

DDoS Risk Calculator

Calculate the Risk and Cost of a DDoS Attack on Your Website

CALCULATE NOW →



Skipfish – Web Application Security Scanner for XSS, SQL Injection, Shell injection

By [GURUBARAN S](#) - June 4, 2018 0



Skipfish

Free Cloud Linux VPS



Newsletter

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.

Main Feature

Signup to get Hacking News & Tutorials to your Inbox

Name

Email *

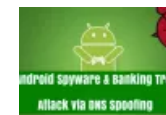
Subscribe

Most Popular



Rubella Macro Builder – A Malware Development Crimeware Kit Selling in...

April 30, 2018



Android Spyware & Banking Trojan Attack via DNS Spoofing that Poses...

April 20, 2018

3 Dangerous Ransomware Families

- 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
```



Author Arrested in Poland and Seized the...

March 19, 2018



Chrome 63 comes with more Stability, Security Enhancements, and Site Isolation

December 7, 2017



Hidden Cryptocurrency Miner Coinhive's Rapid Growth and it's Prevention Techniques

November 18, 2017

Recommended



4 Cybersecurity Risks We will Face With New WhatsApp Status...



5 Methods to Secure Your Company's Data from Cybercriminals



Infosec-Resources



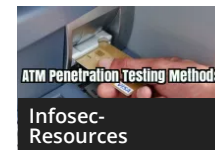
Hacks

```
root@kali: ~  
File Edit View Search Terminal Help  
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/
```

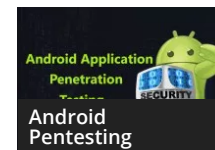
A perfect way to Start and Strengthen your Cyber Security Career



Advanced ATM Penetration Testing Methods

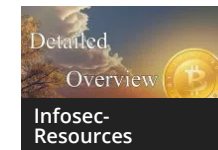


An Important Protection Approach to Tackle Internet Security Issues at Work

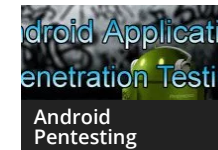


Android Application

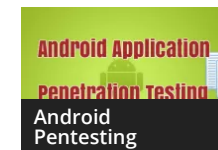
Adobe & Microsoft released New Critical Security updates for software...



All that You Should Know About Bitcoins and How Does Bitcoin...



Android Application Penetration Testing – Part 1



Android Application

```

root@kali: ~
File Edit View Search Terminal Help
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

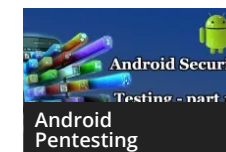
```

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

Penetration
Testing – Part 8



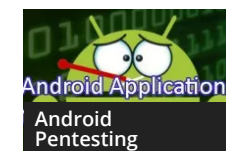
Android
Application
Penetration
Testing – Part 10



Android
Application
Penetration
Testing – Part 12



Android
Application
Penetration
Testing Part – 4



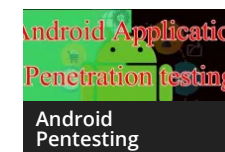
Penetration
Testing – Part 9



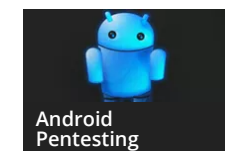
Android
Application
Penetration
Testing – Part 11 –
Android Checklist



Android
Application
Penetration
Testing – Part 5



Android
Application
Penetration
Testing Part 2

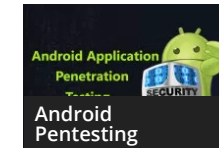



```

root@kali: ~
File Edit View Search Terminal Help
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

```

Android
Application
Penetration
testing Part 3



Android
Application
Penetration
Testing- Part 7

Android
Application
Penetration
Testing Part 6



APT Group Cyber
Attack to Hack
Various
Companies Web
Servers Using...


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: 286, 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
Code: 200, length: 0, declared: text/html, charset: [none] [show trace +]

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.

[illegible]

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

- 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.

Need to specify -e to avoid binary responses for reporting.

- Author: Google Inc, Michal Zalewski, Niels Heinen, Sebastian Roschke
- License: Apache-2.0

Also Read

- [Masscan-Worlds fastest scanner.](#)
- [Cracking WPA/WPA2 passwords with Fluxion.](#)

Share and Support Us :



SOURCE

skipfish

TAGS

Kali Linux

Kali Tool

skipfish

Webapplication

GURUBARAN S



<http://gbhackers.com>

Gurubaran is a PKI Security Engineer. Certified Ethical Hacker, Penetration Tester, Security blogger, Co-Founder & Author of GBHackers On Security.



RELATED ARTICLES

MORE FROM AUTHOR



Penetration Testing with your WordPress Website- Detailed Explanation



Most Important Web Server Penetration Testing Checklist



XSSer – Automated Framework Tool to Detect and Exploit XSS vulnerabilities



Most Important Web Application Security Tools & Resources for Hackers and Security Professionals



Web Application Firewall Detection using Kali Linux- WAFW00F



OWASP TOP 10 – 2017 Released After Four years – Critical Web Application Security Risks



0 Comments

GBHackers on Security

 Login ▾

 Recommend

 Share

Sort by Best ▾

Start the discussion...

LOG IN WITH



OR SIGN UP WITH DISQUS 

Name

Be the first to comment.

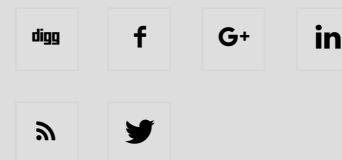


ABOUT US

GBHackers on Security is Advanced Persistent Cyber Security Online platform which including Cyber Security Research, Web Application and Network Penetration Testing, Hacking Tutorials, Live Security Updates, Technology updates, Security investigations With dedicated Cyber security Expert Team and help to community more secure.

Contact us: admin@gbhackers.com

FOLLOW US



[Home](#) [TECH NEWS](#) [Infosec- Resources](#) [OWASP – Top 10](#) [Privacy Policy](#) [Contact Us](#)

© GBHackers on Security 2016 - 2018. All Rights Reserved