I. Web (Server-Side Vulns)

Diego Soria y Jaime García

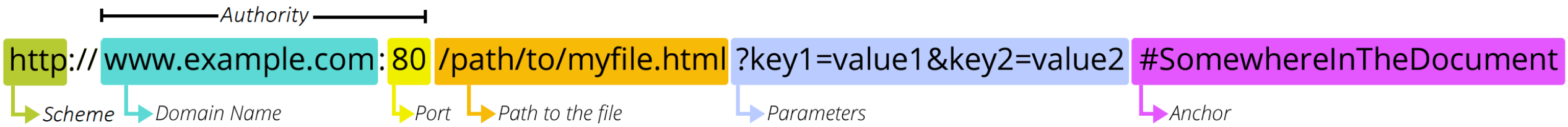
Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

ÍNDICE

URL

URL: Uniform Resource Locator



PARTES COMUNES:

- Scheme (protocolo)
- ***Authority*** (userinfo@host:port)
- *Path*: ruta al recurso
- *Parameters*: pares clave-valorfile://localhost/etc/passwd
- Anchor: sección espefífica de la página

EJEMPLOS

- https://google.es/search?q=como+ganar+dinero
- ftp://ftp.funet.fi/pub/doc/rfc/rfc1738.txt
- mailto:raul.martin@urjc.es?subject=Que+aula+es

Funcionamiento de una página web

Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

Archivos esenciales en una web

Los archivos esenciales son 3, un lenguaje de marcado HTML, uno de estilo CSS y otro funcional JavaScript

Universidad Rey Juan Carlos

HTML: Hyper Text Markup Lenguage

HTML es un lenguaje de marcado, que se forma por etiquetas y texto plano.

```html
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Solo HTML</title>
</head>
<body>
    <h1>Bienvenido a mi página web</h1>
    <p>Este es un ejemplo básico de una página web utilizando solo HTML.</p>
</body>
</html>
```

Universidad Rey Juan Carlos

HTML: Hyper Text Markup Lenguage

Universidad Rey Juan Carlos

CSS: Cscading Styles Sheet

Se utiliza para dar estilo al contenido estructurado. También se puede usar con otros lenguajes como XML o SBG

```
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>HTML con CSS</title>
    <link rel="stylesheet" href="styles.css"> <!-- Vincula el CSS -->
</head>
<body>
    <h1>Bienvenido a mi página web</h1>
    <p>Este es un ejemplo básico de una página web utilizando HTML y CSS.</p>
</body>
</html>
```

Universidad Rey Juan Carlos

CSS: Cscading Styles Sheet

Se utiliza para dar estilo al contenido estructurado. También se puede usar con otros lenguajes como XML o SBG

```css
/* Estilos generales */
body {
    font-family: 'Helvetica Neue', Arial, sans-serif;
    background-color: #282c34;
    color: #fff;
    margin: 0;
    padding: 0;
    display: flex;
    flex-direction: column;
    justify-content: center;
    align-items: center;
    height: 100vh;
}
```

```css
/* Estilo del título */
h1 {
    color: #61dafb;
    font-size: 3em;
    text-transform: uppercase;
    letter-spacing: 5px;
    border-bottom: 2px solid #61dafb;
    padding-bottom: 10px;
    margin-bottom: 20px;
}

/* Estilo del párrafo */
p {
    color: #b0bec5;
    font-size: 1.5em;
    max-width: 600px;
    text-align: center;
    line-height: 1.6;
    margin: 20px;
    border-left: 4px solid #61dafb;
    padding-left: 15px;
    box-shadow: 0 4px 10px rgba(0, 0, 0, 0.3);
}
```

