] <slot idle>

[!] Scan aborted by user, bailing out!
[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 651
[+] Looking for duplicate entries: 651
[+] Counting unique nodes: 115
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 651
[+] Generating summary views ...
[+] Report saved to '202/index.html' [0×673b8a8e].
[+] This was a great day for science!

┌──(root㉿Zacker)-[/home/zack]
└─# 
```

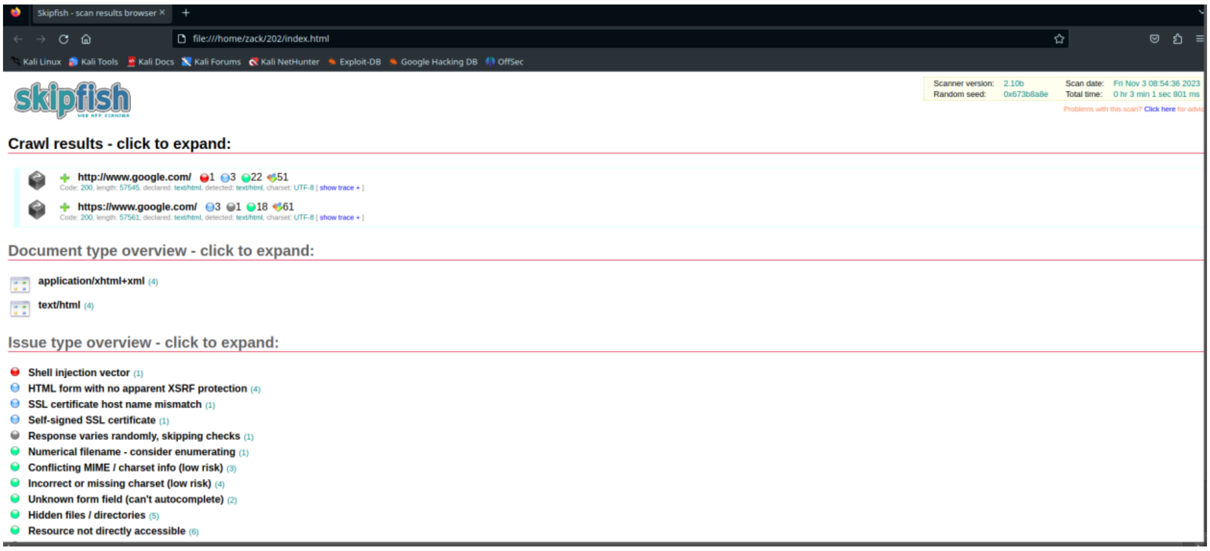
View Vulnerabilities Test Results:

6) Once the scan is completed or if you end it early, Skipfish will generate a ton of output files in the location specified when using the –o option to designate an output folder. Click on Files, then Home and you should see the ‘202’ folder.





7) To see the results, click on the index.html file, which will bring up an Internet browser. You can click through the drop-down boxes to see your results. See the example reports section for more information



Scanner version: 2.10b
Random seed: 0x673b8a8e
Scan date: Fri Nov 3 08:54:36 2023
Total time: 0 hr 3 min 1 sec 801 ms

Problems with this scan? Click here for advic

Crawl results - click to expand:

http://www.google.com/ ●1 ●3 ●22 ●51
Code: 200, length: 57545, declared: text/html, detected: text/html, charset: UTF-8 [show trace +]

https://www.google.com/ ●3 ●1 ●18 ●61
Code: 200, length: 57561, declared: text/html, detected: text/html, charset: UTF-8 [show trace +]

Document type overview - click to expand:

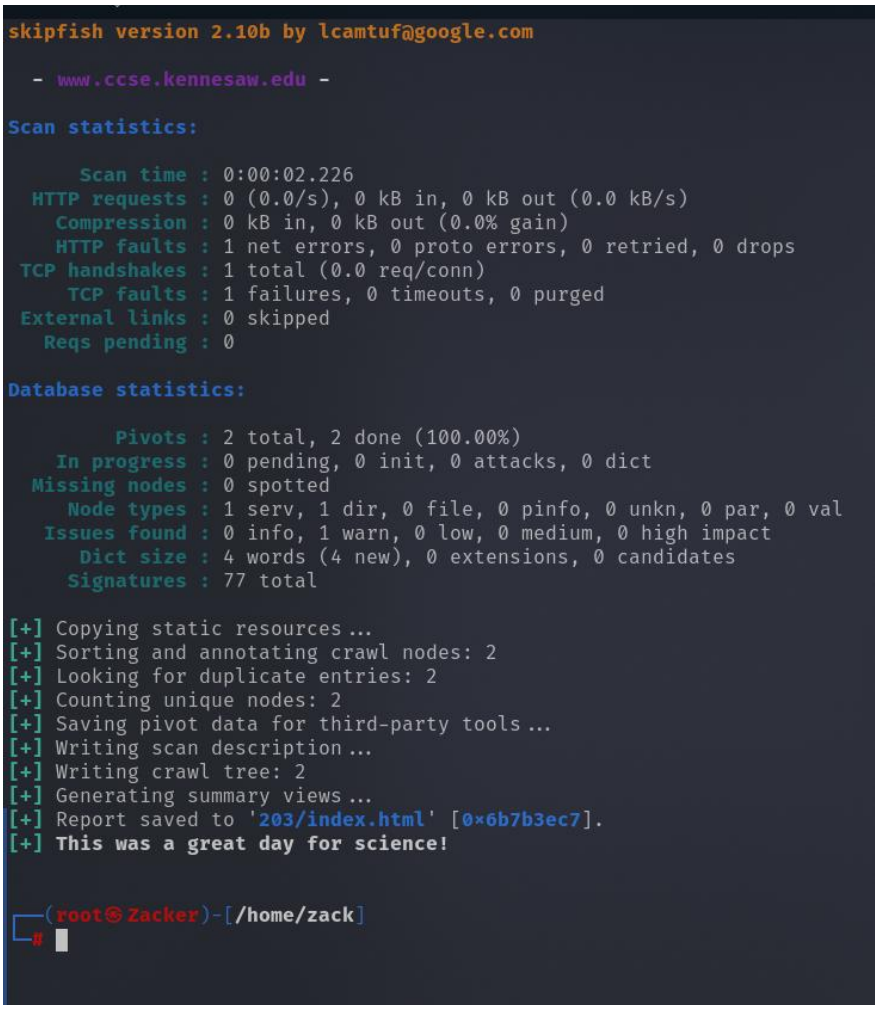
application/xhtml+xml (4)
text/html (4)

Issue type overview - click to expand:

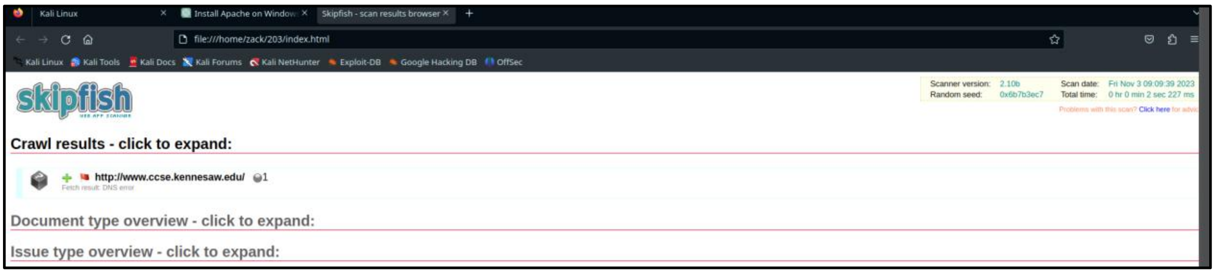
● Shell injection vector (1)
● HTML form with no apparent XSRF protection (4)
● SSL certificate host name mismatch (1)
● Self-signed SSL certificate (1)
● Response varies randomly, skipping checks (1)
● Numerical filename - consider enumerating (1)
● Conflicting MIME / charset info (low risk) (3)
● Incorrect or missing charset (low risk) (4)
● Unknown form field (can't autocomplete) (2)
● Hidden files / directories (5)
● Resource not directly accessible (6)

8) The results here details where security vulnerabilities are at risks. Since this is google.com, there are no high impact vulnerabilities to worry about. There are some warnings and medium issues.

9) **Run the skipfish for http://ccse.kennesaw.edu and provide a screenshot of your results. [100 point]**



