

```
0K . 100% 33.2M=0s
-04-10 04:13:31 (33.2 MB/s) - â€˜tortoisehg/index.htmlâ€™ saved [1564/1564]
22-04-10 04:13:31-- https://www.mercurial-scm.org/release/windows/
ing existing connection to www.mercurial-scm.org:443.
request sent, awaiting response... 200 OK
th: unspecified [text/html]
modified header missing -- time-stamps turned off.
22-04-10 04:13:31-- https://www.mercurial-scm.org/release/windows/
ing existing connection to www.mercurial-scm.org:443.
request sent, awaiting response... 200 OK
th: unspecified [text/html]
ng to: â€˜windows/index.htmlâ€™
0K ..... 558K
50K ..... 1.09M
00K ..... 112M
50K ..... 1.11M
00K ..... 104M
50K ..... 113M=0.2s
-04-10 04:13:31 (1.47 MB/s) - â€˜windows/index.htmlâ€™ saved [276310]
22-04-10 04:13:31-- https://www.mercurial-scm.org/release/?C=N;O=A
ing existing connection to www.mercurial-scm.org:443.
request sent, awaiting response... 200 OK
th: unspecified [text/html]
modified header missing -- time-stamps turned off.
22-04-10 04:13:31-- https://www.mercurial-scm.org/release/?C=N;O=A
ing existing connection to www.mercurial-scm.org:443.
request sent, awaiting response... 200 OK
th: unspecified [text/html]
ng to: â€˜index.html?C=N;O=Aâ€™
0K ..... 145M
50K ..... 181M=0.001s
-04-10 04:13:31 (159 MB/s) - â€˜index.html?C=N;O=Aâ€™ saved [92197]
22-04-10 04:13:31-- https://www.mercurial-scm.org/release/?C=N;O=A
```



URI size: Web Server Identifier

By Maurice LAMBERT <mauricelambert434@gmail.com>

<https://github.com/mauricelambert/>

<https://github.com/mauricelambert/WebServerIdentifier>

Content

1. Vulnerabilities, intrusion and Web
2. Identifying Web Servers
3. HTTP – URI size
4. Identifying Web Servers – URI size
5. Examples
6. Accuracy
7. Limits
8. Conclusion

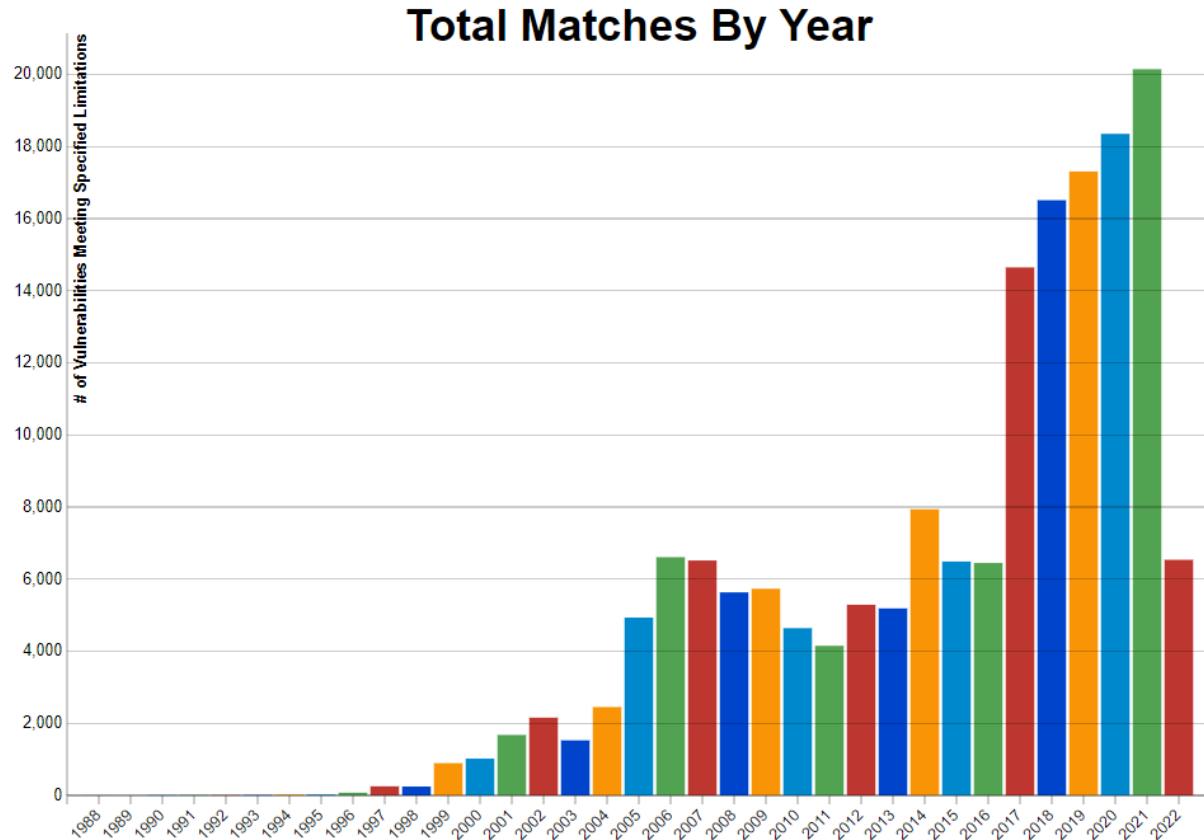
```
GET / HTTP/1.1
User-Agent: Mozilla/4.0
Host: 127.0.0.1
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 27 Jul 2009 12:28:53 GMT
Server: Apache/2.2.14 (Win32)
Last-Modified: Wed, 22 Jul 2009 19:15:56 GMT
Content-Length: 88
Content-Type: text/html
Connection: Closed

<html>
    <body>
        <h1>Hello, World!</h1>
    </body>
</html>
```