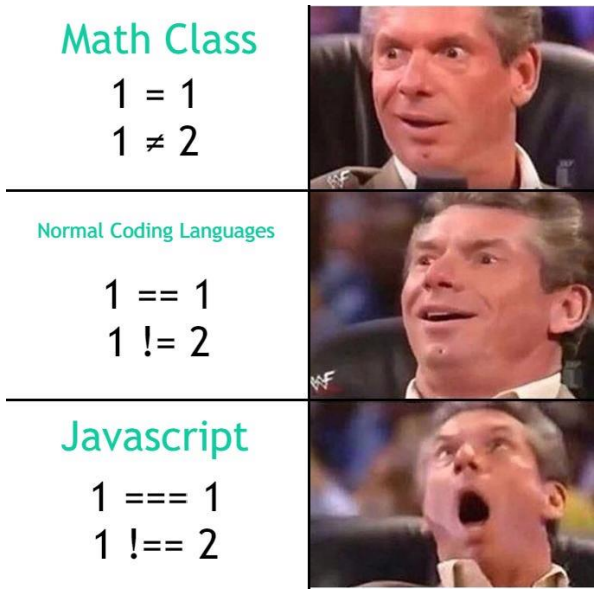
Universidad Rey Juan Carlos

CSS: Cscading Styles Sheet

Universidad Rey Juan Carlos

JavaScript

JavaScript es un lenguaje de programación dinámico que permite agregar interactividad y funcionalidades complejas a las páginas web




```html
<!DOCTYPE html>
<html lang="es">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>HTML, CSS y JavaScript</title>
    <link rel="stylesheet" href="styles.css"> <!-- Vincula el CSS -->
</head>
<body>
    <h1>Haz clic en este título</h1>
    <p>Este es un ejemplo básico de una página web utilizando HTML, CSS y JavaScript.</p>

    <script src="script.js"></script> <!-- Vincula el JavaScript -->
</body>
</html
```

Universidad Rey Juan Carlos

JavaScript

JavaScript es un lenguaje de programación dinámico que permite agregar interactividad y funcionalidades complejas a las páginas web