```
skipfish version 2.10b by lcamtuf@google.com

  - www.ccse.kennesaw.edu -

Scan statistics:

      Scan time : 0:00:02.226
  HTTP requests : 0 (0.0/s), 0 kB in, 0 kB out (0.0 kB/s)
    Compression : 0 kB in, 0 kB out (0.0% gain)
    HTTP faults : 1 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 1 total (0.0 req/conn)
     TCP faults : 1 failures, 0 timeouts, 0 purged
 External links : 0 skipped
   Reqs pending : 0

Database statistics:

         Pivots : 2 total, 2 done (100.00%)
    In progress : 0 pending, 0 init, 0 attacks, 0 dict
  Missing nodes : 0 spotted
     Node types : 1 serv, 1 dir, 0 file, 0 pinfo, 0 unkn, 0 par, 0 val
   Issues found : 0 info, 1 warn, 0 low, 0 medium, 0 high impact
      Dict size : 4 words (4 new), 0 extensions, 0 candidates
     Signatures : 77 total

[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 2
[+] Looking for duplicate entries: 2
[+] Counting unique nodes: 2
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 2
[+] Generating summary views ...
[+] Report saved to '203/index.html' [0x6b7b3ec7].
[+] This was a great day for science!


┌──(root㉿Zacker)-[/home/zack]
└─# 
```



Scanner version: 2.10b Scan date: Fri Nov 3 09:09:39 2023
Random seed: 0x6b7b3ec7 Total time: 0 hr 0 min 2 sec 227 ms

Problems with this scan? Click here for advi

Crawl results - click to expand:

http://www.ccse.kennesaw.edu/ 1

Fetch result: DNS error

Document type overview - click to expand:

Issue type overview - click to expand:

Conclusion and References:

Most of the problems reported by skipfish should self-explanatory, assuming you have a good gasp of the fundamentals of web security. If you need a quick refresher on some of the more complicated topics, such as MIME sniffing, you may enjoy our comprehensive Browser Security Handbook as a starting point: http://code.google.com/p/browsersec/