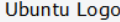
Vulnerabilities, intrusion and Web

- Web usage increases every year
- The number of web servers increases every year
- The number of vulnerabilities and their criticalities have increased
- Major vulnerabilities affect the most used web servers
- The number of scanners testing public IPs to find critical vulnerabilities increases
- The number of intrusions going through web services is increasing



Identifying Web Servers

- Headers (Server, realm, ...)
- Specific content (title, comments, text...)
- Specific path/URI (icon, default path, ...)
- HTTP status
- Signatures (favicon, default index and error pages, ...)
- Whatweb
- Google dorks

 **Apache2 Ubuntu Default Page**

Bravo! It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

HTTP – URI size

- HTTP RFC do not defined the maximum URI size
 - <https://www.rfc-editor.org/rfc/rfc1945>
 - <https://www.rfc-editor.org/rfc/rfc2068#page-63>
- Error 414 has been added in HTTP/1.1
- Web servers don't always follow RFCs
 - Recommended error codes are not respected

```
1 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
2 <html><head>
3 <title>414 Request-URI Too Long</title>
4 </head><body>
5 <h1>Request-URI Too Long</h1>
6 <p>The requested URL's length exceeds the capacity
7 limit for this server.<br />
8 </p>
9 </body></html>
10
```

Request-URI Too Long

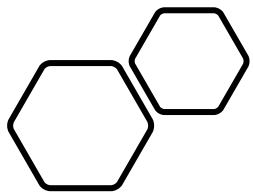
The requested URL's length exceeds the capacity limit for this server.

État	414 Request-URI Too Long ?
Version	HTTP/1.1
Transfert	423 o (taille 248 o)
▼ En-têtes de la réponse (175 o) Texte brut	
?	Connection: close
?	Content-Length: 248
?	Content-Type: text/html; charset=iso-8859-1
?	Date: Mon, 11 Apr 2022 11:35:32 GMT
?	Server: Apache