```
function cambiarColor() {
    const titulo = document.querySelector('h1');
    titulo.style.color = titulo.style.color === 'blue' ? '#61dafb' : 'blue';
}

document.querySelector('h1').addEventListener('click', cambiarColor);
```

JavaScript


index.html
Open with Arc
HAZ CLIC EN ESTE TÍTULO
Este es un ejemplo básico de una página web utilizando HTML, CSS y JavaScript.

Frameworks

Universidad
Rey Juan Carlos

Universidad Rey Juan Carlos

¿Qué frameworks existen?

Existen muchos frameworks para dar dinamismo a nuestras páginas, algunos ejemplos serían PHP y Python con su módulo de Flask

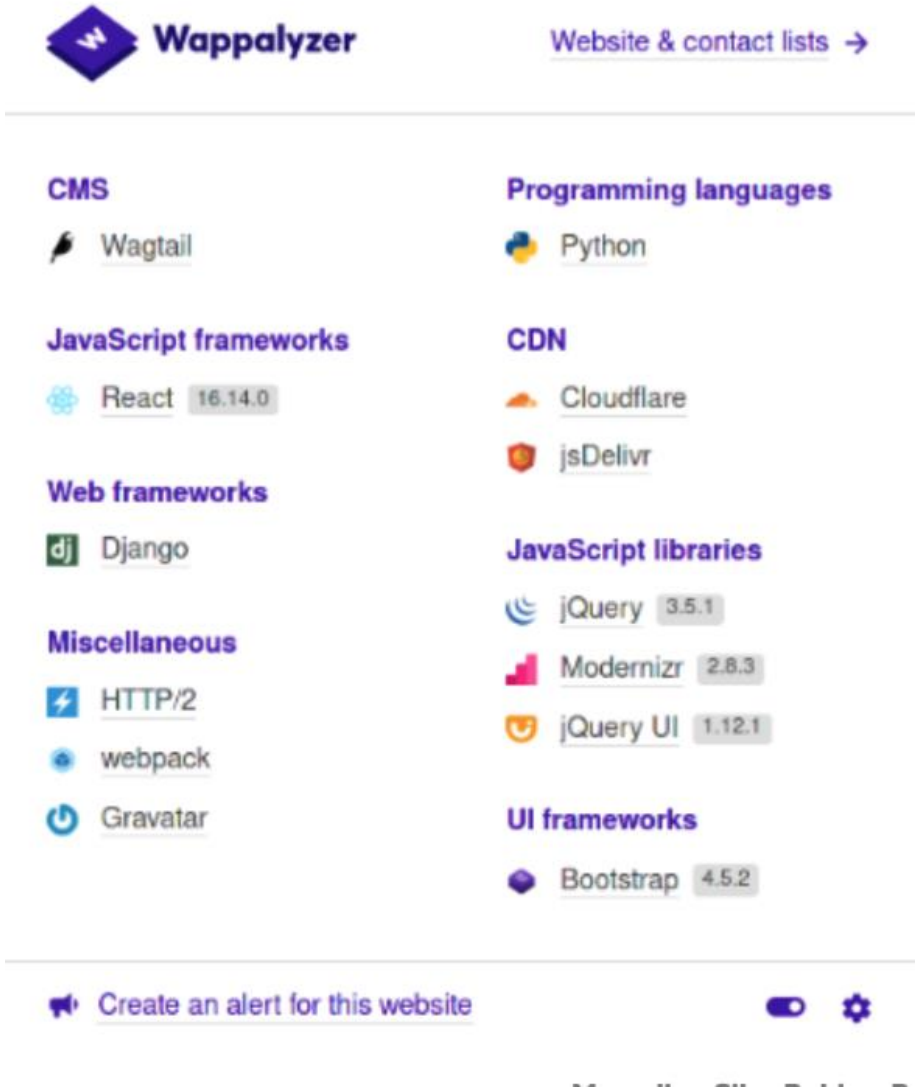
PHP

```
"0000" == 0                 => TRUE
"0e12" == 0                 => TRUE
"1abc" == 1                 => TRUE
"0abc" == 0                 => TRUE
"0e12345" == "0e54321"      => TRUE
"0e12345" <= "1"            => TRUE
```

