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.

Also, learn an **Advanced Web Hacking & Penetration Testing Course** – Scratch to Advance

Main Feature

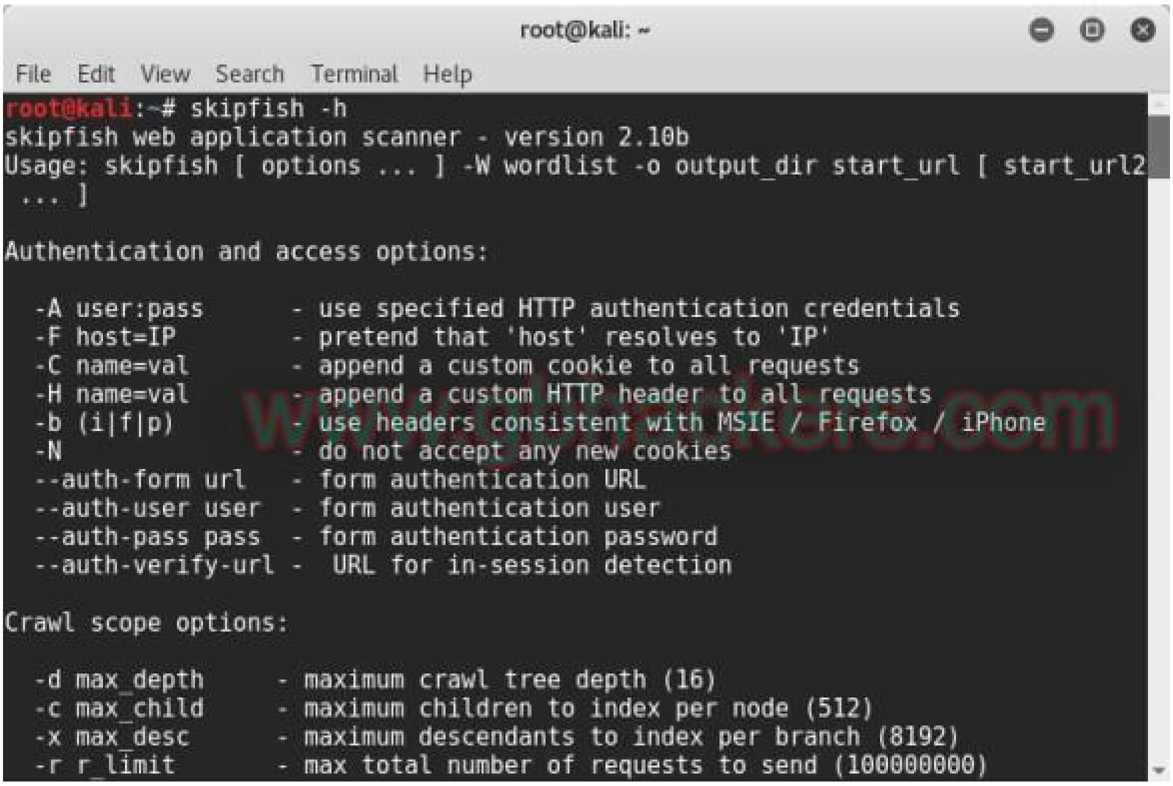
- 500+ against Internet targets, 2000+ requests per second on LAN / MAN networks, and 7000+ requests against local instances.
- Automatic word list construction based on site content analysis.
- Heuristic recognition of obscure path and query-based parameter handling schemes.
- Snort style content signatures which will highlight server errors, information leaks or potentially dangerous web applications.
- Bundled security checks are designed to handle tricky scenarios: **Stored XSS** (path, parameters, headers), blind SQL or XML injection, or blind shell injection.

Also Read : **Commix – Automated All-in-One OS Command Injection and Exploitation Tool**