Identifying Web Servers – URI size

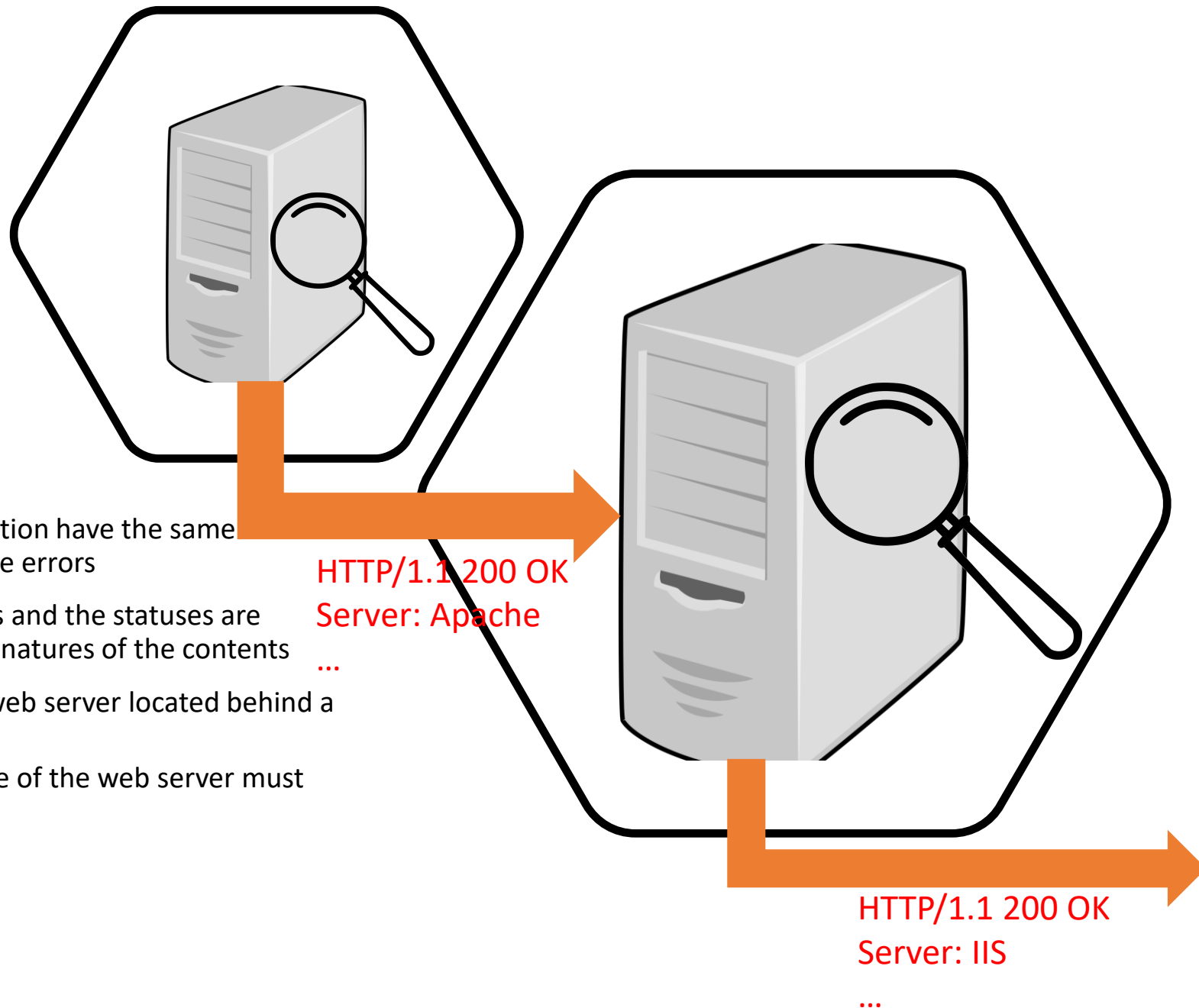
- Request the target with large URI
 - Random query string
- Analyze the response
 - If the server responds or the error code is specific, relaunch a request with a smaller query string
 - Else relaunch a request with a greater query string
- The maximum size of URLs is specific to each server





