

Identification of Web Technologies

Intro

Once we have identified the web domain or have expanded the attack surface by identifying *subdomains*, the next thing to do is **identify the technologies** that run after those domains. Knowing things like, what *application servers are running*, what *programming languages the web server has been developed*, among others, will later serve as input for the [vulnerability analysis](#) and then for the *exploitation of those vulnerabilities*.

For this, different technologies have been developed such as **WhatWeb** and **Web analytics**

WhatWeb

Intro

WhatWeb is a web application scanner that will analyze technologies behind it such as:

- The type of programming language
- The server on which the web application is running
- The web application server
- Web application library types
- Application Server Versions
- Email addresses
- account IDs
- SQL Errors
- Wordpress sections or other content manager
- Session Cookies (this can be used to impersonate a user)
- And more

This is achieved thanks to the fact that it incorporates a list of large *plugins* that are updated through the community

WhatWeb in action

To use whatweb we only have to execute the command:

whatweb <http://target.website>

And the result on the screen would be something like this:

```
whatweb http://192.168.20.134:8080 40 B/s +0 B/s 192.168.20.128
http://192.168.20.134:8080 [302 Found] Apache[2.4.7], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)],
IP[192.168.20.134], PHP[5.5.9-1ubuntu4.14], RedirectLocation[portal.php], X-Powered-By[PHP/5.5.9-1ubuntu4.14]
http://192.168.20.134:8080/portal.php [302 Found] Apache[2.4.7], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTTPServer[Ubuntu
Linux][Apache/2.4.7 (Ubuntu)], IP[192.168.20.134], PHP[5.5.9-1ubuntu4.14], RedirectLocation[login.php], X-Powered-By[PHP/5.5.9
-1ubuntu4.14]
http://192.168.20.134:8080/login.php [200 OK] Apache[2.4.7], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Unbu
tu Linux][Apache/2.4.7 (Ubuntu)], IP[192.168.20.134], PHP[5.5.9-1ubuntu4.14], PasswordField[password], Script, Title[bWAPP - L
ogin], X-Powered-By[PHP/5.5.9-1ubuntu4.14]
```

In case we want the information in more detail, we just have to execute the command as follows

whatweb -v http://target.website

And the result on the screen would be something like this

```
Δ ~ > whatweb -v http://192.168.20.134:8080
WhatWeb report for http://192.168.20.134:8080
Status      : 302 Found
Title       : <None>
IP          : 192.168.20.134
Country     : Netherlands, zz

Summary     : Apache[2.4.7], HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)], PHP[5.5.9-1ubuntu4.14], RedirectLocation[portal.php], X-Powered-By[PHP/5.5.9-1ubuntu4.14]

Detected Plugins:
[ Apache ]
    The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

    Version      : 2.4.7 (from HTTP Server Header)
    Google Dorks : (3)
    Website      : http://httpd.apache.org/

[ HTTPServer ]
    HTTP server header string. This plugin also attempts to identify the operating system from the server header.

    OS           : Ubuntu Linux
    String        : Apache/2.4.7 (Ubuntu) (from server string)

[ PHP ]
    PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. This plugin identifies PHP errors, modules and versions and extracts the local file path and username if present.

    Version      : 5.5.9-1ubuntu4.14
    Google Dorks : (2)
    Website      : http://www.php.net/

[ RedirectLocation ]
    HTTP Server string location. used with http-status 301 and 302

    String        : portal.php (from location)

[ X-Powered-By ]
    X-Powered-By HTTP header
```

For cases where we want to analyze several subdomains and have stored them in a.txt file (see the section *Subdomain Identification*) we can pass this file to Whatweb so that, with a single analysis, it can scan all the sites. We do this with it with the command:

whatweb -i Subdomains.txt

And the result would look like this

```
Δ ~ > whatweb -i Subdomains.txt
WhatWeb report for http://192.168.20.134:8080
Status      : 302 Found
Title       : <None>
IP          : 192.168.20.134
Country     : Netherlands, zz

Summary     : Apache[2.4.7], HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)], PHP[5.5.9-1ubuntu4.14], RedirectLocation[portal.php], X-Powered-By[PHP/5.5.9-1ubuntu4.14]

Detected Plugins:
[ Apache ]
    The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

    Version      : 2.4.7 (from HTTP Server Header)
    Google Dorks : (3)
    Website      : http://httpd.apache.org/

[ HTTPServer ]
    HTTP server header string. This plugin also attempts to identify the operating system from the server header.

    OS           : Ubuntu Linux
    String        : Apache/2.4.7 (Ubuntu) (from server string)

[ PHP ]
    PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML. This plugin identifies PHP errors, modules and versions and extracts the local file path and username if present.

    Version      : 5.5.9-1ubuntu4.14
    Google Dorks : (2)
    Website      : http://www.php.net/

[ RedirectLocation ]
    HTTP Server string location. used with http-status 301 and 302

    String        : portal.php (from location)

[ X-Powered-By ]
    X-Powered-By HTTP header
```

If we want to see more detailed information, we can add the command -v

Be careful, as this merger of can generate a lot of network traffic


Web analytics

Intro

Web analytics It is a tool very similar to **whatweb**, which does not allow us to remove the technologies that run behind a web application.

Webalizer is *much simpler than whatweb*, Because it does not have the same number of plugins, it does not analyze as many things as whatweb does, but, since it is simpler, it is faster and since it is less known, many security tools do not detect it. Furthermore, if we have a very large list of subdomains it is *faster* what to use **whatweb**

Webanalyse in action

The first thing is to install it, since it does not come installed in  kali but we can install it with the command

go install -v github.com/rverton/webanalyze/cmd/webanalyze@latest

Once downloaded we just have to perform the command

web analysis -host http://target.website

And the result would look like this:

```
🐼 > ~/De/webanalyze-master > webanalyze -host http://192.168.20.134:8080/login.php
:: webanalyze           : v0.3.9
:: workers              : 4
:: technologies         : technologies.json
:: crawl count          : 0
:: search subdomains    : true
:: follow redirects     : false

2024/06/24 19:35:39 warning: technologies.json is older than a week
http://192.168.20.134:8080/login.php (0.0s):
  Apache HTTP Server, 2.4.7 (Web servers)
  PHP, 5.5.9 (Programming languages)
  Ubuntu, (Operating systems)
```