To Run this Web application security scanner

Step1: To get all the parameters of type **skipfish -h**

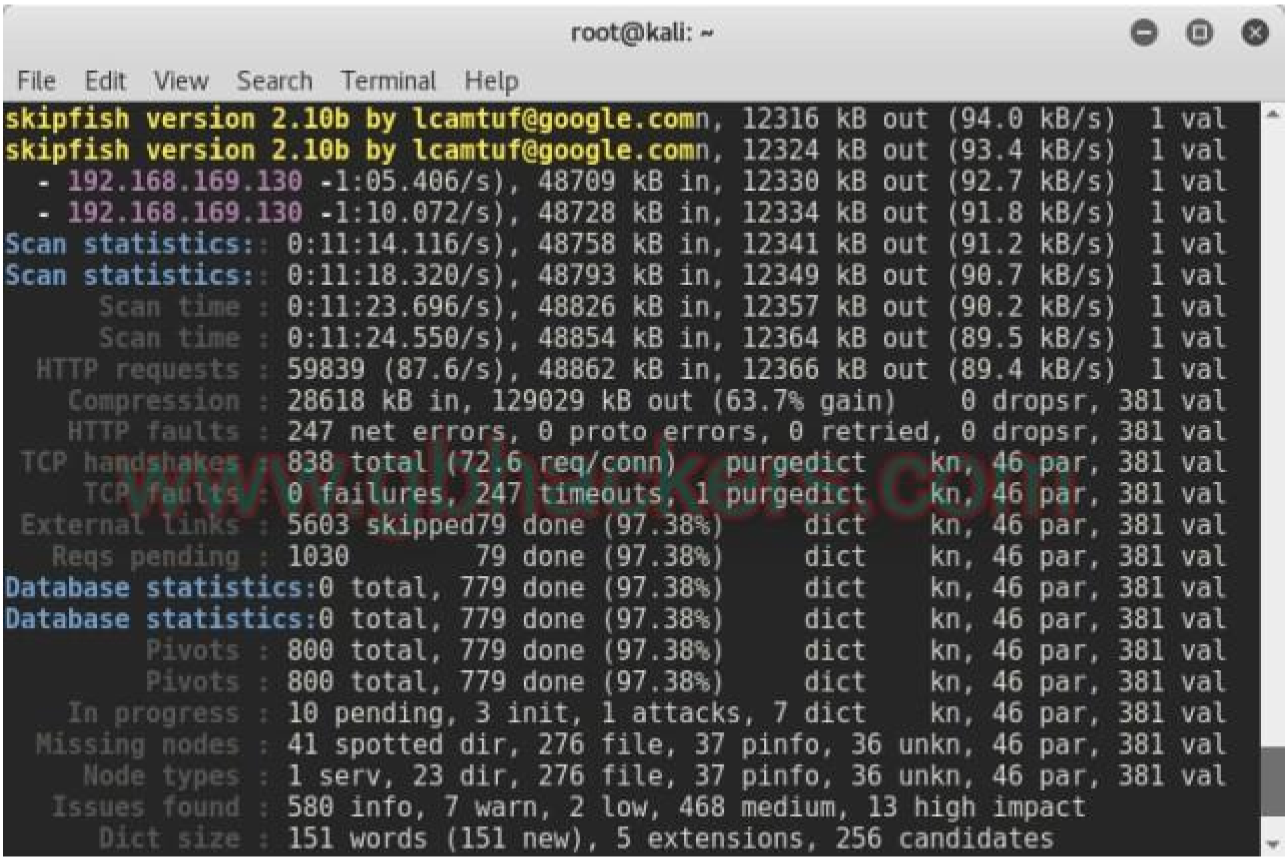
```
root@kali:~# skipfish -h
```



```
root@kali:~# 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

Crawl 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)
```