Identifying Web Servers – URI size

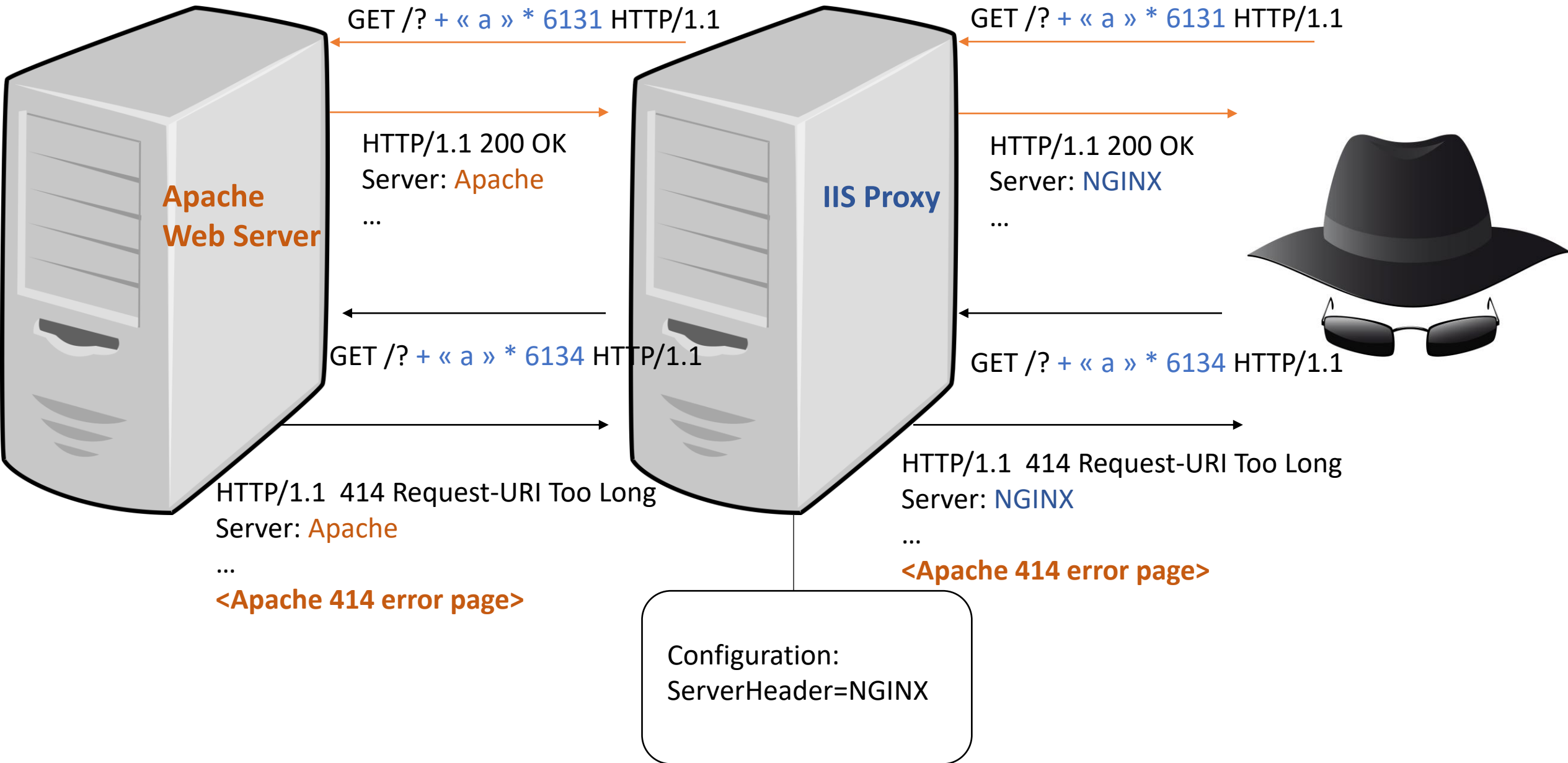
- Some servers that shouldn't be in production have the same maximum URI size but have different code errors
- In the case where the maximum URI sizes and the statuses are identical, it is possible to compare the signatures of the contents ...
- In some cases it is possible to identify a web server located behind a web proxy
 - Prerequisite: The maximum URI size of the web server must be less than that of the web proxy