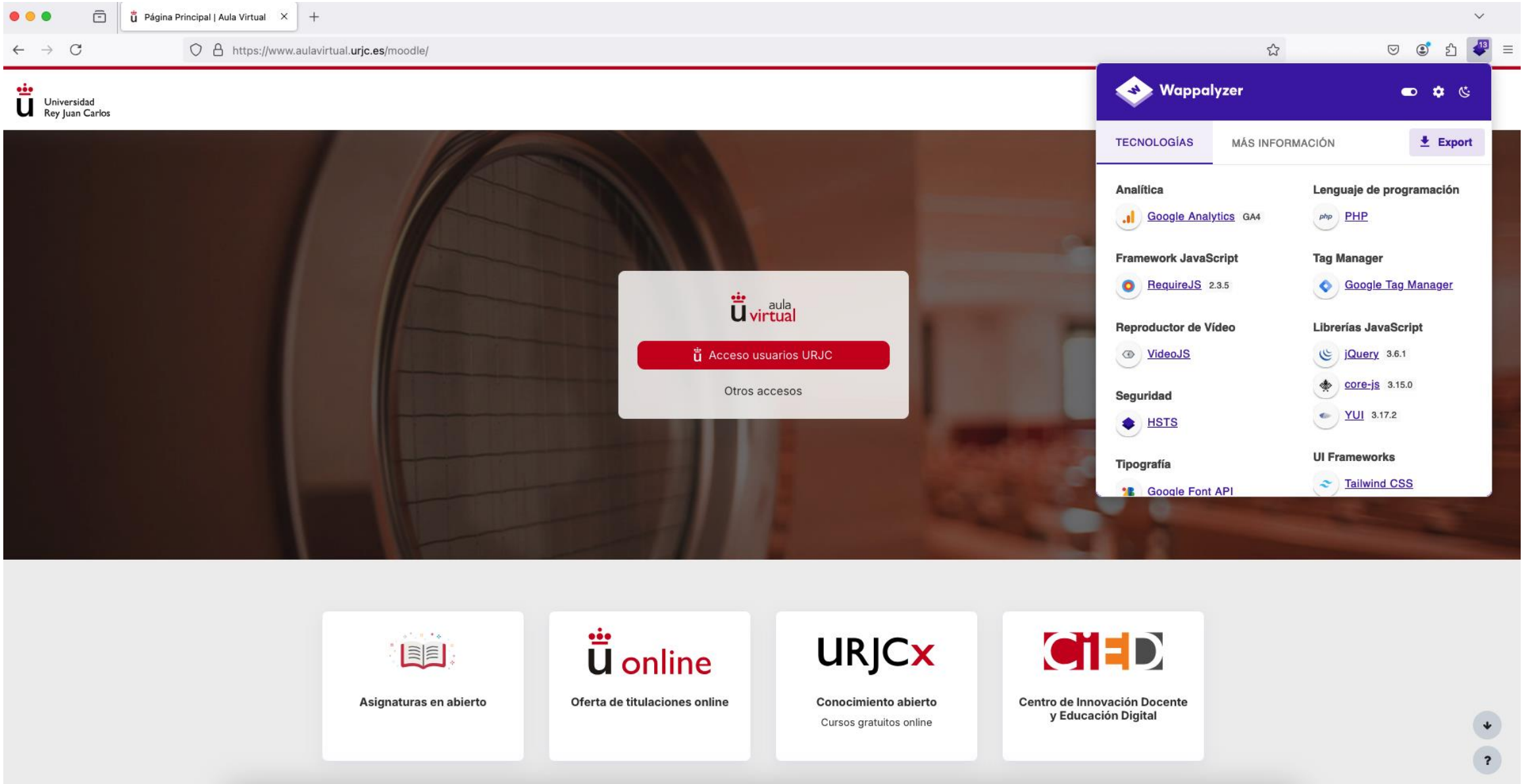
FLASK Y JINJA2

Formas de analizar el framework: wappalyzer

Wappalyzer



Formas de analizar el framework: wappalyzer



Universidad Rey Juan Carlos

Formas de analizar el framework: wappalyzer

Analítica

Google Analytics GA4

Framework JavaScript

RequireJS 2.3.5

Reproductor de Vídeo

VideoJS

Seguridad

HSTS

Tipografía

Google Font API

LMS

Moodle

Lenguaje de programación

PHP

Tag Manager

Google Tag Manager

Librerías JavaScript

jQuery 3.6.1

core-js 3.15.0

YUI 3.17.2

UI Frameworks

Tailwind CSS

Bootstrap 4.6.2

Universidad Rey Juan Carlos

Formas de analizar el framework: Whatweb

```
$ whatweb google.com
http://google.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[gws], IP[142.250.200.78],
RedirectLocation[http://www.google.com/], Title[301 Moved], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]

http://www.google.com/ [200 OK] Cookies[AEC], Country[UNITED STATES][US], HTML5, HTTPServer[gws], HttpOnly[AEC],
IP[142.250.200.68], Script, Title[Google], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[0]
```

HTTP y HTTPS

HTTPS

Estos son los protocolos que hacen que la web funcione, la diferencia entre ellos es que HTTPS es HTTP con TLS, es decir cifrado.

HTTPS va a añadir los siguientes pasos al HTTP

- Cifrar la petición con una clave simétrica
- Enviar el mensaje
- El que reciba la petición lo descifra con la misma clave simétrica

Universidad Rey Juan Carlos

HTTPS

- La información se transmite como **texto**
- Es un protocolo **sin estado**, el servidor no tiene memoria
- Nos centraremos sobre todo en la versión 1.0/1.1. Las versiones 2.0 y 3.0 son muy diferentes

```
GET /index.html HTTP/1.1
Host: google.es
Cabecera2: valor2
Cabecera3: valor3
```

Petición

```
HTTP/1.1 301 Moved Permanently
Location: http://www.google.es/
Content-Type: text/html; charset=UTF-8
Content-Length: 218
[\n\n]
<HTML><HEAD>
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.es/">here</A>.
</BODY></HTML>
```