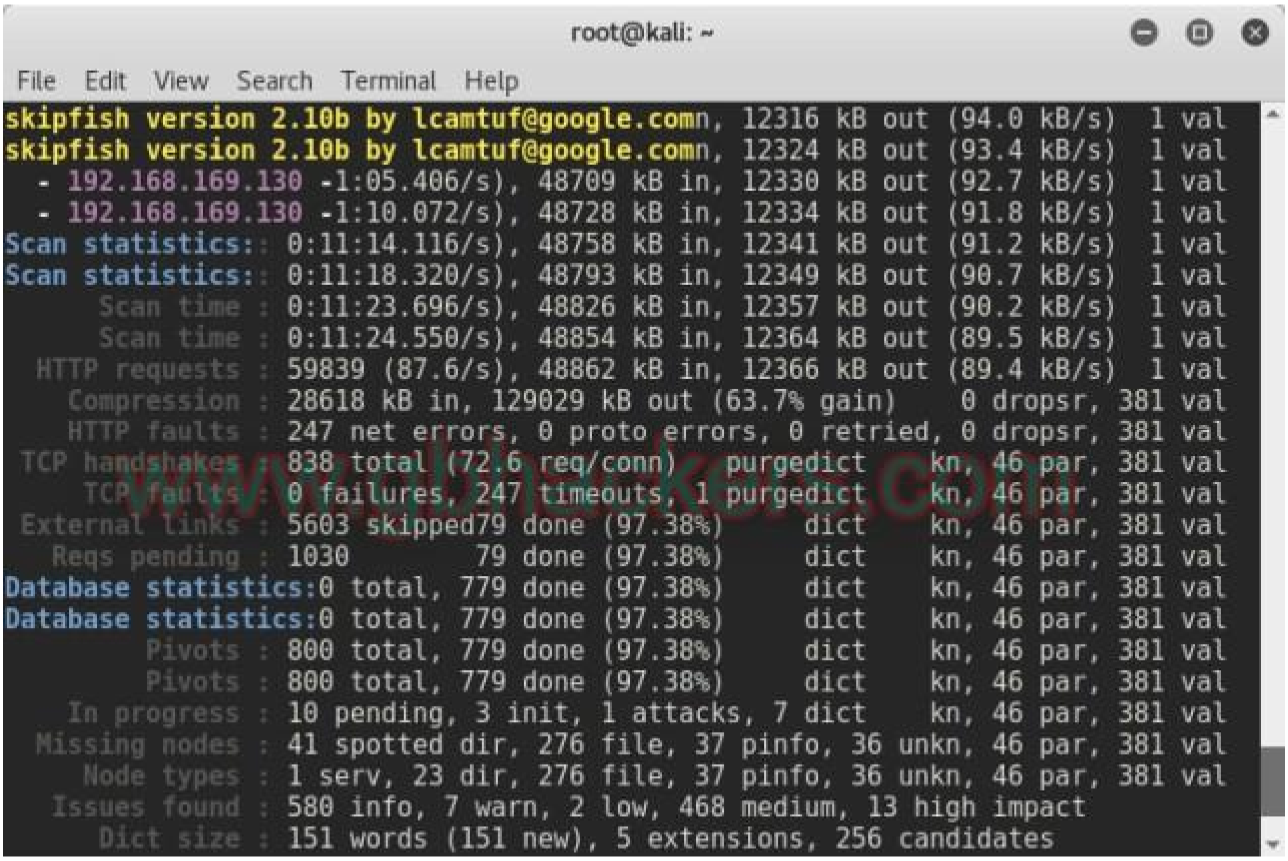
Step2: To scan the target and to write the output in the directory.