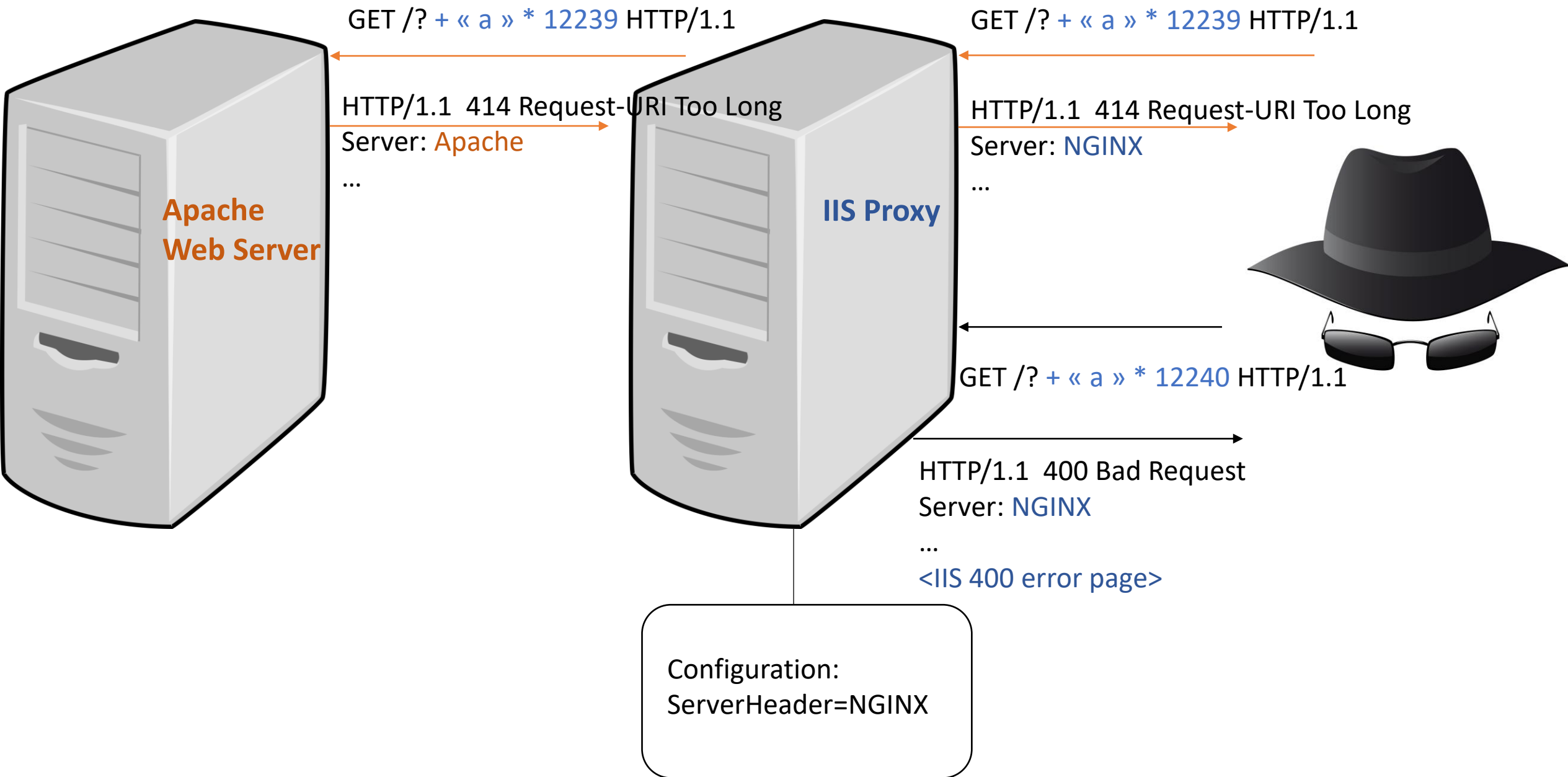


Examples

- In these examples, the web server is an Apache HTTPD (maximum URI size: 6133), the web proxy is an IIS (maximum URI size: 12241[status: 400]-12284[status: 414]) with a configuration to change the HTTP Server header to "NGINX".
- Scenarios:
 1. Detect the Apache Web Server to exploit CVE-2021-42013
 2. Detect the IIS Web Proxy to exploit CVE-2021-31166