Respuesta

Universidad Rey Juan Carlos

HTTPS

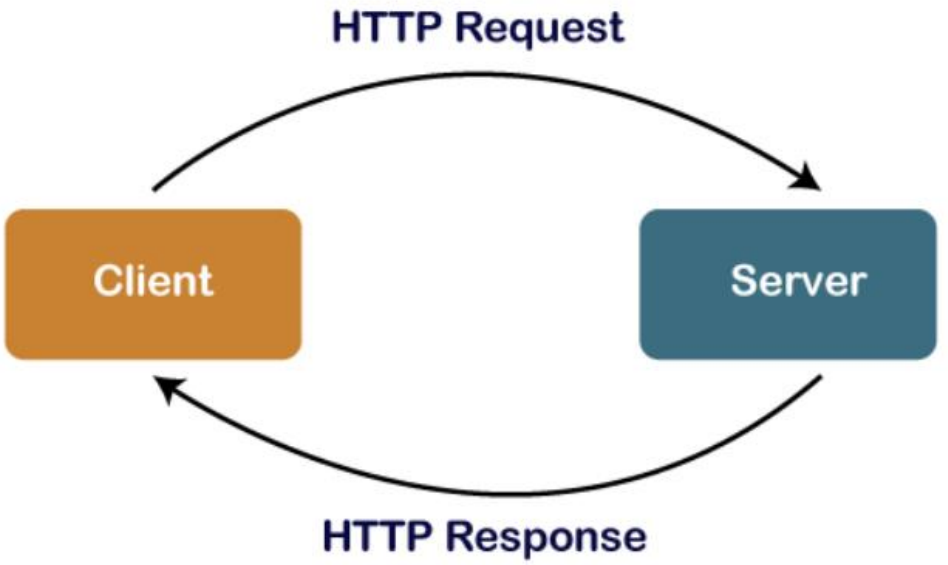
En el ejemplo de antes se ve como realizaba un GET, pero existen más métodos HTTP

- **POST**: Es el más utilizado junto a GET, suele servir para realizar peticiones en las que se envían datos, como podría ser un login.
- **HEAD**: Te devuelve las mismas cabeceras que si hicieras un GET pero no llega a descargar ficheros, por ejemplo si te fuera a descargar una imagen, solo te devolvería el content-length.
- **PUT**: Es similar a POST, pero es idempotente, es decir que si se realiza la misma petición varias veces, solo tendrá efecto la primera.
- **DELETE**: Borra recursos del servidor, normalmente este es un método que quieres quitar de tu web.

Más información aquí: https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods

Códigos de estado

¿ERROR 404? Ya iba tocando saber que significa



Más información sobre los códigos de estado: https://developer.mozilla.org/es/docs/Web/HTTP/Status

Universidad Rey Juan Carlos

PREGUNTAS

¿Qué indica el protocolo "https://" en una URL?

Universidad Rey Juan Carlos

PREGUNTAS

¿Qué lenguaje de marcado define la estructura de una página web?

Universidad Rey Juan Carlos

PREGUNTAS

¿Qué protocolo encripta los datos, HTTP o HTTPS?
Y, ¿que dos métodos de encriptación se utilizan?

Universidad Rey Juan Carlos

PREGUNTAS

¿Qué método HTTP se usa para enviar datos al servidor?

Herramientas

F12

RETO

FUZZING

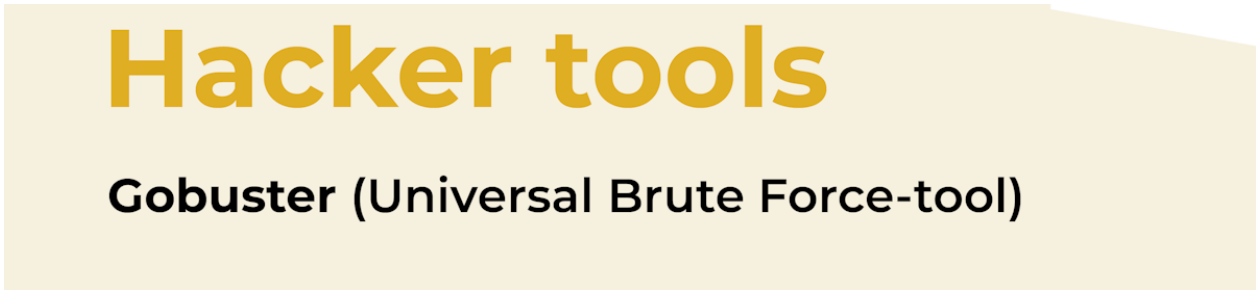
Universidad Rey Juan Carlos

FUZZING

Fuzzing nos sirve para descubir directorios, parámetros o demás campos de una página web, por fuerza bruta

Si recordamos, lo que es el Código de estado, realizando peticiones a una página web, podemos comprobar si un recurso existe o no.

Para ello existen diferentes herramientas: wfuzz, ffuz, dirb, gobuster.
Hoy os voy a hablar de la más potente de ellas.



Cookies

Universidad
Rey Juan Carlos

Cookies

¿Qué son las Cookies?