root@kali:~# skipfish -d -o 202 http://192.168.169.130/

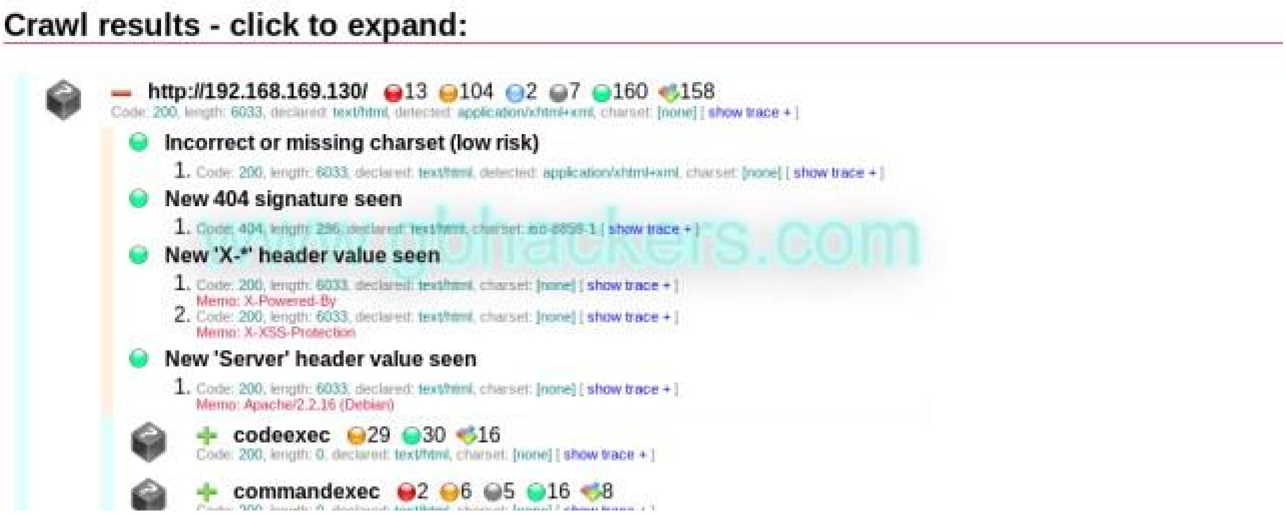


```
skipfish version 2.10b by lcamtuf@google.comn, 12316 kB out (94.0 kB/s)  1 val
skipfish version 2.10b by lcamtuf@google.comn, 12324 kB out (93.4 kB/s)  1 val
  - 192.168.169.130 -1:05.406/s), 48709 kB in, 12330 kB out (92.7 kB/s)  1 val
  - 192.168.169.130 -1:10.072/s), 48728 kB in, 12334 kB out (91.8 kB/s)  1 val
Scan statistics:: 0:11:14.116/s), 48758 kB in, 12341 kB out (91.2 kB/s)  1 val
Scan statistics:: 0:11:18.320/s), 48793 kB in, 12349 kB out (90.7 kB/s)  1 val
      Scan time : 0:11:23.696/s), 48826 kB in, 12357 kB out (90.2 kB/s)  1 val
      Scan time : 0:11:24.550/s), 48854 kB in, 12364 kB out (89.5 kB/s)  1 val
  HTTP requests : 59839 (87.6/s), 48862 kB in, 12366 kB out (89.4 kB/s)  1 val
    Compression : 28618 kB in, 129029 kB out (63.7% gain)    0 dropsr, 381 val
    HTTP faults : 247 net errors, 0 proto errors, 0 retried, 0 dropsr, 381 val
 TCP handshakes : 838 total (72.6 req/conn)  purgedict    kn, 46 par, 381 val
     TCP faults : 0 failures, 247 timeouts, 1 purgedict   kn, 46 par, 381 val
 External links : 5603 skipped79 done (97.38%)     dict    kn, 46 par, 381 val
   Reqs pending : 1030          79 done (97.38%)     dict    kn, 46 par, 381 val
Database statistics:0 total, 779 done (97.38%)     dict    kn, 46 par, 381 val
Database statistics:0 total, 779 done (97.38%)     dict    kn, 46 par, 381 val
         Pivots : 800 total, 779 done (97.38%)     dict    kn, 46 par, 381 val
         Pivots : 800 total, 779 done (97.38%)     dict    kn, 46 par, 381 val
    In progress : 10 pending, 3 init, 1 attacks, 7 dict    kn, 46 par, 381 val
  Missing nodes : 41 spotted dir, 276 file, 37 pinfo, 36 unkn, 46 par, 381 val
     Node types : 1 serv, 23 dir, 276 file, 37 pinfo, 36 unkn, 46 par, 381 val
   Issues found : 580 info, 7 warn, 2 low, 468 medium, 13 high impact
      Dict size : 151 words (151 new), 5 extensions, 256 candidates
```

It will go on scanning through every request, external/Internal links and statistics.



```
skipfish version 2.10b by lcamtuf@google.comn, 12316 kB out (94.0 kB/s)  1 val
skipfish version 2.10b by lcamtuf@google.comn, 12324 kB out (93.4 kB/s)  1 val
  - 192.168.169.130 -1:05.406/s), 48709 kB in, 12330 kB out (92.7 kB/s)  1 val
  - 192.168.169.130 -1:10.072/s), 48728 kB in, 12334 kB out (91.8 kB/s)  1 val
Scan statistics:: 0:11:14.116/s), 48758 kB in, 12341 kB out (91.2 kB/s)  1 val
Scan statistics:: 0:11:18.320/s), 48793 kB in, 12349 kB out (90.7 kB/s)  1 val
      Scan time : 0:11:23.696/s), 48826 kB in, 12357 kB out (90.2 kB/s)  1 val
      Scan time : 0:11:24.550/s), 48854 kB in, 12364 kB out (89.5 kB/s)  1 val
  HTTP requests : 59839 (87.6/s), 48862 kB in, 12366 kB out (89.4 kB/s)  1 val
    Compression : 28618 kB in, 129029 kB out (63.7% gain)    0 dropsr, 381 val
    HTTP faults : 247 net errors, 0 proto errors, 0 retried, 0 dropsr, 381 val
 TCP handshakes : 838 total (72.6 req/conn)  purgedict    kn, 46 par, 381 val
     TCP faults : 0 failures, 247 timeouts, 1 purgedict   kn, 46 par, 381 val
 External links : 5603 skipped79 done (97.38%)     dict    kn, 46 par, 381 val
   Reqs pending : 1030         79 done (97.38%)     dict    kn, 46 par, 381 val
Database statistics:0 total, 779 done (97.38%)     dict    kn, 46 par, 381 val
Database statistics:0 total, 779 done (97.38%)     dict    kn, 46 par, 381 val
         Pivots : 800 total, 779 done (97.38%)     dict    kn, 46 par, 381 val
         Pivots : 800 total, 779 done (97.38%)     dict    kn, 46 par, 381 val
    In progress : 10 pending, 3 init, 1 attacks, 7 dict    kn, 46 par, 381 val
  Missing nodes : 41 spotted dir, 276 file, 37 pinfo, 36 unkn, 46 par, 381 val
     Node types : 1 serv, 23 dir, 276 file, 37 pinfo, 36 unkn, 46 par, 381 val
   Issues found : 580 info, 7 warn, 2 low, 468 medium, 13 high impact
      Dict size : 151 words (151 new), 5 extensions, 256 candidates
```