EXAMPLE



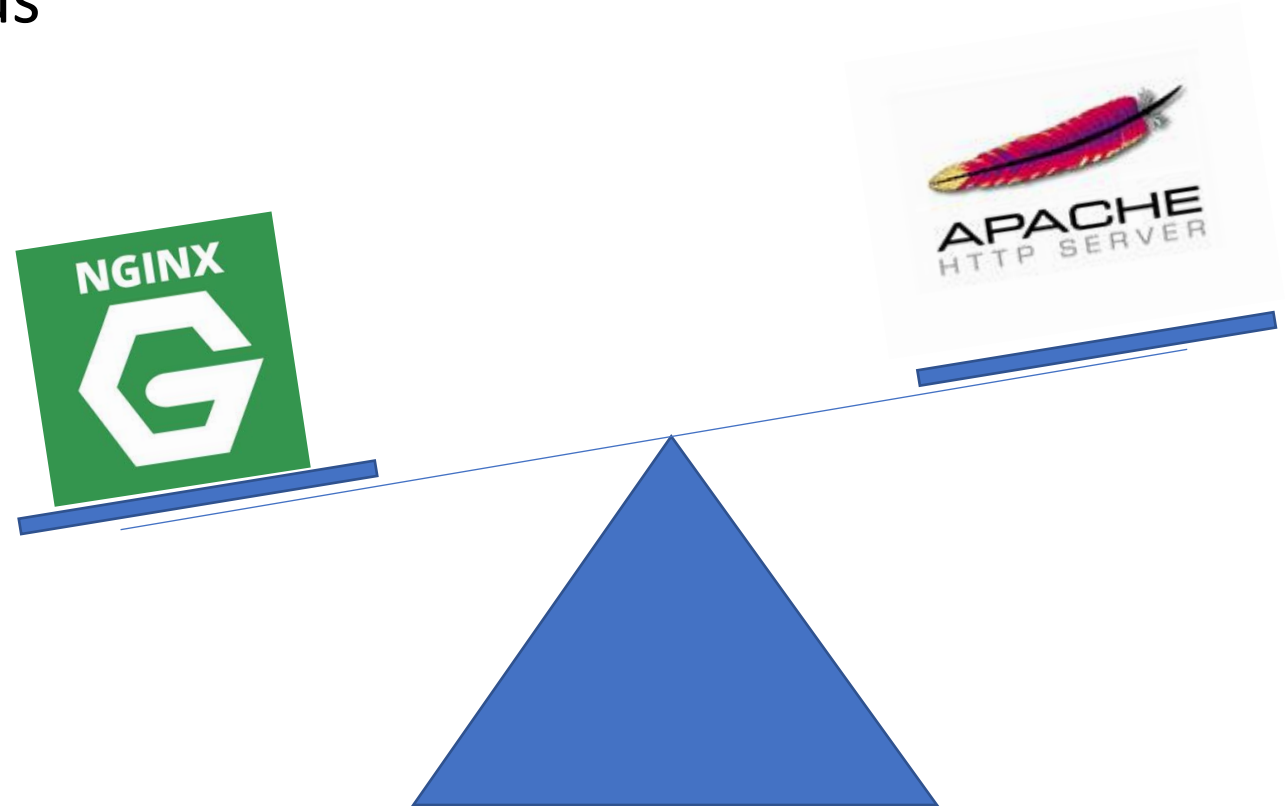


Accuracy

```
view-source:http://127.0.0.1/?aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

1 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
2 <HTML><HEAD><TITLE>Request URL Too Long</TITLE>
3 <META HTTP-EQUIV="Content-Type" Content="text/html; charset=us-ascii"></HEAD>
4 <BODY><h2>Request URL Too Long</h2>
5 <hr><p>HTTP Error 414. The request URL is too long.</p>
6 </BODY></HTML>
7
```

1. Compare maximum URI size
2. Compare HTTP error status
3. Compare error page hash



Request URL Too Long

HTTP Error 414. The request URL is too long.

Limits

- If the Web Proxy have a smaller maximum URI size you cannot identify the Web Server
- If the server uses a framework or language, developers can implement a custom maximum URI size, status and page
- Firewalls can easily block your large and random URI



Conclusion

- It is important to protect your web servers and preventing your server from being identified can discourage attackers from attacking you.
- HTTP does not define all protocol properties, making it easy to identify different implementations
- It's possible to identify Web Servers and Web Proxy with URI size precisely and easily
- Some configurations can protect your web servers from "in depth" detection (detection of a web server behind a Web Proxy)
- It is possible to protect your Web servers with firewalls or development