- Pequeños archivos de texto que se almacenan en el navegador del usuario.
- Crean un "registro" que ayuda a personalizar la experiencia del usuario.

Universidad Rey Juan Carlos

Herramientas

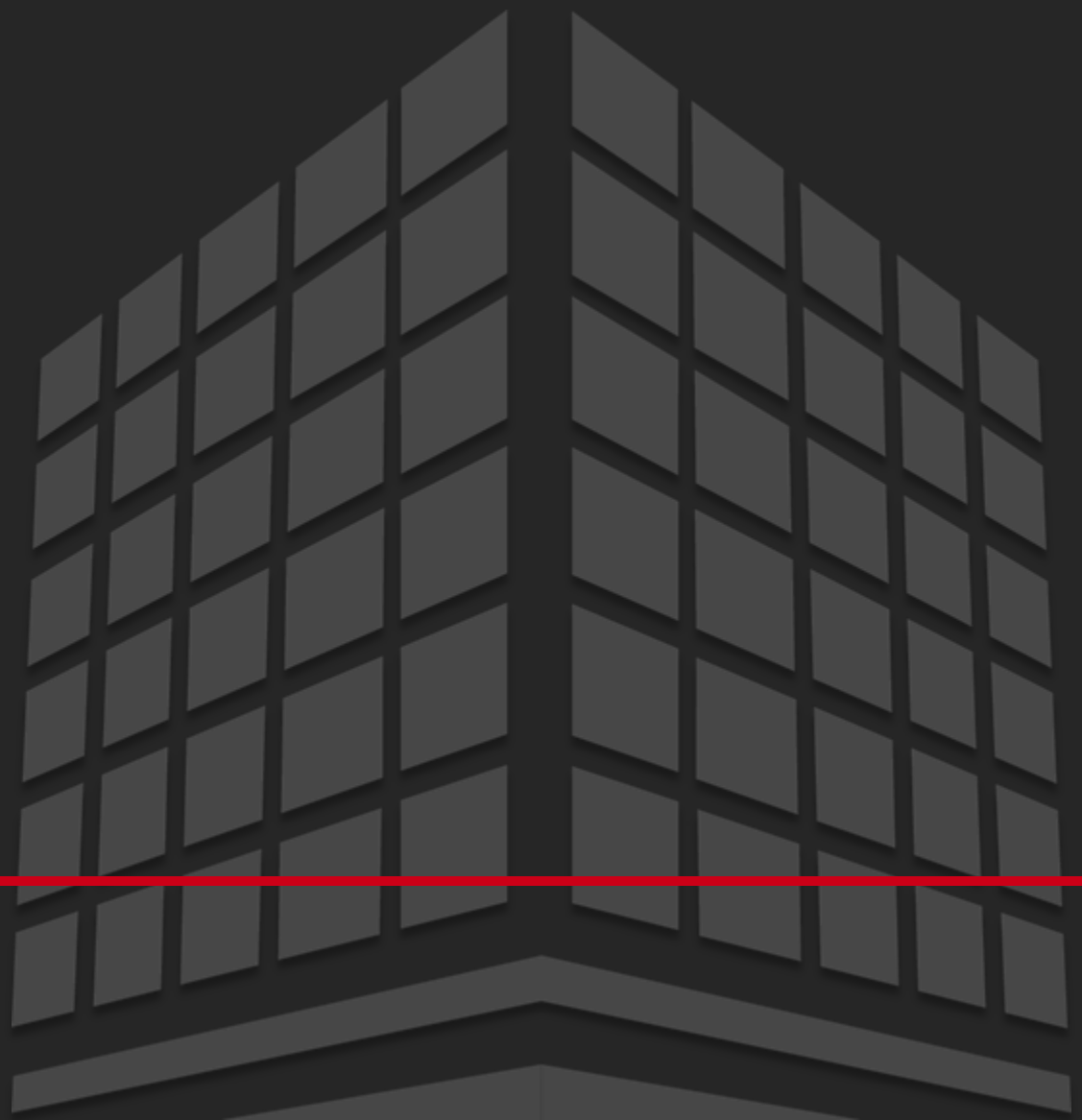
F12

Cookie Editor

RETO DE COOKIES

RETO FINAL

Recordar que el primero se lleva una camiseta



Universidad
Rey Juan Carlos