Crawl results - click to expand:

– http://192.168.169.130/ ●13 ●104 ●2 ●7 ●160 ●158
Code: 200, length: 6033, declared: text/html, detected: application/xhtml+xml, charset: [none] [show trace +]

● Incorrect or missing charset (low risk)

1. Code: 200, length: 6033, declared: text/html, detected: application/xhtml+xml, charset: [none] [show trace +]

● New 404 signature seen

1. Code: 404, length: 296, declared: text/html, charset: iso-8859-1 [show trace +]

● New 'X-*' header value seen

1. Code: 200, length: 6033, declared: text/html, charset: [none] [show trace +]
   Memo: X-Powered-By
2. Code: 200, length: 6033, declared: text/html, charset: [none] [show trace +]
   Memo: X-XSS-Protection

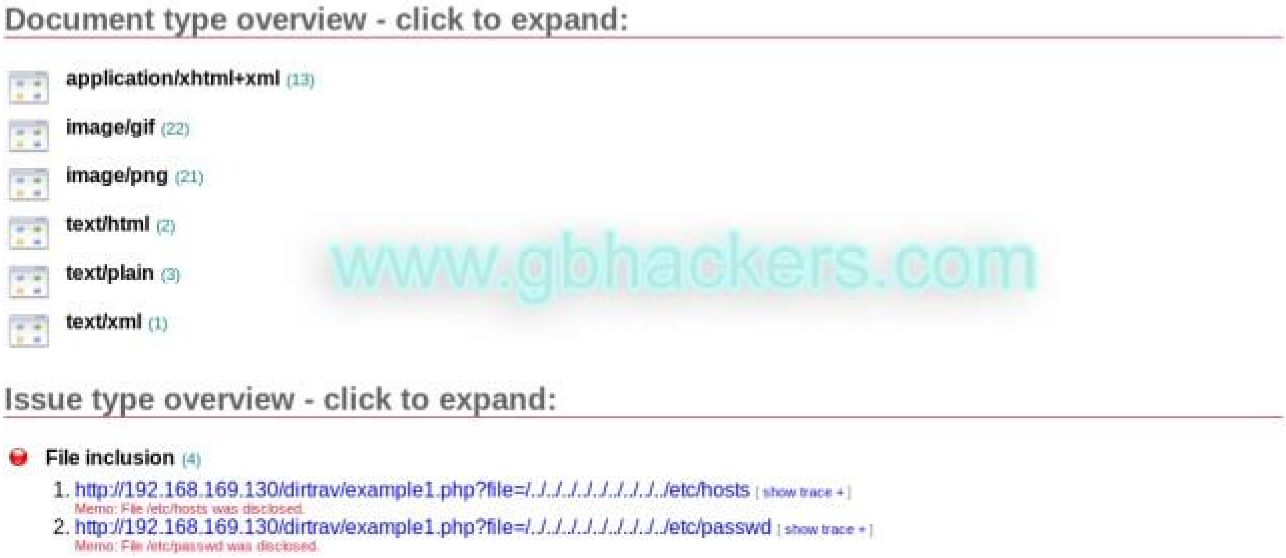
● New 'Server' header value seen

1. Code: 200, length: 6033, declared: text/html, charset: [none] [show trace +]
   Memo: Apache/2.2.16 (Debian)

+ codeexec ●29 ●30 ●16
Code: 200, length: 0, declared: text/html, charset: [none] [show trace +]

+ commandexec ●2 ●6 ●5 ●16 ●8

Once the scan completed it will create a professional web application security assessments.



