

whatweb

WhatWeb is a versatile and powerful tool used in Linux for identifying and analyzing websites. It's primarily used by security professionals, penetration testers, and system administrators to gather information about a web server and the technologies it uses.

Whatweb is a free and open-source tool available on GitHub. Whatweb is a scanner written in the Ruby language. This tool can identify and recognize all the web technologies available on the target website. This tool can identify technologies used by websites such as blogging, content management system, all JavaScript libraries. Whatweb contains more than 180 modules. each module is responsible for grabbing particular information from the target website. Whatweb works as an information-gathering tool and can identify all the email addresses, SQL errors, technology used in the website.

Examples: -

1. To have a simple scan over a website use whatweb command along with the target webpage.

```
(kali@kali)-[~]
└─$ sudo whatweb www.starbucks.com
[sudo] password for kali:
http://www.starbucks.com [301 Moved Permanently] Akamai-Global-Host, Country[UNITED STATES][en], HTTPServer[AkamaiGHost], IP[104.108.223.186], RedirectLocation[https://www.starbucks.com/], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], UncommonHeaders[x-content-type-options,ak-cache-status]
https://www.starbucks.com/ [200 OK] Country[UNITED STATES][en], Frame, HTML5, IP[104.108.223.186], Open-Graph-Protocol, Script[application/json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Starbucks Coffee Company], UncommonHeaders[content-security-policy,x-nextjs-cache,x-azure-ref,x-content-type-options,ak-cache-status], X-Powered-By[Next.js]

(kali@kali)-[~]
└─$ whatweb -s 3 --log-json=output.json www.starbucks.com

http://www.starbucks.com [301 Moved Permanently] Akamai-Global-Host, Country[UNITED STATES][en], HTTPServer[AkamaiGHost], IP[104.108.223.186], RedirectLocation[https://www.starbucks.com/], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], UncommonHeaders[x-content-type-options,ak-cache-status]
https://www.starbucks.com/ [200 OK] Country[UNITED STATES][en], Frame, HTML5, IP[104.108.223.186], Open-Graph-Protocol, Script[application/json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Starbucks Coffee Company], UncommonHeaders[content-security-policy,x-nextjs-cache,x-azure-ref,x-content-type-options,ak-cache-status], X-Powered-By[Next.js]
```

2. To have a output in json format use `--log-json=file_name` along with the target web page.

```
(kali@kali)-[~]
└─$ whatweb -s 3 --log-json=output.json www.starbucks.com

http://www.starbucks.com [301 Moved Permanently] Akamai-Global-Host, Country[UNITED STATES][en], HTTPServer[AkamaiGHost], IP[104.108.223.186], RedirectLocation[https://www.starbucks.com/], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], UncommonHeaders[x-content-type-options,ak-cache-status]
https://www.starbucks.com/ [200 OK] Country[UNITED STATES][en], Frame, HTML5, IP[104.108.223.186], Open-Graph-Protocol, Script[application/json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Starbucks Coffee Company], UncommonHeaders[content-security-policy,x-nextjs-cache,x-azure-ref,x-content-type-options,ak-cache-status], X-Powered-By[Next.js]

(kali@kali)-[~]
└─$ cat output.json
[{"target": "http://www.starbucks.com", "http_status": 301, "request_config": {"headers": {"User-Agent": "whatweb/0.5.5"}, "plugins": {"Akamai-Global-Host": {"Country": {"string": "UNITED STATES"}, "module": "US"}, "HTTPServer": {"string": "AkamaiGHost"}, "IP": {"string": "104.108.223.186"}, "RedirectLocation": {"string": "https://www.starbucks.com/"}, "Strict-Transport-Security": {"string": "[\"max-age=31536000; includeSubDomains; preload\"]"}, "UncommonHeaders": {"string": "[\"x-content-type-options,ak-cache-status\"]"}}, {"target": "https://www.starbucks.com/", "http_status": 200, "request_config": {"headers": {"User-Agent": "whatweb/0.5.5"}, "plugins": {"Country": {"string": "UNITED STATES"}, "module": "US"}, "Frame": {"string": "HTML5"}, "IP": {"string": "104.108.223.186"}, "Open-Graph-Protocol": {"string": "application/json"}, "Script": {"string": "application/javascript"}, "Strict-Transport-Security": {"string": "[\"max-age=31536000; includeSubDomains; preload\"]"}, "Title": {"string": "Starbucks Coffee Company"}, "UncommonHeaders": {"string": "[\"content-security-policy,x-nextjs-cache,x-azure-ref,x-content-type-options,ak-cache-status\"]"}, "X-Powered-By": {"string": "Next.js"}}]

(kali@kali)-[~/home/kali]
└─$ cat output.json
```

3. To scan for plugins like Apache, WordPress, PHP, etc use `--plugins` flag along with the target webpage.

```
(root@kali)-[~/home/kali]
└─$ whatweb --plugins=Apache,WordPress,PHP www.starbucks.com

http://www.starbucks.com [301 Moved Permanently]
https://www.starbucks.com/ [200 OK]
```

4. In order to scan for the aggressive mode use **-a** along with the target domain.

```
root@kali:~# curl -s -A 'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36' https://www.starbucks.com/
http://www.starbucks.com [301 Moved Permanently] Akamai-Global-Host, Country[UNITED STATES][us], HTTPServer[AkamaiGHost], IP[104.108.223.186], RedirectLocation[https://www.starbucks.com/], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], UncommonHeaders[x-content-type-options,ak-cache-status]
https://www.starbucks.com/ [200 OK] Country[UNITED STATES][us], Frame, HTML5, IP[104.108.223.186], Open-Graph-Protocol, Script[application/json,text/javascript], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Starbucks Coffee Company], UncommonHeaders[request-context,content-security-policy,x-nextjs-cache,x-azure-ref,x-content-type-options,ak-cache-status], X-Powered-By[Next.js]
```