Document type overview - click to expand:

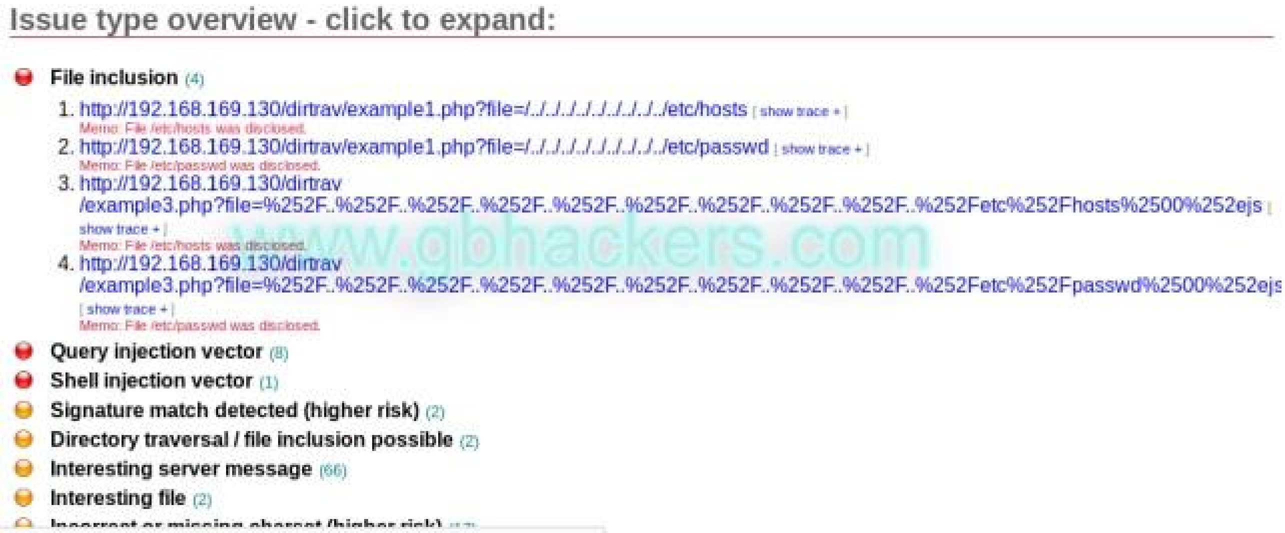
- application/xhtml+xml (13)
- image/gif (22)
- image/png (21)
- text/html (2)
- text/plain (3)
- text/xml (1)

Issue type overview - click to expand:

● File inclusion (4)

1. http://192.168.169.130/dirtrav/example1.php?file=/../../../../../../../../../etc/hosts [show trace +]
   Memo: File /etc/hosts was disclosed.
2. http://192.168.169.130/dirtrav/example1.php?file=/../../../../../../../../../etc/passwd [show trace +]
   Memo: File /etc/passwd was disclosed.

Output consist of various sections such as document type and Issue type overview.



Issue type overview - click to expand:

● File inclusion (4)

1. http://192.168.169.130/dirtrav/example1.php?file=/../../../../../../../../../etc/hosts [show trace +]
   Memo: File /etc/hosts was disclosed.
2. http://192.168.169.130/dirtrav/example1.php?file=/../../../../../../../../../etc/passwd [show trace +]
   Memo: File /etc/passwd was disclosed.
3. http://192.168.169.130/dirtrav/example3.php?file=%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252Fetc%252Fhosts%2500%252ejs [show trace +]
   Memo: File /etc/hosts was disclosed.
4. http://192.168.169.130/dirtrav/example3.php?file=%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252F..%252Fetc%252Fpasswd%2500%252ejs [show trace +]
   Memo: File /etc/passwd was disclosed.

● Query injection vector (8)
● Shell injection vector (1)
● Signature match detected (higher risk) (2)
● Directory traversal / file inclusion possible (2)
● Interesting server message (66)
● Interesting file (2)
● Incorrect or missing charset (higher risk)

For scanning Wildcard domains

```
root@kali:~# skipfish -D .192.168.169.130 -o output-dir1 http://192.168.169.130/
```

You need to customize your HTTP requests when **scanning big sites**.

-H To insert any additional, non-standard headers.
-F To define a custom mapping between a host and an IP.
-d Limits crawl depth to a specified number of subdirectories.
-c Limits the number of children per directory.
-x Limits the total number of descendants per crawl tree branch.
-r Limits the total number of requests to send in a scan.

skipfish also 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.